Gloria Treider

Investigation of the Gap Between Traditional IP Network Security Management and the Adoption of Automation Techniques and Technologies to Network Security

Master’s thesis in IT Security Management
Supervisor: Vasileios Gkioulos
Co-supervisor: Håkon Gunleifsen
December 2023

Master’s thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Department of Computer Science

NTNU
Norwegian University of
Science and Technology

Gloria Treider

Investigation of the Gap Between Traditional IP Network Security Management and the Adoption of Automation Techniques and Technologies to Network Security

Master's thesis in IT Security Management
Supervisor: Vasileios Gkioulos
Co-supervisor: Håkon Gunleifsen
December 2023

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Department of Computer Science

NTNU
Norwegian University of
Science and Technology

Abstract

In the realm of network and network security automation, this thesis unveils a complex landscape of challenges and opportunities. The research sheds light on the intricacies inherent in automating large IP networks, prompting a transformation in the perspectives of organizational leaders tasked with network management. The central objective of this thesis is to investigate and substantiate the existing gap in the application of network automation techniques and technologies within network and network security systems. It clarifies multiple dimensions within the complex landscape, assisting organizations in their decision-making when evaluating automation technique solutions.

To achieve this goal, we critically examine the contemporary literature on network security and automation, offering a comprehensive review of traditional network security methodologies alongside the potential automation techniques available for enhancing network security. Additionally, we analyze factors influencing the adoption of network security automation through rigorous surveys and interviews. Our findings underscore the multifaceted nature of network automation, illuminating the complex landscape that organizations shall navigate when considering automation solutions. By addressing the gap in the current state of network automation, we contribute to a deeper understanding of this evolving field.

The validation of our findings involves engaging with two distinct groups of participants, academic professionals in IT education and experienced IT professionals responsible for managing extensive networks. Their insights, experiences, and suggestions validate our research, providing a holistic perspective on the automation of network and network security processes. In conclusion, our research catalyzes change within the field of network automation. We highlight the existence of organizational silos and emphasize that breaking down these barriers is essential for achieving the overarching goal of automating network and network security tasks. Our work is poised to raise awareness among stakeholders and inspire meaningful shifts in network management paradigms.

Sammendrag

Innenfor området nettverks- og nettverkssikkerhetsautomatisering avdekker denne oppgaven et komplekst landskap av utfordringer og muligheter. Forskningen som er gjennomført, belyser de intrikate elementene som er innebygd i automatiseringen av store IP-nettverk, noe som igjen fører til en transformasjon i perspektivene til organisatoriske ledere som har ansvaret for nettverksstyring. Den sentrale målsetningen med denne oppgaven er å undersøke og underbygge det eksisterende gapet i bruken av nettverksautomatiseringsteknikker og -teknologier innen nettverks- og nettverkssikkerhetssystemer. Det gir klarhet på flere dimensjoner innenfor det komplekse landskapet, og hjelper organisasjoner med beslutningstakingen når de vurderer løsninger for automatiseringsteknikker.

For å oppnå dette målet, undersøker vi kritisk den samtidsorienterte litteraturen om nettverkssikkerhet og automatisering, og tilbyr en grundig gjennomgang av tradisjonelle nettverkssikkerhetsmetodikker, samt de potensielle automatiseringsteknikkene som er tilgjengelige for å forbedre nettverkssikkerheten. I tillegg analyserer vi faktorer som påvirker implementeringen av nettverkssikkerhetsautomatisering gjennom grundige undersøkelser og intervjuer. Våre funn understreker nettverksautomatiseringens mangfoldige natur og belyser det komplekse landskapet organisasjoner skal navigere når de vurderer automatiseringsløsninger. Ved å adressere gapet i dagens tilstand for nettverksautomatisering, bidrar vi til en dypere forståelse av dette stadig utviklende feltet.

Valideringen av våre funn innebærer samhandling med to forskjellige grupper deltakere, akademiske fagpersoner innen IT-utdanning og erfarne IT-fagfolk som er ansvarlige for styring av omfattende nettverk. Deres innsikt, erfaringer, og forslag fungerer som en verdifull bekreftelse av vår forskning, og gir et helhetlig perspektiv på automatiseringen av nettverks- og nettverkssikkerhetsprosesser. Avslutningsvis fungerer vår forskning som en katalysator for endring innen feltet for nettverksautomatisering. Vi fremhever eksistensen av organisatoriske siloer og understreker viktigheten av å bryte ned disse barrierene for å oppnå det overordnede målet om å automatisere oppgaver innen nettverks- og nettverkssikkerhet. Vårt arbeid er i ferd med å øke bevisstheten blant interessenter og inspirere til meningsfulle endringer i nettverksstyringsparadigmer.

Acknowledgement

I would like to express my heartfelt gratitude to all the individuals who participated in this research, representing a participating university and various companies. Their invaluable contributions through surveys and interviews were instrumental in shaping the validation process of our study.

A special word of appreciation goes to my colleague, Erlend Bjørnson Barkbu, who provided early support for both the idea and the problem statement, setting the foundation for this research endeavor.

Most importantly, I extend my sincere thanks to my supervisors, whose unwavering guidance and constructive feedback were pivotal throughout this research journey. I am deeply indebted to Associate Professor Vasileios Gkioulos and, in particular, to Håkon Gunleifsen, Ph.D., for their consistent support, engaging discussions, and insightful input from inception to completion.

I would also like to acknowledge Professor Sokratis Katsikas, whose initial support made this research possible. Without his encouragement, this work might never have come to fruition.

Last but certainly not least, I extend my heartfelt appreciation to my family, who patiently stood by me as I dedicated countless hours to this research alongside my daily responsibilities, sacrificing precious time that we could have spent together. Your unwavering support has been my anchor throughout this journey.

Contents

Abstract . . . . **i**
Sammendrag . . . . **ii**
Acknowledgement . . . . **iii**
Contents . . . . **iv**
Figures . . . . **vii**
Tables . . . . **xiii**
1 Introduction **1**
1.1 Topics Covered By the Research 1
1.2 Keywords 2
1.3 Research Objective 2
1.4 Problem Description 3
1.5 Hypothesis 4
1.6 Justification, Motivation, and Benefits 4
1.7 Research Questions 6
1.8 Planned Contribution 6
1.9 Scope and Purpose 7
1.10 Related Works 8
1.11 Ethical and Legal Considerations 9
1.12 Document Structure 10
2 Methodology **13**
3 Background **15**
3.1 SWOT Analysis 15
3.2 OSI Model 17
3.3 Definitions 17
3.4 Network Security Resilience in CIS IP Networks 19
3.4.1 CIS IP Network Security 19
3.4.2 Cyberattacks Targeting Critical Infrastructure Sectors 20
3.5 Traditional Network Security Techniques and Technologies 21
4 Results **22**
4.1 Theoretical Contribution 23
4.1.1 Summary of the State-of-the-Art Review 23
4.1.2 The Relation Between SotA and RQs 28
4.1.3 The Gap Observed in the SotA Studied in this Research . . . 28

4.2 Traditional Network Security Management - Summary SWOT Analysis - RQ1 . . . 29
4.3 Contributions of Existing Automation Techniques and Technologies - RQ2 . . . 35
4.3.1 Path Control in Network Devices - Operation Plans - RQ2 . . . 36
4.3.2 Application of SDN to Operational Planes - RQ2 . . . 39
4.3.3 Orchestration and Network Function Virtualization - RQ2 . . . 42
4.3.4 Automation Methods and Tools - RQ2 . . . 44
4.3.5 Automation of Firewalls - RQ2 . . . 51
4.3.6 Application of Machine Learning to NSA - RQ2 . . . 53
4.3.7 Network Automation Simulation Platforms - RQ2 . . . 59
4.4 Influential Factors in Network Security Automation Adoption - RQ3 60
4.4.1 Learning and Skills Development Motivation - RQ3 . . . 61
4.4.2 Challenges and Issues in NSA - RQ3 . . . 62
4.4.3 Benefits and Use Cases of IP Network Automation - RQ3 . . . 69
4.4.4 Drawbacks and Vulnerabilities in IP Network Automation - RQ3 . . . 74
4.4.5 SWOT Analysis of NSA Techniques and Technologies - RQ3 76
4.5 CCAM and Summary Analysis of the Results . . . 80
4.6 Key Findings - RQ1 & RQ2 & RQ3 . . . 90

5 Results Validation . . . 92
5.1 Interviews . . . 93
5.2 Surveys . . . 94
5.3 Results Validation Utilizing Surveys and Interviews . . . 96
5.3.1 Structure and Relevance of the Questions . . . 96
5.3.2 Validation of Results, Problem, and Hypothesis . . . 98
5.3.3 Summary . . . 109
5.4 Validation of Key Findings - RQ1 & RQ2 & RQ3 . . . 110

6 Discussion and Conclusion . . . 113
6.1 Limitations . . . 113
6.2 Future Work . . . 114
6.3 Conclusion . . . 117

Bibliography . . . 120

Acronyms . . . 133

A In-Depth Methodology Insights . . . 140

B Glossary . . . 145
B.1 OSI Model Overview . . . 145
B.2 Detailed Examples on Cyberattacks Targeting Critical Infrastructure Sectors . . . 147
B.3 Traditional Network Security Technique and Technologies - Contextualizing RQ1 . . . 148
B.3.1 IP Network Firewalls and Basic Network Security Strategies - RQ1 . . . 148
B.3.2 Demilitarized Zone Network Security Architecture - RQ1 . . . 155

B.3.3 Zone-Based Network Security Architecture - RQ1 156
B.3.4 Micro-segmentation Network Security Architecture - RQ1 . . 158
B.3.5 Zero Trust Network Security Architecture - RQ1 162
B.4 CIS General IP Network Architecture 163
B.5 Information Security Related Terms and Concepts 164
B.6 Network Automation Simulation Platforms - RQ2 168
C Criteria Used to Categorize the State-of-the-Art 174
D Table Utilized to Work with the State-of-The-Art 176
E Review of a Selection of Resources in the SotA 190
F Comprehensive SWOT Analysis of Traditional Network Security Management Characteristics - RQ1 202
F.1 SWOT Analysis of Traditional Firewalls and DMZ Network Security Architecture - RQ1 202
F.2 SWOT Analysis of Zone-based Network Security Architecture - RQ1 205
F.3 SWOT Analysis of Micro-Segmentation Network Security Architecture - RQ1 207
F.4 SWOT Analysis of Zero Trust Network Security Architecture - RQ1 . 208
G Survey Questions 211
H Comprehensive Review of Survey Results 223
H.1 General Questionnaire Responses 223
H.2 Scientific Personnel Answers to Group-Specific Survey 245
H.3 IT Professionals' Answers to Group-Specific Survey 274
I In-Depth Review of the Interviews 311
I.1 Interviews with the IT Network Professionals 311
I.2 Interview with a Network Team Leader 313
I.3 Interview with a Scientific Personnel 314
I.4 Brief Summary of the Interviews 315
J Experimenting with Artificial Intelligence 317

Figures

1.1 Document navigation roadmap. The figure is created by the author. 12

2.1 The five steps in methodology explained in this chapter. The figure is created by the author. 13

3.1 Strengths, Weaknesses, Opportunities, and Threats (SWOT) table for reference in further analysis. The figure is created by the author. 16

4.1 The overview of the Results Chapter. The figure is created by the author. 23
4.2 Concise presentation of Section 4.3. The figure is created by the author. 35
4.3 Forwarding all traffic through the control plane. Figure inspired of Figure 5-1 in [27, p. 329]. 36
4.4 Forwarding all traffic through data plane. Figure inspired of Figure 5-3 in [27, p. 331]. 37
4.5 Centralized controller management for network devices. The figure is inspired by Figure 9-14 [17, p. 305]. 38
4.6 OpenFlow made the communication between data plane SDN and control plane SDN possible. The figure is created by the author. . . 38
4.7 The Application layer is positioned atop the three network device layers. The presence of both northbound and southbound APIs within this architecture is also illustrated. The figure is created by the author. 39
4.8 Three layers in the network devices. The figure is created by the author. 40
4.9 Inspired by [50, Figur 2], the figure depicts the relation between NFV, VNFs, and orchestration in network automation. 43
4.10 Our categorization of DevOps tools. The figure is created by the author. 46
4.11 Collaboration tools overview. The figure is created by the author. . . 47
4.12 Building tools overview. The figure is created by the author. 47
4.13 Testing tools overview. The figure is created by the author. 48
4.14 Deployment tools overview. The figure is created by the author. . . 48

4.15 Overview of the tools utilized for running the code. The figure is created by the author. 49
4.16 Venn diagram illustrating the combination of ML and SDN, which, in line with the claims studied in the SotA, results in effective and intelligent NSA. The figure is created by the author. 54
4.17 Connection between controller and application layer where AI also plays a role and communicates with management functions. The controller and orchestrator layer in this figure matches the corresponding layer shown in Figure 4.7, which communicates through southbound API with the data plane below it. The figure is created by the author. 55
4.18 Presentation of the concepts related to ML in the SotA. The figure is created by the author. 56
4.19 Presentation of the concepts related to deep learning in the SotA. The figure is created by the author. 57
4.20 Presentation of the concepts related to ML methods for security technique automation in combination with SDN, discussed in the SotA. The figure is created by the author. 58
4.21 Concise presentation of Section 4.4. The figure is created by the author. 61
4.22 The analysis cube comprises three defined dimensions: network security methods and technologies on the **X**-axis, automation methods on the **Y**-axis, and the operation planes of network devices on the **Z**-axis, illustrating the problem's complexity. The figure is created by the author. 80
4.23 Illustration of the Combination Cube Analysis Model (CCAM). The figure has been created by the author. 82
4.24 ITAT represents three different actors, each with its approach to network and network security automation solutions. The figure is created by the author. 83
4.25 Combination Cube Analysis Model (CCAM) with details of each of the axes. The figure is created by the author. 85
4.26 Application of the content presented in Figure 4.25 to the structure presented in Figure 4.22. The figure is created by the author. 85
4.27 The author has employed a Rubik's Cube to exemplify complexities and dependencies, featuring various colors, sides/faces, and squares within it. The picture is taken by the author. 86
4.28 One side of Rubik's Cube representing the organizational needs of a single organization. The squares are filled in with examples of the various needs one organization can have. Additionally, the degree of each need is distinct and unique for each organization. The figure is created by the author. 87

4.29 One side of Rubik's Cube representing the organizational needs of a single organization. In this exemplification, more fields are displayed compared to the number of fields or squares depicted in Figure 4.28. The figure is created by the author. 87
4.30 The Rubik's Cube while turning to apply the options. The pictures are taken by the author. 88
4.31 One side of the Rubik's Cube before it is turned to apply the proper options to each need of the organization. The figure is created by the author. 88
4.32 The final state of the Rubik's Cube after different needs are filled with different options for each organization. The picture is taken by the author. 89

B.1 Evolution of OSI model. The figure is inspired by Figure 1-15 at [26, Chapter 1 p. 33]. 146
B.2 Simple strategy of utilizing DMZ, also called perimeter zone, in traditional network architecture for separation of the internal network and its resources, from the external network while keeping some public resources available for public access. The figure is created by the author. 156
B.3 Zone-based defense network security architecture. The figure is created by the author. 157
B.4 Data Center, vApp, VM, and tag depicted, only VMs that have the same tag can communicate with each other. The figure is created by the author. 160
B.5 First and second line of defense in micro-segmentation. The concept drawn in this figure is inspired by Figure 2.1 in [39, p. 19]. 161
B.6 Security zones in industry, depicted in layers inspired by [153]. . . 164

H.1 Scientific personnel survey answer to question 2 224
H.2 IT professional survey answer to question 2 225
H.3 Scientific personnel survey answer to question 3 226
H.4 IT professional survey answer to question 3 226
H.5 Scientific personnel survey answer to question 4 227
H.6 IT professional survey answer to question 4 227
H.7 Scientific personnel survey answer to question 5 228
H.8 IT professional survey answer to question 5 228
H.9 Scientific personnel survey answer to question 6 229
H.10 IT professional survey answer to question 6 229
H.11 Scientific personnel survey answer to question 7 230
H.12 IT professional survey answer to question 7 230
H.13 Scientific personnel survey answer to question 8 231
H.14 IT professional survey answer to question 8 231
H.15 Scientific personnel survey answer to question 9 232
H.16 IT professional survey answer to question 9 233

H.17 Scientific personnel survey answer to question 10 234
H.18 IT professional survey answer to question 10 234
H.19 Scientific personnel survey answer to question 11 235
H.20 IT professional survey answer to question 11 235
H.21 IT professional survey answer to question 12, where ten respondents (40%) answered CCNA to this question 235
H.22 Scientific personnel survey answer to question 13 236
H.23 IT professional survey answer to question 13 237
H.24 IT professional survey answer to question 14 where seven people have, among others, mentioned DevNet Associate as their network automation-related certifications 237
H.25 Scientific personnel survey answer to question 15 238
H.26 IT professional survey answer to question 15 238
H.27 IT professional survey answer to question 16 239
H.28 Scientific personnel survey answer to question 17 240
H.29 IT professional survey answer to question 17 240
H.30 Scientific personnel survey answer to question 18 241
H.31 IT professional survey answer to question 18 241
H.32 Scientific personnel survey answer to question 19 242
H.33 IT professional survey answer to question 19 243
H.34 Scientific personnel survey answer to question 20 244
H.35 IT professional survey answer to question 20 244
H.36 Scientific personnel survey answer to question 21 245
H.37 Scientific personnel survey answer to question 22 247
H.38 Scientific personnel survey answer to question 25 249
H.39 Scientific personnel survey answer to question 26 250
H.40 Scientific personnel survey answer to question 30 254
H.41 Scientific personnel survey answer to question 32 255
H.42 Scientific personnel survey answer to question 33 256
H.43 Scientific personnel survey answer to question 34 257
H.44 Scientific personnel survey answer to question 35 258
H.45 Scientific personnel survey answer to question 36 259
H.46 Scientific personnel survey answer to question 37 260
H.47 Scientific personnel survey answer to question 39 262
H.48 Scientific personnel survey answer to question 40 263
H.49 Scientific personnel survey answer to question 42 265
H.50 Scientific personnel survey answer to question 43 266
H.51 Scientific personnel survey answer to question 44 267
H.52 Scientific personnel survey answer to question 45 268
H.53 Scientific personnel survey answer to question 46 269
H.54 Scientific personnel survey answer to question 47 270
H.55 Scientific personnel survey answer to question 48 271
H.56 Scientific personnel survey answer to question 50 273
H.57 IT professional survey answer to question 21 274

H.58 IT professional survey answer to question 22 275
H.59 IT professional survey answer to question 23 276
H.60 IT professional survey answer to question 24 277
H.61 IT professional survey answer to question 25. The numbers on the sectors present the number of people who apply to the specific sector, and the numbers on the left side, connected with each color, present the number of years of experience in working with network and network security techniques and technologies. We have removed number four, representing four years of experience, as there was no response received in that sector. 278
H.62 IT professional survey answer to question 26 279
H.63 IT professional survey answer to question 27 280
H.64 IT professional survey answer to question 28. The bars in the bar chart represent the number of people utilizing network automation, also marked vertically. The percentage of their utilization of these techniques is shown in the horizontal axis in this figure. . . . 281
H.65 IT professional survey answer to question 29 283
H.66 IT professional survey answer to question 30 285
H.67 IT professional survey answer to question 31 286
H.68 IT professional survey answer to question 32 287
H.69 IT professional survey answer to question 33 288
H.70 IT professional survey answer to question 34 289
H.71 IT professional survey answer to question 35 290
H.72 IT professional survey answer to question 36 291
H.73 IT professional survey answer to question 37 292
H.74 IT professional survey answer to question 38 293
H.75 IT professional survey answer to question 39 294
H.76 IT professional survey answer to question 40 295
H.77 IT professional survey answer to question 42 297
H.78 IT professional survey answer to question 43 298
H.79 IT professional survey answer to question 44 299
H.80 IT professional survey answer to question 45 300
H.81 IT professional survey answer to question 46 301
H.82 IT professional survey answer to question 47 302
H.83 IT professional survey answer to question 48 302
H.84 IT professional survey answer to question 49 303
H.85 IT professional survey answer to question 50 304
H.86 IT professional survey answer to question 51 305
H.87 IT professional survey answer to question 52 306
H.88 IT professional survey answer to question 53 307
H.89 IT professional survey answer to question 54 310

J.1 Python code for login to a web page provided by AI 318
J.2 Python code suggested by AI for how to open a Python API 319

J.3 Python code suggested by AI about how to run a Python script . . . 319
J.4 Python code suggested by AI about how to run a Python script at a specific time . . . 320
J.5 Python code suggested by AI about how to run a Python script . . . 321
J.6 Python script suggested by AI for telling a Python script to run another Python script . . . 321

Tables

4.1 Summary of the SotA along with the relevant criteria, linking each resource to its corresponding topic or subject. For additional details, refer to Appendix C. 25
4.2 The relation between RQs and the SotA in a brief summary 28

5.1 The alignment between the Research Question (RQ)s and the survey questions is evident. While the survey questions directed at scientific personnel primarily pertain to RQ2, they also carry an implicit relevance to RQ3. 96

B.1 The firewall rule; is to be implemented manually on the three firewalls mentioned, and to allow the network connection from an external source to a specific server located in the secure zone. 158

D.1 The categorization the literature reviewed in the state-of-the-art based on the defined criteria 177

H.1 Scientific personnel survey answer to question 22 in table format with details of each answer 247
H.2 Scientific personnel survey answer to question 27 251
H.3 Scientific personnel survey answer to question 29 253
H.4 Scientific personnel survey answer to question 38 261
H.5 Scientific personnel survey answer to question 41 264
H.6 IT professional survey answer to question 41 296

Chapter 1

Introduction

This chapter serves as an introductory framework for the research presented in this thesis. It begins by outlining the core topics under investigation and introducing the keywords relevant to this study. Subsequently, we mention research objectives before providing a comprehensive overview of the problem at hand and outlining the central hypothesis.

In addition to problem identification and hypothesis formulation, this chapter offers essential sections on justification, motivation, anticipated benefits, and the Research Question (RQ)s. Furthermore, we delve into the planned contributions of this research, its scope and purpose, and an exploration of related works that provide context and support for our research questions. Moreover, ethical and legal considerations that guided our investigation, including insights gleaned from surveys and interviews, will be discussed. We conclude this chapter with a brief preview of the document's overall structure, offering readers a roadmap for navigating the content that follows.

1.1 Topics Covered By the Research

Study of the State-of-the-Art (SotA), presented in Section 4.1 and the other contents of the Chapter 4, underscores the compelling advantages of automation techniques and technologies in enhancing the efficiency, reliability, and resilience of network security. Conversely, it also highlights the underutilization of novel network automation methods within the field.

In this research endeavor, our primary focus revolves around several pivotal topics concerning the automation of IP network security:

- **IP Network Knowledge:** We provide an in-depth understanding of IP networks, different network security architectures, various types of IP network firewalls, associated technologies, structural intricacies, and effective man-

agement techniques.
- **Network Automation Expertise:** We delve into the realm of network automation, including the exploration of relevant simulation platforms, enabling readers to gain a comprehensive grasp of these crucial technologies.
- **Factors Affecting Success:** We shed light on the critical factors influencing the successful implementation of automation techniques and technologies in network security. This encompasses an exploration of challenges, use cases, and vulnerabilities related to network automation.
- **SWOT Analysis:** An analysis of the Strengths, Weaknesses, Opportunities, and Threats (SWOT) associated with network security techniques, technologies, and automation methods is presented, providing a holistic perspective on their implications.
- **Multidimensional Analysis Model:** We introduce an analysis model designed to assess complex multidimensional situations, offering a structured framework for evaluating the application of automation in network security.
- **Validation through Surveys and Interviews:** To validate our findings and insights, we share details of surveys and interviews conducted as part of our research process.

By delving into these core topics, our objective is to offer a comprehensive understanding of the automation of IP network security and its profound implications within the field. This knowledge serves as the bedrock upon which our research is constructed, and it will be further elucidated in the subsequent chapters of this thesis.

1.2 Keywords

Firewall, network automation, software-defined networking (SDN), information security, network infrastructure challenges, Critical Infrastructure Sectors (CIS), Return on Investment (ROI), network management, machine learning.

1.3 Research Objective

Our primary objectives are twofold:

Firstly, we seek to cultivate heightened awareness within the realm of network security. We aim to inspire the automation of all tasks and processes that possess the potential for automation. Secondly, we endeavor to illuminate the challenges and barriers associated with the underutilization of automation in firewalls and network management. Through this, we aim to equip organizations with a deep understanding of these obstacles, with the ultimate goal of enhancing efficiency, bolstering resilience, and fortifying the reliability of large-scale network security.

1.4 Problem Description

The proliferation of network-connected devices has ushered in a pressing demand for more efficient service delivery while concurrently meeting heightened customer expectations in terms of service quality [1, 2]. In Critical Infrastructure Sectors (CIS), the integration of Industrial Internet of Things (IIoT) technology involves passing through the designed air gap intended to isolate control systems, including Supervisory Control and Data Acquisition (SCADA), from the internet. This evolution enables remote control and management of the systems [3, 4]. In tandem with the expansion of networks and the increasing cyber threats targeting them, there emerges a compelling necessity for automation in the execution, updating, and security aspects of network management [1, 5, 6].

Traditionally, network security management has been predominantly manual, entailing the manual implementation, updates, and maintenance of various components. However, this approach is fraught with pitfalls, including susceptibility to errors, unwieldiness, and substantial time consumption [5, 7, 8]. Particularly within the CIS networks, the security of communication channels is paramount to ensuring the expected level of safety and availability [3]. The concept of automating network implementation has surfaced as a possible means to potentially augment both the efficiency and security of networks [5].

While confidentiality stands as the foremost concern in conventional information technology, the critical infrastructure domain, reliant on Operational Technology (OT), places paramount importance on availability and integrity [9, p. 12]. As networks increasingly connect the control systems of critical infrastructure to the internet, the security of communication lines becomes the foundational pillar underpinning the functionality and safety of operational technology [3].

On the one hand, for many years, suppliers and equipment providers, as well as academia, have proposed their exclusive solutions for network automation, each operating within its silo, to enhance network security. They have also introduced distinct methods for education and skills development in the field of network security automation [3, 10–14].

On the other hand, within organizations and industries, network security systems continue to be predominantly managed manually [15, 16]. This raises questions such as: 'What factors influence the decisions companies make regarding the techniques and technologies they employ in network security?' and 'Is it the organizational culture and leadership decisions that impact the techniques and technologies employed in network security, or is it due to a lack of proficiency in network automation that this process progresses slowly?

1.5 Hypothesis

As data, networks, and technologies continue to evolve, the imperative to automate all feasible tasks becomes increasingly evident. This drive toward automation seeks to bolster efficiency, resilience, and the simplification of network security management, making tasks both easier and less error-prone [2]. It is our contention that the primary challenge in harnessing automation techniques for network security lies in the shortage of knowledge and competence among network personnel and effective management capable of steering teams with the appropriate strategies for this endeavor.

Despite the availability of numerous technologies and techniques aimed at facilitating network security automation, as highlighted in the problem description, we assume that a significant number of companies have yet to fully embrace these technologies [8, 15, 16].

Given the intricate nature of this domain, which encompasses various dimensions of technology, knowledge, and possibilities, the need arises for Information Technology (IT) professionals boasting diverse competencies across multiple fields[1] [2, 11, 15, 17]. Consequently, the progression and success of implementing Network Security Automation (NSA)[2] as a cultural and long-term strategy within organizations boasting extensive networks[3] hinge significantly on the leadership and managerial prowess capable of guiding collaborative efforts and enhancing the knowledge and competencies of network operations personnel [2, 11, 15, 16].

Building upon this comprehension, we propose the following hypothesis: ***We posit that, given the requisite skills, diverse knowledge, and competency among IT professional team members, as well as the intricate considerations inherent in strategy planning, the progress and advancement of Network Security Automation (NSA) predominantly hinge on the organizational competence of team leaders in orchestrating these multifaceted elements.***

1.6 Justification, Motivation, and Benefits

As a network engineer with two years of experience managing various CIS company networks and firewalls, the author of this paper has encountered a prevailing reliance on manual processes within the industry. This observation has led to questions about the apparent gap between existing research advocating for network security automation and its limited adoption in practice. Despite the wealth of available literature and documented knowledge on automation in network security, many CIS companies continue to adhere to traditional, manual methods.

---

[1] For a more comprehensive explanation regarding the combination of multiple fields, please refer to Chapter 4 Section 4.5.

[2] Refer to Chapter 3 Section 3.3, for further clarification on our interpretation of NSA.

[3] In this thesis, when referring to extensive and large networks, our primary focus is on CIS IP networks.

Transitioning from an academic environment to the corporate world revealed a notable disparity between what was taught in university programs and the technologies employed by organizations. For instance, technologies such as Cisco's Developer Network (DevNet) and automation techniques were not adequately covered in our university curriculum, even though we had completed CCNA and CCNP study materials. This disparity prompted us to investigate the reasons behind this discrepancy.

This research aims to explore the coexistence of traditional network security technologies[4] and architectures with the potential automation techniques and technologies that could enhance them. We seek to understand why automation has not been more widely integrated into today's network infrastructure. In Chapter 3, we will discuss how CIS networks have become one of the prime targets for cyberattacks due to their extensive reach and ability to pay ransoms. Discovering the answers to the research questions, addressed in Section 1.7, will help justify the adoption of NSA techniques[5] in specific situations.

As highlighted in Section 1.4, the critical role of network technology in the CIS cannot be understated [3]. Continuous availability and integration of technology are essential in this industry [9]. However, as we will explain in Chapter 3, the vulnerability of these systems to cyberattacks highlights the importance of securing network communications and control. This research focuses on enhancing network security's resilience to cyber threats through the implementation of automation techniques and technologies.

Despite extensive literature advocating for automation in network management [8, 10, 11, 18][6], progress has been slow [15, p. 24]. This observation raises questions about the potential obstacles hindering the widespread adoption of NSA techniques, which motivates our investigation into the related challenges.

In conclusion, this research aims to provide a multidimensional perspective on the complexities of NSA, helping organizations tailor their practices to suit their unique structures. Through a Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis of existing models, we help companies identify NSA solutions that fit their requirements and capabilities, while also evaluating the need for automation techniques. Furthermore, this research clarifies the benefits of NSA for companies that may have previously overlooked its potential. It serves as a comprehensive resource to support informed decisions regarding the integration of automation technology into network security structures.

---

[4] Within this thesis, our focus on **technology** encompasses the methodologies and tools utilized for task execution.

[5] In the context of this thesis when we mention **techniques**, we are delving into the particular architectural and procedural methods employed to achieve tasks.

[6] In this thesis, where we refer to multiple references at one point for our rationale, this is because they complete each other as no one reference alone was able to support our rationale. This approach underscores the importance of employing several resources, as they complement one another and collectively provide comprehensive support for the aimed rationale.

1.7 Research Questions

This section presents the research questions raised in this thesis. These questions aim to determine the following:

1. What types of traditional network security techniques and technologies exist, and what are their characteristics in traditional network approaches?
2. What existing network automation techniques and technologies contribute to enhanced resilience, reliability, and efficiency in network security management?
3. What factors play a pivotal role in influencing the adoption and successful implementation of network security automation techniques and technologies within organizations and industries managing large-scale networks?

1.8 Planned Contribution

This thesis makes the following significant contributions:

1. **Emphasizing Network Security Importance:** Highlighting the importance of effective, resilient, and reliable network security in large networks, such as in CIS networks, and providing SWOT analyses of the existing traditional network security techniques and technologies before the application of Network Security Automation (NSA).
   This work conforms with RQ1 by emphasizing the significance of network security. It also sheds light on the complexities related to the process of review, choice, and implementation of network automation strategy in these network environments. Additionally, we offer a demonstration of the existing complexities in a multidimensional situation that needs to be managed and the challenges that need to be overcome. This aspect aligns with RQ3, further enriching our understanding of network security in large networks.
2. **Comprehensive Overview of NSA:** We provide a comprehensive overview of NSA techniques and technologies, including factors influencing its success, such as challenges, use cases, and vulnerabilities. This addresses RQ2 and RQ3 and incorporates a SWOT analysis.
3. **Balanced Assessment of SotA:** Our work includes a comprehensive exploration of the SotA concerning network and network security automation, addressing both the positive and negative aspects of NSA. This approach aligns with RQ2 and RQ3, setting our research apart. Remarkably, this balanced perspective is found in only approximately 15% of the over 100 scientific resources meticulously registered and reviewed within this thesis.
   Most of these resources tend to exclusively emphasize the strengths, opportunities, and advantages of employing automation techniques and technologies to enhance network and network security solutions. Conversely, some focus solely on the weaknesses, threats, and disadvantages introduced into

the network and network security by the application of automation techniques and technologies. Moreover, even those resources that do examine both sides of the issue often employ different methods. Our unique approach involves presenting this analysis within the framework of a SWOT analysis, a method seldom used among the wide array of resources we've studied in this regard.

4. **Novel Analytical Model - CCAM:** We introduce the Combination Cube Analysis Model (CCAM)[7], an innovative analytical model for network and network security automation. CCAM aids in structuring various possibilities and assessing multiple dimensions in decision-making processes. This model clarifies complexities and assists organizations in aligning network automation with their vision, mission, and values. Additionally, the model Information Technology Actors Triangle (ITAT) within CCAM outlines the involvement of various actors in different circumstances.
   This CCAM methodology serves as a robust foundation for conducting novel analyses related to network and network security automation techniques and technologies. The analysis sheds light on the complexities and dependencies of different parameters, helping organizations find their desired and customized automation model, while researchers can select their preferred path for combining various dimensions and conducting their research.
5. **Identifying the Knowledge-Practice Gap:** Our research exposes the disparity between academic knowledge, research results, and experimental findings in network and network security automation and the limited adoption of these technologies in enterprises managing large networks. Through surveys and interviews with network professionals and academic personnel, we validate our research results and the suggested hypothesis, bridging the gap between theory and practice.

1.9 Scope and Purpose

This thesis delves into the realm of traditional techniques, architectures, and technologies currently employed by companies, aiming to provide a thorough overview of the existing landscape. With a specific focus on firewalls and network management, we explore various network and network security automation methods within the context of our State-of-the-Art (SotA) study, shedding light on the diverse technologies in this domain.

Within each topic, our focus is to provide illustrative instances, enabling us to later delve into the multifaceted dimensions of the complex problem and offer a holistic understanding. When it comes to automation techniques, we furnish examples corresponding to elements referenced in the SotA, offering readers a concise overview.

---

[7] See Section 4.5.

In Section 4.3.6, where Machine Learning (ML) is discussed, we aim to provide an exhaustive yet concise overview of this field within the scope of our SotA study.

Regarding the validation process, we engage individuals closely involved in network and network security management, as well as those responsible for imparting IT knowledge to students. Interviews and surveys with these participants hold high value, as they provide invaluable insights from professionals actively engaged in the field, helping to validate our research findings.

Furthermore, the SWOT analysis presented for various network security techniques within this thesis aligns with the mitigation methods outlined in the resources studied in our SotA for each case.

1.10 Related Works

In this thesis, we have proposed a hypothesis as outlined in Section 1.5. The research questions, introduced in Section 1.7, serve as the foundation for our study, guiding us toward answers that will help evaluate our hypothesis. Consequently, our focus is on works closely related to our hypothesis, while a broader literature review addressing the research questions is detailed in Section 4.1 within the State-of-the-Art (SotA) review. Regrettably, there are few scientific research works that align directly with our perspective. Nevertheless, we present here an overview of the relevant works we have identified so far.

Kian W. et al. [16, p. 73-78] have undertaken research closely related to our work. Their study provides insights into interviews conducted with 30 network technicians, exploring their concerns, challenges, and perspectives on network automation. The findings from this research are pertinent to our study and were conducted between August and September 2022.

McGillicuddy S., in a research report by Enterprise Management Associates (EMA)[8], highlights the dilemma where network professionals lack programming skills, and programmers struggle to comprehend networking concepts. This discrepancy results in network security automation becoming a complex and challenging task for participating companies. In a report published by EMA in February 2022, the following citations shed light on this issue:

“Networking guys know the network very well, but we’re not programmers. Programmers are great at coding, but they don’t understand networks at all. There are very few people who can put networking into code, said a network architect with a $50 billion global consulting company” [15, p. 22].

“It’s difficult to find people who know how to automate,” said a network engineer with a $3 billion North American medical research company. “I think there is a lack

---

[8] The IT firm EMA conducts research on data management issues, involving a diverse range of companies, including small, medium-sized, and large enterprises, in their surveys and research activities [15].

of professionals on the market. That's a big challenge, finding people who know the data centers and how to automate" [15, p. 22].

B. Choi briefly in [11], emphasizes the importance of network engineers acquiring programming and automation skills. The book touches upon our problem statement by stating:

"In fact, the industry started to demand more hybrid engineers with network programming skills on top of their existing responsibilities. In short, the market wanted more network engineers who could think and code like real application developers using one or more programming languages and open source programs" [11, p. xxv].

Amin, R., Reisslein, M., & Shah, N. [13] highlight the relationship between the cost and budget allocated for investing in network automation and the enhancement of network personnel's competence in this field. The resource underscores the deficiency in network automation proficiency as a factor influencing companies' assessment of Return on Investment (ROI) in network automation.

Both Kian W. et al. [16] and McGillicuddy S. and his research team [15] underscore the apprehension among network professionals regarding the implementation of changes and network automation for managing network and network security. This fear centers around the potential disruption of a company's production environment, making technicians cautious about implementing automated changes and apprehensive about addressing any arising issues [16, 19].

1.11 Ethical and Legal Considerations

For the surveys and interviews conducted as part of this study, we have adhered to the regulations outlined in the General Data Protection Regulation (GDPR) established by the European Union [20, Art. 6, Art. 13]. The following key points are included in the research information form to inform survey and interview subjects:

1. Obtaining the consent of survey and interview subjects is our top priority.
2. Subjects will receive prior information about the research topic and problem description.
3. Subjects are informed of their right to withdraw consent, allowing them to withhold their information from our analysis.
4. The option of anonymizing their identity will be presented to survey and interview subjects.
5. Information provided by survey and interview subjects will be anonymized to safeguard the privacy of the individuals involved, as well as that of their respective organizations and customers.
6. If the survey and interview subjects mention colleagues or students, that information will also be anonymized.

7. Subjects will be asked for consent regarding the publication of their statements in the thesis, with the option to decline.
8. Written information about their privacy and confidentiality rights will be provided to subjects before obtaining consent.
9. Data collected through surveys and interviews will adhere to GDPR transparency rules [20, Art. 12], and subjects will have access to their data upon request.
10. If interview subjects wish to exercise their rights under GDPR [20, Art. 17], their data will be promptly deleted upon request. Additionally, they will be informed of their right to restrict the processing of the data they have shared with us, following GDPR [20, Art. 18].
11. Our foremost commitment is to conduct this research scientifically and legally, prioritizing the informed participation of individuals and ensuring the utmost security and confidentiality of their data throughout the research process [21].

1.12 Document Structure

The structure of this thesis, outlined in Figure 1.1 as a document navigation roadmap, is as follows:

- **Chapter 1:** In this introductory chapter, we lay the foundation by presenting the key topics covered in the research. We introduce essential keywords and elucidate our research objective and problem description. Additionally, we provide context through our hypothesis, justification, motivation, and the anticipated benefits of our study. Furthermore, we present the research questions that guide our investigation. This chapter also delves into our planned contributions, scope, purpose, and related works, alongside ethical and legal considerations concerning our surveys and interviews.
- **Chapter 2:** In Chapter 2, we delve into the methodology employed in our research. For the sake of conciseness, the details of this methodology are presented in the Appendix A.
- **Chapter 3:** This chapter provides the theoretical background necessary to understand the core content of this thesis. One of the topics covered includes the Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis methodology. Additionally, this chapter points to the concept of OSI model. This chapter also explores the significance of network security in Critical Infrastructure Sectors (CIS) networks. More detail on the mentioned topics is made available as an extensive glossary of terms and concepts that are fundamental to our discourse in Appendix B. The parts that have been extracted and placed in various appendices are for the sake of conciseness in the thesis. This also encloses a comprehensive examination of traditional network security techniques and technologies, including firewalls and network security architectures. This examination is based on the study of the

SotA and contributes to answering RQ1.

- **Chapter 4:** In this chapter, we present the research results derived from our thorough investigation. We commence by discussing the theoretical contributions arising from our comprehensive study of the SotA. Subsequently, we offer a summarized SWOT analysis of traditional network security techniques and technologies. More detailed information can be found in Appendix F for the sake of conciseness. This analysis forms the other aspect of addressing RQ1. Following that, we delve into Network Security Automation (NSA), exploring related techniques and technologies to address RQ2. Within the NSA section, we cover various aspects, including the application of automation in firewall technologies, the integration of ML into NSA, associated challenges, use cases, and vulnerabilities. The concluding part of this section offers a SWOT analysis of NSA, based on our findings from the SotA, addressing both RQ2 and RQ3. Furthermore, this chapter provides a comprehensive view of existing complexities using an analytical model, demonstrating the multidimensional factors that shall be considered. We explain the interdependencies between different dimensions using the Combination Cube Analysis Model (CCAM), contributing to our response to RQ3. In conclusion, we present key findings and then summarize the entire Results chapter.
- **Chapter 5:** This chapter begins with a description of the interview and survey questions used in our research. A detailed overview of the survey questions is provided in Appendix G, a comprehensive review of survey results in Appendix H, and an in-depth examination of interviews in Appendix I, all for the sake of conciseness. The chapter then proceeds to validate the results by comparing them with the outcomes of the survey and interview analyses. This validation process also reaffirms the problem statement and hypothesis introduced in Chapter 1. At the end of this chapter, we affirm the key findings presented at the end of Chapter 4.
- **Chapter 6:** This chapter discusses research limitations, and future work suggestions, and concludes our research.
- **Appendices:** At the end of this thesis, Appendix A presents details about our methodology. Thereafter, Appendix B provides an overview of the concepts and definitions in a glossary format. This part is presented in the form of an appendix to at the same time provide the necessary information about our topics available, and make Chapter 3 more concise. Then, in the Appendix C the criteria used to categorize the SotA resources, which we have defined for the convenience of our research are presented. Appendix D further lists the SotA resources utilized in our research which were presented in categorized format in Table 4.1 in Chapter 4. Appendix E provides a review of a selection of the resources reviewed in the SotA study. Appendix F presents a comprehensive SWOT analysis of traditional network security management characteristics which is relevant to RQ1. All these are made available in the format of an appendix to make the main part of the thesis

shorter, at the same time as having other parts that are necessary to confirm the research and its results available for the readers. Other appendixes thereafter include Appendix G where the questions used in the surveys are presented, Appendix H where the results of the survey are reviewed comprehensively, and Appendix I where the interviewers done are reviewed in depth. The final Appendix, Appendix J provided in this thesis presents an experiment with artificial intelligence.

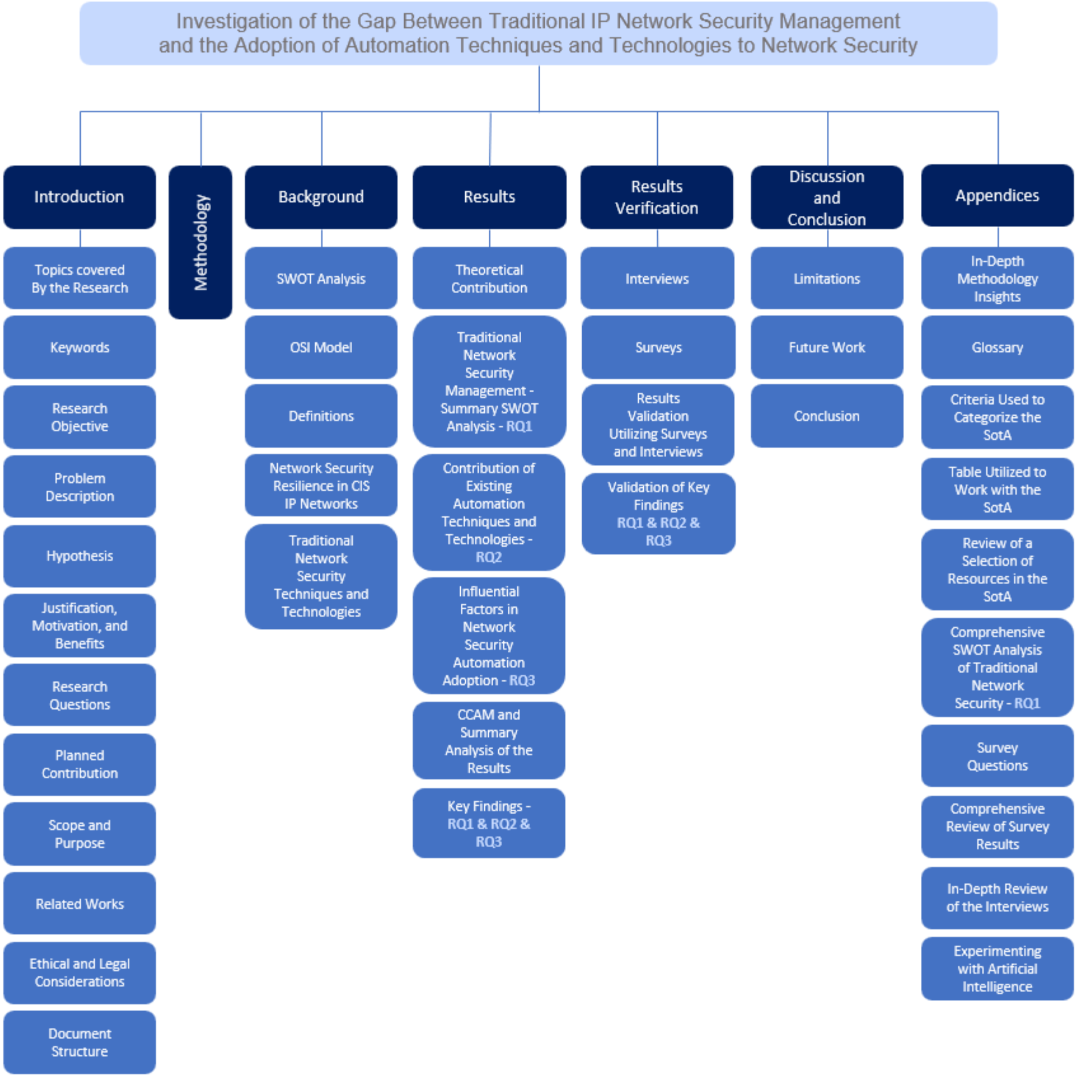

Investigation of the Gap Between Traditional IP Network Security Management and the Adoption of Automation Techniques and Technologies to Network Security
Introduction
Methodology
Background
Results
Results Verification
Discussion and Conclusion
Appendices
Topics covered By the Research
Keywords
Research Objective
Problem Description
Hypothesis
Justification, Motivation, and Benefits
Research Questions
Planned Contribution
Scope and Purpose
Related Works
Ethical and Legal Considerations
Document Structure
SWOT Analysis
OSI Model
Definitions
Network Security Resilience in CIS IP Networks
Traditional Network Security Techniques and Technologies
Theoretical Contribution
Traditional Network Security Management - Summary SWOT Analysis - RQ1
Contribution of Existing Automation Techniques and Technologies - RQ2
Influential Factors in Network Security Automation Adoption - RQ3
CCAM and Summary Analysis of the Results
Key Findings - RQ1 & RQ2 & RQ3
Interviews
Surveys
Results Validation Utilizing Surveys and Interviews
Validation of Key Findings RQ1 & RQ2 & RQ3
Limitations
Future Work
Conclusion
In-Depth Methodology Insights
Glossary
Criteria Used to Categorize the SotA
Table Utilized to Work with the SotA
Review of a Selection of Resources in the SotA
Comprehensive SWOT Analysis of Traditional Network Security - RQ1
Survey Questions
Comprehensive Review of Survey Results
In-Depth Review of the Interviews
Experimenting with Artificial Intelligence

Figure 1.1: Document navigation roadmap. The figure is created by the author.

Chapter 2

Methodology

In this chapter, we present the methodology employed in our research, offering a succinct explanation of each step. Our methodology commences with a clear problem description, the formulation of a hypothesis, and the precise definition of the research question. Subsequently, we undertake an exhaustive exploration of the State-of-the-Art (SotA) and a comprehensive evaluation of the results, with data collection primarily grounded in the SotA study. Additional information about each of the steps in our methodology is provided in Appendix A.

To bolster the credibility of our findings, we rigorously validate the results obtained through this process by conducting interviews before reaching a conclusive standpoint. It is essential to note that, during this process, we remain open to the possibility that our initial hypothesis may require refinement or justification. In such instances, we proffer recommendations for the subsequent iteration of our research in the form of future work, which is expounded upon in Chapter 6, Section 6.2. Therefore, the phases guiding the implementation of our research, as depicted in Figure 2.1, unfold as follows:

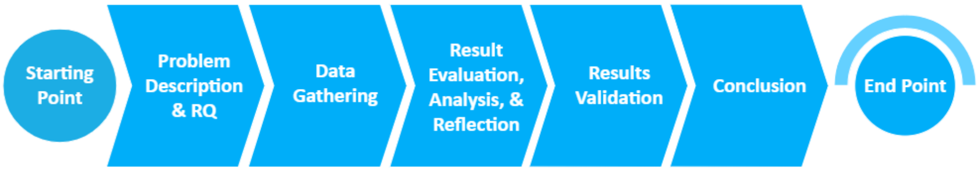


Figure 2.1: The five steps in methodology explained in this chapter. The figure is created by the author.

1. **Problem Description and Research Questions:** Our methodology initiates by identifying research gaps through an exhaustive SotA analysis. This initial phase informs the subsequent steps, enabling us to articulate a well-defined problem and formulate hypotheses. These hypotheses provide a clear roadmap for our investigation, directly addressing the respective Research Question (RQ)s presented in Chapter 1 Section 1.7.
2. **Data gathering:** The subsequent pivotal phase revolves around data collec-

tion via an in-depth SotA study, as elucidated in Chapter 4, Section 4.1. The selection criteria for these documents prioritized the most recent articles relevant to our research topic. For information gathering, we extensively utilized reputable scientific databases, including Google Scholar, ScienceDirect, IEEE Xplore, Research Gate, Springer Link, OPTICA Publishing Group, IOPScience, Penn State (psu.edu), Taylor & Francis Group, Hindawi, and Gartner, to meticulously search for and retrieve the relevant documents. Our comprehensive data collection encompasses:

- **Data Related to Network Security Management Techniques RQ1:** We gather information on existing network security management techniques, technologies, and architectures, including their characteristics within traditional network security paradigms, yet excluding automation techniques.
- **Data on Network Automation Contributions RQ2:** We collect data that specifically highlights the contributions of current network automation techniques and technologies, particularly in enhancing the resilience, reliability, and efficiency of network security management.
- **Factors Affecting Automation Adoption RQ3:** We investigate key factors influencing the adoption of network security automation techniques and technologies within organizations and industries managing large networks.

3. **Result Evaluation, Analysis, and Reflection:** After data collection, our methodology employs rigorous evaluation and analysis of the acquired data within the SotA framework. This analysis encompasses various approaches, including Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis and the Combination Cube Analysis Model (CCAM), expounded upon in distinct sections of Chapter 4 and resulting in key findings.
4. **Results Validation:** Ensuring the robustness of our research findings, we deductively[1] undertake validation through surveys and interviews. These interactions involve scientific personnel from an academic institution and proficient IT experts with specialization in IP networks, network security, network automation, or related domains, hailing from diverse large companies to answer RQ3. Chapter 5 meticulously presents this validation process, aimed at deducing and confirming the accuracy of our problem statement, hypotheses, and findings derived from the SotA study and concluding in validation and summarizing of key findings.
5. **Conclusion:** In the final phase of our methodology, we synthesize our research findings, acknowledging any encountered limitations and providing valuable suggestions for future research endeavors. This culmination of our research journey is comprehensively detailed in Chapter 6.

---

[1] By deductively validating our research results, we mean that, through surveys and interviews, we sought feedback from participants to assess the accuracy of our findings derived from the SotA analysis [22].

Chapter 3

Background

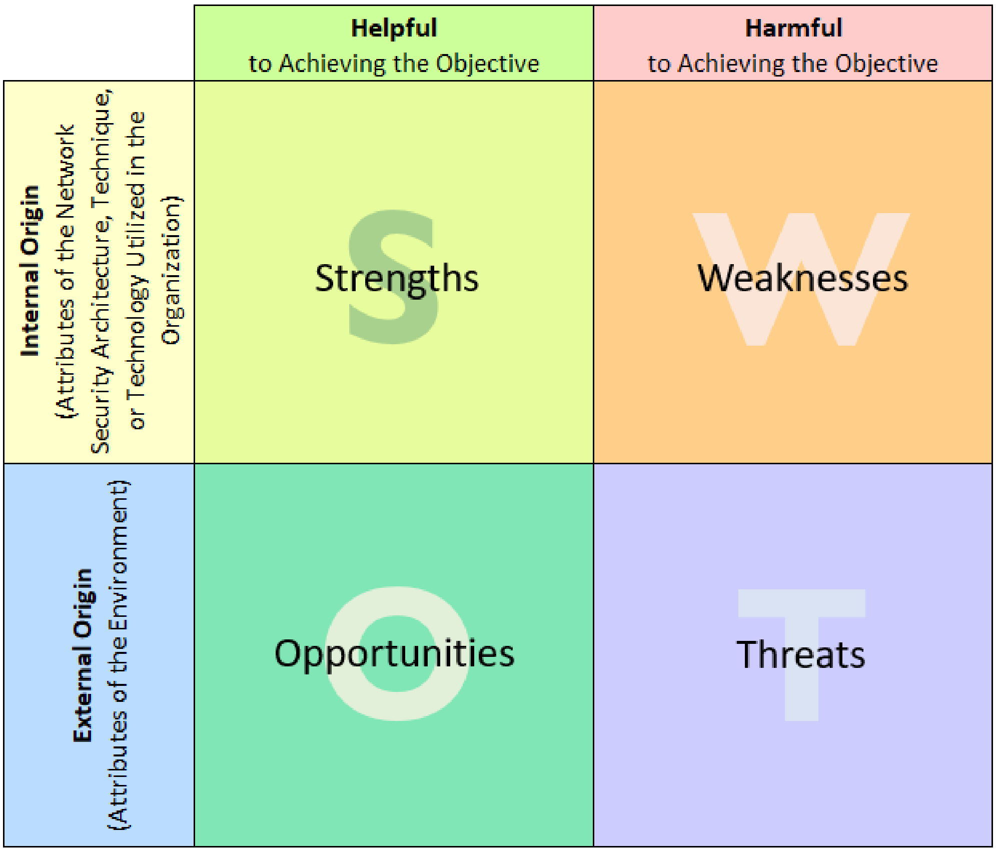
This chapter lays the groundwork for the results presented in Chapter 4 through essential background information. It covers the theoretical background of the SWOT analysis methodology and the relevance of the OSI model to the network concepts in our research. The section on definitions outlines the context for discussing Network Security Automation (NSA). Furthermore, it underscores the significance of network security resilience in Critical Infrastructure Sectors (CIS) IP networks and explores instances of cyberattacks targeting CIS. The chapter concludes with a brief explanation of traditional network security techniques and technologies. For more comprehensive details on CIS IP network architecture, information security terms, and elaborations on traditional network security, please refer to Appendix B.

3.1 SWOT Analysis

In this Master's thesis, we have utilized SWOT analysis to investigate the characteristics of each of the network security architectures and the automation techniques and technologies we present. Here in this section, we explain the SWOT analysis methodology [23], so in future sections, we will refer to it.

Every network security technology, technique, and architecture we review has some advantages (**helpful**) in achieving objectives for the organization's network and network security needs and therefore brings some **strengths** with itself. At the same time, the **weaknesses** of each model of network security architecture, technique, or technology will have some disadvantages (**harmful**) in achieving objectives for the organizations that utilize it [24].

Moreover, each of the explained network security technologies, techniques, and architectures, based on their strengths, bring some **opportunities** to the external environments of the organizations utilizing them while the weaknesses they impose on the organizations will be vulnerable to external **threats** that already



	Helpful to Achieving the Objective	**Harmful** to Achieving the Objective
Internal Origin (Attributes of the Network Security Architecture, Technique, or Technology Utilized in the Organization)	Strengths	Weaknesses
External Origin (Attributes of the Environment)	Opportunities	Threats

Figure 3.1: Strengths, Weaknesses, Opportunities, and Threats (SWOT) table for reference in further analysis. The figure is created by the author.

exist in the external environments of the organizations [24].

Therefore, it is essential for organizations that want to choose their network security architecture and the supporting automation techniques and technologies, at the same time, to be aware of the positive effects of each model, which are the strengths and the opportunities, being aware of the opposing sides which also arrives with each architecture model and technologies. This negative side is the weaknesses and threats each specific network security architecture encounters.

This is because when the organizations are aware of the weaknesses and the threats encountering their network security architecture, techniques utilized, and technologies leveraged, they can decide better if they need to upgrade it to a more secure system in case they wish to cover the existing gaps by utilizing some techniques, workarounds, or substitute technologies, or even if they will accept the risk based on their risk appetite.

As also depicted in Figure 3.1, while knowing all four sides of each technique utilized for network security by leveraging a SWOT analysis, an organization's leaders, managers[1], and network architects can discuss to find out if the risks that exist exceed their risk appetite or is it below the defined risk threshold for their organization.

By leveraging this SWOT analysis in our research work, we investigate and map internal **strengths** and **weaknesses** in addition to external **opportunities** and **threats** to each of the network security architecture, and automation techniques and technologies we review. The facts gathered in the SWOT analyses are in the scope of the SotA studied in this research. This SWOT analysis allows us to make an overview of the characteristics of the network security architecture of the organizations to help the assessment of their needs to NSA techniques and technologies [25]. It also gives the possibility to put light on the NSA characteristics in a holistic manner to see the circumstances more comprehensively.

3.2 OSI Model

The Open Systems Interconnection model (OSI model) model, is a conceptual framework that standardizes the functions of a communication system or network into seven layers. These layers, from the physical transmission of bits to the user interface, include physical, data link, network, transport, session, presentation, and application layers [26]. For more information on OSI model model please see Appendix B. The relevance of this to our research comes up where for the automation of network and network security devices, we need to contact these using Application Programming Interface (API)s and applying different automation tools and technologies. This is more explained in Chapter 4.

3.3 Definitions

This section provides an in-depth exploration of the contextual framework that underpins our perspective on network security and Network Security Automation (NSA)[2].

Network Security and Network Security Automation

The reasoning and the context in which we use the concept of network security and what we put into it are explained here. When discussing this concept, we see three parts involved. These include firewalls, network configurations, and

---

[1] In this thesis, we refer to 'leaders' as higher-level decision-makers within an organization and 'managers' as individuals responsible for supervising and working closely with network and network security technical teams.

[2] The explanations for the terms and concepts utilized within this thesis can be found in the glossary provided in Appendix B, and include concise information about OWASP Top Ten and CWE, which are referenced in our discussions. Additionally, you will find brief definitions of information security-related terms and concepts in that glossary, as we employ these terms throughout this thesis.

finally different network security architectures. In this thesis, we categorize all these three parts as the traditional manner of managing network security. Network Security Automation (NSA) thereafter, builds on what these traditional network security elements put into network security context.

First, network configurations are included in parameters that will affect network security. For instance, maintaining numerous unused device network interfaces in an 'up' state instead of a 'down' state has a detrimental effect on network security. Because the unused network interfaces on devices that are in a 'no shut' state can be misused by a cyberattacker to perform malicious tasks on the network. The same applies to examples with many unused Virtual Local Area Network (VLAN) interfaces not configured in a secured manner or other types of negligence in securing the network configurations [27, 28].

These types of negligence, especially in large networks such as in CIS networks, where for instance, a power supply company has locations in different countries with distance and network to manage, will become out of control and very difficult, if not impossible, to handle and patch manually [2]. However, in the example mentioned above, if having automated code for routinely checking interfaces, VLAN, and other components in the network that need to be configured in a specific manner or removed if not in use, the task will be done whenever the code is running automatically. This makes the network configuration both secure, manageable and under control [2]. That is why we consider network configuration related to network security and include it in our discussions about network security automation [5].

Second, in this context, when discussing network security automation, we also include firewalls. This is because, today, firewalls are an essential part of the network that seeks to secure each part behind it from the external world, for instance, from the internet. These firewall elements could be router hardware, firewall software applications, or another element that plays the role of the firewall. In any way, they are dedicated to the security of the networks and, virtually or physically, are placed in different network locations based on different network security strategies. Some firewalls are to secure access from the internet to Demilitarized Zone (DMZ), where usually the web servers of the company and additional security-related elements such as honeypots or proxy servers are located, and some stay between the DMZ and the internal network of the company.

Nevertheless, there are many strategies on how to implement and utilize firewalls [29]. The strategy and architecture of how to design and implement network security is the third element we put into the context when discussing network security. What we mean to point out here is that the context in which we speak about network security includes firewalls, network configuration elements that can affect network security, and network security-specific elements. Also, the context in which we speak about network security automation will be built on the above-mentioned elements in the processes to be managed automatically by different types of automation techniques and technologies. For a thorough exploration of firewall-related topics, DMZ, perimeter network, comprehensive firewall explanations, and detailed information on architecture and network design, please refer to Appendix B.

3.4 Network Security Resilience in CIS IP Networks

This section explains why CIS network needs to be managed more effectively, and its security needs to be resilient. Everyone uses networks and firewall services for their protection. This includes a simple individual Personal Computer (PC), small or medium enterprise networks, or large companies that are providing their customers with different network and network security services. When security is vital for everyone, some domains still deserve more attention. These are the networks of the companies that provide critical services to great parts of society, such as emergency services, energy, financial, and transport systems sectors [30].

If these sectors get damaged for any reason, the harm will affect a significant part of society [9]. Also, as most of these sectors are driven by either large companies or by governments, the chance of cyber criminals getting paid and their appetite for conducting cyber attacks is much higher. Simply large companies and governments have a greater ability to pay the ransom than small or medium companies [31].

Furthermore, in addition to large networks being more demanding to secure, the reputation of the company will be in danger if they transparently tell the customers and the stakeholders that they have received harm by cyberattacks, or their services practically get shut down by a cyberattack [32]. Those are good reasons why putting more attention to large networks and the necessity of adopting automation techniques and technologies in their network security is crucial [33]. You will find a detailed explanation of the CIS general IP network architecture in Appendix B.

3.4.1 CIS IP Network Security

By connecting the CIS IP network to the external world, despite conducting security measures, we need to raise the resilience of these networks. This is necessary for keeping the critical infrastructure safe from the access, harm, and manipulation of the adversary [34].

For instance, the healthcare industry is said to be one of the biggest producers of big data [30, 35]. In this case, all transformed data needs to be analyzed and secured while it is passed through the network and the firewalls. The importance of providing QoS for the data that transfers through the network traffic is also been highlighted.

All these necessary services that are needed for the security and resilience of the CIS network, in addition to the complexity of the network zones and their layers make the management of the IP network security even more difficult if the tasks are to be controlled and managed totally with human work [5]. This is where the resources studied in the SotA, presented in Section 4.1 point to the utilization of NSA techniques and technologies as the answer to the problem of this complexity. More detail on network layers and zones is depicted using Figure B.6 in Appendix B.

3.4.2 Cyberattacks Targeting Critical Infrastructure Sectors

Critical Infrastructure Sectors (CIS) has since long been a tempting target for cybercriminals. Any motivation that cybercriminals could have for the cyberattacks they conduct on CIS IP networks and IT resources, such as financial gain, revenge, recognition, and achievement, or other motivation factors, does not have much to say in this discussion [32]. The effect of their cyberattacks, however, is critical here, as they sometimes have managed to do damage on CIS network and their facilities, and in some cases, the damage has been even worse with effect on hundreds of thousands of people who were dependent on specific services provided by one of the CIS [31]. This is why we have chosen to put light on CIS networks as one of the most significant network security areas that need to be resilient, reliable, and at the same time, work in an efficient manner [32].

Examples of the cyber attacks that have targeted and caused damage to CIS companies are many. These include the cyber attacks on SolarWinds Orion [36], affecting 18,000 customers; the cyberattack on the Ukraine Power Grid [37], impacting more than 225,000 Ukrainian people; and the ransomware attack on Colonial Pipeline [31, p. 1], resulting in 16,000 gas stations in the United States falling out of service. You will find more information about these instances of cyber attacks on CIS in the Appendix B. This gives a picture of the reasons for the concerns about the network security of CIS companies and the necessity of using better and more novel methods, such as utilizing automation technology and techniques, to close the security gaps in large networks [33].

In summary, we underscore the paramount importance of cybersecurity measures within CIS networks. As previously discussed, these networks are both extensive and intricate, complicating the task of managing and securing them, as we will further elaborate in this thesis. In the upcoming sections and the following chapter, we will delve into the critical necessity of implementing resilient and dependable network security architectures [38]. Simultaneously, we will address the challenges associated with network security management [2].

The three instances of cyberattacks highlighted in this section emphasize the urgent need to incorporate additional security technologies and techniques into network architectures. Concurrently, we must find ways to streamline and simplify network security management while maintaining resilience.

3.5 Traditional Network Security Techniques and Technologies

Traditional network security involves key concepts such as micro-segmentation and Zero Trust Architecture (ZTA). Micro-segmentation, as exemplified by solutions like VMware [39], entails dividing a network into distinct segments, enhancing security through nuanced control and specific rules governing northbound and southbound communications. By assigning tags to Virtual Machine (VM)s and configuring East-Westbound firewall rules, communication within segments is facilitated.

ZTA, a paradigm shift from perimeter-based security, continuously assesses access and identity using Machine Learning (ML) for threat analysis [40]. ZTA dynamically grants access rights based on real-time needs, leveraging Software-defined Networking (SDN) and ML techniques [41] to simplify complex security methodologies. Notably, micro-segmentation contributes to ZTA by providing a refined approach to network segmentation [39, 40]. For more information on traditional network security techniques and technologies refer to Appendix B.

Chapter 4

Results

In this chapter, we commence by presenting the theoretical contributions of this research. Following that, we offer a summarized overview of traditional network security architecture and firewall management, aligning with the objectives of addressing Research Question (RQ) 1. This presentation takes the form of a Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis[1]. To maintain conciseness, the comprehensive SWOT analysis of traditional network security techniques and technologies is made available in Appendix F, while the related theoretical elaborations are provided in Appendix B.

In the next two sections, we examine Network Security Automation (NSA) techniques and technologies from various angles while also conducting a SWOT analysis. This analysis, similar to what was done for traditional network and network security techniques and technologies, is based on the findings of the SotA study. In our review of NSA, we explore path control in network devices, the application of Software-defined Networking (SDN) to operational planes, orchestration, Network Function Virtualization (NFV), and automation methods and tools.

We also investigate the automation of firewalls, the application of Machine Learning (ML) to NSA, experimenting, and practicing network automation, as well as the motivation related to skill-building in NSA-related competency. While our primary focus in Section 4.3 has been on addressing RQ2, in Section 4.4 we subsequently shift our focus to answering RQ3 by reviewing challenges and issues, use cases, and vulnerabilities in addition to providing a SWOT analysis.

Thereafter, we proceed this chapter with the Combination Cube Analysis Model (CCAM) and a summary analysis of the results. This will present a novel model for explaining the existing complexities and dependencies that impact the application and utilization of NSA in network and network security. Finally, the key findings of

---

[1] To ensure a clear link between the elements in the SWOT analysis and their corresponding references, we opt for a textual format presentation, omitting the usual tabular format. You can refer to Chapter 3, Section 3.1, for the complete SWOT table, along with the accompanying explanations.

our research related to RQ1, RQ2, and RQ3 will be presented. Here, for the readers' convenience, Figure 4.1 is provided to assist in navigating between different sections of this chapter.

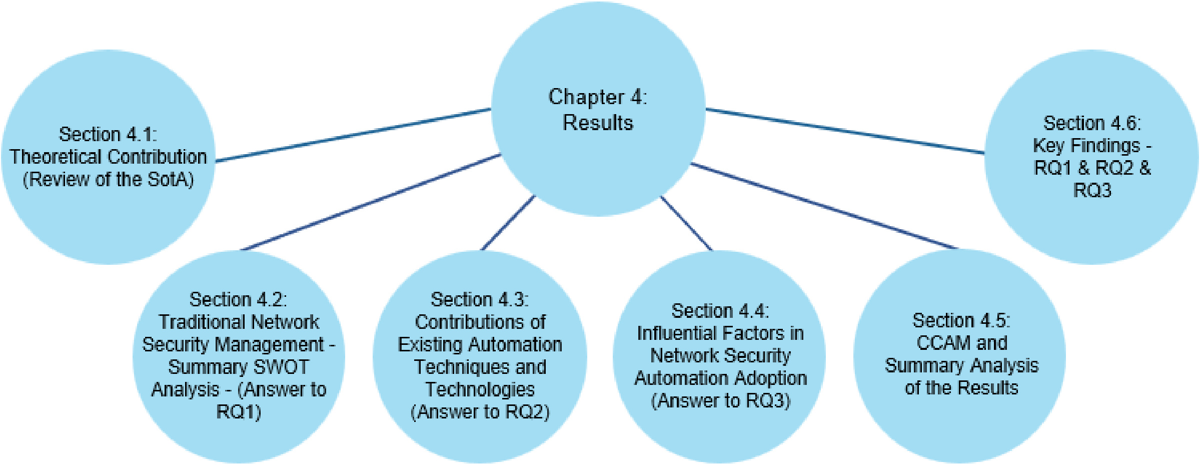

Chapter 4: Results
Section 4.1: Theoretical Contribution (Review of the SotA)
Section 4.6: Key Findings - RQ1 & RQ2 & RQ3
Section 4.2: Traditional Network Security Management - Summary SWOT Analysis - (Answer to RQ1)
Section 4.3: Contributions of Existing Automation Techniques and Technologies (Answer to RQ2)
Section 4.4: Influential Factors in Network Security Automation Adoption (Answer to RQ3)
Section 4.5: CCAM and Summary Analysis of the Results

Figure 4.1: The overview of the Results Chapter. The figure is created by the author.

4.1 Theoretical Contribution

This section presents the resources studied in the State-of-the-Art (SotA) as the theoretical contribution to our investigation. These resources, consisting of books, papers, articles, and experimental research results, are categorized by relevance in Table D.1, presented in Appendix D. The categorization criteria for the resources, also found in Table 4.1, are listed in Appendix C in a more comprehensive manner. These criteria are defined to assist us in working with the resources and utilizing them in our research. Table 4.1 provides a summary of the SotA review, showcasing the relation of the resources studied to the topics related to our research. Subsequently, Table 4.2 depicts the relation of the resources studied in the SotA to the Research Question (RQ)s before discussing the gap observed in the studied resources. Finally, a more comprehensive review of a selection of the resources presented in the SotA is provided.

4.1.1 Summary of the State-of-the-Art Review

This section summarizes the literature reviewed in the SotA. Table 4.1 provides a consolidated overview of the resources studied in the SotA to find the answers to the RQs. In this table, the criteria defined in Appendix C, is one more time mentioned and noted by the letter 'C', which stands for 'Criterion', and the number given to each criterion in Appendix C, next to it.

The categorization of the resources which are shown in detail in Appendix D

Table D.1, and summarized in Table 4.1, helps us to see the relation of resources to different topics related to our investigation. The criteria defined also make a more systematic work with the resources possible and utilizing them in our research results feasible.

As you will see in this summary of the SotA, the reviewed literature in this research implies that network automation is increasingly receiving more attention, and researchers are putting time and effort into emphasizing the importance of the application of this technology.

C1: While we have investigated more than 100 scientific documents that are related to network and network security management, and registered 100 of those with details in Table 4.1, it shows that 87% of the registered resources are related to utilizing network automation as the method for efficiency and resilience of network security.

C2: Above 82% of the literature reviewed suggest utilizing SDN to automate network and network security, with 40.5% of these documents directly suggesting Python as the open-source programming language to be taken advantage of in this relation, and 12.5% of these suggesting the Ansible automation tool being utilized.

C3:70% of the resources among the SotA points to change management in traditional networks being challenging and needing NSA to be applied.

C4: Out of the SotA studied in this research, about 25% suggest ML utilization in network and network security automation for raising resiliency against cyber threats and efficiency of the network and network security management. 84% of these resources suggest ML combined with SDN techniques and technologies, while the remaining resources suggest and discuss only ML as the solution to the problem.

C5: About 16% of the studied resources point out the challenges related to multi-vendor solutions utilized in network and network security technologies. This is while only one of the resources points to the fact that there are different solutions, products, and technologies provided by different vendors and utilized by the companies' and organizations' network and network security solutions. That mentioned resource, however, does not point at the challenges that the multi-vendor combination of technologies brings to organizations. Following other resources in the SotA, this challenge could affect an organization's network and network security in both negative and positive ways [42, 43].

C6: 15% of the resources reviewed in this research point at network segmentation as one of the network security measures that raise network security, while only 13% of the resources that mention network segmentation do not discuss it in combination with network automation techniques.

Table 4.1: Summary of the SotA along with the relevant criteria, linking each resource to its corresponding topic or subject. For additional details, refer to Appendix C.

Topic the resource is related to	**Link to the related resource**
The resource is related to network automation **C1**	[1, 2, 5–8, 10–17, 34, 35, 39–110]
Using or mentioning SDN with any of programming languages such as Python, automation tools such as Ansible, or other programming languages as a solution to network automation or the resource does not emphasize a specific programming language but mentions SDN as a solution **C2**	[1, 2, 5, 6, 8, 10, 11, 13–17, 34, 35, 39–52, 54, 56–68, 70–108, 110, 111]
Change management, including updates and upgrades, in traditional networks as a challenge **C3**	[1, 2, 5–8, 10–12, 15–17, 35, 41–51, 53–62, 64–76, 78–80, 82–85, 88–95, 102–107, 111, 112]
Suggesting ML as one solution to NSA **C4**	[5, 40, 41, 44, 45, 48, 50, 54–57, 62, 65, 69, 73, 74, 77, 78, 83, 87, 88, 106, 109, 110, 113]
Point out the challenge related to multi-vendor solutions utilized in the networks **C5**	[8, 10, 42–44, 49, 58, 59, 76, 84, 85, 94, 104, 105, 111, 114]
Discussing network segmentation as a solution to the complexity of network security and architecture **C6**	[1, 5, 17, 29, 39–41, 48, 52, 56, 61, 73, 84, 88, 113]
The importance of the competency in network automation techniques among the network engineers who manage the network's daily tasks emphasizing the human factor **C7**	[2, 5, 10–13, 15–17, 47, 49, 70, 76, 79, 80, 83–85, 105]
Cost and/or limitations that SDN might bring into the systems leveraging it **C8**	[5, 6, 8, 10, 13–17, 42, 43, 45–52, 56, 59–61, 63, 65, 69, 70, 72–74, 76, 78, 79, 81, 82, 85, 87, 91, 94, 96–102, 104, 106, 109, 112]
The relation between raising security in networks or handling security challenges by leveraging SDN techniques and technologies **C9**	[2, 5, 6, 8, 10, 13–17, 34, 35, 40–45, 47–52, 54, 56, 58, 59, 61, 63, 64, 66–68, 70–78, 80–85, 87–105, 107, 111]

Continued on the next page

Table 4.1 – Continued from the previous page

Topic the resource is related to	**Link to the related resource**
Giving an overview of network automation technology and techniques, SDN, ML, and IaC, explained in the resources **C10**	[1, 2, 5, 6, 8, 10, 17, 35, 43–45, 47–52, 56, 57, 61, 65, 66, 69–75, 77–87, 90–94, 99, 103, 105, 106, 108–111]
Providing a taxonomy of the NSA techniques it presents **C11**	[5, 44, 45, 48, 57, 82, 86, 93]
Putting light on advantages, disadvantages, threats, and opportunities (SWOT characteristics) regarding the NSA techniques it presents **C12**	[2, 5–8, 13–17, 34, 35, 42, 43, 45–54, 56–59, 61, 63–68, 70, 71, 73–78, 80–87, 89–112]
Presenting the use case customized to each NSA technique it presents **C13**	[1, 2, 7, 10, 17, 35, 43, 45, 47, 51, 52, 56, 57, 59, 66, 68, 74, 76, 81–87, 89–91, 93, 94, 103, 104, 106, 108, 109, 111]
Discussing traditional network technologies, techniques, and/or architecture such as network segmentation, zero trust, DMZ, zone-based, or zero trust **C14**	[26–29, 39–41, 67, 88, 112–118]
Evaluation of the gap related to the existing competency in network automation and organizational culture in cultivating and encouraging network automation on the one hand, and the lack of utilization of network automation techniques and technologies on the other hand (**Related work to our research**)	[15, 16]

C7: Around 19% of the reviewed resources in the SotA point to the importance of network automation competency and skills building for those who work with network and network security in organizations.

C8: About 50% of the resources studied in the SotA point to either costs or limitations or both which can be imposed on systems when leveraging SDN. Among those resources 31% elaborate on the limitations related to network automation and utilization of SDN or ML, in combination with discussions about costs or separated from that. Noteworthily, we did not find any resource that specifically paid attention to the statistics related to the costs of the utilization of network automation which could have been interesting for our research and the further SWOT analysis in this investigation.

C9: Around 70% of the resources reviewed in the SotA discuss the positive and/or negative effect of NSA regarding raising more security and resiliency against cyber attacks in the network and network security systems.

C10: Around 61% of the resources give an overview of the network automation technology they discuss that, for instance, could be related to SDN, ML, or even IaC.

C11: 8% of the resources studied provide a taxonomy of the technologies they present and discuss related to NSA.

C12: About 74% of the SotA points out the advantages of the network automation techniques and technologies. Among those resources, 86.5% discuss advantages related to NSA, and 63.5% point out the opportunities in this regard. This is while only 31% of those resources discuss disadvantages of utilizing NSA at this point of time when these technologies still have many unknown sides to us, and only 20% of the same resources elaborate on threats imposed to network and network security while applying NSA techniques and technologies.

C13: while 36% of the resources studied in the literature review point out the use cases customized to each of the network security automation techniques they present and examine.

C14: Finally, around 16% of the SotA discuss traditional network technology, techniques, and architectures, while about 1/3 of these documents are at the same time pointing at network automation as a necessary part of technologies involved in building efficient and resilient network and network security infrastructure.

Related work to our research: When it comes to finding related work to our research, after reviewing more than 100 resources, we have found two resources, which are less than 2% of the literature reviewed in our study of the SotA, that have something in common with what we are investigating in this research.

4.1.2 The Relation Between SotA and RQs

Further, in the review of the SotA, as shown in Table 4.2, around 14% of the resources we have studied are related to answering RQ1, around 87% are to provide answer to RQ2, and finally, about 29% are to help us with finding answers to RQ3.

Table 4.2: The relation between RQs and the SotA in a brief summary

RQ Number	Index of the Related Resources
RQ1	[26–29, 39, 41, 67, 88, 112–116, 118]
RQ2	[1, 2, 5–8, 10–17, 34, 35, 41–111, 119]
RQ3	[6, 15, 16, 34, 42, 43, 48–53, 59, 61, 76, 81, 90–102, 112, 119]

For the sake of conciseness in this chapter, we have included a review of a selected set of resources from the SotA in Appendix E. The categorization of these selected resources within that appendix is determined by their relevance to the RQs addressed in this thesis.

4.1.3 The Gap Observed in the SotA Studied in this Research

The preceding overview highlights a noticeable gap in the existing literature concerning network automation techniques and technologies. Specifically, there is limited discussion and comprehensive review of the disadvantages, threats, and limitations posed by the emerging NSA techniques on companies and organizations leveraging them. Our investigation reveals a scarcity of resources delving into this aspect. Notably, only two research works [15, 16], as detailed in Chapter 1, Section 1.10, address the identified problem and the corresponding research gap.

In the realm of statistics about NSA utilization, an examination of scientific resources reveals a notable absence of comprehensive research addressing inquiries related to the underlying issues of our investigation. This gap extends to a lack of scientific resources covering statistics on the costs associated with the utilization of various NSA solutions. For instance, there is a dearth of evaluations gauging the practicality and application of the presented methods and techniques within organizations. Furthermore, there is insufficient exploration into the types of organizations that tend to adopt specific NSA techniques and technologies. Ultimately, the scarcity extends to identifying which NSA solutions are better suited for distinct organizational needs.

While assessing the spectrum of ML methodologies, a crucial consideration is to inquire about the practical implementation of the presented techniques and technologies within the companies that require and can potentially adopt them. Notably, a significant gap in the literature lies in the lack of evaluations regarding the practicality of the methods outlined. Many of the documents reviewed and referenced in this section omit an assessment of the real-world utilization of the proposed approaches. Our suggested approach to address this gap will be expounded upon in Chapter 6, Section 6.2, providing valuable insights for future consideration.

4.2 Traditional Network Security Management - Summary SWOT Analysis - RQ1

Research Question (RQ)1 focuses on existing traditional network security techniques and technologies and their characteristics in traditional network approaches. In this regard, the application of methods such as micro-segmentation and Zero Trust Architecture (ZTA) proves effective in fortifying security; however, it introduces a daunting challenge, manual management complexity. The incorporation of these techniques into network security architecture significantly amplifies the intricacy of control and management [39].

For instance, the detailed examination of traditional firewall management complexities underscores the challenges associated with manual implementation [39]. This manual burden extends across various aspects, from DMZ reliance to the incorporation of micro-segmentation and ZTA, manifesting in the need for individual rules per connection per host.

The magnitude of this manual work becomes evident as we, in this section, conduct a summarized Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis on traditional network security techniques and technologies. The comprehensive version of this SWOT review is provided in Appendix F, emphasizing the need for automation to streamline and alleviate the escalating complexities associated with traditional network security techniques and technologies[2].

Common Strengths

Drawing from an examination of the SotA, the following represents the shared strengths of the four traditional network security techniques and technologies, as analyzed through SWOT analysis:

1. **GUI-Based Interface:** All four network security architectures leverage GUI-based interfaces, making them user-friendly and accessible for individuals with varying levels of expertise [39, 118, 120, 121][3].
2. **Ease of Rule Management:** GUI-based platforms simplify the process of adding, configuring, and managing security rules for these architectures, reducing the need for advanced programming skills [39, 118, 120, 121].
3. **Enhanced Security:** These architectures prioritize network security by utilizing firewalls and other security measures, which helps protect network

---

[2] For more information about traditional network security techniques and technologies and the challenges imposed by them on the workload in IP network security, please see Appendix B.

[3] In this SWOT analysis, where we draw upon multiple resources as references for our rationale, these referred resources complement each other. This implies that, together, they enhance the insights highlighted by the SWOT analysis.

resources [39, 118, 120–122].

4. **DMZ Integration:** Traditional Firewalls and DMZ Network Security Architecture, as well as Zone-based Network Architecture, utilize DMZ zones effectively to separate external and internal networks, improving security [39, 123–125].
5. **Zero Trust Approach:** Zero Trust Network Security Architecture stands out for its approach in providing information security, reducing the misuse of stolen credentials, preventing compromised account movement, quick attack detection, and protection against insider threats [40].
6. **Machine Learning Integration:** Zero Trust Network Security Architecture has the capability to incorporate machine learning techniques for analyzing encrypted network traffic, aiding in information classification and malicious traffic identification [40].

Common Weaknesses

Based on the study of the SotA, the identified weaknesses in the four traditional network security techniques and technologies, as analyzed through SWOT analysis, include:

1. **Complex Rule Management:** In larger networks, managing, updating, and tracing incidents manually becomes challenging due to the presence of thousands of rules and configurations [76, 90, 92].
2. **Cost Implications:** The cost of firewall applications and related services from vendors and third parties can be a burden for companies implementing these architectures [43, 120, 126].
3. **Expertise and Personnel:** Larger networks often require more skilled network professionals to manage network security, which can raise network management costs [2, 76, 90].
4. **Security Holes:** The rapid growth of uncontrolled security holes in firewalls and network security can occur due to the inability to review and delete unused rules effectively [76, 90, 92, 93].
5. **Vendor Dependence:** Some of these architectures, particularly when heavily reliant on vendor products, can lead to vendor and vendor security dependencies [42, 76, 90, 92, 93].
6. **Transition Challenges:** The transition from traditional network infrastructure to architectures like micro-segmentation can be more challenging if done manually [76].
7. **Single Points of Failure:** Zero Trust Network Security Architecture contains single points of failure, such as the Policy Engine (PE) and Policy Administrator (PA), which could lead to vulnerabilities if compromised [40].
8. **Vulnerabilities to Attack Vectors:** Zero Trust Network Security Architecture is vulnerable to various attack vectors, including Mirai botnets, DoS, DDoS, and root hijacking, which can pose security risks [40].

9. **Accidental Disruption:** Accidental shutdown of the Policy Engine (PE) or Policy Administrator (PA) can occur, particularly if implemented based on cloud services, leading to potential disruptions [40].
10. **Phishing and Social Engineering:** Vulnerabilities exist in the architecture where accounts can be compromised through phishing and social engineering attacks [40].
11. **Data Protection:** Information gathered by Zero Trust Architecture's analytical engines may become targets for cyber attackers if not protected by strong access policies [40].

Common Opportunities

Drawing insights from the study of the SotA, the potential opportunities within the four traditional network security techniques and technologies, as evaluated through SWOT analysis, are as follows:

1. **Cost-Effective Security:** The use of GUI-based firewall applications in Traditional Firewalls and DMZ Network Security Architecture and Zone-based Network Architecture can reduce costs related to hiring highly skilled personnel, making security more cost-effective [39, 43, 120, 121, 126].
2. **Simplified Management:** GUI-based firewall applications and simpler architecture, as seen in Traditional Firewalls and DMZ Network Security Architecture and Zone-based Network Architecture, are well-suited for companies with smaller networks, leading to easier management and lower skill acquisition costs [39, 123, 124].
3. **Improved Security:** Micro-Segmentation Network Security Architecture's zero trust approach reduces the likelihood of fast-spreading cyberattacks, enhances cyber hygiene, and provides a higher level of internal network security [39].
4. **Enhanced Collaboration:** Zero Trust Network Security Architecture offers opportunities for secure communications between different enterprises, fostering inter-collaboration [40].
5. **Remote Work Enablement:** Zero Trust Network Security Architecture enables secure remote work by providing strong security measures for employees accessing organizational resources remotely [40].
6. **Cloud Service Adoption:** Zero Trust Network Security Architecture expands the possibilities of using various cloud service providers securely, allowing access control for IaaS and SaaS services [40].
7. **Policy Compliance Assurance:** It assures policy compliance within organizations, simplifying what could otherwise be a challenging task [113].
8. **Reduction of Attack Surface:** By combining with network security architectures like micro-segmentation and utilizing security measures such as Multi-Factor Authentication (MFA), Identity Access Management (IAM), and Zero Trust Network Access (ZTNA), Zero Trust Network Security Architecture re-

duces the attack surface [40].

Common Threats

In light of the examination of the SotA, the perceived threats associated with the four traditional network security techniques and technologies, as assessed through SWOT analysis, encompass:

1. **Insufficiency in Larger Networks:** Traditional Firewalls and DMZ Network Security Architecture, Zone-based Network Architecture, and Micro-Segmentation Network Security Architecture may become insufficient in larger networks such as CIS or data center networks. Handling thousands of firewall rules manually becomes unmanageable, leading to reduced security and control [2, 40, 42, 76, 90, 92, 93, 127, 128].
2. **Complex Management:** Managing firewalls with many rules, especially in large networks, can become complex and challenging when done manually, potentially leading to security issues [42, 76, 90, 92, 93, 127, 128].
3. **Deprecated and Unmanaged Rules:** Manually managing firewall applications in large networks with numerous security rules can lead to the existence of deprecated, unmanaged rules, making it easier for adversaries to compromise the network's security [2, 42, 76, 90, 92, 93, 127, 128].
4. **Vendor Compromise:** Firewall applications delivered by vendors and third parties can compromise network security when targeted in cyber attacks, such as supply-chain attacks or malicious payloads [36].
5. **Vulnerability in Rule Tracing**: Zone-based Network Architecture and Micro-Segmentation Network Security Architecture, while more suitable for larger networks, become more challenging to trace logs and incidents when managed manually [42, 76, 90, 92, 93, 127, 128].
6. **Reduced Security:** Deprecated rules and configurations that are difficult to find and delete while manually managing network configurations and firewalls can reduce security in both Zone-based Network Architecture and Micro-Segmentation Network Security Architecture [42, 76, 90, 92, 93, 127, 128].
7. **Disruption Due to Policy Changes:** Zero Trust Network Security Architecture is vulnerable to disruptions in enterprise operations caused by unapproved changes to rules [40].
8. **Network Traffic Interception:** Cyber attackers may intercept and block network traffic to policy administrators or policy engines, affecting user accounts in the enterprise network [40].
9. **DoS and DDoS Attacks:** Enterprise network disruption and loss of connectivity may occur during DoS or DDoS attacks, even if access is granted by the Policy Administrator (PA) [40].
10. **Insider Attacks:** Insider attacks can still compromise assets protected by Zero Trust Network Security Architecture [40].

11. **Information Reconnaissance:** Cyber attackers may gain valuable information about interesting accounts and potential targets by reconnaissance of the information gathered by the management tools in Zero Trust Network Security Architecture [40].

Summary of the SWOT Analysis

The analysis provided in this section, based on the study of the SotA, indicates that, on the one hand, the strengths of traditional network management include factors such as easy-to-manage security rules, integration with DMZ and ML, a provided zero-trust approach, and enhanced security. On the other hand, we have enumerated eleven weaknesses in this SWOT analysis, including, but not limited to, vendor dependency and complexity regarding rule management.

We have also enumerated the opportunities existing in traditional network management approaches, such as cloud service adoption, and the opportunities created because of providing GUI-based interfaces. At the same time, we have encountered eleven threats, including, but not limited to, insufficiency in larger networks, the existence of deprecated and unmanaged rules, reduced security, and vulnerability in rule tracing.

In addition to the SWOT analysis presented here, the information reviewed in the SotA regarding traditional network management also indicates how complex the management of network and network security will become when adding higher security measures to network architecture. As explained, while single hosts would receive sufficient security by adding and managing firewall applications, small companies would have more advantage in separating their internal network from the external network, the so-called internet, by utilizing DMZ [39].

Moving toward larger companies, there is a need to utilize more complicated network security architecture, such as adding zone-based defense to network architecture for separating assets and network resources in different zones [122]. However, by adding this approach, we have added more complexity to the network security architecture, which we need to overcome properly.

Despite this high level of complexity introduced to networks of large companies, we still need a higher level of cybersecurity. This is the level of cybersecurity that we can achieve by utilizing micro-segmentation network security architecture, where a zero-trust manner of network security is baselined in the network. But now, we have implemented even more security rules and policies to manage this type of network security architecture. Here, even two hosts need several rules implemented to be allowed to communicate with each other [39]. For more information regarding traditional network security techniques and technologies and their management, as well as additional details on micro-segmentation and ZTA, please refer to Appendix B.

The resources reviewed in the SotA indicate that vendor products can get compromised by different cyberattack vectors and affect the security of their customers. Adding to this, the information explained about network firewalls and their complexities, we need to find techniques and technologies beyond human capabilities to manage these types of complexities in network security management [2].

The resources studied in the SotA, presented in Section 4.1, also suggest that this problem shall be solved by utilizing network automation techniques and technologies. Hence, the coming section will review network automation techniques and technologies based on what we have studied in the SotA, the challenges related to these, their use cases, their vulnerabilities, and finally, a SWOT analysis of NSA techniques and technologies.

4.3 Contributions of Existing Automation Techniques and Technologies - RQ2

Up to this point, we've explored the traditional approach to handling network security techniques and technologies, addressing RQ1. In the following section, we delve into network automation techniques and technologies, which play a pivotal role in enhancing the resilience, reliability, and effectiveness of network security management, addressing RQ2. Within this context, we examine various related concepts, including network traffic forwarding across the operational planes of network devices, orchestration, and Network Function Virtualization (NFV).

Furthermore, we explore the implementation of SDN within operational planes, along with a comprehensive review of the automation techniques and tools highlighted in the SotA. Subsequently, we provide a brief overview of firewall automation and ML technologies, both recommended in the SotA for potential use in Network Security Automation (NSA), either in conjunction with or independently from SDN technologies. Additionally, we briefly touch upon the potential of simulation platforms, recognizing their impact on advancing and ensuring the success of NSA. For more in-depth information on specific simulation platforms, please refer to the details provided in Appendix B. To facilitate easy navigation through this section, Figure 4.2 provides a concise summary of its contents for the reader's convenience.

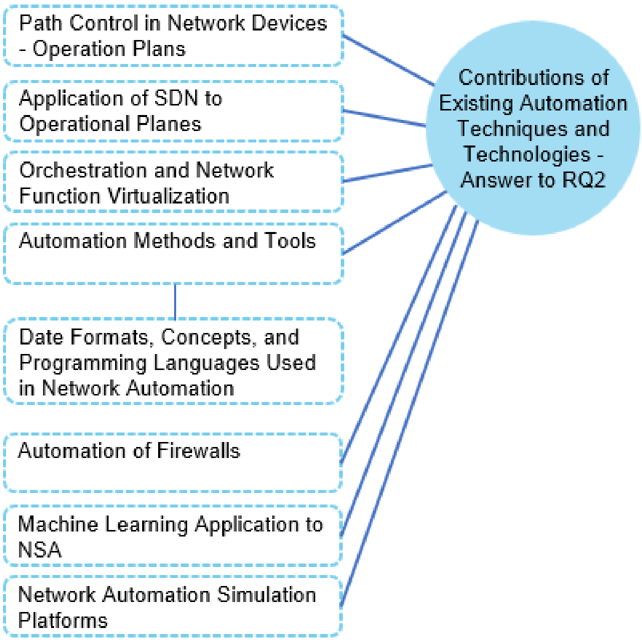

Path Control in Network Devices - Operation Plans
Application of SDN to Operational Planes
Orchestration and Network Function Virtualization
Automation Methods and Tools
Date Formats, Concepts, and Programming Languages Used in Network Automation
Automation of Firewalls
Machine Learning Application to NSA
Network Automation Simulation Platforms
Contributions of Existing Automation Techniques and Technologies - Answer to RQ2

Figure 4.2: Concise presentation of Section 4.3. The figure is created by the author.

4.3.1 Path Control in Network Devices - Operation Plans - RQ2

This section delves into RQ2, exploring how existing network automation techniques and technologies contribute to bolstering resilience, reliability, and efficiency in network security management. Over time, network devices have evolved. Initially, these devices were structured around three distinct planes including the data plane, the control plane, and the management/policy plane. In this discussion, we focus on layer-three devices due to their versatility, as they encompass routers, layer-three switches, and routers with implicit firewall functionalities.

This thesis delves into the realm of traditional techniques, architectures, and technologies currently employed by companies, aiming to provide a comprehensive overview of the existing landscape. With a specific focus on the automation of firewalls and network management, we explore various network and network security automation methods within the context of our SotA study, shedding light on the diverse technologies in this domain.

Originally, all network traffic passed through the control plane, as depicted in Figure 4.3. However, through the separation of the control and data planes, illustrated in Figure 4.4, it became possible to allocate the control plane to other responsibilities. With this separation, data packets were now routed through the data plane, while routing packets were directed through the control plane. This evolutionary step resulted in faster network packet forwarding and released the control plane's resources for other decision-making processes [27, Chapter 5].

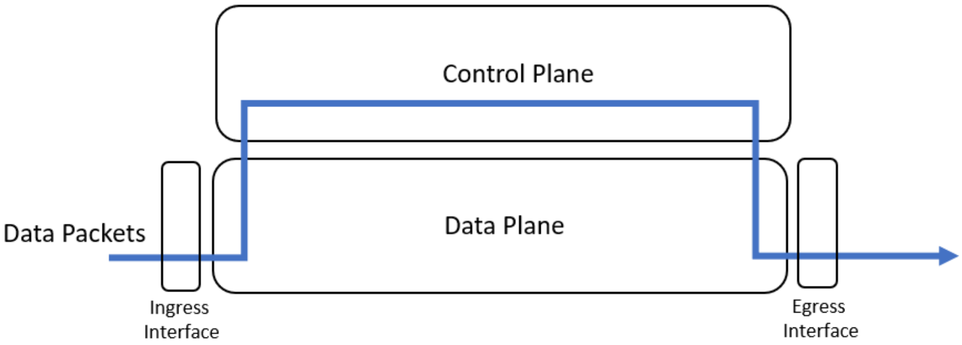


Figure 4.3: Forwarding all traffic through the control plane. Figure inspired of Figure 5-1 in [27, p. 329].

As the evolution continued, the data plane retained its role in packet and frame forwarding through the interfaces, while the management plane focused on routing policies. Further progression in this evolution allowed for the creation of a distinct control plane, incorporating software-based processing. The management plane gained the capability to provision the control plane using modern protocols and methods, including the Network Configuration Protocol (NETCONF), Representational State Transfer Configuration Protocol (RESTCONF), as well as the Command-Line Interface (CLI)/Secure Shell (SSH), Network Time Protocol (NTP)[4], System Logging Protocol (syslog) event messaging[5], and Simple Network Management Protocol (SNMP)[6], all of which have been available since earlier stages [27, Chapter 5][17, Chapter 9].

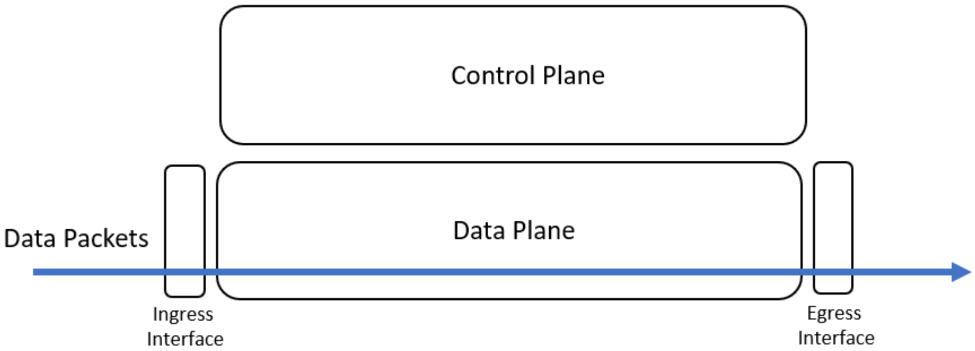


Figure 4.4: Forwarding all traffic through data plane. Figure inspired of Figure 5-3 in [27, p. 331].

Furthermore, the ongoing evolution of network architecture and network devices has led to the current possibility of employing a single controller for multiple devices. In this setup, decisions related to packet or frame forwarding calculations are made in one or more controllers, which are distinct from the devices that comprise the data plane [17, Chapter 9]. Figure 4.5 illustrates routers and switches with a shared central controller serving as the management point for all these devices.

As stated in Section 3.3, network automation directly contributes value to network security. Consequently, the automation, administration, and management of devices enhance the efficiency, resilience, and reliability of network security management. In this context, the separation of the control plane from the data plane, along with the emerging trend of centralizing controller management, marks a pivotal stage and serves as the cornerstone for the integration of automation into network security [17, Chapter 9].

It's important to consider that relying solely on a single central controller could introduce the vulnerability of a single point of failure into our network ar-

---

[4] NTP refers to the protocol used to synchronize the clocks of internet and network devices. This synchronization of clocks plays a crucial role in various aspects, such as tracking events and incidents, coordinating updates across devices, and performing other tasks that rely on a centralized clock time distributed across different stratum layers [129].

[5] The syslog protocol refers to a standard that involves collecting information and message logs from network devices and applications, subsequently transmitting them to a server for further handling and analysis [130].

[6] The SNMP, which succeeded the NETCONF protocol, is designed for network monitoring and does not play a role in network configurations [76, Chapter 6].

chitecture. To address this concern, implementing redundancy and deploying a multi-controller platform emerges as a viable solution [45]. In this context, redundant controllers offer a robust and dependable alternative while avoiding the risk associated with a single point of failure [16, p. 74].

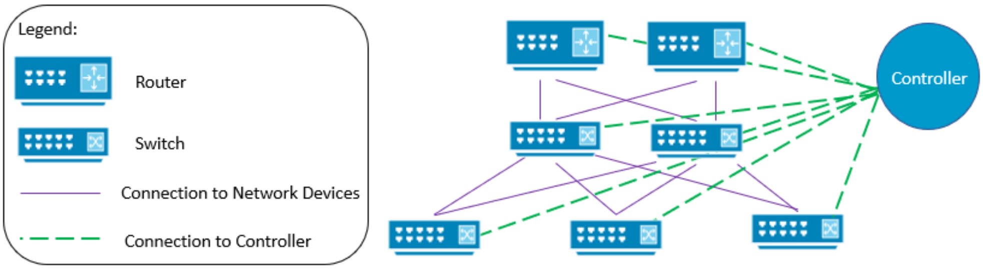


Figure 4.5: Centralized controller management for network devices. The figure is inspired by Figure 9-14 [17, p. 305].

The point at which SDN becomes a part of our equation is when we separate the controller from the data plane. SDN operates more efficiently within logical controllers as opposed to physical controllers [86]. In this context, SDN takes on the responsibility of managing communication between network devices as the centralized software controller.

OpenFlow: The OpenFlow standard, introduced in 2008, brought significant changes to the network industry in 2011. Its implementation marked a pivotal moment by enabling communication between the data forwarding plane and the SDN controller [76, Chapter 3]. OpenFlow, as an essential automation tool, defines the communication protocols between the SDN data plane and the SDN control plane [76, Chapter 5]. Through the adoption of SDN, it became feasible to leverage a hybrid architecture comprising both legacy and new SDN-enabled network devices [47].

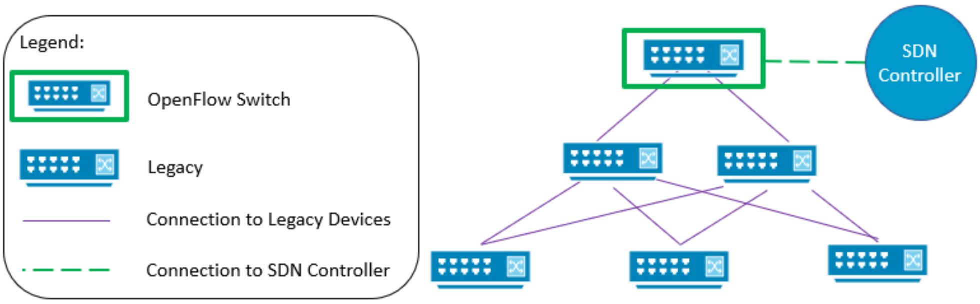


Figure 4.6: OpenFlow made the communication between data plane SDN and control plane SDN possible. The figure is created by the author.

Figure 4.6 illustrates a hybrid approach to implementing network automation, capitalizing on the capabilities of SDN and OpenFlow. In this hybrid network automation architecture, a combination of OpenFlow network devices and legacy devices is employed. The packages that employ the OpenFlow protocol are referred to as Open Daylight and OpenvSwitch [76, Chapter 6 and 9][10, p.265-271].

We assume existing network automation techniques enhance resilience, reliability, and efficiency in network security management, particularly in layer-three devices. The evolution of network devices, involving the separation of control and data planes, facilitates faster packet forwarding. The integration of SDN and OpenFlow standardizes communication, enabling a hybrid architecture for improved network automation.

4.3.2 Application of SDN to Operational Planes - RQ2

Focused on RQ2, this section investigates the role of current network automation techniques and technologies in enhancing resilience, reliability, and efficiency in network security management. In this section, we aim to provide a precise definition of the SDN concept within the scope of this thesis. This is necessary because various definitions of SDN exist, each associated with different network elements and concepts. For instance, Cisco DevAsc 200-901 [10] presents SDN as a model, which we will explore further here. Additionally, scientific papers mentioned in Section 4.1 and Appendix E, such as [1, 5, 6, 45–47], also adhere to the same concept of SDN. This particular concept breaks down SDN into three distinct abstracted elements including the controller, southbound Application Programming Interface (API)s, and northbound APIs, as depicted in the figure 4.7.

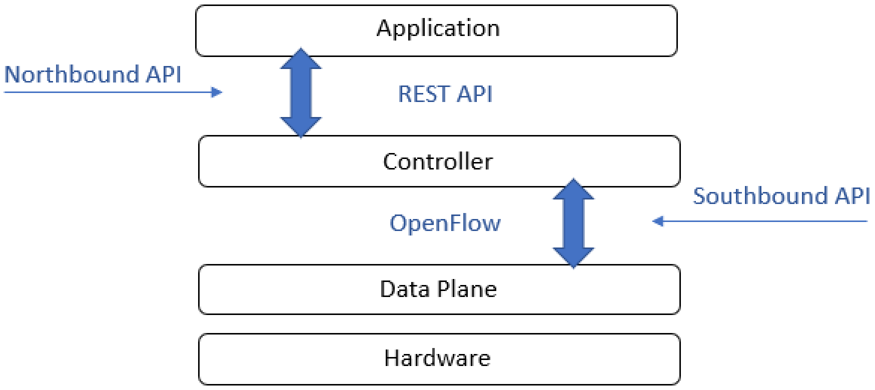


Figure 4.7: The Application layer is positioned atop the three network device layers. The presence of both northbound and southbound APIs within this architecture is also illustrated. The figure is created by the author.

DevAsc 200-901 [10, p. 865-871] presents a definition of this concept that aligns with our work. This definition categorizes network layers into three primary elements including the data plane, control plane, and hardware, as illustrated in

Figure 4.8. This abstracted structural division applies to switches, routers, and access point devices. The device interfaces are situated within the hardware layer. As briefly mentioned earlier, all communication between these interfaces flows through the data plane layer. The control plane is responsible for managing policies, rules, and protocols to control and issue commands to the data plane within the device.

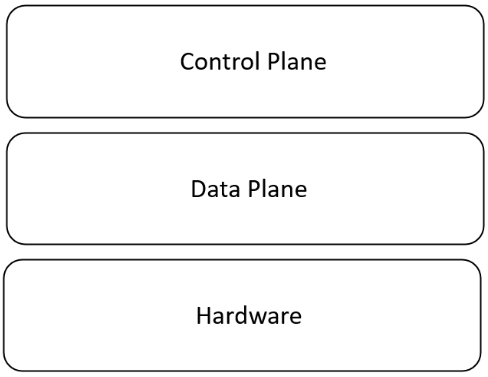


Figure 4.8: Three layers in the network devices. The figure is created by the author.

In a distributed control plane architecture, network management involves the administration of devices one by one. This entails logging into each device and configuring the necessary commands, which can be quite cumbersome [76, Chapter 1]. Now, envision a scenario where there are 500 or more devices to manage, a situation not uncommon in CIS networks. These devices may be dispersed across various locations with considerable distances between them, spanning different municipalities or even different countries across continents. In such a case, gaining access to each of the network devices becomes an arduous, if not near-impossible, task.

By incorporating the concepts of OpenFlow, API, and SDN into IP networks[7], we gain the ability to simultaneously manage multiple devices from a single controller point. [10, Chapter 6 p.272-290] elaborates on this concept by introducing an additional layer to the three-layer architecture depicted in Figure 4.8. In Figure 4.7, the application layer is included, and both the northbound and southbound APIs are clearly defined. The REST protocol facilitates communication within the northbound API, connecting the application and controller interfaces.

The OpenFlow protocol facilitates communication within the southbound API, connecting the controller and the data plane interfaces. The centralized control

---

[7] An IP network refers to the interconnection of computer devices using the Internet Protocol (IP) to enable communication between them. These devices within an IP network may include Personal Computer (PC)s, routers, switches, or various other types of devices capable of network communication, each assigned an IP address per Network Interface Card (NIC).

plane efficiently manages all devices. In this context, the layer positioned between the centralized control plane and the data plane of the devices serves as the southbound API, while the layer adjacent to the application layer assumes the role of the northbound API, as depicted in Figure 4.7. These APIs are managed programmatically.

Managing network APIs involves various techniques, with the choice of platforms, technologies, and programming languages depending on individual preferences, needs, knowledge, or available resources.

Furthermore, in an SDN architecture, the layers consist of the application, controller, and infrastructure layers. The latter layer manages security, network elements, and data center components. In this architectural framework, the northbound interface communicates with the application layer, while the southbound interface communicates with the infrastructure layer.

There is a wide array of programming languages and platforms available for communication between the application and control layers. Some examples of these programming languages and automation tools suitable for developing useful programs for SDN APIs include Python, Ansible, Puppet, and Chef [10, Chapter 15 p.742-798].

Services and applications, such as Deep Packet Inspection (DPI), IDS and IPS, monitoring, load balancing, and even QoS functions, are part of the application plane. Additionally, they encompass business functions and cloud orchestration related to the application plane. In contrast, SDN in the data plane leverages OpenFlow and the utilization of flow tables [48, 50].

Within the control plane, the northbound API utilizes programming languages such as Python, Java, and RESTCONF APIs to communicate with the application plane. Meanwhile, the southbound API employs NETCONF, SNMP, OpenFlow, and OpenvSwitch to establish communication with the data plane [48].

Some researchers delve even deeper into the topic, exploring scenarios in which the application plane resides within the cloud and communicates with the control plane via the northbound API [51, 111]. This evolutionary step in network automation through SDN introduces new opportunities and challenges to the realms of networking and network security.

The potential to manage network and network security devices using cloud services opens up the possibility of collaborating with various cloud vendors, aligning with each organization's unique requirements, capabilities, and priorities [51, p. 8-13].

Regarding the diversity of vendors, it's worth noting that this technological advancement, while offering new opportunities, also presents challenges [111]. On one hand, the progress achieved through the separation of the control plane and the data plane has enabled vendors to offer their services to customers in either one of the planes, rather than both simultaneously.

Companies like Cisco have developed their versions of SDN to keep pace with the rapidly evolving trend toward softwareization of the control plane in the market [111]. On the other hand, the separation of these two planes has empowered customers to pick and choose components from each plane to align with their preferences and requirements. This is where vendors have launched the OpenDaylight open-source project, aligning with their customers' interests. However, a lingering challenge is for both customers and vendors to identify the most suitable control plane for each specific scenario [111, p. 210].

We assume current network automation techniques enhance resilience, reliability, and efficiency in network security management, focusing on defining SDN within the thesis scope. This assumption aligns with the concept that SDN, through its architectural layers and APIs, facilitates efficient communication and management of network devices. Additionally, we acknowledge the challenges and opportunities introduced by SDN, particularly in managing network and network security devices using cloud services, suggesting potential collaboration with various cloud vendors.

4.3.3 Orchestration and Network Function Virtualization - RQ2

Research Question (RQ)2 guides the content of this section, examining the impact of existing network automation techniques and technologies on improving resilience, reliability, and efficiency in network security management. In recent years, CIS networks, which are typically distributed across different locations, have transitioned network resources from physical to virtual, a process also referred to as Network Function Virtualization (NFV). These virtualized network resources include but are not limited to, routers, switches, firewalls, and load balancers [76, Chapter 10]. For additional details, please refer to Section B.4 in Appendix B.

NFV has facilitated the scaling up of resources, and orchestration plays a pivotal role in controlling these virtualized network resources. It also enables the application of network automation workflows to these virtual resources [76, Chapter 11]. Some resources in the SotA literature elaborate on the relationship between NFV, orchestration, and network automation [50]. NFV fundamentally transforms network functions, which have traditionally relied on hardware, into software-based implementations. NFV comprises three key components including NFV infrastructure, software-defined Virtual Network Functions (VNF), which include functionalities like firewalls and Network Address Translation (NAT) within the network, and Management and Network Orchestration (MANO) [50]. This is illustrated in Figure 4.9.

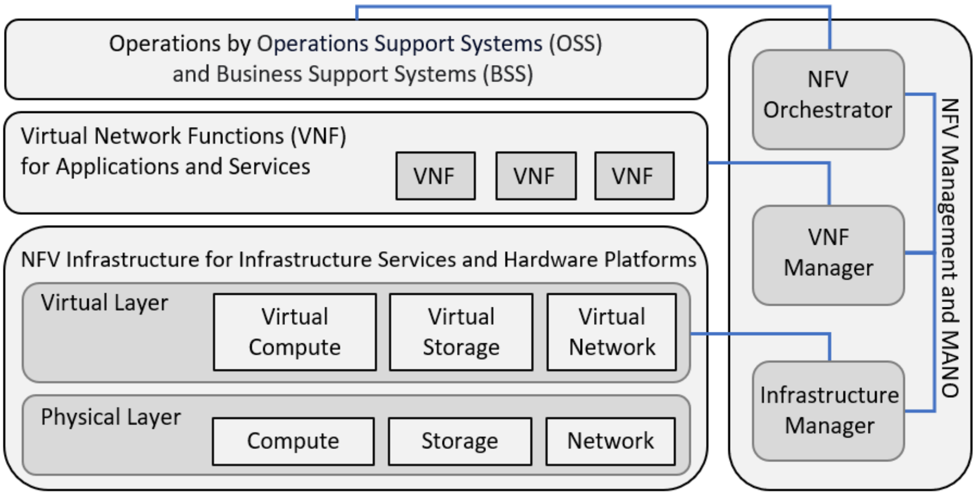

Operations by Operations Support Systems (OSS)
and Business Support Systems (BSS)
Virtual Network Functions (VNF)
for Applications and Services
VNF
VNF
VNF
NFV Infrastructure for Infrastructure Services and Hardware Platforms
Virtual Layer
Virtual Compute
Virtual Storage
Virtual Network
Physical Layer
Compute
Storage
Network
NFV Orchestrator
VNF Manager
Infrastructure Manager
NFV Management and MANO

Figure 4.9: Inspired by [50, Figur 2], the figure depicts the relation between NFV, VNFs, and orchestration in network automation.

NFV has enabled the agile addition and removal of network functions, providing flexibility in network functionalities [50]. Figure 4.9 illustrates the management of VNFs by the VNF manager, the management of virtual layer functionalities by the infrastructure manager, and how the NFV orchestrator MANO connects Operations Support Systems (OSS) and Business Support Systems (BSS)[8] operations within the NFV architecture.

When discussing automation within SDN, it encompasses programming knowledge, culture, and the ability to manage network security. It's essential to briefly explain the broader concept of orchestration and its relationship with various automation techniques and technologies. Several tools and platforms facilitate orchestration, with container orchestration being one notable example. While orchestration offers an automated approach to managing systems and software, the availability of diverse tools such as Ansible, Chef, Puppet (which serves both as an automation and configuration management tool), Salt, Kubernetes, and Terraform allows individuals to choose the most suitable and functional options for their specific needs, whether it be for automation, configuration management, container orchestration, or infrastructure as code [79, 111][10, Chapter 15].

Orchestration technology, which was initially used in Development and Operations (DevOps) and cloud operations, has now integrated with IT automation to advance NSA [106, 111]. This integration opens up the possibility of leveraging programming and DevOps competencies, as well as utilizing various tools, platforms, and technologies to enhance network and security management cap-

---

[8] OSS and BSS points to IT systems that have critical functionalities such as network planning and inventory systems as OSS, and billing, customer orders and notifications systems as BSS [50, 131].

abilities.

Within the context of NFV and orchestration, we assume that existing network automation techniques significantly enhance resilience, reliability, and efficiency in network security management. This assumption is supported by the transformative impact of NFV, transitioning traditional hardware-dependent network functions into software-based implementations. Furthermore, orchestration, now integrated with IT automation, expands the horizons of NSA, providing opportunities to leverage programming and DevOps competencies for enhanced network and security management capabilities.

4.3.4 Automation Methods and Tools - RQ2

In alignment with RQ2, this section provides insights into how contemporary network automation techniques and technologies actively contribute to the augmentation of resilience, reliability, and efficiency in network security management. Numerous tools are available for automating various tasks, each contributing to specific processes. These tools serve different purposes, such as deployment, building, testing, running, and collaboration. One example of an open-source automation tool is Ansible, which is primarily used for configuration management and orchestration. Ansible, categorized under deployment tools widely employed in network automation, simplifies this task by pushing configurations to network devices within the network infrastructure [10, 89][70, Chapter 10].

Another example is Docker, an orchestration tool that functions as a container image containing all the necessary components for installation and operation. When we run a Docker image, the associated service runs, and shutting down the image halts the service as well [79, Chapter 7]. Docker and Kubernetes[9] are notable orchestration tools known for their ability to automatically adjust the number of running containers and replace damaged containers without the need for time-consuming repairs [79, p. 92-93].

Furthermore, within the realm of microservice architecture, there's a service known as *Chaos Monkeys*, as referenced in the SotA resources. This service, in a microservices environment, intentionally shuts down running containers and rebuilds them. This automated capability, where the system can rebuild any failed components, enhances the robustness, scalability, availability, and elasticity of services that incorporate *Chaos Monkeys* technology for automation [108, p. 101].

Continuous Integration and Continuous Delivery

Some of the SotA resources acknowledge the apprehension among network professionals when it comes to implementing changes and managing network security through automation [15, 16]. This fear primarily revolves around the po-

---

[9] Google utilized the open-source Kubernetes deployment system to serve billions of users with the containers required to run and deliver the content of essential applications [106].

tential disruption of the company's production environment, which is considered a real and critical environment. Consequently, technicians are hesitant to introduce automated changes into the enterprise production environment, and they encounter challenges when it comes to rolling back changes or resolving any issues that may arise as a result [16, 19].

To address this issue, certain SotA resources propose the adoption of Continuous Integration and Continuous Delivery (CI/CD) practices, along with relevant tools and processes [10, 17]. According to their findings, implementing CI/CD can increase the likelihood of success in automation while effectively separating the production environment from the testing environment. The CI/CD cycle also offers the opportunity to review change processes and revert to previous stages if the new changes prove to be ineffective. In this context, the Global Information Tracker (Git) repository, used for version control and team collaboration, along with the GitHub platform, which employs the Git repository system, are not the sole options but are among the most widely used tools that contribute to the CI/CD process cycle [17, Chapter 4].

Developers employ the Continuous Integration (CI) process to merge their new code into a repository, such as a Git repository [70]. They leverage the Continuous Delivery (CD) process to release tested and approved changes into the organization's production network environment. CD also facilitates rapid feedback from customers and users, enabling developers to enhance their code based on user input [70].

Development and Operations

Numerous authoritative resources emphasize the importance of collaboration between programmers and network professionals for integrating automated changes into the production environment [10, 17, 70, 89]. According to these sources, teamwork is essential in this process, and it involves using Development and Operations (DevOps) processes and tools to synchronize their efforts.

DevOps, as some SotA resources suggest, is intended to foster knowledge sharing and eliminate silos in favor of teamwork [53]. Traditionally, development and security teams often operate in separate silos, with security measures added to code products after delivery. However, the concept of Development Security Operations (DevSecOps) advocates for programming and security teams collaborating during the development process [53]. Similarly, the need for collaboration between programming and network teams is evident in the concept of Development Network Operations (DevNetOps), as network automation relies on combining programming knowledge and DevOps principles with network expertise in organizations [105].

It's crucial to clarify the distinction between CI/CD and DevOps. CI/CD refers to practices related to the development and reliable delivery of code changes [17].

In contrast, DevOps encompasses all processes, technologies, and ideas used in product development and teamwork approaches [105]. CI/CD processes and related tools are subsets that contribute to the larger framework of DevOps.

Figure 4.10 presents five main categories of DevOps tools including build, test, deploy, run, and collaboration. These categories are based on information from various SotA resources and support the entire dynamic DevOps process [17, 105]. Subsequent figures will provide subcategories and examples of tools used in these DevOps categories.

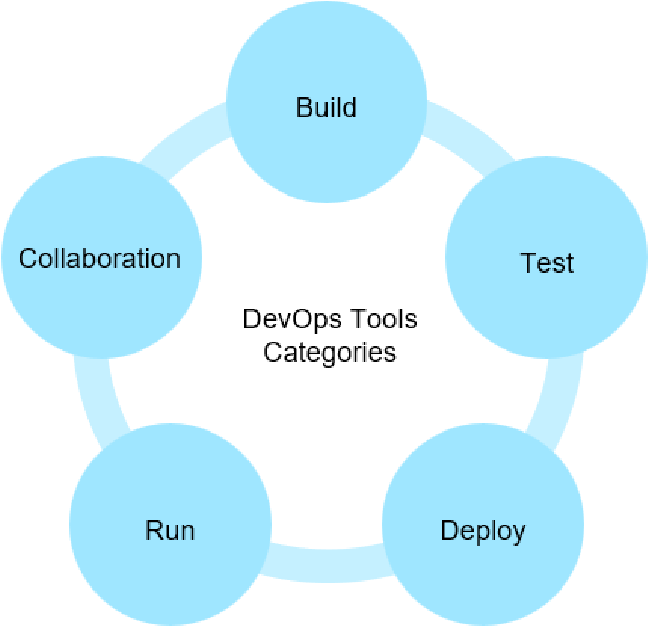


Figure 4.10: Our categorization of DevOps tools. The figure is created by the author.

Figure 4.11 focuses on collaboration tools, categorized into three subcategories including knowledge-sharing tools (e.g., github.pages, Confluence, and Microsoft SharePoint), communication tools (e.g., Microsoft Teams, Slack, and Discord), and application lifecycle management tools (e.g., Trello, Microsoft Visual Studio, and JIRA).

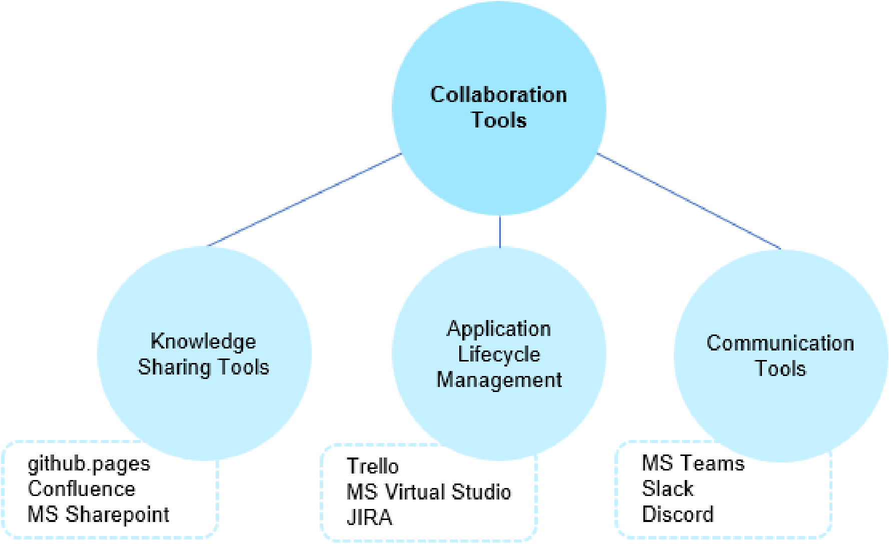


Figure 4.11: Collaboration tools overview. The figure is created by the author.

Figure 4.12 divides building tools in DevOps into subcategories of Supply Chain Management/Value Chain Management (SCM/VCM) and Continuous Integration (CI). Examples of SCM/VCM tools include Git, GitHub, GitLab, and Bitbucket, while CI-related tools encompass TeamCity, Jenkins, Bamboo, and Go.

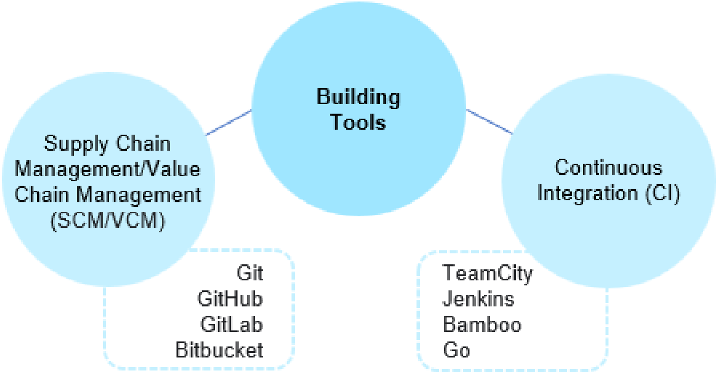

Building Tools
Supply Chain Management/Value Chain Management (SCM/VCM)
Continuous Integration (CI)
Git
GitHub
GitLab
Bitbucket
TeamCity
Jenkins
Bamboo
Go

Figure 4.12: Building tools overview. The figure is created by the author.

Numerous testing tools are available, and Figure 4.13 provides examples of these tools, including Load Impact, .js, cucumber, Unit.net, Specflow, Test NG, Selenium, and pytest.

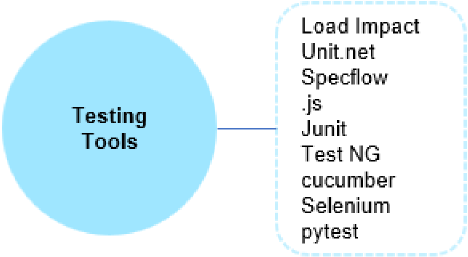


Figure 4.13: Testing tools overview. The figure is created by the author.

Figure 4.14 provides an overview of deployment tools, which are categorized into three subcategories including deployment management, configuration management/provisioning, and artifact management. This overview aims to present a set of related tools based on the study of the SotA, helping to provide a comprehensive understanding.

Deployment tools within this overview include juju, ElasticBox, Rundeck, and Capistrano. Configuration management/provisioning and artifact management tools are discussed extensively and are well-known in the field of automation, drawing from the resources used in this thesis [10, 11, 70, 79]. The overview of provisioning tools, as shown in Figure 4.14, includes Chef, Vagrant, Puppet, SaltStack, Ansible, Terraform, CF Engine, and PowerShell DSC. These tools are primarily used for provisioning and configuring infrastructure. In addition to provisioning tools, there are also other tools related to artifact management, such as DockerHub, and software development, including Python and package management with Nexus and Bower.

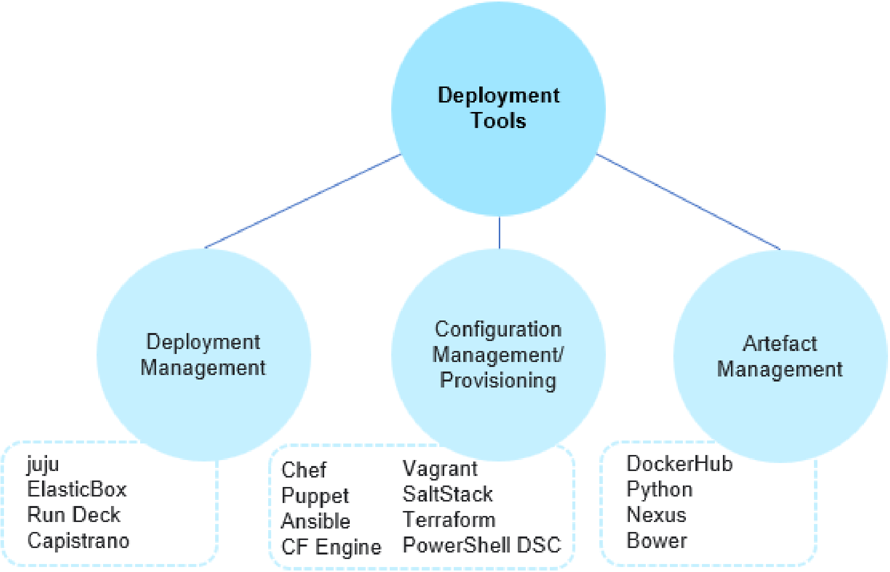


Figure 4.14: Deployment tools overview. The figure is created by the author.

The final category of DevOps tools presented here focuses on tools related to executing code scripts for the final product. Figure 4.15 provides an overview of these tools, where Splunk, Kibana, Logstash, and OpsGenic serve as examples of logging/monitoring tools; Docker Swarm, Kubernetes, Nomad, and Mesos represent orchestration/scheduling tools; and OpenStack, Appfog, Microsoft Azure (MS Azure), and Flynn exemplify Cloud/PaaS/IaaS tools.

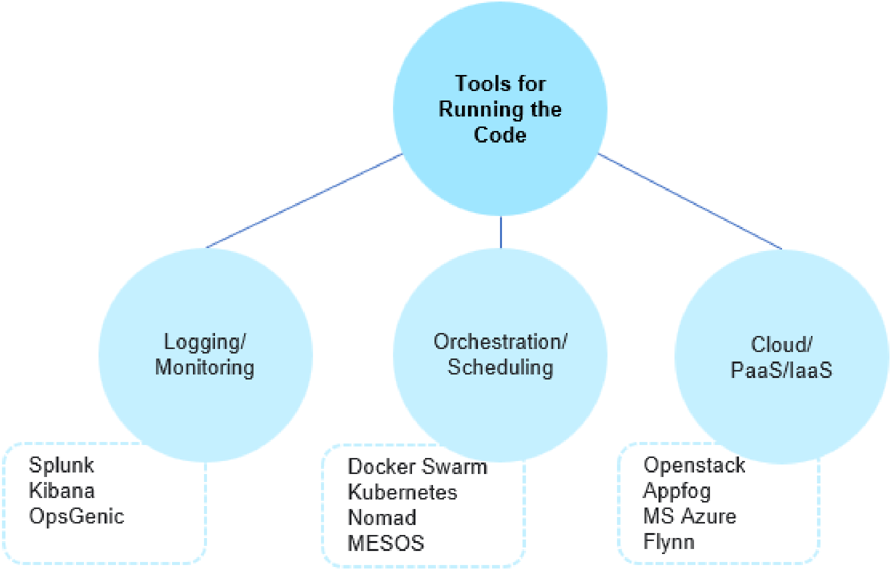


Figure 4.15: Overview of the tools utilized for running the code. The figure is created by the author.

A wide variety of tools is available for use in any of the presented categories within the DevOps cycle. Developers can select a combination of tools that best aligns with their specific needs, competencies, and possibilities. The tools introduced in the categories shown in Figures 4.11 to 4.15 have been recommended by various resources in the SotA literature examined in this research work [5, 10, 11, 17, 79][10].

Network Automation Data Formats, Concepts, and Programming Languages

In this section, we discuss some of the data formats, concepts, and programming languages used in network automation. Following the State-of-the-Art (SotA), these data formats are utilized to make the programmatic management of network and network security possible.

YAML, XML, JSON, and YANG: Yet Another Markup Language (YAML), Extensible Markup Language (XML), JavaScript Object Notation (JSON), and Yet An-

---

[10] In this thesis, when we reference multiple resources simultaneously, it's important to note that each resource does not encompass all the information we convey. Instead, these resources complement one another, working in tandem to provide evidence for the points we are making.

other Next Generation (YANG) are mentioned as data formats used in network automation [10, Chapter 12]. YAML, a data serialization format, is known for its human-readable syntax and is widely utilized in working with tools and platforms like Docker and Kubernetes for configuration purposes [10, Chapter 5]. Ansible playbooks, for example, are written in YAML [70]. XML is recognized for its readability and is commonly used for parsing data between APIs and web services [10, Chapter 5]. JSON, with its straightforward syntax, is widely employed for data transport between different applications [10, Chapter 5].

YANG, on the other hand, plays a crucial role in network automation. Network Configuration Protocol (NETCONF), Representational State Transfer Configuration Protocol (RESTCONF), and gRemote Procedure Calls (RPCs) are YANG network protocols that support model-driven programmability [10, Chapter 12]. YANG was developed to address the challenges of using automation techniques for communicating with network devices, particularly via the Command-Line Interface (CLI), and to automate the implementation and monitoring of network devices. Additionally, the HTTP-based RESTCONF protocol offers a functional interface for NETCONF and YANG data [10, Chapter 12].

REST: When referring to RESTful, Rest API, RESTCONF, or just REST, they all pertain to the same concept. The difference lies in the fact that REST is the architectural style, whereas Rest API or RESTful is the Application Programming Interface (API) that enables the use of the REST architectural style across different platforms [80, Chapter 2].

Other Technologies: In addition to REST, other technologies fulfill roles similar to REST. Here, we briefly mention some of these to emphasize that possibilities in automation techniques and technologies extend beyond our current discussion. These technologies, developed by different vendors, include but are not limited to **RPC**, mainly used by Microsoft, Apple, and IBM. Google has developed the **gRPC** [80, Chapter 10], and **GraphQL** is utilized by companies like Facebook, Twitter, and Instagram [80, Chapter 13]. **REST** itself is employed by various vendors, including Google, Facebook, Twitter, and even Amazon [80, Chapter 1].

Python: The versatile open-source programming language Python has gained significant popularity in the field of network automation, as highlighted by numerous resources [10, 11, 17, 49]. *Netmiko* and *Paramiko* are two renowned libraries frequently used in Python for network automation [10, 58]. For example, resources studied in the SotA demonstrate an experiment where the creation of VLANs on a layer three switch was achieved by running a script created using these two Python libraries [58]. Both libraries use SSH when connecting to switches, with Netmiko simplifying the connection process by offering the ConnectHandler method [58, p. 98-99].

Netmiko has the advantage of being compatible with various vendors, making it a multi-vendor solution [8, 84, 85]. This characteristic allows Netmiko to reduce costs and increase scalability, which is valuable in scenarios involving Bring Your Own Device (BYOD) and multi-vendor environments for target devices connecting to the network [85, Chapter 3]. Another Python library worth mentioning is the Network Automation and Programmability Abstraction Layer with Multivendor support (NAPALM), which interacts with network devices using a suitable API [83].

Ansible: As mentioned at the beginning of this section, Ansible is one of the most widely used automation tools for automating network processes [10, 53, 70, 89]. Functioning as both an orchestration and deployment tool, Ansible is agentless and straightforward, providing flexibility and efficiency in automation and configuration management [2, 10].

Jenkins: The continuous integration and automation server, Jenkins, enables developers to collaborate and push their changes to the production environment after building and testing. This open-source integration tool works seamlessly with automation-related tools such as Ansible and version control systems like Git, and it can also be integrated with configuration management tools like Puppet for comprehensive automation and configuration management [2, 10].

Kubernetes: Serving as the solution technology for managing containers and enabling scalable updates while containers are running, Kubernetes encompasses the management and configuration of network functionalities such as routing and port forwarding [103]. This open-source technology streamlines the automatic deployment of changes and enhances the management of microservices [90].

4.3.5 Automation of Firewalls - RQ2

This section is dedicated to addressing RQ2, shedding light on how current network automation techniques and technologies positively influence resilience, reliability, and efficiency in network security management. In the realm of network security, automation plays a pivotal role in enhancing resilience, simplifying management, and reducing complexity [2, 65, 66, 92].

This section delves into the automation of firewalls, a critical aspect of network security architecture, with a focus on micro-segmentation, packet exchange load reduction, and the integration of SDN. As we explore the adoption of automation technologies and techniques, we unveil the challenges faced and the innovative solutions proposed by researchers and major companies in the field. The future outlook suggests a promising trajectory for further advancements in automating IP network firewalls, underscoring the transformative potential of automation in network security management.

Micro-Segmentation: Micro-segmentation, in simple terms, involves dividing a network into secure segments to enhance overall security. This network security architecture serves as an illustrative model of why NSA is imperative, emphasizing its role in fortifying the network's security [39, p. 12].

Even within a micro-segmentation architecture, where Kubernetes is employed to enhance network security, the recommendation is to automate firewall rules. This approach becomes particularly crucial as networks scale, emphasizing the need for automated firewall management in large-scale environments [90, p. 478].

In the realm of micro-segmentation, the intricacies extend beyond its conceptual benefits. Managing micro-segmentation manually proves to be an arduous task, particularly when considering the need for rules governing every host-to-host connection within the same network segment. The establishment of firewall rules for each interaction becomes an exponential challenge. For instance, in a network with numerous Virtual Machine (VM)s utilizing the same network segment, each VM requires specific configurations, including tags, security groups, and precise firewall rules to enable communication [39].

Without the aid of automation, the manual creation of these rules for every potential connection multiplies exponentially, making network management cumbersome and practically unfeasible. This underlines the essential role of automation in alleviating the management burden associated with micro-segmentation, ensuring efficient and secure communication among hosts. For a more in-depth exploration of this network security architecture and its application in micro-segmentation, please refer to Appendix B.

Packet Exchange Load Reduction: It is vital to automatically reduce the packet exchange load within the SDN layer while managing network security solutions, such as firewalls, routers, and switches in large networks like data centers [91, p. 2]. Consequently, the adoption of Stateful Distributed FireWall (SDFW) for SDN is proposed to alleviate the burden on network devices [91].

SDN and Automation: Research conducted suggests that the automation of firewalls and the integration of SDN into network security architecture address the complexity challenge effectively [91, p. 5]. By leveraging SDN for automating application gateway firewalls, the controller can be relieved from the decision-making burden for individual packets, offloading the processing of similar packet flows to the data plane [91, p. 5].

Enhancing Network Security: SDN is hailed as a revolutionary technology that liberates companies from vendor-locked features and solutions, opening up opportunities for innovation in network security tailored to their specific needs and network security architecture [94]. Additionally, the utilization of the Mininet testbed demonstrates how various components contribute to the automation of IP network firewalls, reducing the complexity of network security management and lessening the manual workload on human resources and network devices [94]. With diverse solutions available for different aspects of network security technologies and techniques, network professionals can customize the framework to suit their preferences and organizational requirements [94, p. 8].

Challenges and Solutions: While recognizing major companies such as Amazon, Facebook, and Google for their adoption of SDN in managing IP network automation, researchers also highlight the downsides of this automation technology and propose solutions to mitigate these challenge [92]. Emphasizing the importance of the correctness of firewall rules, various models are developed to verify the consistency and error-free implementation of automatically managed rules in SDN. Different researchers suggest using TLS+ and TLC[11] for confirming the correctness of firewall rules in an SDN approach [92, 107].

Future Outlook: Researchers have made significant progress in identifying and proposing solutions for automating IP network firewalls. It is also mentioned that future research will further demonstrate how automation technologies and techniques make tasks manageable and reduce complexities in network security management [94, p. 8]. As far as the results of our study and research suggest, Fortinet[12] has been the only company to utilize ML in a small portion of the automation of the firewall services they offer to their customers [94].

4.3.6 Application of Machine Learning to NSA - RQ2

Research Question (RQ)2 forms the basis for this section, which scrutinizes the contributions of existing network automation techniques and technologies toward fortifying resilience, reliability, and efficiency in network security management. This section provides a brief overview of the knowledge related to Machine Learning (ML) extracted from the SotA in this research work. ML is a vast field in itself, requiring a deep understanding and insight for utilization. It is often considered the domain of data scientists [109, 110].

In exploring the extensive realm of ML within the context of NSA, it becomes evident that the sheer multitude of ML-related methods and applications poses a challenge to comprehensive coverage. This complexity is magnified by the diverse techniques, algorithms, and frameworks involved, necessitating a focused overview. As we delve into the intricate landscape of ML applications, from mitigating DDoS attacks to enhancing the resilience of ZTA, it underscores the intricate nature of integrating ML into NSA, further emphasizing the need for a nuanced approach.

While we attempt to shed light on the breadth of ML applications in network security, it is crucial to acknowledge the inherent difficulty in encapsulating the entirety of this expansive field. This section aims to offer a succinct glimpse into ML's diverse applications within NSA, recognizing the challenges posed by the extensive array of techniques and methodologies. As we navigate through the

---

[11] TLS+ serves as a tool for specifying firewall rules, while TLC is a tool employed for the verification of firewall rules and policies. These tools are referenced in various resources related to the automation of firewall rules and policies [92, 107].

[12] Fortinet, has incorporated ML into the Fortinet Endpoint Detection Response (FortiEDR) component of the firewall services provided to their customers. In this context, ML is utilized to perform IDS tasks within Fortinet's firewall services [94]. You can find more details on this in Appendix B.

intricate interplay of ML and network security, the inclusion of detailed figures in the subsequent section serves as a supplementary resource, providing a more comprehensive reference for readers to delve into the intricate details of ML within the context of NSA.

Therefore, we will not conduct an in-depth investigation of this area but rather provide a concise glimpse of the knowledge discussed in the resources studied in the SotA, particularly related to network automation and SDN-based automation. We include this brief overview because both network automation resources and network security architecture documents, such as Zero Trust Architecture (ZTA), have suggested the application of ML to NSA [40, 78].

Following the results of the SotA, there are various ways, methods, and experiments used to practice network security by incorporating ML. Some of these approaches are closely linked with SDN, while others suggest NSA independently without incorporating SDN techniques and technologies. This section discusses some of the SotA resources in this context. One thing is evident which is integrating ML into NSA demands knowledge and expertise in this field.

As shown in Section 4.1, more than 20% of the scientific resources listed in Table 4.1, extracted from the SotA in this research, indicate that applying ML to NSA and combining these methods will result in more resilient and efficient network security. This is also depicted in Figure 4.16.

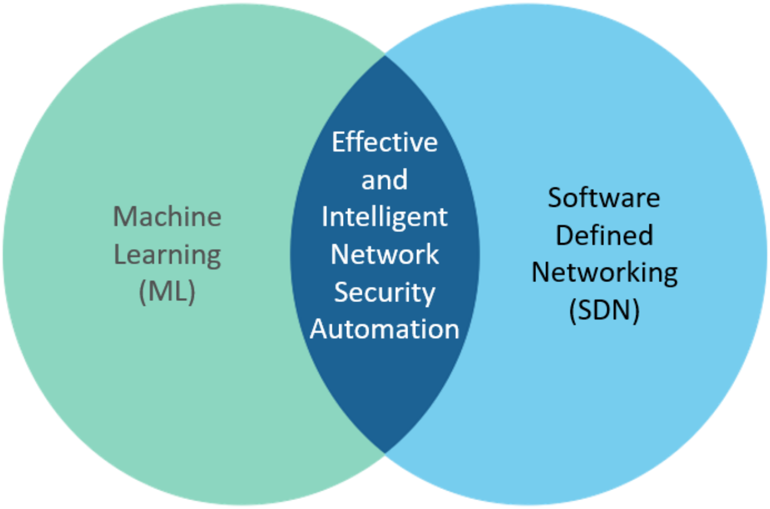


Figure 4.16: Venn diagram illustrating the combination of ML and SDN, which, in line with the claims studied in the SotA, results in effective and intelligent NSA. The figure is created by the author.

As mentioned in Section 4.4.2, to work with network automation, one needs to know networks and firewalls, in addition to network development and automation. Incorporating knowledge of ML in network automation adds another layer of complexity to the required competency.

This is where, once again, the necessity of teamwork with members who have competency and knowledge in the different required fields in a DevOps fashion is evident. This was also emphasized in Section 4.3.4.

In experimenting with Zero Touch Management (ZTM), the interface of Artificial Intelligence (AI) is connected to the network [57]. In this experiment, the AI layer facilitates communication between the controller and orchestration layer on one side and the management functions layer for information exchange on the other side. This architecture is illustrated in Figure 4.17. The controller and orchestrator layer, as the highest layer in the network, is connected to the northbound interface via REST API [57].

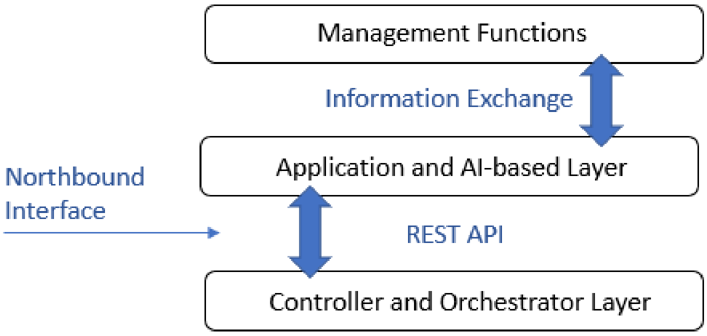


Figure 4.17: Connection between controller and application layer where AI also plays a role and communicates with management functions. The controller and orchestrator layer in this figure matches the corresponding layer shown in Figure 4.7, which communicates through southbound API with the data plane below it. The figure is created by the author.

While OpenFlow in SDN contributes to optimizing network security through automation, many resources suggest the application of ML to enhance the effectiveness and resilience of this process [44]. Three elements are proposed to increase the Return on Investment (ROI) for stakeholders and researchers. These elements are tool automation, high-performance computing, and ML technology [55]. Figure 4.18 illustrates the concepts related to ML discussed in SotA. In an experiment with an intelligence-slicing framework, ML algorithms such as Decision Tree (DT), Discriminant analysis (LDA), Support Vector Machine (SVM), and Nearest Neighbor (NN) were applied to the 5G network [56].

Using ML algorithms like Naive Bayes, k-Nearest-Neighbor (kNN), Decision Table, HyperPipes, OneR, and ZeroR provides an analysis of tens of firewall rules to evaluate the efficiency of SDN in this context [65]. In this case, the criteria used for evaluating the results of the analysis include Kappa Coefficient-Statistics, F Measure, and Root Mean Squared Error (RMSE) [65]. We will not delve into the details of the methods used for analysis and evaluation, but we will briefly mention the methods used to establish the connection between SDN and the ML methods used for automation.

According to another research, SDN is presented as a fundamental solution to the complexity of different types of network security and the associated security challenges [5]. While discussing automation through SDN to mitigate threats in complex networks, researchers classify the level of complexity in network automation using four parameters which include self-optimization, self-configuration, self-healing, and self-adaptation. These levels of complexity differentiate between proactive and reactive defense. ML and deep learning, along with some other techniques, fall under the category of reactive defense [5, p. 68].

According to some resources, the ML approach consists of two main phases which incorporate training and decision-making. ML algorithms are categorized into four main categories including Semi-Supervised, Reinforcement Learning (RL), Unsupervised Learning (USL), and Supervised Learning (SL) [45, p. 397-403].

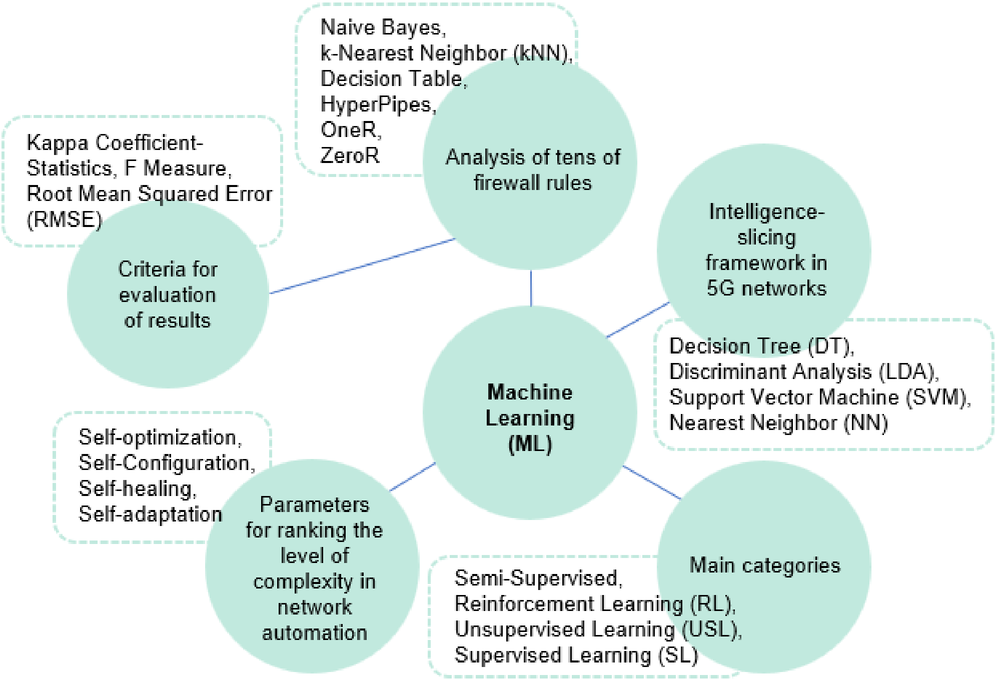

Naive Bayes,
k-Nearest Neighbor (kNN),
Decision Table,
HyperPipes,
OneR,
ZeroR
Analysis of tens of firewall rules
Kappa Coefficient-Statistics, F Measure, Root Mean Squared Error (RMSE)
Criteria for evaluation of results
Intelligence-slicing framework in 5G networks
Decision Tree (DT),
Discriminant Analysis (LDA),
Support Vector Machine (SVM),
Nearest Neighbor (NN)
Machine Learning (ML)
Self-optimization,
Self-Configuration,
Self-healing,
Self-adaptation
Parameters for ranking the level of complexity in network automation
Main categories
Semi-Supervised,
Reinforcement Learning (RL),
Unsupervised Learning (USL),
Supervised Learning (SL)

Figure 4.18: Presentation of the concepts related to ML in the SotA. The figure is created by the author.

Another experiment with ML explains how every task can be automated. TensorFlow, PyTorch, Convolution Architecture for Fast Feature Embedding (Caffe2), Microsoft Cognitive Toolkit, and MatLab are the frameworks mentioned as useful for training with deep learning models [77]. Figure 4.19 shows the concepts related to deep learning in the SotA.

Moreover, there are methods related to deep learning[13] about network security, which works in conjunction with SDN. With high accuracy, the deep learning methods Deep Belief Propagation (DBP), Stacked Auto Encoder (SAE), Convolutional Neural Network (CNN), Gated Recurrent Unit (GRU), and Long Short-Term Memory (LSTM) contribute to the mitigation of DDoS attacks in the network's layer three and layer four, while the methods Multilayer Perceptron (MLP) and Long Short-Term Memory (LSTM) mitigate DDoS attacks on the application layer of the network [5, p. 69].

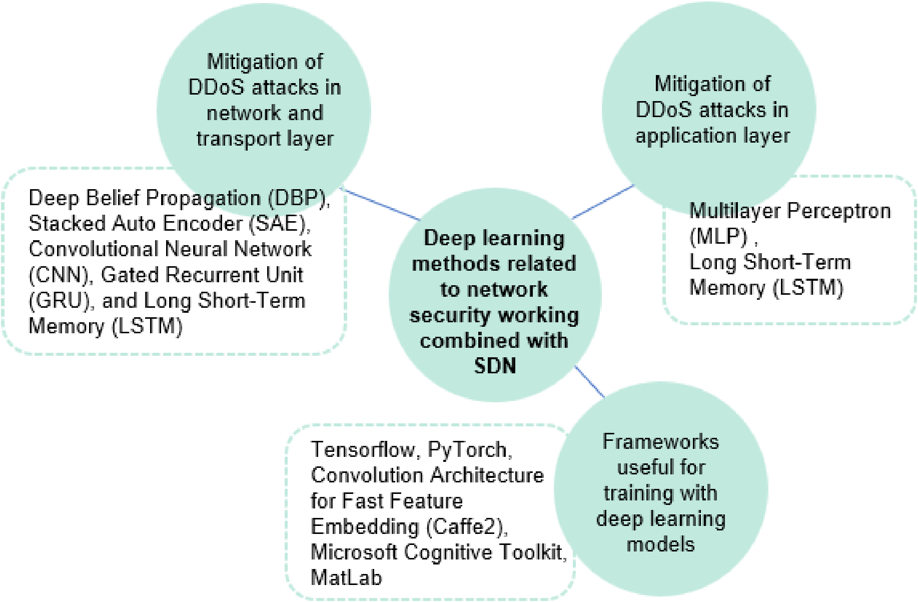

Mitigation of DDoS attacks in network and transport layer
Mitigation of DDoS attacks in application layer
Deep Belief Propagation (DBP), Stacked Auto Encoder (SAE), Convolutional Neural Network (CNN), Gated Recurrent Unit (GRU), and Long Short-Term Memory (LSTM)
Deep learning methods related to network security working combined with SDN
Multilayer Perceptron (MLP) , Long Short-Term Memory (LSTM)
Tensorflow, PyTorch, Convolution Architecture for Fast Feature Embedding (Caffe2), Microsoft Cognitive Toolkit, MatLab
Frameworks useful for training with deep learning models

Figure 4.19: Presentation of the concepts related to deep learning in the SotA. The figure is created by the author.

For the mitigation of the vulnerabilities of an automated network based on SDN technology, leveraging detection and mitigation strategies by utilizing ML techniques such as kNN, Neural Networks (NN), convolutional NN, SVM, DT, and RF is suggested [48]. These concepts are presented in Figure 4.20.

ML-related methods for automation of the security techniques combined with SDN mentioned by the SotA also include k-Nearest Neighbors (KNN), Random Forest (RF), Artificial Neural Network (ANN), Support Vector Machine (SVM) for mitigation of DDoS attacks against the network's layer three and layer four , which are the network and transport layers. Fuzzy Logic (Fuzzy L.) is suggested for the

---

[13] Machine learning and deep learning are both AI techniques whereas ML is more easily adaptable to human interference, while in deep learning the attention is more paid to the algorithms that are structured in the way human brain works [5].

mitigation of DDoS attacks in the application layer of the network. Hidden Markov Model (HMM) is suggested for the mitigation of scanning attacks in addition to DDoS attacks on the application layer [5, p. 69][44, p. 129]. For more details on network layers please see Appendix B.

SDN has made it possible to leverage ML in network security to introduce more intelligence in different methods [45]. This concept is depicted in Figure 4.16. In addition, the ML algorithms such as Bayer's theory, k-Means, Self-Organizing Maps (SOM), and Random Forest can be utilized to raise efficiency and resilience, in addition to intelligently managing security tasks in the networks [5, 48].

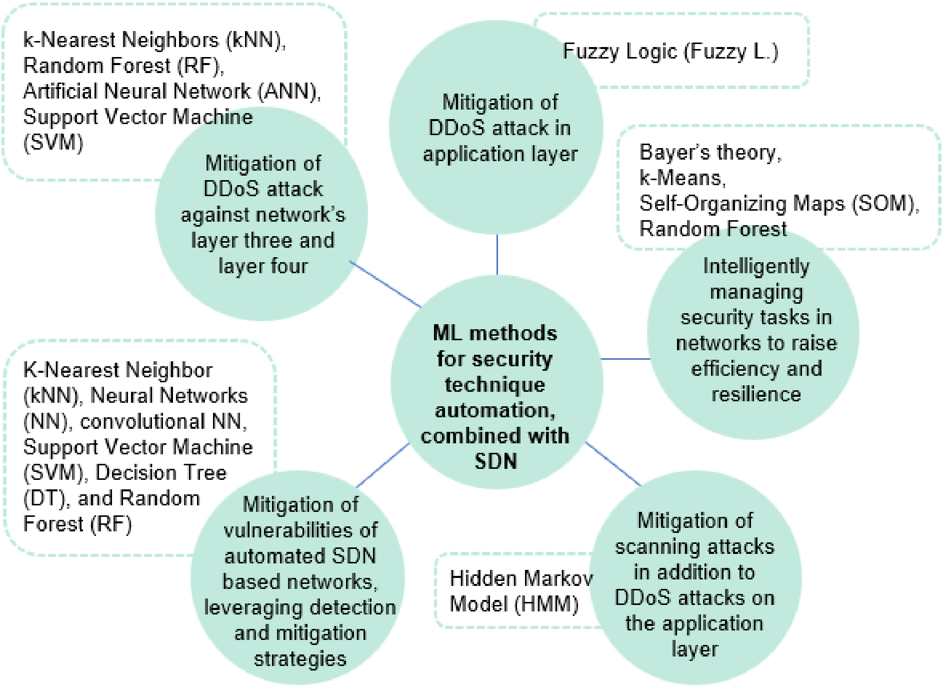

k-Nearest Neighbors (kNN),
Random Forest (RF),
Artificial Neural Network (ANN),
Support Vector Machine (SVM)
Mitigation of DDoS attack against network's layer three and layer four
Mitigation of DDoS attack in application layer
Fuzzy Logic (Fuzzy L.)
Bayer's theory,
k-Means,
Self-Organizing Maps (SOM),
Random Forest
Intelligently managing security tasks in networks to raise efficiency and resilience
ML methods for security technique automation, combined with SDN
K-Nearest Neighbor (kNN), Neural Networks (NN), convolutional NN, Support Vector Machine (SVM), Decision Tree (DT), and Random Forest (RF)
Mitigation of vulnerabilities of automated SDN based networks, leveraging detection and mitigation strategies
Hidden Markov Model (HMM)
Mitigation of scanning attacks in addition to DDoS attacks on the application layer

Figure 4.20: Presentation of the concepts related to ML methods for security technique automation in combination with SDN, discussed in the SotA. The figure is created by the author.

By applying intelligence using ML to network security and network function automation, the possibilities for utilizing different methods in IDS expand significantly, raising the security of the network [45]. Further, the application of ML for making the security of the network in Zero Trust Architecture (ZTA) more resilient is highly recommended [113].

ML can be utilized by enterprises to investigate the encrypted network traffic to determine if its content is malicious or benign [113]. It is also recommended to utilize ZTA network data and logs in improving the training of ML algorithms, further enhancing detection and log analysis of the network traffic [113, p. 29-

30]. Utilization of ML in this relation also makes the incident response analysis much more effective [113, p. 34].

Nevertheless, with the progress of technology, we can see that today everyone does not need to code as Azure ML provides a full platform for the utilization of ML without having much knowledge in coding [109]. The solution provided by this cloud service provider makes users able to analyze data by utilizing a GUI-based interface, which makes it unnecessary to know the complicated ML algorithms for providing analysis of data.

As researchers increasingly include AI to solve IP network tasks more programmatically, we would like to concisely point to this as a new trend where one can even use AI to prepare the process in a desired task that needs to be automated by using programming techniques [57, 132]. We observed that this type of open and available AI for everyone makes it possible to utilize complete codes, suggested by open AI, without having deep knowledge and competency in programming. In this relation, Appendix J demonstrates an interaction with ChatGPT[14] to test the AI's capability in making a code that someone asks.

Concluding this exploration of ML applications in NSA, the intricacies and vastness of ML-related methods emerge as formidable challenges for comprehensive coverage. Despite our efforts to provide a concise overview, the extensive array of techniques and methodologies in ML necessitates further in-depth exploration. The forthcoming detailed figures in the subsequent section aim to serve as a valuable resource for readers seeking a deeper understanding of ML within the context of NSA.

4.3.7 Network Automation Simulation Platforms - RQ2

Delving into RQ2, this section offers an exploration of how existing network automation techniques and technologies play a pivotal role in elevating the resilience, reliability, and efficiency of network security management. Here, we delve into the possibilities for testing, learning, training, and skills building in the network, network security, and NSA techniques and technologies, emphasizing the significance of simulation platforms that can provide such opportunities.

The need for competency in network automation is highlighted in the resources discussed and presented in Chapter 4.1. Consequently, working with routers, switches, and firewall devices becomes essential to gain practical experience. However, obtaining these devices may not be feasible for everyone in a work or home lab setting. Emulators in virtual environments serve as valuable alternatives, easing and facilitating the necessary practices. For a concise overview of available network automation technologies for education and training, alongside the relev-

---

[14] ChatGPT is one of the new and controversial open Artificial Intelligence (AI) technologies, provided in different platforms, performing a freely available API which can intelligently assist users in their needs.

ant resources featured in the SotA that emphasize these technologies, please refer to Appendix B, Section B.6.

The SotA discusses lab environments such as GNS3, Cisco Developer Network (DevNet) Sandbox, and Mininet, providing valuable resources for individuals interested in enhancing their network and network security skills. Despite the critical need for access to lab environments for practical learning, the SotA also emphasizes significant challenges and drawbacks associated with existing advanced labs, which may impact their availability and utility. Additional details on these topics, including Cisco, GNS3, and other lab environments, can be found in Appendix B.

This thesis explores one reason why network professionals may hesitate to adopt network and network security automation techniques and technologies - namely, their apprehension regarding automation [16]. To delve deeper into this issue, we conducted interviews and surveys with network professionals employed in large companies. Consequently, we posit that conducting testing before implementing solutions can instill greater confidence in network professionals, enabling the customization of solutions tailored to each network's specific needs. For a concise overview of the interviews and surveys validating our results and hypothesis, refer to Chapter 5, while a detailed review can be found in Appendix I.

Moreover, management within a company may harbor reservations when deciding whether to embrace automation, fearing potential disruptions to network configurations [17]. Test-driven automation emerges as a solution, allowing for the gradual incorporation of automation into existing networks. In this approach, tests are written first, and automation code is deployed in the production environment only after the tests have successfully passed [70].

4.4 Influential Factors in Network Security Automation Adoption - RQ3

In this section, we address the crucial factors influencing the adoption and effectiveness of NSA techniques and technologies within organizations and the broader industry, particularly those tasked with managing extensive networks. These factors are examined through various lenses, encompassing challenges, practical use cases, opportunities for learning and skill development, vulnerabilities, and a comprehensive SWOT analysis, collectively addressing RQ3.

Within the challenges we explore, we delve into the issues concerning the integration of ML into NSA. We emphasize the significance of relevant knowledge and skills, underlining the motivation for enhancing competencies, as one of the pivotal contributing factors. We also address matters such as management and revocation challenges within automation-driven network security, budget-related obstacles, and lastly, the intricacies associated with the operational planes and the (in)compatibility of existing technology with NSA.

Furthermore, we briefly examine the use cases and vulnerabilities associated with network automation techniques and technologies as mentioned in the SotA. Following this, we present a SWOT analysis of NSA techniques and technologies, drawing from the information extracted from the SotA. For the reader's convenience, Figure 4.21 offers a succinct overview of the section's contents, aiding in easy section navigation.

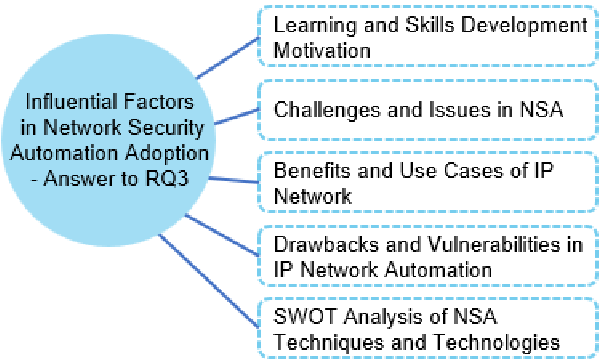

Influential Factors in Network Security Automation Adoption - Answer to RQ3
Learning and Skills Development Motivation
Challenges and Issues in NSA
Benefits and Use Cases of IP Network
Drawbacks and Vulnerabilities in IP Network Automation
SWOT Analysis of NSA Techniques and Technologies

Figure 4.21: Concise presentation of Section 4.4. The figure is created by the author.

4.4.1 Learning and Skills Development Motivation - RQ3

This section delves into RQ3, exploring the factors that significantly impact the adoption and successful implementation of network security automation techniques and technologies within organizations managing large-scale networks. There have been numerous efforts by different companies to standardize a method for evaluating the competency of IT personnel in various fields.

This involves passing related examinations provided by companies that manage these services, resulting in the achievement of relevant certifications that signify the approved level of competency in each field. Examples of such companies include Cisco[15], Juniper[16], Fortinet[17], and Red Hat[18], which offer clear pathways for career development, training, and certifications. These initiatives motivate IT

---

[15] Cisco offers a clear and continuously updated Cisco Certification Path for individuals interested in enhancing their skills and competency in the field of network knowledge.

[16] The Juniper Certification Tracks, provided by the company Juniper, make it easier for those who are interested in choosing their path for knowledge and skills building in IP networking and security.

[17] Fortinet, an IT security company, offers a well-defined path for Fortinet Certification and Training, allowing individuals to acquire knowledge and skills related to their specific IT security products.

[18] Red Hat provides an overview of the opportunities for obtaining Red Hat Certifications in their domain of knowledge and skills.

professionals to enhance their competency, which is verified through the examination processes [26–28, 115, 116].

These certifications not only pertain to knowledge in network and network automation using SDN methodologies but also extend to AWS, Google, and other companies and universities that offer certification paths for building knowledge and skills in ML. We emphasize the importance of motivation for learning and skills building because the enhancement of IT personnel's competency in network automation is highlighted as a highly valuable and decisive factor in the progress of NSA by the SotA [10, 15–17].

4.4.2 Challenges and Issues in NSA - RQ3

Research Question (RQ)3 guides this section, focusing on the pivotal factors that influence the adoption and successful implementation of network security automation techniques and technologies in organizations overseeing large-scale networks. In this section, we review the most significant challenges related to the automation of network and network security tasks in the scope of the literature review. We also discuss these where appropriate or where the answer to the specific challenge is found through the study of the SotA.

The challenges we bring to light in this section include challenges in the application of ML to NSA, the importance of skills and knowledge needed, management and revocation issues in network automation, challenges related to budget and Return on Investment (ROI), security and operational plane related challenges while applying automation techniques, and finally, the need to practice automation in network and network security as a long term strategy and not a one time task.

1. Challenges in Application of ML to Network Security Automation

Some resources in the SotA discuss the challenges of applying ML to network automation techniques [50]. The challenges mentioned are related to the data that ML needs to utilize for training the models and producing the proper models that suit each network. These challenges include the storage needed for large amounts of data, processing and cleaning up this data to make it desirably, being able to extract related data in real-time, integrity-related problems, and also privacy-related issues when it comes to processing the data [50, p. 19-21].

As this resource implies, processing data for building proper ML models is a time- and resource-consuming process. This challenge comes in addition to other challenges, such as the need to be able to interpret the results reliably and handle the complexities that can appear in the process of working with the data.

lack of high-quality data sets that are standardized in addition to the data that already exists without being labeled, not being representative, and lack of validation and attributes are mentioned as significant challenges in the application of

ML to NSA [48, p. 23]. It is mentioned that SDN data is different from traditional network data; hence it needs different frameworks for ML analysis. This is because the existing ML-based methods are not based on SDN, and the data that is gathered needs to be trained in a proper environment for SDN models [48, p. 23][45].

Last but not least, yet, there is no blueprint made about what is the best practice on how to utilize ML in network automation based on the different needs of the organizations, and to solve the complexity of the processes still we need research work on management integration and network control in a network that is based on orchestration and automated by SDN/NFV [44, p. 127].

2. Skills and Knowledge in Network, Firewall, and Network Automation Matters

The network is managed by network engineers with different levels and types of competency. One network engineer could be competent in managing routers and switches at a professional level, while another network engineer could be competent in Enterprise or in Data Center networks. The level of competency also differs. For instance, Cisco[19] divides these into three levels which are associate, professional, and expert [26].

It takes time to build skills in network automation. Adding to this, if someone is adding automation competency to their network knowledge, this will need time to build the competency and experience. Following this, newer network engineers with less competency, have a lower cost for companies that pay their salaries rather than the more competent network engineers with long experience in this field [10, Chapter 1]. However, not every network engineer has competency in their field to automate services and processes [11]. The lack of network professionals with competency in automation is one of the challenges that the automation of networks, network security, and firewall management is facing. We can also mention an extract from the research done by EMA, which points to this fact:

> *"Individuals who work within a data center operations team were more likely to struggle with skills gaps, which makes sense since these teams might have more expertise with physical facilities than with network technology." "Networking guys know the network very well, but we're not programmers. Programmers are great at coding, but they don't understand networks at all. There are very few people who can put networking into code", and "It's difficult to find people who know how to automate" [15, p. 22].*

It is emphasized by the resources in the SotA that to manage the complexity of the network automation techniques, it is required that one is familiar with and master the network environment, concepts, options, and related tools [12]. This is

---

[19] The American company Cisco, is one of the companies that provide services in network and communication globally [26].

to be able to overcome the difficulties in the large-scale networks that for instance Internet Service Provider (ISP)s need to manage and control.

2a. Network Management Competency: To manage networks and network security, by the rules and techniques implemented one needs to have network knowledge and competency. The more experience one acquires, the better and more professional the job on network and network security management is done [26–28, 115, 116]. This includes both the management of technologies such as ACLs and NAT that require pure network knowledge and techniques such as how to architecture the network so it is more secure.

2b. Firewall Management Competency: To manage firewall platforms traditionally via their GUI, one needs to get familiar with the application that represents the firewall. This process needs to be done manually by opening each firewall GUI and implementing the change of any type into it. Also, one needs to have network knowledge as each firewall rule is based on network subnets or hosts as the source or destination of the firewall rule [39, 121, 126].

2c. Network Automation Competency: To automate the network security and firewall management processes one needs to be able to program these processes using any of the automation technology and techniques mentioned in Section 4.3. This competency is needed in addition to the base competency, which is network knowledge, and the additional competency, which is familiarity with the specific firewall platform that the company uses. This is because a programmer can not provide network automation tasks without having knowledge and competency in network [11].

The resources in the SotA mention that when a company has already set a budget to cover the costs for SDN based devices, even if 20% of the network devices are going to be changed to support automation, and 80% remain legacy performing a hybrid model of network automation, still, the costs related to learning and training network personnel to earn the needed competency for network automation is a challenge for the companies [13].

In a survey conducted with network technicians in August 2022, 7.9% expressed their fears of making mistakes by automating the processes in the production environment [16]. In the same survey, 44.7% expressed they lacked knowledge and training resources to build skills in network and network security automation. Moreover, 13.2% of them meant that the existing automation technologies are overwhelming and it is difficult to find out what is better for the organization's network and network security to go for. Also, 34.2% related the problem of lack of automation in their company's network to the lack of budget and financial problems.

The above-mentioned survey also shows that more than 2/3 of the network technicians, who work for service providers and have participated in the interviews, emphasize that they are more comfortable working with networks manually rather than working with automated processes, while at the same time, they believe that network automation will make tasks easier for them [16]. Nevertheless, almost the same number of them agree that network automation will cover tasks that are monotone, repetitive, and boring. Another fact coming out from the interviews done by Kian W. et al. [16] is that the participants do not believe that in the best case, more than 70% of the network tasks can be automated, and neither the majority of them believed that more than 20% to 30% of the tasks could be automated at all.

3. Network Automation a Management Issue

While moving toward network automation where the controller is managed programmatically, as explained earlier in this section, we need to follow the principles for success in Development and Operations (DevOps) [10, 17]. One of the key factors in organizations to success with DevOps is to support network automation as a culture by the management in the organizations [15, 19, 133]. To make teams of developers, security, and network take distance from a silo manner of working, and cultivate the culture of knowledge sharing, and promoting solutions through DevOps processes, the organization needs to support this as a culture among the leaders and managers [15, 53].

In the report published by EMA in 2022 [15], it is stated that approximately 33% of the challenges related to implementing network automation are associated with the skill gap. Additionally, 36% of the assessed success factors pertain to hiring skilled automation experts. This underscores the critical need for management in organizations to support and elaborate on motivation mechanisms for network personnel to build their knowledge and training, becoming one of the influential factors in developing automation competency and skills within the organization's network infrastructure [133, p. 221-234].

There are many challenges when planning a network and network security automation strategy. Organizations have different network structures and utilize different products for their network and network security [11, 43]. This is one of the factors making it difficult to plan a standard solution and strategy to automate all existing traditional networks and their security solutions. Also, not all legacy network and network security products are compatible with automation technologies [1, 5]. Some organizations have multi-vendor products in their network systems in addition to employing outsourced network technicians from different IT consulting companies [15, 16]. With many different needs in organizations and the dependency on the competency of network professionals, human skills must be supported by management and in place [83].

4. Network Automation Revocation Issues

Utilizing network automation in enterprise networks requires the competency of the network personnel while this challenge multiplies with the revocation issues [49, p. 17]. According to the same resource, automated processes are much more difficult to revoke, and the recovery of the issue as a small bug in the software running on the control plane can cause hours of outage on the network until someone with knowledge and competency in network automation, manage to fix it. Some research reports point to the challenge of revocation where software bugs make a 37% and automation changes not being revocable 23% of the existing challenges current efforts in organizations to automate network processes are facing [15, 19].

5. Budget and Return on Investment Matters

While Return on Investment (ROI) is critical for organizations it is evaluated that 34.2% of the challenges of NSA are related to lack of budget and financial barriers in the organizations [16]. On the one hand, it is mentioned that one of the reasons why companies do not go for automation of network security technologies is the cost and the budget related to it [13].

This is because not all devices support OpenFlow, SDN, and other automation technologies, which means they need to be replaced by new devices and that the companies' budget is limited [13]. Moreover, some companies can introduce hybrid solutions in network automation, explained in Section 4.3.1, to temporarily overcome the problem of legacy devices not letting in automation techniques totally [13].

On the other hand, moving towards hybrid solutions gives them a chance to gradually replace legacy devices despite having a limited budget. Even with having 20% of the network devices automation-based and 80% legacy-based, it still reduces the network traffic by 32%, which is a better quality even when not all devices work by automation technologies.

Another cost parameter is related to building the competency and training of the network personnel so that they can manage the new automated technologies [13]. Time and budget saving are mentioned as significant characteristics of network automation by the resources in the SotA [12]. However, while mentioning the improvement of network security as an advantage of utilizing automation techniques and technologies in network and network security, budget and economic challenges for organizations as a consequence of this strategy are pointed to [47, p. 1483-1504].

A Network Zero Touch Provisioning (NetZTP) approach in network automation for achieving a high level of ROI for organizations is suggested by the resources in the SotA [7]. Experiments show that thousands of hours of work will be saved by utilizing automation techniques in the network [7]. This compensates for the investment organizations make in skills building and training of the already-employed network personnel, in addition to hiring professionals who already have network automation competency [7].

Hence, while the fear of lack of budget in organizations exists, the experiments done show that investing in network and network security automation pays back and saves the capital of the organizations [7]. Not only this is proved by experiments accomplished, but also, when reducing human error or other factors that reduce the security of the network, this pays back by delivering better security in the network with fewer incidents and ambiguities in network security [7]. In return, this will raise the trust of the customer and the stakeholders in the services the organization delivers [2, 8].

As also explained in the sections above, by utilization of SDN capabilities many problems related to multi-vendor costs can be reduced and the scalability of the network can be raised [94]. An instance of these possibilities is the capabilities of different libraries of Python programming language, such as *Netmiko* which utilizes SSH protocol for communication and authentication between devices, or this Python library's contribution to multi-vendor compatibility when it comes to for instance Bring Your Own Device (BYOD)s. Another capability of Python libraries for example is the *orionsdk* Python library which helps devices to interact with SolarWinds [85].

6. Security and Operational Plane Challenges in NSA

As mentioned earlier in this chapter, one of the challenges related to the separation of the control plane and the data plane is the selection of the suitable control plane, for each scenario for network implementation with its characteristics [111, p. 210].

The challenges related to network automation are pointed to as first and foremost, the need to answer the question regarding how much of the network needs to be automated [50, p. 18]. We need to decide if we are talking about a zero-touch model or other models. What model is suitable for each organization as each organization has a unique network proper to itself [16]. Further, one of the resources in the SotA suggests two scenarios for their assessment [50].

In the first scenario, where it is chosen to provide a zero-touch[20] model, we face the challenge where there are limitations to adopting the system to the automation changes in the network. In the second scenario, every decision element in systems related to network and network security starts from scratch. This brings flexibility, at the same time taking significant time to adapt the decision elements to the network configurations [50, p. 18-19]

Several challenges related to SDN network automation architecture are mentioned by the SotA [14]. First, the problem of high throughput on the centralized

---

[20] Zero-touch NSA model points to a network management architecture where devices are automatically managed by utilizing network automation techniques [57]. This model, which also is called Network Zero Touch Provisioning (NetZTP), has shown that thousands of hours of work will be saved by utilizing network automation techniques and technologies [7].

controller and having this solution centrally brings the vulnerability of a single point of failure into the network security architecture. Second, when placing several controllers in the network architecture to cover the problem of a single point of failure, we face the question of how many controllers should be utilized to overcome the problem. Finally, resources in the SotA see it challenging to keep the data plane of the devices updated because the dynamic deployment of this process brings inconsistency in packet handling which impacts device connectivity, access control, and even the forwarding loops [14].

As network security automation is highly dependent on programming and SDN, it is appropriate to consider risks related to SDN as the factors that raise the challenges in network security automation [48]. counts several risk factors related to the security of SDN are counted as essential to review when considering network security automation [48].

Among these risk factors, we can mention unauthorized access, data leakage, loss of data integrity, being vulnerable against malware threat vectors while having a lack of security in the design of the applications, incorrect configurations, and loss of control when weak security is designed into the application where even vulnerability to the threat vectors such as DoS and DDoS attacks are present [48]. The latter risk factor if exposed, can for instance knock down a controller which is not redundantly set up and hence is a bottleneck in the network [48, p. 4].

As the SDN becomes dependent on programming and the strength of the programming techniques used, one can utilize Open Web Application Security Project (OWASP) guidelines to build strong security into programming design and architecture for building a strong SDN for network security automation. One of the resources in the SotA mentions that while security features are implemented in traditional and legacy networks solutions, SDN controller automation, which still is new for organizations and the providers of automation technologies and tools, yet is not fully supported [16, p. 73-78]. For an explanation about OWASP please see Appendix B.

The same resource points at SDN controller as a single point of failure and an attractive target for cybercriminals to conduct their attacks against. The programming interfaces between the SDN controller and the devices connected through the southbound interface are mentioned to be one of the vulnerable points in the NSA architecture [16, p. 74].

Memory limitation for the storage of the flow rules, the central controller as a single point of failure in front of DDoS attacks, security issues such as authentication, scalability, and consistency in distributed controllers, and finally, the possibility of DDoS attack on communication channels between the devices and the controllers are mentioned to be known as the significant challenges in NSA [48, p. 4]. When it comes to the application plane, a challenge is the lack of standards for access rights. Regarding the control plane, the increase in the response time when the number of switches that are connected and managed by one single controller grows has been a problem. The data plane's limited size for the entry of the flows has also been mentioned as a significant challenge [48, p. 22].

7. Network Automation as a Long Journey and Not a One-time Task

Building the competency of automation in network engineers takes time. What also takes time is to automate the processes of the network, network security, and firewalls. These processes could, for instance, be related to monitoring processes, updating, or implementation. The tasks need to be programmed, programs need to be tested, and after success in the test, to be implemented to automate the job. Finally, the implemented automation processes need to be updated as the technology change and evolve. This makes network automation a long journey that needs the attention and investment of the leaders of the company [11, 17, 49].

According to the SotA, some disadvantages that can be raised by automating network processes include the disappearance of manual tasks in the processes of network security management, loss of human contact, machines taking over the human-managed tasks [16]. But as one of the research reports states, companies are already reducing the number of their employees while at the same time giving more tasks to fewer people [15]. This implies that network security automation will be a solution to this situation [16]. While resources in the SotA enumerate the advantages of NSA, some of these are mentioned as revealing more time that can be used for creative work, improving capital expenditure and operational expenditure, and easing routines of the organizations [16].

4.4.3 Benefits and Use Cases of IP Network Automation - RQ3

Addressing RQ3, this section examines the key factors shaping the adoption and effective implementation of network security automation techniques and technologies within industries managing extensive networks. Based on the study of the SotA and the instances mentioned in the literature reviewed in this research, automation techniques and technologies are to be applied to both the management of firewall applications, network architectures such as DMZ, zone-based defense architecture, micro-segmentation network security architecture, and zero-trust network security architecture.

Every task that is managed by a CLI or an application that has an API can be programmed to be managed automatically [5]. The point, however, is how beneficial and practical it will be to utilize automation techniques in both the configuration and security of the networks [60].

1. Network Optimization, Load Balancing, Raising Efficiency and Availability, Monitoring, and Measurement Operations

Routing services in IP networks, such as network traffic optimization, secure routing, migration between IPv4 and IPv6, multi-homing, and path protection, are among the use cases of network automation using SDN [111]. Other use cases include load balancing to improve flexibility, efficiency, and availability, as well as monitoring and measurement operations based on preferences [111].

According to Cisco's official guide for teaching development network installation and configuration tasks, in addition to tasks related to network, optimization, and troubleshooting are among the use cases of network automation [10]. Also, managing networks continuously, where risks and human errors can be reduced, is among the use cases where network automation is useful [10, Chapter 1].

2. Conducting Application Awareness Through Deep Packet Inspection and Migration Strategies

Moreover, application awareness, provided by deep packet inspection, and network management tasks for Wide Area Network (WAN), enterprise, and data centers, by automatically adapting policies dynamically, are among the other use cases for network automation using SDN [10]. Finally, the possibility of programming operations and actions using SDN has made migration strategies from legacy devices to new technologies and the utilization of cloud orchestration a reality [111, p. 213-215].

3. Facilitating NSA in Data Centers and Enhancing Resiliency by Redefining Operations at Run-time

One of the most helpful use cases for SDN is mentioned to be in the automation of network and network security tasks in data centers [68]. Another task mentioned to be automated is redefining network operations at runtime in the production environment [34]. This also provides higher resiliency in the network of CIS, such as the network implemented to manage smart grids [34].

Data centers are mentioned by the SotA as a considerable scenario where network automation is useful [2]. Different types of data centers, including cloud data centers, enterprise data centers, and edge data centers, can take advantage of the automation of tasks [2]. This includes large data centers where servers need to be redundant and flexible and require significant network services.

4. Automating Complex and Repetitive Tasks and Simplifying Testing

In large data centers' networks, which need to support data center servers and various network facilities, network tasks become repetitive. Tasks performed by humans are error-prone, so they are better fulfilled by utilizing automation techniques and technologies [2, Chpater 1].

Furthermore, the growth of data center network facilities and equipment, such as routers, cables, and switches, is explosive. Managing all of these resources manually is unrealistic. The resources in the SotA emphasize that manual engineering of such enormous data center networks would not permit the tasks to be accomplished realistically due to the insufficient number of hours available for managing large networks [2, Chpater 1].

By automating repetitive and routine tasks, network automation contributes to the more effective delivery of organizational tasks, making complex activities more feasible [8, 134]. Moreover, design and testing in SDN are mentioned as simpler than in traditional network architecture. The time of healing is less than 0.1 milliseconds compared to over 10 milliseconds in traditional network architecture, and it is predictable, unlike the traditional network architecture, which is not predictable [134]. All of these align with the mission, vision, and values of CIS organizations [135, 136][21][22].

5. Migration at Run-time and Unlimited Opportunities

Some tasks, such as resource reallocation, handling compromised network traffic, migrating VMs at runtime, rate limiting network traffic, labeling and prioritizing network traffic, and installing new flow entries for specific policy enforcement using SDN, are enumerated by the resources in the SotA to enhance network security [34, p. 5]. They emphasize the possibilities provided by SDN for security functionalities in the network as limitless, specifically highlighting 'unlimited opportunities' in the security functionalities of critical infrastructure networks [34, p. 3].

6. Conducting Network Tasks More Efficiently and With Fewer Errors

Simulations conducted in a GNS3 lab environment by the resources in the SotA show that network administration tasks, such as backup and restore, routing, implementation, and network management in a virtual environment, are more efficient and less error-prone when done using network automation [2, 8].

7. Enhancing Security Resilience Through the Automation of Firewalls

Firewalls can be automated using SDN to reduce the risk of cyberattacks [66]. Different types of firewalls, including hardware, software, and virtual firewalls, have been demonstrated by researchers to improve security when automated using SDN and software-defined firewalls [67].

8. Protecting Company Reputation by Reducing Security Risks to the Network

The costs of automating traditional technologies in network and network security are discussed by the SotA. They emphasize that the costs associated with implementing automation techniques and technologies do not diminish the importance

---

[21] Statkraft, a renewable energy leader company, mentions a vision of working in newer ways which are more efficient and the values of utilizing the solutions that are more effective smarter ways to create value for their company and their customers [136].

[22] Cybersecurity & Infrastructure Security Agency (CISA) also points at the importance of a mission that includes reducing risk to their cyber and physical infrastructures, in addition to a vision of providing a secure and resilient critical infrastructure for their people in the USA [135].

of automating network and network security [76].

They highlight that the costs related to the impact of data breaches and cyberattacks are even higher than the costs of automation projects. The importance is also related to the effect of cyberattacks, which can damage a company's reputation when the network infrastructures supporting affected services are compromised. Even without considering the costs of security breaches, the cost and number of work hours required for manual data center management are prohibitively high [76, Chapter 2][38].

While certain resources advocate for further investigation to establish the ROI of network automation [16], others have already delved into the topic, highlighting that network automation, despite initially incurring high costs, ultimately leads to a reduction in Opex. This outcome stems from the fact that once systems are programmed and set to run automatically, there is a diminished need for manual labor and human intervention in task execution [137, p. 68-69].

9. Providing Quality of Service (QoS)

SDN is pointed to as being used in providing Quality of Service (QoS) in networks of CIS, such as in the healthcare sector, where a huge amount of data is transferred and needs to be secured [35]. Other resources in the SotA also highlight QoS as one of the use cases of SDN, mentioning contributions to Load Balencer (LB) and security services as additional use cases of SDN technology in network security automation [82].

10. Saving Energy and Enhancing Agility by Providing Bandwidth on Demand While Reducing Capex and Opex With Less Overhead

While providing an overview that allows everyone to choose the proper orchestration approach, the resources in the SotA explain the use cases of the discussed SDN methods [93]. According to their research, RPC/REST APIs and NETCONF/RESTCONF are utilized in the network virtualization of data centers. Additionally, these communication methods assist in migrating VMs, saving energy, contributing to operating service systems, improving the efficiency of security functions of firewalls, enhancing content delivery in networks, and reducing Capital expenditures (Capex)[23] and Operational Expenditure (Opex)[24] with less overhead.

When it comes to service providers and transport networks, the use cases mentioned by the research groups in the SotA for the above-mentioned communication methods include the reduction of Opex, contribution to testing and diagnosis in operational network services, providing bandwidth on demand to enhance agility while reducing Opex, enabling more effective troubleshooting, and extending the lifetime of on-premises equipment [93]. In addition to this, the improvement

---

[23] Capex points to a company's funds used for managing their physical assets such as upgrading or maintaining their buildings or their technologies [93].

[24] Opex means the costs related to the money an organization uses on its ongoing operations for managing their daily business [93].

in the utilization of LB, IPS, IDS, and firewalls are enumerated. All the mentioned use cases here reduce the costs of network security management while increasing functionality, availability, resilience in cybersecurity, and efficiency [93].

11. Simplifying Network Management While Useful for Enforcing Security Policies and Functionalities

Regarding networks in campuses, enterprises, and homes, use cases of RPC/REST APIs and NETCONF/RESTCONF communication methods explained by the resources studied in the SotA include enforcing security policies and security functions such as firewalls, virus scanning, protection against spam, and handling Intrusion Prevention Systems (IPS) [52, 93]. According to those resources, other use cases in this relation include simplifying management functionalities, such as planning for maintenance or outsourcing, managing traffic like LB, monitoring and migrating, as well as managing resources and bandwidth at a reliable level - all are functionalities of network automation by utilizing SDN that are mentioned.

12. Facilitating Updated and Accurate Documentation of Network and Network Inventory

Another instance of use cases for network automation is when there is a need to see what configurations are in use. For instance, when determining which Virtual Local Area Network (VLAN)s are in use to add a new unused VLAN to the network, logging into each device to input the required command and inspect the list of VLANs is necessary [8]. Moreover, this difficulty applies to other types of tasks as well, and this manual process is error-prone and time-consuming [8]. Another useful functionality of network automation is where one can build network inventory [83, p. 344-376], or even manage Cisco IOS devices or Juniper devices, here also by utilizing the Ansible automation tool [83, p. 40-119].

When these types of tasks are done with a pre-written script, which has already been tested and functions properly, the task could be done either partially automated, where an engineer runs a Python script by executing a line of PowerShell command, or arranged to run automatically by an automation script. The single command could be run at a planned time, and it could also be set to update the documentation of the network. So anytime one needs to check what VLANs are in use and which ones can be deleted if not in use, the documentation could already be updated and ready to use [7, 11].

13. Similarly Beneficial Beyond IP Networks and Their Security in Various Technology Contexts

The importance of the automation of systems by SDN is emphasized by the SotA where different use cases beyond the automation of the network are enumerated [84]. Among these, we recognize cloud data centers, data-centric networks, open network architecture, mobile and cellular data networks, the network of IoT, and finally the network of 4G and 5G.

In other research works, five main categories are presented as the use cases of the application of network automation by SDN technologies [43]. These categories include the automation of traffic engineering, mobility, wireless operations related to the measurement and monitoring of the network and network resources, and finally security management of the network. For instance, DDoS detection is mentioned as one of the application areas related to the automation of security tasks, and QoSFlow as one of the application areas related to the automation of traffic engineering [43, p. 40-41].

14. Simplifying the Complexity of Multi-vendor Network Environments

The complexity of multi-vendor networks is more easily manageable by utilizing different automation techniques and technologies such as NAPALM and the automation tool Ansible [83, p. 186-215]. Another use case of network automation is the management of AWS resources where the Ansible automation tool can be used [83, p. 216-247]. Utilizing Ansible, we can also deploy and operate Azure networking resources. For instance, one can define user-defined routes, create subnets, set up virtual networks, or deploy network security groups [83, p. 248-279].

Regarding the problem complexity caused by utilizing multi-vendor services and products, the resources studied in the SotA explain that while managing a network that is utilizing products, services, and solutions delivered by different vendors is already a complex task to overcome, automating the network will add an extra level of complexity to the problem [44, p. 134]. They also point out how updating, upgrading, and implementing changes in these networks require a long time from weeks to months to be done. They suggest that network automation will be able to manage the problem related to multi-vendor network environments in a flexible, agile, and efficient manner [44].

4.4.4 Drawbacks and Vulnerabilities in IP Network Automation - RQ3

Research Question (RQ)3 frames the discussion in this section, shedding light on the factors that bear significant influence on the adoption and successful integration of network security automation techniques and technologies in industries dealing with large-scale networks. In this section, we will discuss the vulnerabilities of automation techniques and technologies as outlined in the SotA. In some cases, if the literature studied has suggested solutions to specific vulnerabilities, those will also be briefly mentioned.

1. Centralized Monitoring as a Single Point of Failure

In the OpenFlow SDN architecture, centralizing monitoring within the control plane introduces a single point of failure that could pose problems in the event of cyberattacks [34]. A critical cyberattack vector against such vulnerabilities in CIS IP networks, which demand high reliability and availability, is the Denial of Service (DoS) attack [9].

2. Compared to Legacy Devices Increased Exposure to Security Vulnerabilities

SDN, when compared to legacy devices, exhibits a higher susceptibility to security vulnerabilities [78]. However, resources in the SotA suggest that ML can provide a solution. In their research, they demonstrate how cyberattacks, such as DoS, SYN floods[25], or other service-specific attacks in SDN, can be detected by applying ML to Intrusion Detection Systems (IDS). Their research is based on simulation and dataset approaches [78].

3. Dependency on Software Technologies

SDN automation technology has both strengths and weaknesses when it comes to vulnerabilities to cyberattacks [81]. SDN can enhance threat detection based on the possibilities that software technology provides. However, resources in the SotA also enumerate vulnerabilities related to the dependency on software technology [81]. For instance, the SDN platform is susceptible to Distributed Denial of Service (DDoS) attacks targeting the control and application planes.

4. Security Risks Arising from Centrality in Network Security Automation

The resources in the SotA highlight vulnerabilities in SDN, which can pose security risks in automated networks [48]. These vulnerabilities include unauthorized access, data leakage, data modification, malicious applications, configuration issues, and DoS attacks. One of the most discussed vulnerabilities in SDN-based automated networks is related to the centralized controller employed by this network automation architecture [48]. The same resource suggests employing strategies like ML, blockchain, honeynets, network slicing, and moving target defense, each with subcategories of methods, to mitigate DDoS attacks in SDN-based automated networks [48, p. 6].

5. Centralization of Control: Vulnerabilities to MitM Attacks

Centralizing control in SDN makes the network vulnerable to Man-in-the-Middle (MitM) attacks [102]. Experiments conducted by research groups show that a network utilizing SDN and a centralized controller is vulnerable to cyberattacks such as ARP-poisoning [102]. Additionally, the centralized controller introduces a single point of failure into the network security architecture, leaving the network vulnerable to DoS and DDoS attack vectors that could be conducted through a MitM attack [99, 101]. In addition to susceptibility to DoS and DDoS attacks, the centralized controller is also vulnerable to buffer overflow cyberattack vectors [100].

6. Characteristics of SDN NSA: Security Challenges

The resources in the SotA also enumerate characteristics of SDN NSA that pose

---

[25] SYN flood cyber attack is a DDoS attack vector that makes a network resource unavailable for legitimate traffic by consuming all available network traffic path [48].

security challenges in the network [59, Chapter 14 p. 351-375]. These characteristics include not only the centralized controller but also the open programmable interface of SDN, the virtualized network logic, the utilization of third-party network services, and the protocol of forwarding device management. Concurrently, the research works discuss security services based on SDN that can programmatically and in real-time control anomalies in the network and changes in network behavior, while simultaneously restricting potential attack vectors [59].

4.4.5 SWOT Analysis of NSA Techniques and Technologies - RQ3

This section is dedicated to RQ3, investigating the critical elements that play a pivotal role in shaping the adoption and successful deployment of network security automation techniques and technologies in organizations with large-scale network infrastructures. This section presents a Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis of automation techniques and technologies explained in this chapter. In this SWOT analysis, we enumerate strengths, weaknesses, opportunities, and threats related to network automation techniques and technologies. The characteristics of these four categories are explained in detail in Chapter 3, Section 3.1.

Utilizing a SWOT analysis offers a more comprehensive overview of the characteristics of the NSA in this context. It also helps in understanding the factors influencing the application of related techniques and technologies. This, in turn, addresses RQ3, which focuses on the key elements significantly impacting the adoption and effective implementation of NSA methods and technologies in organizations and industries overseeing extensive network infrastructures. It is important to note that in this SWOT analysis, where we cite multiple resources to support our rationale, these referenced sources work together in a complementary fashion, reinforcing the points made by the SWOT analysis.

Strengths

1. Less error proneity due to human error, because network security tasks are managed by codes that are pre-scripted and tested [5].
2. More effective management of rules on firewalls and network security configuration programmatically [5].
3. Fills the gap of unmanageability of thousands of network and firewall security rules in zone-based network security architecture [2].
4. Fills the gap of unmanageability of exponential growth of the network and firewall security rules and configurations in micro-segmentation network security architecture. The gap that makes an avalanche effect of unmanaged and outdated rules as holes on firewalls [2].
5. Efficiency improvement in zone-based and micro-segmentation network security architectures by utilizing automation of the network security management [90].

6. Raising resilience by automatically controlling and updating network configurations, network security, and firewall rules; easing the problem of network holes in gigantic networks such as in CIS [48].
7. Reducing the time of implementations, changes, and updates to network security and firewalls by managing many tasks [2].
8. Automation of repeatable tasks to release time and energy of network personnel to work on more complicated tasks [2].
9. Making possible for developing robust security into network infrastructure which has a flexible and programmable character in addition to providing insight on security challenges [48].
10. Unique features in SDN, such as the threat monitoring entity that is centralized and can be configured programmatically, raise resiliency against malicious cyber attacks [48].
11. By being open for research and invention, providing possibilities for organizations to independently from vendors develop and implement their desired solutions, and release from vendor-locked features [48, 94].
12. Improvement in routing optimization, resource management, QoS prediction [45].
13. Traffic classification by utilizing fine-grained network management, improving also Deep Packet Inspection (DPI) [45].
14. Efficiency in utilizing IDS solutions by introducing intelligence in network analysis and inspection which raises network security and resilience [45, p. 412].
15. Optimizing the workload on the resources by the centralized controller hence raising the intelligence and speed in network traffic [91].
16. Possibility to control and manage networks remotely in an intelligent, easy, and efficient manner [91].
17. Supporting the high level in isolation of users in cloud service provider environment which makes multi-tenancy in cloud solutions a reality for among others application developers [91].
18. Hiding the physical details in the low-level network makes it possible for users to focus on what tasks they want to accomplish rather than how to accomplish those tasks.
19. Other methods and technologies such as ML are compatible and applicable to SDN automation techniques and technologies, and can be utilized to fill the security gaps that SDN suffers from [78].

Weaknesses

1. Requires and is highly dependent on highly skilled IT personnel with both network and programming skills [17].
2. Cost of paying more skilled network personnel who can manage network automation as the more skilled network personnel has more knowledge and experience in the field which requires a higher salary [11].

3. Automation as new technology presents challenges in areas such as the interaction between automation tools and management tools, the requirement to define automation needs, the necessity for strong leadership in IT, and issues related to budget and cost that demand attention and resolution by organizations [11, 76].
4. Old infrastructures might not have API to be able to interact with automation tools [76].
5. High excessive aggregated burden on centralized devices if not redundant [48].
6. Vogue standards, such as authorization, about the security mechanisms in automation-based networks. This could for instance add complexity to the management of authentication and authorization mechanisms [48].
7. Limited memory for storing flow rules in SDN makes it vulnerable for DDoS attack [48].
8. Increasing in controller's response time when adding the number of SDN switches that are managed by a single controller [48].
9. Limitation of flow entry size in the data plane [48].
10. Possibility for raising inconsistencies in SDN controller when applications issue various rules in packet processing to the application plane. This can cause problems in the controller which if not redundant, drive the whole network in a nonfunctional state [92].

Opportunities

1. Managing network security and firewall rules automatically which makes the management tasks be done more effectively [90].
2. A smaller number of low-skilled network personnel are required as the repeatable tasks will be accomplished by automation [11, 90].
3. Enables self-service networking which frees resources that otherwise were set to manage the tasks manually [91].
4. Both small, medium, and big companies such as CIS can take advantage of this technology and the related techniques [11, 90].
5. More work is accomplished with fewer people consequently reducing the number of employees needed for the same amount of tasks [2].
6. Limitless possibilities with SDN in providing security solutions in network infrastructure [34].
7. The possibility of monitoring all network resources in real-time [90].
8. Utilizing advanced threat prevention, load balancing, and providing migrations operations related to VMs without heavily putting load and impacting network resources [91].
9. Saving time and budget for organizations that utilize it [12].

Threats

1. Due to high skill demanding technology, loss of skilled personnel can leave automated infrastructure out of supervision [11, 90].
2. Architectures based on SDN OpenFlow have a single point of failure where the control plane provides a centralized monitoring [34]. This makes the network even more vulnerable against the threat of buffer overflow, DoS, and DDoS attacks [98, 100, 101].
3. Following the vulnerability of the centralized controller as a single point of failure, the network is exposed to the threat vectors such as manipulation of the network, in addition to compromising the application because of the SDN managed network being possible to supervision by the third-party application [99].
4. The combination of different methods raises the complexity of the network which makes the management of the automated networks more difficult and ambiguous for the owners and consequently, the existing ambiguities will open vulnerabilities that attackers are interested in taking advantage of [5].
5. Raising vulnerabilities related to spoofing attacks such as MAC, IP, and VLAN tag spoofing on controller [48].
6. Due to removing intelligence from the devices that are managed by a centralized controller, raising vulnerabilities related to cyberattack vectors such as MitM attack [101, 102].
7. Raising vulnerabilities that lead to synchronization failure or misconfiguration while utilizing distributed controllers [48].

Summary of the SWOT Analysis

In summarizing the SWOT analysis, the strengths of Network Security Automation (NSA) techniques and technologies include the reduction of human error, programmatic management of firewall rules, and efficiency improvement in various network architectures. On the flip side, weaknesses involve dependence on highly skilled personnel, higher associated costs, and challenges in interaction between automation tools.

Moving to opportunities, the automatic management of network security and reduced reliance on low-skilled personnel stand out. Additionally, opportunities arise with the enablement of self-service networking and the applicability of NSA across companies of all sizes. However, potential threats to NSA techniques and technologies include the risk of losing skilled personnel, vulnerabilities in SDN architectures, and increased network complexity leading to potential security issues. This succinct summary provides a glimpse into the key aspects influencing the adoption and effectiveness of NSA techniques and technologies.

4.5 CCAM and Summary Analysis of the Results

This section offers a multi-dimensional analysis of the findings presented in this chapter. We have introduced a Combination Cube Analysis Model (CCAM)[26] to provide a detailed perspective on the complexity of the problem, the various dimensions inherent in the bigger picture, and their interdependencies. As illustrated in Figure 4.22, three instances of these dimensions are combined into a cubic pattern design, where the three axes of the cube represent distinct categories. These three dimensions were previously elaborated on in more detail within this chapter.

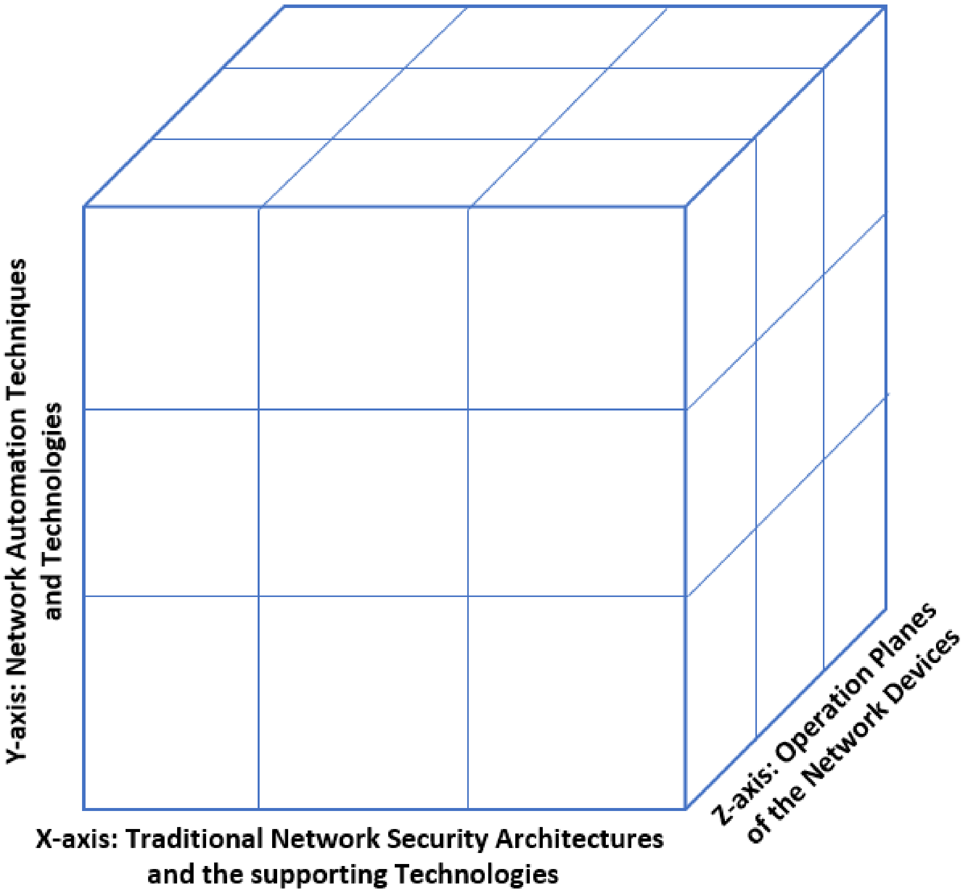

Y-axis: Network Automation Techniques and Technologies
X-axis: Traditional Network Security Architectures and the supporting Technologies
Z-axis: Operation Planes of the Network Devices

Figure 4.22: The analysis cube comprises three defined dimensions: network security methods and technologies on the **X**-axis, automation methods on the **Y**-axis, and the operation planes of network devices on the **Z**-axis, illustrating the problem's complexity. The figure is created by the author.

The categories attached to each of the axes of the cube in Figure 4.22 are as follows:

---

[26] We pronounce this abbreviation as */se:saem/*.

- The **X**-axis represents traditional network security methods and supporting technologies[27].
- The **Y**-axis represents network automation methods and technologies[28].
- The **Z**-axis represents the operation planes of the devices, including the data plane, control plane, and management plane[29].

In this 3D cubic model analysis, we demonstrate that by applying network automation techniques to conventional network security architectures and their supporting technologies, we enhance network efficiency, resilience, and security functionalities [5, 76]. As previously discussed in this chapter, each traditional network security method and technology impacts various operational planes in network devices. Similarly, the application of automation methods also influences different operational planes in network devices.

However, it's important to note that not all technologies used in various network security architectures or operational planes can be automated. For example, many legacy network technologies lack proper APIs, making them unsuitable for automation [104]. In such cases, progress on the Y-axis, representing automation techniques and technologies, remains stagnant as they cannot be applied to legacy technologies. This underscores the necessity for organizations to update their devices to make them automation-compatible [104].

This also brings to light the discussion surrounding costs and limitations associated with network and network security automation [104].

Figure 4.22 illustrates that within each dimension of the CCAM, we find elements from each of the three categories, intersecting with elements from the other two categories at specific coordinates. For example, a FortiGate firewall can be automated using the Python programming language, the Ansible automation tool, or other automation methods. This CCAM, inspired by the McCumber Cube used in cyber security [138], aligns with the findings presented in this thesis's results. This multi-dimensional analysis sheds light on the complexity of the various factors to consider when determining what to employ.

Furthermore, it's worth noting that the illustration presented in Figure 4.22 is not limited to only these dimensions. Additional dimensions can be introduced during decision-making analysis, extending our review beyond the initial three dimensions. Although a three-dimensional figure may not fully visualize all potential dimensions, we utilize this representation to convey the insights gathered from the SotA research reviewed in this study.

While we will continue to refer to this representation as CCAM, we recommend referencing Figure 4.23 for a more comprehensive understanding of complexity. In Figure 4.23, one can interchange each dimension and assess its impact

---

[27] See Section 3.5.

[28] See Section 4.3.4.

[29] See Section 4.3.1.

on the resulting coordinates when combined with other existing dimensions.

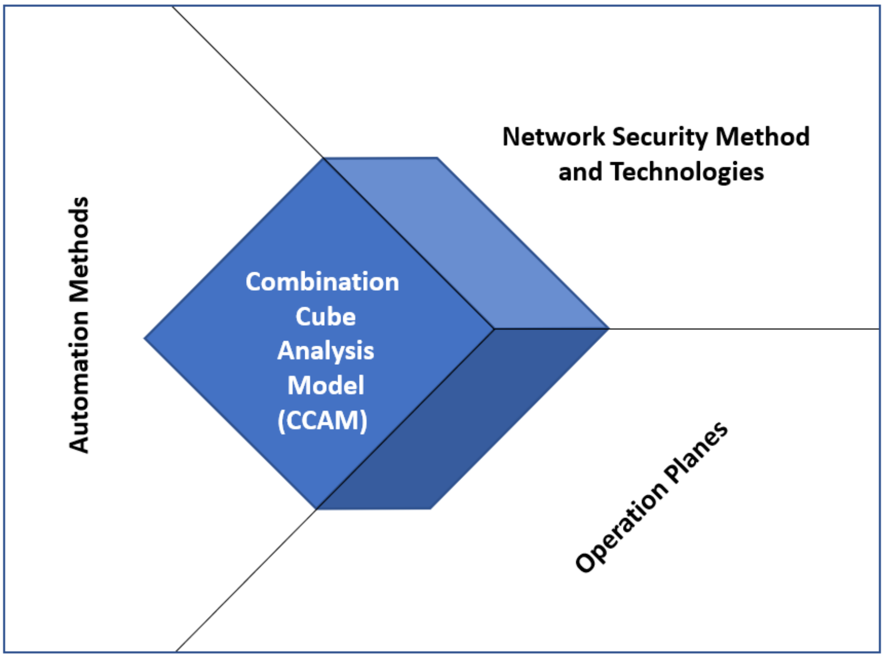

Network Security Method and Technologies
Automation Methods
Combination Cube Analysis Model (CCAM)
Operation Planes

Figure 4.23: Illustration of the Combination Cube Analysis Model (CCAM). The figure has been created by the author.

We can consider adding additional dimensions, such as different cost models. In this scenario, the elements along this axis would represent costs that can be evaluated in a manual implementation of network and network security solutions, a partially automated approach, or even a fully automated solution.

Another dimension to consider is the presence of various actors in the broader context, each offering their solutions and approaches for automating network and network security. This concept is visualized in Figure 4.24, which we refer to as the Information Technology Actors Triangle (ITAT)[30]. In Figure 4.24, we outline the three primary actors identified in our SotA research including **academic researchers**, **solution and equipment providers**, and **organizations and industry**.

In our examination of academic researchers' solutions, we have thoroughly investigated and presented their suggestions in Chapter 4.1 of the SotA study [35, 44, 73, 74, 76, 82], and we continue to explore these ideas in Chapter 4.

---

[30] Information Technology Actors Triangle (ITAT) is an abbreviation suggested by this thesis which is pronounced as /i:ta:t/.

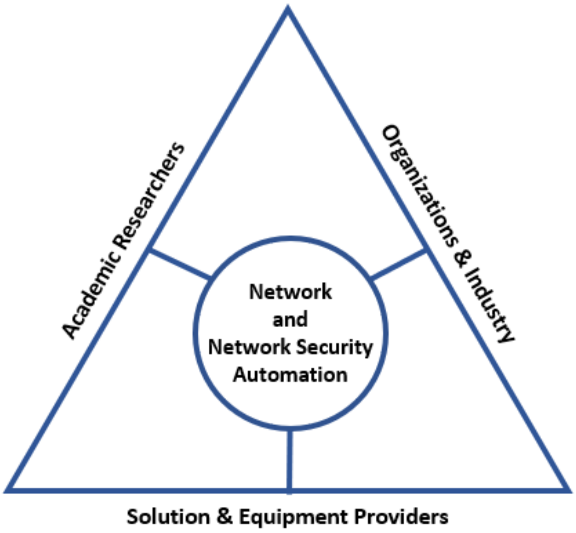


Figure 4.24: ITAT represents three different actors, each with its approach to network and network security automation solutions. The figure is created by the author.

We have also presented many of the solutions suggested by solution and equipment providers in the SotA study [17, 39, 121, 126] and in Chapter 4. However, the last actor presented in Figure 4.24, organizations and industry, and their publications and approaches in this regard were not represented in the SotA. This is because the methods they employ are often practical and seldom published, usually only documented in confidential materials. To address this, we included participants from various organizations and industries in our surveys and interviews. They provided us with valuable insights and answers as part of our validation process.

As ITAT demonstrates, everyone who is seeking to automate their network and network security solutions can choose from the solutions offered by any of these three actors. However, each dimension in ITAT encompasses all the actors related to that specific dimension.

For example, various organizations have their unique models for network and network security, along with preferences for vendors and different products [42, 91, 94, 95]. In the realm of solution and equipment providers, multiple entities are involved, including Cisco, Juniper, Fortinet, VMware, and RedHat. These are briefly addressed in Section 4.2 and more thoroughly explained in Appendix B.

Lastly, concerning the third actor, academic researchers, a glimpse of their suggestions for automating network and network security solutions is provided in the overview of the SotA.

Adding another dimension, which represents the competency required to manage various operation planes, network security methods and technologies, and automation methods, introduces an additional factor for decision-making. It's worth recalling that the necessity for IT personnel with adequate skills and competency to efficiently manage network and network security was discussed in Section 4.4. Furthermore, an organization's needs and possibilities, aligned with its mission and vision, constitute yet another dimension that can influence the outcome of their assessment [134–136].

Combination and Dependency of Different Dimensions

Here, we provide an example of combining different elements from various dimensions of the CCAM. In this thesis, we have presented the following examples of traditional network security architecture strategies:

1. Simple rule set per single or multiple firewall basis without a specific network security strategy.
2. Demilitarized Zone (DMZ) with the utilization of firewalls and policy rules.
3. Zone-based network security architecture in addition to DMZ strategy in network security architecture and firewalls.
4. Micro-segmentation network security architecture, which includes the DMZ and Zone-based architecture strategies, along with the use of firewalls.
5. Zero-touch network security architecture, incorporating all four security strategies mentioned above.

By incorporating security measures into our protection strategies, we enhance network resilience. However, this added complexity can pose challenges in managing large networks [42, 91]. To address this complexity, automation becomes a valuable solution [2].

In the context of network and network security automation techniques and technologies, we have primarily focused on three distinct approaches, as determined by our SotA study. These pertinent and viable techniques include SDN, ML, and IaC-based NSA. As suggested by the findings presented in the SotA of this thesis, these automation techniques and technologies can be effectively used in combination[31], a practice we recommend, although we acknowledge that such a combination can introduce increased complexity [5].

In Section 4.3, we introduced the concept of the three operational planes including the data plane, the control plane, and the application plane. It was explained that, provided that the technology allows and an API exists to communicate with the platform or device, automation techniques can be applied to each of these operational planes [93]. Therefore, by considering only these three dimensions, we can propose a CCAM, as illustrated in Figure 4.25.

---

[31] See Section 4.1.

It's important to emphasize that these dimensions are interdependent. As explained earlier, if the network infrastructure relies on legacy devices that lack compatibility with automation technologies, the utilization of automation becomes unfeasible [104]. This same interdependency extends to other dimensions as well. For instance, the network security architecture and its complexity vary based on the specific needs of the organization. Therefore, it's crucial to recognize the interconnectedness of the dimensions within the CCAM. Now if we apply what is shown in Figure 4.25, Figure 4.26 will appear.

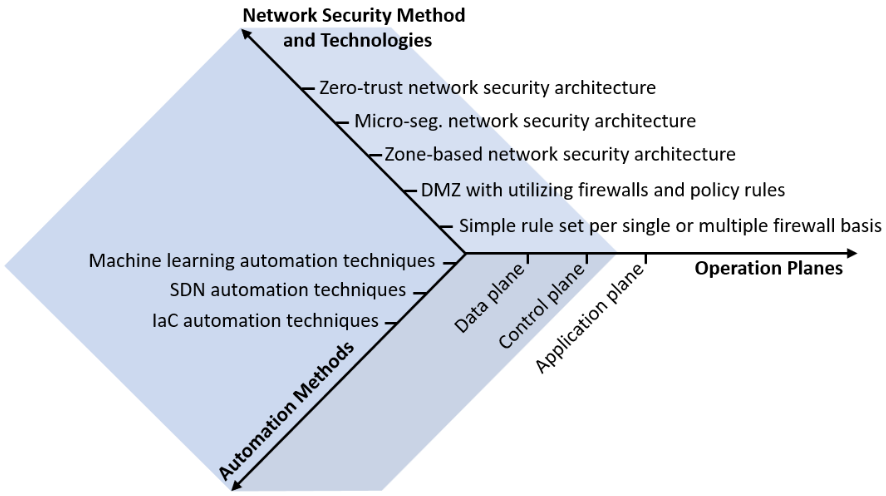

Network Security Method
and Technologies
Zero-trust network security architecture
Micro-seg. network security architecture
Zone-based network security architecture
DMZ with utilizing firewalls and policy rules
Simple rule set per single or multiple firewall basis
Machine learning automation techniques
SDN automation techniques
IaC automation techniques
Operation Planes
Data plane
Control plane
Application plane
Automation Methods

Figure 4.25: Combination Cube Analysis Model (CCAM) with details of each of the axes. The figure is created by the author.

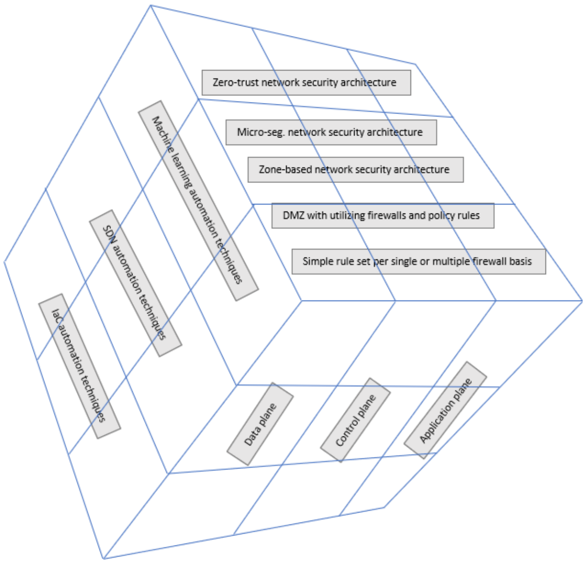

Zero-trust network security architecture
Micro-seg. network security architecture
Zone-based network security architecture
DMZ with utilizing firewalls and policy rules
Simple rule set per single or multiple firewall basis
Machine learning automation techniques
SDN automation techniques
IaC automation techniques
Data plane
Control plane
Application plane

Figure 4.26: Application of the content presented in Figure 4.25 to the structure presented in Figure 4.22. The figure is created by the author.

Exemplification Utilizing Rubik's Cube

In this section, we utilize Rubik's Cube to exemplify the complexity and dependencies in this context. Here, we redefine the dimensions and characteristics of the elements using Rubik's Cube for the sake of exemplification. The Rubik's Cube shown in Figure 4.27 has six sides or faces, and for this example, we equate them to six organizations. In this illustration, colors represent options, and each square that should be filled with a color represents an organization's specific needs in each field.

To clarify, in this exemplification using Rubik's Cube:

1. **Each side/face of the Rubik's Cube:** represents an organization. Therefore, a six-sided Rubik's Cube corresponds to six organizations[32].
2. **Each square:** symbolizes what each organization requires in each field, akin to the dimensions in the CCAM discussed earlier in this section.
3. **Each color:** signifies the options available to fill in each field, which aligns with the parameters in each dimension of the CCAM, as shown in Figure 4.25.

Figure 4.27: The author has employed a Rubik's Cube to exemplify complexities and dependencies, featuring various colors, sides/faces, and squares within it. The picture is taken by the author.

Figure 4.28 depicts one side of the Rubik's Cube with the exemplification of organizational needs named on each square.

---

[32] The related limitations are discussed in Chapter 6 Section 6.1.

NSA Technologies	Competency of IT professionals	NSA Techniques
	The Existing Network Infrastructure	Management Competency
	Possibilities for Infrastructure Improvements	

Figure 4.28: One side of Rubik's Cube representing the organizational needs of a single organization. The squares are filled in with examples of the various needs one organization can have. Additionally, the degree of each need is distinct and unique for each organization. The figure is created by the author.

As previously mentioned in this section, a single organization may have more than nine fields of needs, as illustrated in Figure 4.29. The number of fields can vary based on the type and mission of the organization.

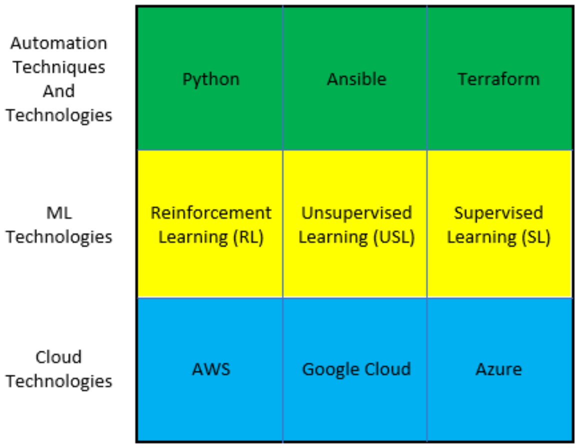
NSA Technologies	NSA Techniques	Possibilities for NSA Competency Enhancement	Competency of IT professionals
Company's Budget	Company's Mission, Vision, and Values	Management Competency	
Solution and Service Providers		Market's Possibilities	The Very Security Challenges and Vulnerabilities
	Possibilities for Infrastructure Improvements	Existing Traditional Network Infrastructure	Operational Planes

Figure 4.29: One side of Rubik's Cube representing the organizational needs of a single organization. In this exemplification, more fields are displayed compared to the number of fields or squares depicted in Figure 4.28. The figure is created by the author.

Now, using colors, we can assign different colors to each need, referred to as squares per side. As mentioned earlier, colors represent various options for addressing each need, with many options available for each field. These options were briefly outlined in Section 4.3. Figure 4.30 illustrates how these options can be applied to each side by rotating the rows and columns of the cube.

Figure 4.30: The Rubik's Cube while turning to apply the options. The pictures are taken by the author.

For example, one of the organizational needs could be the automation of network security. To address this need, options for the methods to apply might include utilizing the Ansible automation tool or using the Terraform automation tool. Figure 4.31 illustrates how these options can be applied to meet each need of the organization.



Automation Techniques And Technologies	Python	Ansible	Terraform
ML Technologies	Reinforcement Learning (RL)	Unsupervised Learning (USL)	Supervised Learning (SL)
Cloud Technologies	AWS	Google Cloud	Azure

Figure 4.31: One side of the Rubik's Cube before it is turned to apply the proper options to each need of the organization. The figure is created by the author.

Finally, when all organizational needs are filled with proper related options, the Rubik's Cube will look like what is shown in Figure 4.32.

Figure 4.32: The final state of the Rubik's Cube after different needs are filled with different options for each organization. The picture is taken by the author.

The exemplification in this section was intended to demonstrate the existing complexities and dependencies in what we discussed above in CCAM.

Summary

In this section, the results examined a 3D analysis model referred to as the Combination Cube Analysis Model (CCAM) to delve into the interplay of factors that influence the adoption and implementation of network security automation techniques. The CCAM is depicted with three axes, symbolizing traditional network security methods and technologies, network automation methods, and the operational planes of network devices. The results underscored the significance of automation in enhancing network efficiency but highlighted the limitations of automating certain technologies, especially legacy ones.

The section introduced additional dimensions, including cost models and the roles of various actors (academic researchers, solution and equipment providers, and organizations and industry), as outlined in the Information Technology Actors Triangle (ITAT), within the context of automation. To aid in understanding the complex interdependencies, a Rubik's Cube analogy was employed. This section aimed to offer insights into the intricacies of network security automation within large-scale networks, addressing RQ3 through our research findings.

4.6 Key Findings - RQ1 & RQ2 & RQ3

This section presents our key findings through the study of the SotA and the SWOT analysis related to research questions.

Our Key findings for Research Question 1

In this section, we present our key findings for RQ1.

Key Finding 1: User-Friendly and Effective for Smaller-Scale Networks: Traditional network security techniques and technologies, including GUI-based interfaces and simplified rule management, excel in user-friendliness. They are particularly suitable for individual hosts and smaller-scale enterprises. These approaches prioritize ease of use and enhance security for organizations with more manageable network infrastructures.

Key Finding 2: Challenges in Scaling for Larger Networks: However, these conventional methods and technologies face limitations when applied to larger-scale networks. The complexities of managing thousands of security rules, cost implications, and the need for highly skilled personnel become significant challenges. As network size increases, the effectiveness of these traditional approaches diminishes, making them less suitable for larger and more complex network architectures.

Our Key findings for Research Question 2

Here, you'll find our key findings about RQ2.

Key Finding 3: Automated Network Security Enhances Resilience: Network security automation techniques and technologies, such as SDN and fine-grained network management, significantly contribute to enhanced network resilience. Automation helps in reducing errors, automatically updating configurations, and efficiently managing security rules. These advancements lead to fewer vulnerabilities and a more robust defense against cyber threats.

Key Finding 4: Improved Efficiency in Network Security Management: Automation not only enhances resilience but also boosts the efficiency of network security management. It streamlines tasks, optimizes resource utilization, and allows for real-time monitoring. This efficiency improvement helps organizations effectively manage security across large-scale networks, minimizing response times to security incidents.

Our Key findings for Research Question 3

Our key findings for RQ3 are outlined in this section.

Key Finding 5: Skill Gap Challenges in Adoption: A key factor influencing the adoption of network security automation is the availability of highly skilled IT personnel with both networking and programming expertise. Organizations that lack personnel with these skills may face hurdles in adopting and implementing automation effectively. Addressing this skill gap is crucial for successful adoption.

Key Finding 6: Cost and Resource Allocation Considerations: The cost of employing skilled network personnel and investing in automation tools can be a significant barrier to adoption. Organizations need to carefully weigh the benefits of automation against its costs. Additionally, budget allocation, leadership support, and the ability to define automation requirements are essential factors that impact successful implementation.

Chapter Summary

In summary, this chapter first presented the theoretical contribution to this research before proceeding to review the characteristics of traditional network security architecture and firewall management using SWOT analysis as part of the response to RQ1. Additionally, we introduced the NSA techniques and technologies discussed in the SotA to address RQ2. Subsequently, we conducted SWOT analysis, examined use cases, and vulnerabilities, and addressed challenges related to NSA techniques and technologies in response to RQ3.

In this chapter, we have synthesized the outcomes derived from an extensive analysis of the SotA. These findings have led us to introduce the CCAM, a multidimensional pattern designed to elucidate the intricate web of contextual intricacies and interdependencies, all of which are pertinent to the problem delineated in Chapter 1. Furthermore, we have concluded this chapter by presenting key insights gleaned from our SotA investigation in response to the research questions. In the forthcoming chapter, we will validate our research outcomes by juxtaposing them with the results acquired from conducted interviews and surveys, thereby substantiating and gauging the credibility of our key findings.

Chapter 5

Results Validation

In order to validate the findings of our investigation into the gap and the problem addressed in this research, we opted to employ both surveys and interviews. Surveys enabled us to efficiently engage with a larger number of participants within a shorter timeframe. At the same time, interviews provided us with a more adaptable and open-ended dialogue with our interviewees, allowing us to capture their perspectives without the constraints of predefined questions, as was the case with our surveys. This approach enabled us to gain deeper insights into their thoughts and ideas without limitations.

It is worth noting that the questions presented here are directly informed by the findings of our study of the SotA, as elucidated in Chapter 4. For instance, we inquire specifically about the participants' familiarity with the Ansible automation tool and the Python programming language as automation configuration tools. This precision is based on the more detailed mentions of these tools within the literature reviewed in this research. Consequently, these questions are formulated in alignment with the comprehensive understanding of the SotA achieved through this research.

In the following sections, we will elaborate on the questions asked during the interviews in Section 5.1 and the questions asked during the survey in Section 5.2, with a comprehensive list provided in Appendix G. The outcomes of the surveys will be presented in Appendix H, with each question juxtaposed alongside its relevant results. The summarized account of the interview results is presented in the following section with a more detailed overview provided in Appendix I. Lastly, in Section 5.3, we will address the validation of the research results as presented in Chapter 4, along with the validation of the problem and hypotheses outlined in Chapter 1.

Detailed discussions of the ethical and legal considerations pertaining to the surveys and interviews can be found in Chapter 1, Section 1.11. The methodology and processes employed for conducting the interviews and surveys are briefly explained in Chapter 2, and thoroughly elucidated in Appendix A. The final section of this chapter validates and summarizes key research findings from Chapter 4.

5.1 Interviews

The questions employed in the surveys exhibit a more comprehensive and detailed structure, while those used in the interviews adopt a broader approach, fostering open discussions that enable participants to freely express their thoughts on the discussed topic, unrestricted by specific queries. The interview questions are intentionally limited in number and are drawn from the questions posed in the surveys.

In the interview method, we engaged participants by asking just one or two questions directly, allowing them to delve into the topic at their discretion. Consequently, the responses collected through interviews were not confined by constraints, enabling participants to articulate their thoughts, emotions, and experiences more extensively. This approach facilitated a fluid and open exploration, guiding us toward a deeper understanding.

For interviews with IT professionals, we initiated conversations with the following questions:

1. Do you employ automation in network security tasks?
2. Could you explain the rationale behind your response?

When engaging with scientific personnel, the conversation began with these questions:

1. Do you introduce students to various automation methods?
2. What is the underlying rationale for your response?

Subsequently, we listened to their insights. While some participants had more to share than others, each contribution proved valuable in shedding light on their perspectives and discussions related to the topic.

In summary, our interviews with IT professionals and a network team leader revealed diverse perspectives on the challenges and solutions in network automation. Notably, the professionals highlighted difficulties in standardizing solutions, emphasized the need for collaboration and competence in automation techniques, and described the current state of network security management as the 'stone age.' A network team leader advocated Network as a Service (NaaS) as a solution, challenging the notion of complete standardization. Additionally, insights from a scientific expert emphasized the importance of teaching students problem-solving skills and the utility of templates. The ten points drawn out from the interview results are as follows:

1. **Standardization Challenges:** Professionals express difficulties in standard-

izing network automation solutions due to diverse organizational needs, varied components, and rapid technological changes.

2. **Team Collaboration:** Collaboration emerges as vital for successful network automation, requiring teamwork similar to DevOps practices, supported by leadership and organizational values.
3. **Manual Network Security Management:** Some professionals describe the current state as the "stone age" of network security, emphasizing the manual handling of tasks, complexity, and lack of automation competency.
4. **Cost and Value of Automation:** While acknowledging initial costs, experts stress the long-term benefits of network automation, providing consistency, scalability, and error reduction, ultimately making tasks more efficient.
5. **NaaS as a Solution:** A network team leader suggests NaaS as a solution for managing diverse networks, challenging the idea of complete standardization.
6. **Consulting Company Role:** The leader sees consulting companies playing a crucial role in navigating the complexity of varied solutions, likening it to solving a Rubik's Cube for each unique customer.
7. **Educational Approach:** A scientific expert underscores the importance of teaching students problem-solving skills rather than specific solutions, aligning with the ever-evolving technological landscape.
8. **Industry Variances:** Varied approaches to network security automation exist among large, medium, and small companies, with challenges arising from differing techniques suggested by academia, industry, and solution providers.
9. **Training Challenges:** Challenges in training include the availability and cost of suitable tools, such as GNS3 and other suitable lab environments for professional training, and the need for practical scenarios for effective learning.
10. **Pedagogical Focus:** Despite industry demands, the university's educational focus remains on teaching students how to learn and find solutions, with an acknowledgment that some topics like DevNet could be considered in the future.

For a comprehensive presentation of the interviews conducted with network professionals from various companies, a network team leader in a large IT consulting company, and one of the scientific personnel at a university, please refer to Appendix I.

5.2 Surveys

In this section, we present the survey questions utilized in our research, targeting individuals with varying levels of expertise and involvement in IT networks and security. Drawing inspiration from a range of sources within the SotA, such as the EMA research report on the future of data center network automation [15] and the work of Chong, W. K., & Grammelb, G. [16], we enriched our inquiry model for assessing the existing gaps in network security automation within organizations.

Our questionnaire consisted of 20 general applicable questions, supplemented by two distinct sets tailored to different groups of participants. These general questions aimed to facilitate comparisons of responses across participants with diverse job roles, aligning with the three key actors outlined in the Information Technology Actors Triangle (ITAT) in the big picture presented in Figure 4.24 of Chapter 4, Section 4.5.

The two specialized categories of questions catered to the unique perspectives and experiences of professors and scientific personnel, who are actively involved in teaching IT-related subjects at universities, and skilled IT professionals, including senior network engineers, network managers, and network and security solution architects, who engage in network and security tasks using various techniques and technologies as part of their daily roles.

It's essential to note that our surveys were conducted anonymously. We emphasized to the participants the importance of providing honest feedback and assured them that:
The survey is entirely anonymous. Therefore, it is crucial to submit your responses since we do not have access to the sender's information, making it impossible for us to send reminders.
If you wish to obtain a copy of your survey responses, you have two options: you can either download them as a PDF immediately upon completing the survey or if you later decide you need to trace your answers in this fully anonymous survey, we will require additional information to assist you in obtaining a copy or deleting your contribution from the results, if necessary.

Furthermore, our survey included inquiries about participants' job types, distinguishing between scientific personnel and IT professionals, as well as their years of professional experience. These background questions played a vital role in our investigation, helping us understand factors influencing the utilization of automation methods and providing validation for our research results.

To enhance the clarity of participant responses, some questions employed reverse psychology. Participants could choose an opposing response option beginning with 'No' if they disagreed with the statement, thus offering a clearer perspective on their views. This approach reduced ambiguity in their selections and facilitated our interpretation of their preferences, especially when not all possible solutions could be assumed or suggested.

As mentioned in the introduction to the current chapter, a comprehensive collection of general questions, questions specific to scientific personnel, and questions specific to IT professionals is available in Appendix G. Furthermore, in Appendix H, before presenting the in-depth review of the survey responses, each question will be individually introduced.

5.3 Results Validation Utilizing Surveys and Interviews

In this section, we embark on the critical task of validating our research findings, centered around the identified gap and the core problem addressed in this study, as initially postulated in Chapter 1, Section 1.5. This validation process entails a meticulous comparison of our research results, the articulated problem, and the initial hypothesis against the insights gleaned from our surveys and interviews. Notably, our survey and interview participants comprised a cohort of 25 IT professionals, augmented by the inclusion of six esteemed members of the academic community actively engaged in university research. It is worth highlighting that the individuals who participated in our interviews were drawn from the same population that contributed to our survey, ensuring a cohesive approach to data collection and analysis.

The deliberate inclusion of scientific personnel in this validation process serves a twofold purpose. First, it enriches our validation process by incorporating diverse perspectives, preventing any undue bias. Second, it enables us to scrutinize the dissonance between the recommendations offered by **academic researchers**, as extensively examined in the SotA literature [35, 44, 73, 74, 76, 82], the solutions and technologies advocated by **solution and equipment providers** as cited within the SotA [17, 26–28, 115, 116], and the practical beliefs and practices prevalent in **organizations and industry**, actively engaged in network and network security operations. This latter perspective is aptly represented by the cohort of IT professionals who participated in our surveys and interviews.

5.3.1 Structure and Relevance of the Questions

In Table 5.1, we present the questions posed to elicit crucial information from our survey and interview participants. We classified these questions into distinct categories to effectively gauge their background, attitudes, and insights concerning the subjects of our research questions.

Table 5.1: The alignment between the Research Question (RQ)s and the survey questions is evident. While the survey questions directed at scientific personnel primarily pertain to RQ2, they also carry an implicit relevance to RQ3.

Relevance of the Questions (below)	Question Categories		
	General Questions **(A)**	Scientific Personnel Group-specific Questions **(B)**	IT Professionals Group-specific Questions **(C)**
Background Registration Questions	2, 3, 11-16	21, 22, 24, 49	21-26, 30, 47, 48
RQ1	4-8, 11, 12	21	22-24, 27
RQ2	9, 10, 13-16	22, 23, 25-48, 50, 51	26-28, 30-33, 38, 39, 45-48
RQ3	17-20	22, 23, 25-48, 50, 51	24, 28-44, 49-54

Background Registration Questions: A subset of our questions, namely questions two, three, and 11 to 16 within the general questionnaire, served to register the participants' backgrounds. These questions provided valuable context for our analysis.

Attitudes Towards Research Questions (RQ)s: Among the general questions, we included inquiries aimed at gauging the participants' attitudes toward the core themes of our research questions. Specifically, questions four to eight and questions eleven and twelve were linked to RQ1, questions nine and ten, as well as questions thirteen to 16, pertained to RQ2, and finally, questions 17 to 20 were associated with RQ3. By employing common general questions for both academic researchers and IT professionals, we enabled a comparative analysis of their responses, considering their different perspectives on the problem.

Scientific Personnel-Specific Questions: Within this category, question 21 was directly linked to RQ1, focusing on the teaching of traditional techniques and technologies to IT students at the university level. Additionally, questions 21, 22, and 24 primarily aimed at capturing background information, while question 49 was designed to gather facts related to their students based on the participants' knowledge. Questions 22, 23, 25 to 48, 50, and 51 were primarily associated with RQ2 but also had implicit connections to RQ3. These questions directly inquired about the state of network and network security automation knowledge teaching at universities and the attitudes of scientific personnel in this regard, with the impact of the registered facts relating to RQ3, focusing on the factors influencing the adoption of these technologies as outlined in RQ2.

For instance, as detailed in Section 4.4.2 of Chapter 4, one of the key challenges concerning the utilization of automation techniques and technologies in network and network security pertains to the availability of IT personnel with adequate knowledge and competency. This knowledge and competency are often acquired through formal education and practical training in relevant subjects at schools and universities. Questions 35 to 39, as explained in the earlier sections of this thesis, were strategically designed to illuminate the gap under investigation, shedding light on scientific personnel's perspectives and attitudes concerning this issue.

IT Professionals-Specific Questions: In the set of questions tailored specifically for IT professionals, we incorporated a series of registration queries aimed at gaining deeper insights into the participants' backgrounds. These inquiries spanned from questions 21 to 26, 30, 47, and 48. Notably, question 22 served as the cornerstone, establishing a foundation for further comprehension and assumptions based on subsequent responses. This pivotal question delved into participants' professional experiences, specifically whether they had worked within CIS companies, particularly in network and/or network security roles. By anchoring their responses to this foundational inquiry, we forged a meaningful connection with the subsequent questions probing their professional backgrounds.

Questions 22 to 24 and 27 directly addressed RQ1, with the latter question also having relevance to RQ2. Questions 26 to 28, 30 to 33, 38, 39, and 45 to 48 were primarily connected to RQ2. Additionally, questions 24, 28 to 44, and 49 to 54 were pertinent to RQ3, with questions 30 to 33 and 39 also implicitly linked to RQ2. Question 28 laid the foundation for subsequent inquiries, while questions 34 and 38 focused on external factors rather than participants' knowledge, beliefs, experiences, or backgrounds.

5.3.2 Validation of Results, Problem, and Hypothesis

The results of the surveys have been instrumental in validating all three RQs, while the interviews primarily aimed at validating RQ3, the problem statement, and the hypotheses outlined in this thesis. An examination of the background information collected from participants reveals that the majority of those engaged in the validation process boast extensive professional experience. For instance, a noteworthy 80% of IT professionals participating in the validation process possess over eight years of relevant experience, and two-thirds of scientific personnel participants have accumulated 20 years or more of professional expertise. This is presented in more detail in Appendix H. This wealth of experience lends added credibility to the responses garnered during the validation process through surveys and interviews.

Validation of Problem

The validation process begins with a thorough examination of the problem. Question two provides insights into the participants' job roles, while questions three to eight shed light on their areas of expertise. Question 22 reveals that 76% of IT professionals either work or have experience in managing large networks, such as those found in CIS. Furthermore, the responses to question 27 from IT professionals indicate that only one person fully utilizes automation techniques. The remainder use them either partially or not at all. This is a clear confirmation of the problem statement outlined in Chapter 1.

This assertion gains further support from the responses to question 28. Here, 76% of IT professionals confirm using automation techniques for 50% or less of their tasks, indicating a reliance on traditional manual methods for the remaining network management responsibilities. These findings are consistent with their familiarity with the traditional methods, as confirmed in questions 4-8, 11, 12, 22-24, and 27. Additionally, the responses to question 29, where participants provide reasoning for their answers to question 27, highlight the multifaceted nature of the problem, aligning with the complexities discussed in Chapter 4 and acknowledged within the SotA.

The validation process, conducted through surveys and interviews, substantiates the existence of the identified gap and the problem statement central to our investigation. This becomes increasingly evident as we explore the correlation between survey questions and each RQ.

Question 24, with an 84% positive response rate, provides evidence of the wide array of products and platforms employed within corporate networks. This underscores the intricacy of existing IP networks. It is important to note that among our IT professional participants, three individuals do not identify as network engineers or architects, and six lack experience with large networks in CIS sectors.

This trend is consistently observed across responses. The notable majority, ranging from 76% to 88%, of IT professionals involved in network engineering or architecture for IP networks possess experience with large IP networks. Yet, they affirm minimal utilization of automation techniques and technologies in their roles. This recognition further enhances the credibility of the responses received, facilitates a clearer understanding of the validation results, and provides additional proof of the problem statement outlined in Chapter 1.

Validation of Results Related to RQ1.A, RQ1.B, and RQ1.C

From the responses provided to questions relevant to RQ1, as detailed in Table 5.1, we can affirm that a significant 96.7% of the participants exhibit familiarity with traditional network firewall implementation and management. Furthermore, all participants demonstrated an understanding of the concept of DMZ. Among scientific personnel, 83% show familiarity, while 96% of IT professionals are familiar with zone-based network security architecture. Additionally, 83.9% of participants confirm their knowledge of micro-segmentation network security architecture, and the same percentage is acquainted with Zero-trust network security architecture. These findings underscore that the majority of the participants possess a strong grasp of conventional network and network security techniques and technologies.

Moreover, half of the scientific personnel and three-quarters of IT professionals have acquired certifications related to traditional network and network security knowledge. This discrepancy highlights IT professionals' greater involvement in obtaining certifications pertinent to their roles compared to scientific personnel. Notably, 67% of scientific personnel acknowledge their role in instructing students on traditional network management techniques and technologies while encouraging them to pursue relevant certifications.

Within the realm of IT professionals, a substantial 76% indicate past or current employment with CIS companies in network or network security capacities. Impressively, 92% have hands-on experience with various firewall management solutions in the context of their network responsibilities, reflecting their extensive familiarity and expertise in traditional network and network security techniques and technologies. Furthermore, 84% of IT professionals report the utilization of diverse platforms from various vendors within their network environments. This necessitates multifaceted competencies for managing distinct networks and network security platforms.

It is notable that a minority of IT professionals, comprising 12%, manage networks without employing any automation techniques or technology, while 84% partially employ network automation techniques and technologies. These findings substantiate that the majority of participants possess knowledge and experience in managing large networks and are well-acquainted with traditional network management methodologies. The utilization of diverse applications, platforms, and products from different vendors in the networks they oversee contributes to the complexity of managing network and network security tasks and processes. This complexity is discussed in detail in Chapter 4.

Validation of Results Related to RQ2.A

When analyzing the questions related to RQ2, we found that a significant 67.7% of participants are familiar with SDN. In contrast, a smaller percentage of participants, specifically 12.9%, indicate familiarity with Machine Learning (ML), and 61.3% confirm their knowledge of IaC. Additionally, 22.6% of participants confirm their familiarity with other automation techniques. However, it's worth noting that 16% of IT professionals express a complete lack of familiarity with network automation techniques.

Interestingly, a resounding 90% of all participants affirm the belief that network automation competency holds significant value in today's market. However, initially, none of the scientific personnel reported having network automation-related certifications. In response to question 14, two of them subsequently mentioned having some network automation-related certifications, introducing a degree of inconclusiveness to the results.

The survey results suggest that IT professionals are more actively pursuing network and network security automation certifications, with 24% holding related certifications. This implies that professionals engaged in managing networks across different organizations possess more hands-on experience and training within network and network security automation environments. This aligns with the responses of scientific personnel, who prioritize imparting foundational knowledge to students, as reflected in their answers to other survey questions. These findings align with insights from interviews with scientific personnel, where an emphasis on the learning process, rather than certification and project outcomes, is evident. The detail of the interview with scientific personnel is available in Appendix I.

Notably, while 56% of IT professionals claim familiarity with network automation lab environments, signifying a significant portion, this ratio among scientific personnel is only 16.7%, representing only one individual. This disparity raises concerns as scientific personnel often require hands-on qualifications to facilitate students' studies and experiments. To draw more definitive conclusions on this matter, a larger sample size of scientific personnel in the survey would be necessary.

Validation of Results Related to RQ2.B

Among academic researchers, 22% have incorporated automation techniques and technologies, including SDN and other automation methods, into their teaching. An additional 33% have introduced IaC to their students. Notably, ML has not been part of the curriculum for any students. Our research indicates that 24% of the resources we examined recommend the integration of ML to enhance network security resilience. Furthermore, a significant 90% of these resources advocate combining ML with SDN for enhanced network security.

All academic researchers unanimously report that their students apply the knowledge gained in network security automation techniques and technologies when they enter the workforce. However, opinions among academic researchers regarding the necessity of including network automation in IT students' studies vary. Some argue that teaching automation techniques is essential to prepare students for future industry demands, while others emphasize the importance of a solid foundational understanding before progressing to more advanced stages of automation.

Validation of Results Related to RQ2.C

52% of IT personnel claim competency and experience in network and network security automation. This provides them with a sense of confidence in its use. However, this assertion contrasts with later responses. Here, 12% acknowledge not utilizing automation techniques at all, and 84% admit to partial usage. This inconsistency introduces uncertainty in the interpretation of their responses.

When evaluating the extent of automation usage in their work, the challenge of inconclusive answers persists. This complicates our ability to draw firm conclusions. Survey responses reveal a diverse range of competencies in various network automation techniques. Moreover, pinpointing the primary reasons for partial or non-utilization of network automation remains elusive, as the responses reflect a wide variety of perspectives, emphasizing the multifaceted nature of the issue. These findings align with our earlier discussions in Chapter 4, highlighting the complexity of network automation influenced by numerous variables.

Notably, 88% of participants concur on the significance of collaborative efforts across teams and knowledge sharing among IT professionals with diverse competencies to achieve network and network security automation goals. They advocate for a shift away from organizational silos. It's worth mentioning that while the majority of respondents initially identified as network engineers or network technical architects, their responses to questions about programming knowledge and expertise display considerable diversity.

This divergence underscores the complexity factors emphasized in Chapter 4, particularly the challenges associated with knowledge transfer. When an employee automates a system and subsequently departs, other team members may struggle to comprehend the system. This is especially true if they lack familiarity with the same technology or programming language. This situation may necessitate a return to manual network and network security management, as highlighted in the interviews. This situation might require a return to manual network and network security management, as emphasized in the interviews. A summarized account of these interviews is presented in Section 5.1, while a detailed version is available in Appendix I.

Validation of Results Related to RQ3.A and Hypothesis

Responses to questions related to RQ3 reveal a consensus among IT professionals regarding the advantages of adopting automation techniques and technologies in network and network security. However, there is a notable 16.7% level of doubt and disagreement among academic researchers. This discrepancy can be attributed to the differing perspectives between these two groups. IT professionals, who are directly engaged in managing extensive network environments, unanimously recognize the need for automation to streamline tasks and processes. Conversely, some academic researchers may not have firsthand experience with large network infrastructures, contributing to their reservations, as suggested by corroborating resources in the SotA [2].

When evaluating the potential benefits of a DevOps approach to teamwork in organizations for automating existing network and network security solutions, 72% of IT professionals agree, while only one academic researcher concurs. In contrast, responses to inquiries regarding the avoidance of diversity and the promotion of standardization in techniques and technologies present a challenge in reaching definitive conclusions. The wide array of responses received serves as a testament to the inherent complexity of the issue. Consequently, we observe nearly equal proportions of agreement and disagreement within both groups, indicating that approximately 50% in each group believe that the advantages of automation outweigh the vulnerabilities introduced by system homogeneity, favoring a reduction in system complexity to enhance security.

Regarding the assertion that the progress in automating network and network security is contingent on the leadership and team-building skills of organization and team leaders, 67% of academic researchers and 84% of IT professionals concur with this claim. These findings, coupled with the responses obtained from background registration questions, which validate the responses and reflect the participants' experience levels, provide strong evidence in support of the hypothesis outlined in Chapter 1, Section 1.5.

Validation of Results Related to RQ3.B

Examining the responses to survey questions, it becomes evident that scientific personnel hold diverse viewpoints on the subject of network automation. Some emphasize the necessity of automation, while others stress the importance of instilling fundamental knowledge in students, prioritizing traditional methods. Interestingly, a majority do not encourage students to pursue certifications in automation techniques and technologies, in contrast to their support for traditional network management certifications.

Notably, around two-thirds of scientific personnel do not perceive a notable disparity between what students learn and what they can practically apply in the context of network automation upon entering the workforce. Universally, scientific personnel participating in this survey unanimously believe that their IT students acquire an adequate understanding, experience, and confidence to effectively employ automation techniques in real-world network and network security scenarios upon graduating from their universities. Many assert that the challenges students encounter during the learning process necessitate a focus on simplicity, emphasizing the teaching of foundational concepts over advanced automation techniques.

The responses provided in the survey, coupled with insights gathered from interviews with scientific personnel, highlight that their perspectives on the importance of automation techniques and technologies significantly influence their approach to educating IT students. A noteworthy concern arises from the relatively low percentage of scientific personnel who are familiar with automation lab environments. These labs are essential for hands-on learning and skill development among students, and instructors must have the means to present, teach, and make them accessible.

Additionally, it’s crucial to recollect the challenges associated with learning lab environments, as discussed in Chapter 4. These challenges include the scarcity, and in some cases, the impossibility of utilizing lab environments that offer easy access and are cost-free for network automation learning, testing, and practice. This issue is also emphasized in the interviews with scientific personnel, where they express the lack of suitable lab environments for network and network security automation skill development.

We perceive these factors, outlined in our results in Chapter 4, as influencing the progress of skills building in network and network security automation among IT personnel. While the absence of free and easily accessible network automation lab environments presents a challenge to competency development among IT personnel, the approach of scientific personnel to prioritize fundamental knowledge over advanced automation techniques is not necessarily negative. They also equip students with the ability to self-learn, which is a valuable skill for continuous education and adaptation. Please refer to Appendix I for a detailed overview of the interview results with scientific personnel.

The responses received from scientific personnel to RQs demonstrate a prevailing emphasis on teaching traditional network management to university students. In contrast, automation techniques and technologies receive less attention from most of them, with a focus on imparting foundational knowledge rather than prioritizing the outcomes associated with automation techniques and technologies. While scientific personnel participating in our investigation confirm possessing a broad understanding of the science related to traditional network management, the diversity of their responses to questions about automation techniques and technologies makes it challenging to draw definitive conclusions. This issue underscores the complexity and lack of standard definitions for automation techniques and technologies, a point also corroborated through the examination of the SotA.

Validation of Results Related to RQ3.C and Hypothesis

Analyzing the responses provided by IT professionals to their group-specific survey questions, we discern that 68% of them employ automation methods in network security to varying degrees, typically falling within the range of 10% to 50%. However, we also observe substantial diversity in the answers received. This diversity becomes more pronounced when respondents cite different reasons to justify their chosen percentage levels. The multitude of responses underscores the complexity of the issue and presents challenges in drawing definitive conclusions.

Among the most frequently cited reasons are a lack of adequate training for network professionals, ambiguities in defining network security automation requirements, and the incompatibility of legacy technology with the changes necessitated by network automation, particularly in utilizing APIs for automation.

In contrast, while Chapter 4 of this study highlights recommendations from numerous resources in the SotA advocating the integration of ML with SDN in network automation to address vulnerabilities, it's noteworthy that among the IT professional participants in this validation process, only one individual possesses knowledge and competency in the field of ML. Conversely, a nearly equal number of participants, close to 50%, express proficiency in automation through the utilization of SDN. This pattern extends to those actively employing the mentioned automation technologies, with just one person employing ML compared to approximately 50% utilizing SDN.

Further insights emerge from responses to questions related to automation technology awareness. It is observed that the number of participants who admit to not being familiar with any automation technology is half of those who claim not to utilize any automation technology, as indicated in their responses to questions 30 and 31. This suggests that even when competency exists, there may be a dearth of suitable contexts to apply it. In light of this assumption, it becomes evident that leadership plays a critical role in providing IT professionals with suitable projects and environments where they can hone and apply their automation skills.

Recognizing that our beliefs and perceptions can influence our actions, we inquired about their perspectives on the ease of using network automation in network and network security roles. In response, 56% indicated agreement with this statement. Additionally, we probed their beliefs regarding the timeline for the widespread adoption of network automation methods. Here, we observed that 52% anticipate active utilization within a relatively short timeframe of two years while 12% envision a longer horizon, estimating it will take more than ten years for substantial adoption to occur.

Regarding the consideration of organizational culture in supporting skills development for IT personnel, 56% confirm that they receive financial support for this purpose. Additionally, 16% affirm that their organizations provide support through practical training and financial means. This observation aligns with responses to questions 11 to 14, where a significant number of participants indicated that they hold various certifications relevant to their roles in network and network security.

Furthermore, it's worth noting that more than half of the participants engaged in network and network security roles acknowledge that certifications and official qualifications serve as strong motivators for them to enhance their skills and put in extra effort. These insights drawn from the survey responses substantiate the observations made in Chapter 4 regarding motivation, training, challenges, and opportunities in the context of automating large network and network security environments.

In addition, 88% of the IT professionals who participated in the survey concur that the support provided by their organization's management and leadership, particularly in relation to the advancement of IT projects and the automation of network security infrastructures, significantly influences the progress of the automation process. This observation aligns with previous questions where 76% of the participants revealed their experience in the network and network security environments of large networks within the context of CIS. Consequently, it can be inferred that the backing of organizational management and leadership plays a pivotal role in the success of network and network security projects, especially within large networks like those found in CIS. This finding lends further support to the hypothesis outlined in Chapter 1.

As outlined in Chapter 4, numerous resources emphasize the importance of training and skill development for IT personnel [2, 11, 49]. In this regard, 92% of the participants agree that support and encouragement from management significantly contribute to the progression of knowledge acquisition, benefiting organizational projects. This finding further substantiates the assertions made in Chapter 4.

When examining the importance of teamwork in achieving network and network security automation objectives, 88% of the participants express agreement that collaboration across teams, involving IT professionals with diverse competencies, coupled with knowledge sharing, is the preferred approach, as opposed to fostering organizational silos. This reaffirms Chapter 4's findings.

Exploring the success factors mentioned in question 40, we received diverse responses that reflected the opinions and experiences of the participants, highlighting the complexity of the issue. This diversity of responses further underscores the multifaceted nature of the challenges discussed in Chapter 4, where some solutions garnered more attention than others.

These factors include providing training for network personnel to enhance their experience in network security automation, supporting and encouraging existing network personnel to expand their knowledge in network automation, and offering practical hands-on labs for network personnel to develop their skills in network automation. The consensus among participants on these factors aligns with the discussions presented in Chapter 4 regarding the significance of training, skills development, and the associated challenges.

Furthermore, participants have also expressed support for factors such as increasing the budget to address the deficiency in funding for phasing out legacy devices that lack automation compatibility, hiring new skilled personnel in network security automation, promoting familiarity with solutions from various vendors in network security and network security automation, aligning middle management with network security automation objectives across various organizational projects, and fostering collaborative teams of programmers and network engineers working in a DevOps manner. These factors closely mirror the points highlighted in Chapter 4.

When participants were asked to briefly explain their choices for these factors, their responses often emphasized the need for clear policies from management, the importance of top-level automation strategies, the presence of clear organizational goals and strategies for the business, referred to as User Stories in DevOps terminology, to effectively anchor the automation strategy across the organization. These responses provide further validation for the accuracy and validity of the hypothesis discussed in Chapter 1, as they underscore the significance of well-defined organizational goals and strategies, in addition to the support of management, as pivotal influencing factors.

Regarding the reasons for potential failures of network security automation projects within organizations, participants offered a range of responses, underscoring the complexity of the issue. However, reasons such as the absence of a well-defined strategy for network security automation by project leaders, insufficient planning for the required budget and costs of network security automation projects, and resistance and apprehension from stakeholders and organizations about automating network security processes and tasks were prominently voted on by participants. This aligns with both the hypothesis outlined in Chapter 1 and the findings discussed in Chapter 4.

Fear of automating tasks and processes is a factor highlighted in the resources presented in the SotA [15, 16]. To delve further into this, IT professional participants in the survey were asked if they feared that automating tasks could lead to system failures, potentially deterring them from introducing network automation. Surprisingly, 88% of respondents reject this fear and express confidence in utilizing automation techniques and technologies within network and network security environments.

This observation leads us to the assumption that the challenge of not implementing automation techniques in network environments may be primarily attributed to a lack of knowledge. This inference is further supported by responses to other survey questions, as participants frequently cited a lack of strategy and organizational planning for automation projects in their open-ended responses. Once again, this reinforces the accuracy of the hypothesis presented in Chapter 1.

Comparing responses to the question about fear of utilizing automation techniques in their current work environments with the previous question on fear of automation in general, we note that 76% of participants answered ‘No’ to this question, indicating a slightly lower ratio than the 88% who did not fear automation in the earlier question. This juxtaposition can be linked to participants’ responses to the question about their comfort level with performing tasks manually or through automation. The majority favored a hybrid solution, which differs from the previous question’s responses. This shift from 88% to 76% suggests apprehension about automating network and network security tasks, confirming SotA findings [15, 16] discussed in Chapter 4.

Responses to the question regarding the preferred method for executing tasks in network and network security infrastructures were diverse, with 68% of participants opting for a hybrid approach. A hybrid solution for network and network security automation was also discussed in Chapter 4 and the SotA [47].

Regarding the percentage of network tasks that can be automated, there was a wide variety of opinions, further emphasizing the complexity of the issue as discussed in Chapter 4. Nonetheless, 60% of participants believed that between 50% to 70% of network tasks could be automated.

Assuming that our actions stem from our feelings of confidence and trust, and in connection with the observations in the SotA regarding IT professionals in this context [15, 16], the survey results indicate that 68% of respondents affirmed their confidence, trust, as well as their possession of adequate knowledge and competency to automate network security tasks within their workplace. These findings align with the Chapter 1 problem statement and hypothesis.

Interestingly, the responses to this question mirrored the results of a question about team collaboration possibilities within the organization, particularly regarding achieving automated solutions for network and network security. This suggests a strong correlation between the outcomes of teamwork and the confidence and trust established among team members who collaboratively completed tasks. This connection reinforces the significance of teamwork and a DevOps approach, as discussed in Chapter 4.

Among the participants, 69% rejected the notion that customer tickets would experience extended resolution times when issues were related to task automation. Notably, a correlation can be observed between these responses and those from a previous question regarding confidence in addressing errors and challenges associated with automation. In that context, 68% of the participants expressed their confidence in resolving errors linked to network and network security solutions automation, while here, 69% dismissed concerns about prolonged customer ticket resolution due to task automation issues.

These findings bolster our confidence in the hypothesis outlined in Chapter 1. Based on the insights gleaned from IT professionals' responses, it becomes increasingly apparent that the primary cause of the issue addressed in Chapter 1 can be attributed to the significance of organizational and team leaders' competencies in fostering teamwork, promoting continuous learning and skill development, and steering diverse teams with varying competencies. These factors play a pivotal role in determining the outcomes of network and network security automation projects.

When we inquired whether IT professionals believe that the automation of procedures and tasks will enhance network security, the responses exhibited a substantial degree of diversity. This diversity once again underscores the intricacy of the problem. Notably, a significant proportion of respondents favored a perspective emphasizing the potential challenges introduced by the automation of network and network security, particularly in terms of both security and network management.

The final question sought their perspective on why automation technologies like SDN, ML, and IaC, widely advocated by numerous academic researchers, are either embraced or overlooked in contemporary solutions for network security automation. The comprehensive responses provided by IT professionals to this inquiry substantiate the points we discussed in Chapter 4, Section 4.5, highlighting the inherent complexity of this issue.

The diversity of these responses complicates the formulation of definitive conclusions. Among their insights, several factors influencing the adoption of automation techniques and technologies in network and network security emerge. While some respondents mentioned that their organizations are already leveraging automation techniques, others cited factors such as the size of their company, the complexity of legacy systems, and the lack of commitment from organizational leadership.

Likewise, factors such as a lack of programming knowledge and related competencies within network teams continued high error rates, licensing costs, time constraints, financial limitations, and resource scarcity, all of which align with our findings and hypothesis, are evident in responses to the aforementioned question. The fact that respondents generally don't dispute the question but instead provide justifications further validates the issue outlined in Chapter 1. A detailed compilation of these responses is presented earlier in this chapter.

Additionally, insights gathered from interviews with IT professionals reaffirm the existence of the problem articulated in Chapter 1. These interviews, as previously presented in this chapter, emphasize various aspects discussed in Chapter 4. These include but are not limited to, network professionals' disinterest in acquiring programming skills, the diverse solutions proposed by various stakeholders as outlined in the ITAT model in Chapter 4, and challenges related to competency and time constraints. Notably, interviewees also stress the importance of teamwork, particularly within a DevOps CI/CD pipeline, and the need for support from organizational leaders in network and network security automation projects.

Furthermore, interviewees highlight the challenges posed by the ever-evolving components in response to advancing technologies. Additionally, they mention issues such as differing organizational requirements and the difficulty in establishing a standardized solution for each organization's unique network. All these factors collectively substantiate the points we presented and discussed in our results within Chapter 4, reinforcing the assertions made in the problem statement and hypothesis outlined in Chapter 1.

5.3.3 Summary

In the extensive research presented in this thesis, a thorough examination was conducted through surveys and interviews to validate various RQs and hypotheses. The participants, comprising IT professionals and scientific personnel, possessed substantial professional experience, with the majority having over eight years in their respective fields, lending credibility to the responses obtained. The validation process confirmed a significant problem statement: the underutilization of automation techniques in network management, particularly in handling large networks.

Key findings indicated that a majority of IT professionals rely on traditional manual methods for network management, with only a small fraction fully embracing automation. This situation aligns with their extensive familiarity with traditional approaches, highlighting the complexity of the problem. The validation process emphasized the existence of a gap in network automation, substantiating the central problem statement.

Additionally, the research delved into specific RQs, such as the participants' familiarity with network security techniques and technologies. It was found that a high percentage exhibited knowledge of traditional network firewall implementation, DMZ, and other related concepts. However, the adoption of advanced automation techniques varied among participants.

Furthermore, the study examined the participants' perspectives on the importance of NSA and the role of certifications. IT professionals displayed a strong inclination toward automation certifications, while scientific personnel emphasized foundational knowledge. The availability of suitable lab environments for hands-on learning also emerged as a concern and impacted skills development.

The participants' responses shed light on the challenges and complexities surrounding NSA, such as the need for collaborative efforts, knowledge sharing, and the avoidance of organizational silos. The significance of organizational leadership, support, and clear strategies in achieving automation goals became evident.

Overall, the research validates the hypothesis that organizational and team leadership, coupled with support for continuous learning and skill development, plays a pivotal role in the success of NSA projects. These findings underscore the multifaceted nature of the challenges within the field of network automation, emphasizing the need for comprehensive solutions and strategies.

5.4 Validation of Key Findings - RQ1 & RQ2 & RQ3

This section presents the validation of the key findings conducted through interviews and surveys. Detailed documentation of these surveys and interviews can be found in Appendix H and Appendix I, along with an overview of the survey questions in Appendix G.

Validation of the Key Findings for the Existing Gap and Problem

The validation process, comprising surveys and interviews, robustly supports the identified gap and the central problem statement of our investigation. This is highlighted by the low adoption of automation techniques among IT professionals managing large networks in CIS. Only one respondent fully utilizes automation techniques, while others partially or completely rely on traditional network security management. The complexity of the problem is underscored by multifaceted responses across various aspects of network engineering, emphasizing the compelling case for addressing the need for enhanced automation in CIS network management.

Validation of the Key Findings for Research Question 1

In this section, we present the validation of the first and second key findings. Key finding 1 is confirmed, and key finding 2 is partially confirmed based on the provided validation information.

Key Finding 1: User-Friendly and Effective for Smaller-Scale Networks

- The summary of validation confirms this key finding. It notes that traditional network security techniques and technologies are user-friendly and suitable for individual hosts and smaller-scale enterprises. This is supported by the majority of participants displaying familiarity with traditional network firewall implementation and management. This key finding is **Confirmed**.

Key Finding 2: Challenges in Scaling for Larger Networks

- The summary of validation partially confirms this key finding, indicating that traditional methods and technologies encounter challenges in larger-scale networks. However, it does not provide detailed specific details on these challenges, such as managing thousands of security rules and the need for highly skilled personnel. Nevertheless, it does mention that some IT professionals partially employ network automation techniques and technologies, suggesting a recognition of challenges in managing large networks. Hence, this key finding is **Partially Confirmed**.

Validation of the Key Findings for Research Question 2

This section includes the validation of both the third and fourth key findings. Here, both key findings related to RQ2 are partially confirmed based on the provided validation information.

Key Finding 3: Automated Network Security Enhances Resilience

- The summary of validation partially confirms this key finding. It notes that a substantial percentage of participants (67.7%) express familiarity with SDN, which is a network automation technology known to enhance network resilience. However, it doesn't provide specific data on the impact of automation techniques on reducing errors or vulnerabilities. Additionally, while 90% believe that network automation competency is valuable, the summary doesn't provide concrete data on the direct relationship between automation and enhanced resilience. Therefore, this key finding is **Partially Confirmed**.

Key Finding 4: Improved Efficiency in Network Security Management

- This key finding is also partially confirmed based on the summary of validation. It mentions that IT professionals are pursuing network and network security automation certifications (24% holding related certifications), which suggests an interest in automation for efficiency. However, it doesn't provide specific data on how automation streamlines tasks or optimizes resource utilization. The summary also highlights the complex nature of network automation, with diverse competencies and challenges in knowledge transfer among IT professionals. Thus, this key finding is **Partially Confirmed**.

Validation of the Key Findings for Research Question 3

The validation of the fifth and sixth key findings is showcased in this section.

Key Finding 5: Skill Gap Challenges in Adoption

- The validation results confirm the existence of skill gap challenges in adopting network security automation. IT professionals unanimously recognize the need for automation to streamline tasks and processes. However, academic researchers, who may not have firsthand experience with large network infrastructures, express reservations, accounting for the 16.7% of doubt and disagreement among them.
- Responses indicate that a lack of highly skilled IT personnel with both networking and programming expertise can hinder successful automation adoption, aligning with the key finding.
- The results highlight the importance of providing training for network personnel to enhance their experience in network security automation, and this resonates with the finding that skill gap challenges affect adoption.
- Therefore, this key finding is **Confirmed**.

Key Finding 6: Cost and Resource Allocation Considerations

- The validation results validate the impact of cost and resource allocation considerations on automation adoption. The cost of employing skilled network personnel and investing in automation tools is recognized as a significant barrier to adoption in the validation results.
- Budget allocation and leadership support are mentioned as essential factors that impact successful implementation, which corresponds to the key finding.
- Consequently, this key finding is **Confirmed**.

Summary: In summary, the validation results confirm both key findings related to RQ3, which investigated factors influencing the adoption of network security automation in large-scale network management, directly connecting to the title of this thesis. Skill gap challenges and cost/resource allocation considerations are recognized as significant factors influencing the adoption and successful implementation of NSA techniques and technologies within organizations managing large-scale networks. The validation results align with the identified challenges and barriers outlined in the key findings concluding that confirmation of Key Findings 1, 5, and 6, while Key Findings 2, 3, and 4 are partially confirmed based on the provided validation information. Overall, the validation results strongly support the validity of the identified challenges and barriers in these key findings.

Chapter 6

Discussion and Conclusion

This chapter delves into the limitations encountered, offers suggestions for future research, and presents the conclusions drawn from this research work.

6.1 Limitations

In the following section, we outline the limitations encountered during this Master's thesis in the following four points:

Access to Real Companies and Environments: Obtaining access to real companies for research, including their production and test environments with active firewalls, proved challenging due to confidentiality requirements and concerns about divulging sensitive information. This limitation restricted our ability to comprehensively examine live working environments and evaluate automation techniques adoption.

Research Scope, Reading Materials, and Related Work: Our research was confined to Network Security Automation (NSA) within the SotA findings, excluding areas such as IoT, Cloud, AI, or Wi-Fi. To inform our study, we meticulously selected recent and pertinent works from a vast body of academic literature. Additionally, we observed a limited body of scientific work that specifically addressed the correlation between network professionals' competency and the adoption of network automation techniques.

Research Infrastructure and Methodology Considerations: Creating a suitable lab environment for testing proved complex and costly. We discussed simulation platforms and automation tools based on the SotA, which may not cover all available options. Areas for potential improvement in our surveys and interviews included expanding the participant pool, implementing feedback, and improving response options and definitions.

Research Methodology Considerations: The SWOT analysis was limited to SotA findings, and we encountered limitations in test environment complexity and the use of visual aids like the Rubik's Cube for illustration purposes. In our validation process, which employed surveys and interviews, we identified areas for potential improvement, including expanding the participant pool, implementing feedback, and improving response options and definitions.

6.2 Future Work

In this section, we explore potential avenues for future research related to the subject matter addressed in this thesis.

Simulation Modelling Using System Archetypes

A promising area for future investigation involves researching the extent to which CIS companies leverage automation techniques, the degree of their implementation, and their long-term strategies. This inquiry can be undertaken by employing security management metrics, a methodology explored in the course IMT4127[1] at the NTNU. By analyzing the annual reports of different companies and applying this metric, we can gauge the efficacy of their security strategies. Subsequently, the outcomes of this assessment can be represented through simulation modeling, employing System Archetypes to create both simple and complex models.

Collaboration with Organizations and Enterprises for Parallel Research

Another compelling suggestion is to conduct similar research in collaboration with one or more companies that are willing to facilitate the investigation. Such cooperation would grant access to the companies' test and production environments, enabling experimentation and the evaluation of various network security architecture solutions discussed in this thesis. An even more comprehensive approach would involve assessing the applicability of the five network security management techniques discussed here in diverse organizational settings, effectively identifying the most suitable solutions for specific use cases. It is important to note that the feasibility of this type of research depends on the willingness of companies to engage and permit access for experimentation on their network firewall environments.

Registration and SWOT Analysis of Other Existing Traditional Network Security Techniques and Technologies, and the Applicable NSA

Future research could delve into a comprehensive examination of additional traditional network security architectures and how NSA techniques and technologies could be seamlessly integrated to enhance network opportunities and resilience.

---

[1] IMT4127 - Security Management Metrics is a subject within the IT Security study program at NTNU, focusing on equipping students with the skills to oversee IT security management. This includes the utilization of metrics and measurements derived from various companies' reports, such as annual reports, in alignment with diverse information security standards like Cobit5, ISO/IEC, and NIST.

This investigation could also entail conducting SWOT analyses of these traditional network security architectures, alongside an assessment of network automation techniques that can complement them. Furthermore, it would be worthwhile to identify mitigation strategies for the threat vectors and vulnerabilities identified during the SWOT analyses. As an initial step, we recommend exploring mitigation methods outlined in NIST SP 800-207 and other relevant resources, particularly those about ZTA.

Research on Solutions to Vulnerabilities of NSA

Continuing our exploration into the future, addressing the vulnerabilities associated with NSA, as discussed in this thesis, will be crucial. Moreover, conducting further research, either through an exhaustive review of the SotA or employing alternative research methodologies, could unveil vulnerabilities not previously addressed in this work. To tackle these vulnerabilities, we propose exploring experimental approaches involving AI and Azure ML. These cutting-edge technologies may offer innovative solutions to fortify the resilience and security of NSA.

Research and Experimentation to Enhance CCAM with AI and ML for Tailored Network Solutions

An intriguing avenue for future research is the exploration of how CCAM, presented in Chapter 4, in conjunction with AI and ML, can recommend customized solutions for various network types. This approach aims to address the complexities highlighted in our analysis, which revolve around determining suitable solutions considering both the capabilities and requirements of different networks. By conducting experiments and research in this direction, we anticipate the development of an AI model capable of suggesting tailored NSA solutions to individual companies. This model would leverage information about their specific needs and capabilities to provide well-fitted recommendations.

In-Depth Research into Factors Impacting NSA Implementation in Traditional Network Security

While our thesis has shed light on the challenges related to the implementation of automation techniques and technologies in network security solutions, there is a compelling need for more extensive research in this area. Section 4.4.2 of this thesis presented the findings of our initial investigation, yet we believe that we have merely scratched the surface. Deeper exploration is warranted to uncover and analyze the undiscovered and unexplored aspects of the challenges, issues, and other factors influencing the application of NSA to traditional network security techniques and technologies. This deeper dive will enable us to gain a comprehensive understanding of the complexities involved in integrating automation into network security.

Research on the Effects of NSA and the Level of Security Provided After the Application to Traditional Network Security

Conduct research to assess the impact of NSA on traditional network security architectures and the resulting level of security. This study should encompass an analysis of the SWOT characteristics of traditional network security architecture both before and after the integration of automation techniques and technologies. Additionally, consider evaluating the SWOT characteristics of other network security architectures to understand their state before and after automation application. Investigate not only the overall progress but also the specific automation techniques and technologies that are most suitable for each traditional network security technique.

Extending Detailed Research on Different Dimensions of the Multidimensional Model, the CCAM, by Comprehensive Examination of Influential Factors on NSA

Extend comprehensive research into the various dimensions outlined in Chapter 4, Section 4.5, within the context of the CCAM. Additionally, explore and expand upon concealed dimensions that could be incorporated into the multidimensional CCAM framework. This expanded research will illuminate previously undiscovered and intricate factors affecting the progress and success of NSA in organizations and industries dealing with extensive networks.

Research and Survey on Existing NSA-Related Research

Considering the vast landscape of existing research in the realm of NSA, it would be valuable to conduct a comprehensive survey. During our exploration of the NSA, we identified thousands of research works related to NSA, offering a substantial resource pool. To enhance accessibility and understanding, we propose creating one or more survey reports categorizing this extensive body of work. Such surveys would provide a structured overview of the various research endeavors in this domain, facilitating a better understanding of the landscape.

Evaluation of the Practicality of NSA Techniques and Technologies

In Section 4.1, we highlighted a significant gap concerning the practical evaluation of methods presented in the resources reviewed in the SotA. To bridge the divide between academic research and the real-world applicability of these methods in contemporary organizations, we recommend incorporating practical evaluations into future research endeavors. Assessing the feasibility and effectiveness of NSA techniques and technologies in real-world scenarios can help refine these approaches, making them more relevant and applicable to today's organizations

Suggested Guiding Research Questions for Future Work

The following are research questions that we believe would be valuable to explore in future work:

1. How promising is network automation in enhancing the quality of CIS network security?

2. What are the essential prerequisites for the successful implementation of network security automation?
3. Under what circumstances should companies consider the adoption of network automation to bolster resilience in their CIS network security?

These guiding research questions can serve as a valuable starting point for further investigations into the realm of NSA and its impact on CIS network security.

6.3 Conclusion

In this thesis, we have explored the challenges presented by the traditional network paradigm in keeping pace with the rapid growth of IP networks [2]. It has become evident that manual management of network security elements, such as firewalls, is no longer tenable in complex environments like data centers and critical infrastructure networks [91]. To address the intricacies of network security management and decision-making, we advocate the adoption of network automation techniques and technologies to enhance firewall implementation and policies, thereby meeting the evolving security needs of networks [90].

Our research has traversed both traditional and automation-driven approaches to network security, guided by an examination of the SotA, to address specific research questions, RQ1, RQ2, and RQ3. In pursuit of answers to RQ3, we have identified factors influencing the progression of network automation, including the challenges faced by industries and organizations managing extensive networks. Using the CCAM, we have structured our findings to illustrate various dimensions and their interdependencies that leaders must consider when making decisions about automating network security tasks.

From our CCAM analysis, we deduce that several dimensions must be considered when assessing and making decisions regarding the automation of network security tasks and processes. These dimensions encompass operational planes, automation methodologies and technologies, network security approaches, the diverse perspectives of involved actors as outlined by ITAT, cost considerations, organizational needs, and the competencies of IT professionals responsible for network and network security tasks. The interplay of these dimensions, depicted by CCAM, contributes to the complexity of the decision-making process.

Through surveys and interviews, we have validated our findings and the problem and hypothesis outlined in Chapter 1. Our research affirms the existence of the identified problem and the validity of our hypothesis. Responses from the validation process underscore the high degree of complexity inherent in this domain. Furthermore, these surveys and interviews reiterate key themes such as complexity, the lack of standardized definitions, the importance of leadership support and effective strategies, as well as the significance of teamwork and competency in the successful application of automation technologies to network security.

Our research underscores the presence of critical vulnerabilities and uncharted territories within NSA that necessitate attention before organizations risk compromising their production network security and the trust of their customers and stakeholders. To address these concerns, we explore potential solutions, including the application of ML, deep learning, and AI to mitigate vulnerabilities and provide robust solutions.

Given the diversity of organizations and their unique needs [25], there is no one-size-fits-all solution to the challenges presented. We acknowledge that tailored decisions, aligned with each organization's specific requirements and capabilities, should be made when applying network automation to enhance network security. As reflected in the SotA presented in this research, this approach aims to bolster the resilience, reliability, and efficiency of IP networks and their security.

In summary, our research findings strongly support the existence of the identified gap and central problem statement. We have confirmed key findings related to user-friendliness, challenges in scaling, skill gap challenges, and cost/resource allocation considerations. While some key findings are partially confirmed, they align with the identified challenges and barriers outlined in these key findings, providing strong support for their validity.

About the author

Gloria Treider is a dedicated network engineer who works as an IT consultant for different companies. She completed her Bachelor's degree in IT Operations and Information Security at NTNU after a year of intensive network administrator studies at Treider Vocational School. With a deep-rooted passion for network management, IT security, and emerging technologies, Gloria has achieved several notable certifications, including CCNA, DevNet, CCSA, ITIL, and various Azure-related certifications like AZ-900 and AZ-700. Furthermore, she successfully undertook the CCNP examination at NTNU. Gloria's commitment to the field extends beyond her academic pursuits. In 2021, she collaborated with three fellow students on a summer job, contributing to articles authored for the Norwegian Water Resources and Energy Directorate (NVE). These articles encompassed topics such as Informasjonssikkerhetsledelse i kraftforsyningen (Information Security Management in Power Supply), IKT-sikkerhetstilstanden i kraftforsyningen 2021 (ICT Security Status in Power Supply 2021), and Sikkerhet i driftskontrollsystemer (Security in Control System Operations) [139–141].

Bibliography

[1] A. A. Barakabitze, A. Ahmad, R. Mijumbi and A. Hines, '5g network slicing using sdn and nfv: A survey of taxonomy, architectures and future challenges,' *Computer Networks*, vol. 167, p. 106 984, 2020.

[2] E. Chou, *Mastering Python Networking: Your one-stop solution to using Python for network automation, programmability, and DevOps*. Packt Publishing Ltd, 2020.

[3] D. P. Ranathunga, 'Auto-configuration of critical network infrastructure,' Ph.D. dissertation, 2017.

[4] G. Falco, C. Caldera and H. Shrobe, 'Iiot cybersecurity risk modeling for scada systems,' *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4486–4495, 2018.

[5] N. M. Yungaicela-Naula, C. Vargas-Rosales and J. A. P.-D. M. Zareei, 'Towards security automation in software-defined networks,' *Computer Communications*, vol. 183, pp. 64–82, 2022.

[6] S. T. Arzo, C. Naiga, F. Granelli, R. Bassoli, M. Devetsikiotis and F. H. Fitzek, 'A theoretical discussion and survey of network automation for iot: Challenges and opportunity,' *IEEE Internet of Things Journal*, vol. 8, no. 15, pp. 12 021–12 045, 2021.

[7] W. Brockelsby and S. Dilda, 'Tactical network automation with netztp and one shot,' in *2019 IEEE 40th Sarnoff Symposium*, IEEE, 2019, pp. 1–3.

[8] G. Santyadiputra, I. Listartha and G. Saskara, 'The effectiveness of automatic network administration (ana) in network automation simulation at universitas pendidikan ganesha,' in *Journal of Physics: Conference Series*, IOP Publishing, vol. 1810, 2021, p. 012 028.

[9] E. Martel, R. Kariger and P. Graf, 'Cyber resilience in the electricity ecosystem: Principles and guidance for boards,' *Center for Cybersecurity and Electricity Industry Community*, 2019.

[10] C. Jackson, J. Gooley, A. Iliesiu and A. Malegaonkar, *Cisco certified devnet associate devasc 200-901 official cert guide*, 2020.

[11] B. Choi, 'Introduction to python network automation,' in *Introduction to Python Network Automation*, Springer, 2021.

[12] A. Bahnasse, F. Bensalah, F. E. Louhab, A. Khiat, Y. Khiat and M. Talea, 'Automation of network simulation: Concepts related to ipv4 and ipv6 convergence,' *Procedia Computer Science*, vol. 155, pp. 456–461, 2019.

[13] R. Amin, M. Reisslein and N. Shah, 'Hybrid sdn networks: A survey of existing approaches,' *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3259–3306, 2018.

[14] O. Michel and E. Keller, 'Sdn in wide-area networks: A survey,' in *2017 Fourth International Conference on Software Defined Systems (SDS)*, IEEE, 2017, pp. 37–42.

[15] S. McGillicuddy, *The future of data center network automation*, 2022.

[16] D. BR[a]b, W. K. Chong[a] and G. Grammelb, 'User fears and challenges in the adoption of network automation,' *Professor Ka Lok Man, Xi'an Jiaotong-Liverpool University, China Professor Young B. Park, Dankook University, Korea Chairs of CICET 2022*, p. 73,

[17] H. Dahir, J. Davis, S. Clark and Q. Snyder, *Cisco Certified DevNet Professional DEVCOR 350-901 Official Cert Guide*. Pearson Education, Limited, 2023.

[18] H. Kim and N. Feamster, 'Improving network management with software defined networking,' *IEEE Communications Magazine*, vol. 51, no. 2, pp. 114–119, 2013.

[19] B. Holz, *Keys to devops success*, 2023, (accessed: 14.03.2023).

[20] E. Union, *General data protection regulation gdpr*, https://gdpr-info.eu/, 2018, (accessed: 20.02.2023).

[21] P. Bhandari, *Ethical considerations in research - types & examples*, https://www.scribbr.com/methodology/research-ethics/, 2022, (accessed: 20.02.2023).

[22] M. Patel and N. Patel, 'Exploring research methodology,' *International Journal of Research and Review*, vol. 6, no. 3, pp. 48–55, 2019.

[23] A. Sarsby, *SWOT analysis*. Lulu. com, 2016.

[24] D. Teoli, T. Sanvictores and J. An, 'Swot analysis,' 2019.

[25] D. Jacobsen and J. Thorsvik, *Arbeidsbok og casesamling til: Hvordan organisasjoner fungerer (5. utg.)* 2019.

[26] W. Odom, *CCENT CCNA ICND1 100-105 Official Cert Guide, Academic Edition*. Cisco Press, 2017.

[27] D. Teare, B. Vachon and R. Graziani, *Implementing Cisco IP routing (ROUTE) foundation learning guide:(CCNP ROUTE 300-101)*. Cisco Press, 2014.

[28] R. Froom and E. Frahim, *Implementing Cisco IP switched networks (SWITCH) foundation learning guide:(CCNP SWITCH 300-115)*. Cisco Press, 2015.

[29] R. W. Anwar, T. Abdullah and F. Pastore, 'Firewall best practices for securing smart healthcare environment: A review,' *Applied Sciences*, vol. 11, no. 19, p. 9183, 2021.

[30] C. Security and I. S. Agency, *Critical infrastructure sectors*, https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors, 2023, (accessed: 14.03.2023).

[31] T. Tsvetanov and S. Slaria, 'The effect of the colonial pipeline shutdown on gasoline prices,' *Economics Letters*, vol. 209, p. 110 122, 2021.

[32] E. A. Parn and D. Edwards, 'Cyber threats confronting the digital built environment: Common data environment vulnerabilities and blockchain deterrence,' *Engineering, Construction, and Architectural Management*, 2019.

[33] K. Dick, L. Russell, Y. Souley Dosso, F. Kwamena and J. R. Green, 'Deep learning for critical infrastructure resilience,' *Journal of Infrastructure Systems*, vol. 25, no. 2, p. 05 019 003, 2019.

[34] H. Maziku, S. Shetty and D. M. Nicol, 'Security risk assessment for sdn-enabled smart grids,' *Computer Communications*, vol. 133, pp. 1–11, 2019.

[35] G. S. Aujla, R. Chaudhary, K. Kaur, S. Garg, N. Kumar and R. Ranjan, 'Safe: Sdn-assisted framework for edge–cloud interplay in secure healthcare ecosystem,' *IEEE Transactions on Industrial Informatics*, vol. 15, no. 1, pp. 469–480, 2018.

[36] K. Eichensehr, 'Not illegal: The solarwinds incident and international law,' *European Journal of International Law (forthcoming 2022), Virginia Public Law and Legal Theory Research Paper*, no. 2022-53, 2022.

[37] D. U. Case, 'Analysis of the cyber attack on the ukrainian power grid,' *Electricity Information Sharing and Analysis Center (E-ISAC)*, vol. 388, pp. 1–29, 2016.

[38] J. M. Boyens, A. Smith, N. Bartol, K. Winkler, A. Holbrook and M. Fallon, 'Cybersecurity supply chain risk management for systems and organizations,' 2022.

[39] S. Keeriyattil and S. Keeriyattil, 'Microsegmentation and zero trust: Introduction,' *Zero Trust Networks with VMware NSX: Build Highly Secure Network Architectures for Your Data Centers*, pp. 17–31, 2019.

[40] S. Rose, O. Borchert, S. Mitchell and S. Connelly, 'Zero trust architecture nist special publication 800-207,' 2020.

[41] X. Yan and H. Wang, 'Survey on zero-trust network security,' in *Artificial Intelligence and Security*, X. Sun, J. Wang and E. Bertino, Eds., Singapore: Springer Singapore, 2020, pp. 50–60.

[42] L. F. Eliyan and R. Di Pietro, 'Dos and ddos attacks in software defined networks: A survey of existing solutions and research challenges,' *Future Generation Computer Systems*, vol. 122, pp. 149–171, 2021.

[43] D. Kreutz, F. M. Ramos, P. E. Verissimo, C. E. Rothenberg, S. Azodolmolky and S. Uhlig, 'Software-defined networking: A comprehensive survey,' *Proceedings of the IEEE*, vol. 103, no. 1, pp. 14–76, 2014.

[44] D. Rafique and L. Velasco, 'Machine learning for network automation: Overview, architecture, and applications [invited tutorial],' *Journal of Optical Communications and Networking*, vol. 10, no. 10, pp. D126–D143, 2018.

[45] J. Xie, F. R. Yu, T. Huang, R. Xie, J. Liu, C. Wang and Y. Liu, 'A survey of machine learning techniques applied to software defined networking (sdn): Research issues and challenges,' *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 393–430, 2018.

[46] H. R. Chi, C. K. Wu, N.-F. Huang, K. F. Tsang and A. Radwan, 'A survey of network automation for industrial internet-of-things towards industry 5.0,' *IEEE Transactions on Industrial Informatics*, 2022.

[47] X. Huang, S. Cheng, K. Cao, P. Cong, T. Wei and S. Hu, 'A survey of deployment solutions and optimization strategies for hybrid sdn networks,' *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1483–1507, 2018.

[48] I. A. Valdovinos, J. A. Perez-Diaz, K.-K. R. Choo and J. F. Botero, 'Emerging ddos attack detection and mitigation strategies in software-defined networks: Taxonomy, challenges and future directions,' *Journal of Network and Computer Applications*, vol. 187, p. 103 093, 2021.

[49] G. Milios, 'Network automation using python,' 2021.

[50] S. T. Arzo, C. Naiga, F. Granelli, R. Bassoli, M. Devetsikiotis and F. H. Fitzek, 'A theoretical discussion and survey of network automation for iot: Challenges and opportunity,' *IEEE Internet of Things Journal*, vol. 8, no. 15, pp. 12 021–12 045, 2021.

[51] O. S. Al-Heety, Z. Zakaria, M. Ismail, M. M. Shakir, S. Alani and H. Alsariera, 'A comprehensive survey: Benefits, services, recent works, challenges, security, and use cases for sdn-vanet,' *IEEE Access*, vol. 8, pp. 91 028–91 047, 2020.

[52] K. Bakshi, 'Considerations for software defined networking (sdn): Approaches and use cases,' in *2013 IEEE Aerospace Conference*, IEEE, 2013, pp. 1–9.

[53] B. Jammeh, *Devsecops: Security expertise a key to automated testing in ci/cd pipeline*, 2020.

[54] M. Gilbert, 'The role of artificial intelligence for network automation and security,' in *Artificial Intelligence for Autonomous Networks*, Chapman and Hall/CRC, 2018, pp. 1–23.

[55] J.-P. Correa-Baena, K. Hippalgaonkar, J. van Duren, S. Jaffer, V. R. Chandrasekhar, V. Stevanovic, C. Wadia, S. Guha and T. Buonassisi, 'Accelerating materials development via automation, machine learning, and high-performance computing,' *Joule*, vol. 2, no. 8, pp. 1410–1420, 2018.

[56] W. Jiang, M. Strufe and H. Schotten, 'Machine learning-based framework for autonomous network management in 5g systems,' in *Proc. 2018 Eur. Conf. on Netw. and Commun.(EuCNC), Ljubljana, Slovenia*, 2018.

[57] E. Coronado, R. Behravesh, T. Subramanya, A. Fernández-Fernández, S. Siddiqui, X. Costa-Pérez and R. Riggio, 'Zero touch management: A survey of network automation solutions for 5g and 6g networks,' *IEEE Communications Surveys & Tutorials*, 2022.

[58] P. Mihăilă, T. Bălan, R. Curpen and F. Sandu, 'Network automation and abstraction using python programming methods,' *MACRo 2015*, vol. 2, no. 1, pp. 95–103, 2017.

[59] B. B. Gupta, G. M. Perez, D. P. Agrawal and D. Gupta, 'Handbook of computer networks and cyber security,' *Springer*, vol. 10, pp. 978–3, 2020.

[60] X. Jia, Y. Jiang and Z. Guo, 'Incremental switch deployment for hybrid software-defined networks,' in *2016 IEEE 41st Conference on Local Computer Networks (LCN)*, IEEE, 2016, pp. 571–574.

[61] Y. Liu, B. Zhao, P. Zhao, P. Fan and H. Liu, 'A survey: Typical security issues of software-defined networking,' *China Communications*, vol. 16, no. 7, pp. 13–31, 2019.

[62] P. Megyesi, A. Botta, G. Aceto, A. Pescapé and S. Molnár, 'Challenges and solution for measuring available bandwidth in software-defined networks,' *Computer Communications*, vol. 99, pp. 48–61, 2017.

[63] S. R. Chowdhury, M. F. Bari, R. Ahmed and R. Boutaba, 'Payless: A low-cost network monitoring framework for software-defined networks,' in *2014 IEEE Network Operations and Management Symposium (NOMS)*, IEEE, 2014, pp. 1–9.

[64] H. Ikarashi, Y. Jin, N. Yamai, N. Kitagawa and K. Okayama, 'Design and implementation of sdn-based proactive firewall system in collaboration with domain name resolution,' *IEICE TRANSACTIONS on Information and Systems*, vol. 101, no. 11, pp. 2633–2643, 2018.

[65] E. Ucar and E. Ozhan, 'The analysis of firewall policy through machine learning and data mining,' *Wireless Personal Communications*, vol. 96, pp. 2891–2909, 2017.

[66] A. Tsuchiya, F. Fraile, I. Koshijima, A. Ortiz and R. Poler, 'Software defined networking firewall for industry 4.0 manufacturing systems,' *Journal of Industrial Engineering and Management (JIEM)*, vol. 11, no. 2, pp. 318–333, 2018.

[67] W. Konikiewicz and M. Markowski, ‘Analysis of performance and efficiency of hardware and software firewalls,’ *Journal of Applied Computer Science Methods*, vol. 9, pp. 49–63, 2017.

[68] M. Suh, S. H. Park, B. Lee and S. Yang, ‘Building firewall over the software-defined network controller,’ in *16th International Conference on Advanced Communication Technology*, IEEE, 2014, pp. 744–748.

[69] E. Ucar and E. Ozhan, ‘The analysis of firewall policy through machine learning and data mining,’ *Wireless Personal Communications*, vol. 96, pp. 2891–2909, 2017.

[70] J. Edelman, S. S. Lowe and M. Oswalt, *Network Programmability and Automation: Skills for the Next-Generation Network Engineer*. " O’Reilly Media, Inc.", 2018.

[71] I. Z. Bholebawa, R. K. Jha and U. D. Dalal, ‘Performance analysis of proposed network architecture: Openflow vs. traditional network,’ *International Journal of Computer Science and Information Security*, vol. 14, no. 3, p. 30, 2016.

[72] J.-I. Castillo-Velazquez, J. Ramos-Estela and W.-R. Marchand-Niño, ‘Comparison for the hardware defined networks vs the software defined networks environments for ipv6 when applied to the backbone of the advanced network reuna,’ in *2021 IEEE Fifth Ecuador Technical Chapters Meeting (ETCM)*, IEEE, 2021, pp. 1–6.

[73] C. E. Hernández Chulde and C. Cervelló Pastor, ‘Lightweight testbed for machine learning evaluation in 5g networks,’ in *JITEL 2019-XIV Conference on Telematics Engineering, Zaragoza, Spain: October 22-24, 2019: proceedings book*, 2019, pp. 1–6.

[74] K. B. Nougnanke, ‘Towards ml-based management of software-defined networks,’ Ph.D. dissertation, Université Paul Sabatier-Toulouse III, 2021.

[75] D. Lee, P. Hong and J. Li, ‘Rpa-ra: A resource preference aware routing algorithm in software-defined network,’ in *2015 IEEE Global Communications Conference (GLOBECOM)*, IEEE, 2015, pp. 1–6.

[76] P. Goransson, C. Black and T. Culver, *Software defined networks: a comprehensive approach*. Morgan Kaufmann, 2016.

[77] P. Martins, F. Sá, F. Morgado and C. Cunha, ‘Using machine learning for cognitive robotic process automation (rpa),’ in *2020 15th Iberian Conference on Information Systems and Technologies (CISTI)*, IEEE, 2020, pp. 1–6.

[78] M. S. Elsayed, N.-A. Le-Khac, S. Dev and A. D. Jurcut, ‘Machine-learning techniques for detecting attacks in sdn,’ in *2019 IEEE 7th International Conference on Computer Science and Network Technology (ICCSNT)*, IEEE, 2019, pp. 277–281.

[79] K. Morris, *Infrastructure as code: managing servers in the cloud*. " O'Reilly Media, Inc.", 2016.

[80] S. Sharma, *Modern API Development with Spring and Spring Boot: Design highly scalable and maintainable APIs with REST, gRPC, GraphQL, and the reactive paradigm*. Packt Publishing Ltd, 2021.

[81] Q. Yan, F. R. Yu, Q. Gong and J. Li, 'Software-defined networking (sdn) and distributed denial of service (ddos) attacks in cloud computing environments: A survey, some research issues, and challenges,' *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 602–622, 2016. DOI: 10.1109/COMST.2015.2487361.

[82] Y. Jarraya, T. Madi and M. Debbabi, 'A survey and a layered taxonomy of software-defined networking,' *IEEE communications surveys & tutorials*, vol. 16, no. 4, pp. 1955–1980, 2014.

[83] A. Rahman, J. Islam, D. Kundu, R. Karim, Z. Rahman, S. S. Band, M. Sookhak, P. Tiwari and N. Kumar, 'Impacts of blockchain in software-defined internet of things ecosystem with network function virtualization for smart applications: Present perspectives and future directions,' *International Journal of Communication Systems*, e5429,

[84] K. Okasha, *Network Automation Cookbook: Proven and actionable recipes to automate and manage network devices using Ansible*. Packt Publishing Ltd, 2020.

[85] A. Ratan, *Practical Network Automation: Leverage the power of Python and Ansible to optimize your network*. Packt Publishing Ltd, 2017.

[86] F. Bannour, S. Souihi and A. Mellouk, 'Distributed sdn control: Survey, taxonomy, and challenges,' *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 333–354, 2017.

[87] O. S. Al-Heety, Z. Zakaria, M. Ismail, M. M. Shakir, S. Alani and H. Alsariera, 'A comprehensive survey: Benefits, services, recent works, challenges, security, and use cases for sdn-vanet,' *IEEE Access*, vol. 8, pp. 91 028–91 047, 2020.

[88] Y. Cao, S. R. Pokhrel, Y. ZHU, R. Ram Mohan Doss and G. Li, 'Automation and orchestration of zero trust architecture: Potential solutions and challenges,' 2022.

[89] R. Romanyak, 'Impact of network automation,' in *SREcon18 Europe/Middle East/Africa (SREcon18 Europe)*, Dusseldorf: USENIX Association, Aug. 2018. [Online]. Available: https://www.usenix.org/node/218938.

[90] D. Bringhenti, G. Marchetto, R. Sisto, F. Valenza and J. Yusupov, 'Introducing programmability and automation in the synthesis of virtual firewall rules,' in *2020 6th IEEE Conference on Network Softwarization (NetSoft)*, IEEE, 2020, pp. 473–478.

[91] M. Caprolu, S. Raponi and R. Di Pietro, 'Fortress: An efficient and distributed firewall for stateful data plane sdn,' *Security and Communication Networks*, vol. 2019, 2019.

[92] Y.-M. Kim and M. Kang, 'Formal verification of sdn-based firewalls by using tla+ (2020),' *IEEE Access*, vol. 8, pp. 52 100–52 112, 2020.

[93] S. H. Krishna and R. Sharma, 'Survey on application programming interfaces in software defined networks and network function virtualization,' *Global Transitions Proceedings*, vol. 2, no. 2, pp. 199–204, 2021.

[94] R. Uddin and M. F. Monir, 'Evaluation of four sdn controllers with firewall modules,' in *Proceedings of the International Conference on Computing Advancements*, 2020, pp. 1–8.

[95] H. Al-Rushdan, M. Shurman, S. H. Alnabelsi and Q. Althebyan, 'Zero-day attack detection and prevention in software-defined networks,' in *2019 international arab conference on information technology (acit)*, IEEE, 2019, pp. 278–282.

[96] S. Xie, C. Xing, G. Zhang, X. Wei and G. Hu, 'Research on ldos attack detection and defense mechanism in software defined networks,' in *Security and Privacy in Social Networks and Big Data: 6th International Symposium, SocialSec 2020, Tianjin, China, September 26–27, 2020, Proceedings 6*, Springer, 2020, pp. 85–96.

[97] M. R. Shaikh, F. Y. Khuhawar, K. Nisar, A. A. Memon and A. S. Khan, 'Vulnerability assessment & analysis of software-defined networking using a virtual testbed,' in *2022 Global Conference on Wireless and Optical Technologies (GCWOT)*, IEEE, 2022, pp. 1–7.

[98] O. Polat and H. Polat, 'An intelligent software-defined networking controller component to detect and mitigate denial of service attacks,' *Journal of Information and Communication Technology*, vol. 20, no. 1, pp. 57–81, 2021.

[99] T. Ubale and A. K. Jain, 'Taxonomy of ddos attacks in software-defined networking environment,' in *Futuristic Trends in Network and Communication Technologies: First International Conference, FTNCT 2018, Solan, India, February 9–10, 2018, Revised Selected Papers 1*, Springer, 2019, pp. 278–291.

[100] R. Swami, M. Dave and V. Ranga, 'Iqr-based approach for ddos detection and mitigation in sdn,' *Defence Technology*, 2022.

[101] A. Pradhan and R. Mathew, 'Solutions to vulnerabilities and threats in software-defined networking (sdn),' *Procedia Computer Science*, vol. 171, pp. 2581–2589, 2020.

[102] E. Christensson, *Man in the middle attacks on software defined network*, 2023.

[103] H. Saito, H.-C. C. Lee and K.-J. C. Hsu, *Kubernetes Cookbook: Practical solutions to container orchestration*. Packt Publishing Ltd, 2018.

[104] L. Csikor, M. Szalay, G. Rétvári, G. Pongrácz, D. P. Pezaros and L. Toka, 'Transition to sdn is harmless: Hybrid architecture for migrating legacy ethernet switches to sdn,' *IEEE/ACM Transactions On Networking*, vol. 28, no. 1, pp. 275–288, 2020.

[105] S. R. Goniwada and S. R. Goniwada, 'Enterprise cloud native automation,' *Cloud Native Architecture and Design: A Handbook for Modern Day Architecture and Design with Enterprise-Grade Examples*, pp. 523–553, 2022.

[106] Y. Chiang, Y. Zhang, H. Luo, T.-Y. Chen, G.-H. Chen, H.-T. Chen, Y.-J. Wang, H.-Y. Wei and C.-T. Chou, 'Management and orchestration of edge computing for iot: A comprehensive survey,' *IEEE Internet of Things Journal*, 2023.

[107] Y.-M. Kim, M. Kang and J.-Y. Choi, 'Formal specification and verification of firewall using tla+ (2017),' in *Proceedings of the International Conference on Security and Management (SAM)*, The Steering Committee of The World Congress in Computer Science, Computer . . ., 2017, pp. 247–251.

[108] N. Dragoni, I. Lanese, S. T. Larsen, M. Mazzara, R. Mustafin and L. Safina, 'Microservices: How to make your application scale,' in *Perspectives of System Informatics: 11th International Andrei P. Ershov Informatics Conference, PSI 2017, Moscow, Russia, June 27-29, 2017, Revised Selected Papers 11*, Springer, 2018, pp. 95–104.

[109] C. Korner and K. Waaijer, *Mastering Azure Machine Learning Perform large-scale end-to-end advanced machine learning in the cloud with Microsoft Azure Machine Learning*. Microsoft Azure, 2020.

[110] A. Rezazadeh, 'A generalized flow for b2b sales predictive modeling: An azure machine-learning approach,' *Forecasting*, vol. 2, no. 3, pp. 267–283, 2020.

[111] M. Jarschel, T. Zinner, T. Hoßfeld, P. Tran-Gia and W. Kellerer, 'Interfaces, attributes, and use cases: A compass for sdn,' *IEEE Communications Magazine*, vol. 52, no. 6, pp. 210–217, 2014.

[112] J. Ai, H. Chen, Z. Guo, G. Cheng and T. Baker, 'Mitigating malicious packets attack via vulnerability-aware heterogeneous network devices assignment,' *Future Generation Computer Systems*, vol. 111, pp. 841–852, 2020.

[113] A. Kerman, O. Borchert, S. Rose and A. Tan, 'Implementing a zero trust architecture,' *National Institute of Standards and Technology (NIST)*, 2020.

[114] K. Neupane, R. Haddad and L. Chen, 'Next generation firewall for network security: A survey,' in *SoutheastCon 2018*, IEEE, 2018, pp. 1–6.

[115] W. Odom, *CCNA Routing and Switching ICND2 200-101 Official Cert Guide*. Cisco Press, 2017.

[116] A. Ranjbar, *Troubleshooting and Maintaining Cisco IP Networks (TSHOOT) Foundation Learning Guide:(CCNP TSHOOT 300-135)*. Cisco Press, 2014.

[117] T. H. Lenhard and T. H. Lenhard, 'The firewall,' *Data Security: Technical and Organizational Protection Measures against Data Loss and Computer Crime*, pp. 81–83, 2022.

[118] S. Karen and H. Paul, 'Guidelines on firewalls and firewall policy special publication 800-41 revision 1,' U.S. Department of Commerce, National Institute of Standards and Technology, Tech. Rep., 2009.

[119] V. Levi, M. Haniak and E. Hamilton, 'A cost-benefit analysis of the network automation programme,' in *Proceedings of CIRED Conference*, Citeseer, 2007.

[120] S. C. Kantheti and R. Manne, 'Performance and evaluation of firewalls and security,' in *An Interdisciplinary Approach to Modern Network Security*, CRC Press, 2022, pp. 69–87.

[121] N. Marshall, M. Brown, G. B. Fritz and R. Johnson, *Mastering VMware VSphere 6.7*. John Wiley & Sons, 2018.

[122] V. Clowe, M. Albert, P. Benisson, J. Palmer, D. Alton, P. Tea-Duncan and R. Charania, *Network security zoning reference architecture*, https://wiki.gccollab.ca/images/9/9d/Network_Security_Zoning_Reference_Architecture.pdf, 2020.

[123] B. Rababah, S. Zhou and M. Bader, 'Evaluation the performance of dmz,' *International Journal of Wireless and Microwave Technologies*, vol. 1, no. 1, pp. 1–13, 2018.

[124] J. Webb, *Network demilitarized zone (dmz)*, 2014.

[125] J. Kwon, C. Hähni, P. Bamert and A. Perrig, 'Mondrian: Comprehensive inter-domain network zoning architecture.,' in *NDSS*, 2021.

[126] VMware, *Nsx administration guide vmware nsx 4.0*, https://docs.vmware.com/en/VMware-NSX/4.0/nsx_40_admin.pdf, 2023, (accessed: 14.03.2023).

[127] Verizon, *Data breach investigations report*, 2019.

[128] M. Jartelius, 'The 2020 data breach investigations report–a cso's perspective,' *Network Security*, vol. 2020, no. 7, pp. 9–12, 2020.

[129] D. L. Mills, *Network time protocol (version 3) specification, implementation and analysis*, https://datatracker.ietf.org/doc/rfc1305/, 2013.

[130] R. Gerhards, *The syslog protocol*, https://www.rfc-editor.org/rfc/rfc5424, 2009.

[131] Microsof, *Streamline your oss and bss*, https://www.microsoft.com/en-ie/industry/operation-business-support-systems/oss-bss, 2023.

[132] S. Tang, J. Kong, B. Niu and Z. Zhu, 'Programmable multilayer int: An enabler for ai-assisted network automation,' *IEEE Communications Magazine*, vol. 58, no. 1, pp. 26–32, 2020.

[133] N. Azad and S. Hyrynsalmi, 'What are critical success factors of devops projects? a systematic literature review,' in *Software Business: 12th International Conference, ICSOB 2021, Drammen, Norway, December 2–3, 2021, Proceedings 12*, Springer, 2021, pp. 221–237.

[134] P. Robertson, 'Software-defined networking changes the paradigm for mission-critical operational technology networks,' *Schweitzer Engineering Laboratories*, p. 8, 2017.

[135] CISA, *A guide to critical infrastructure security and resilience november 2019*, https://www.cisa.gov/sites/default/files/publications/Guide-Critical-Infrastructure-Security-Resilience-110819-508v2.pdf, 2019.

[136] Statkraft, *Statkraft as annual report 2022*, https://www.statkraft.com/globalassets/1-statkraft-public/05-investor-relations/4-reports-and-presentations/2022/q4-2022/statkraft-as-2022-annual-report.pdf, 2022.

[137] Y. Xin, K. Yang, C.-L. I, S. Shamsunder, X. Lin and L. Lai, 'Guest editorial: Ai-powered telco network automation: 5g evolution and 6g,' *IEEE Wireless Communications*, vol. 30, no. 1, pp. 68–69, 2023. DOI: 10.1109/MWC.2023.10077118.

[138] C. Easttom and W. Butler, 'A modified mccumber cube as a basis for a taxonomy of cyber attacks,' in *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, IEEE, 2019, pp. 0943–0949.

[139] F. K. Tøien, J. Fagermyr, G. Treider and H. Remvang, 'Informasjonssikkerhetsledelse i kraftforsyningen. (Norwegian) [On leadership in information security in power supply systems],' *The power supply must strengthen the work with ICT security*, 2021. [Online]. Available: https://publikasjoner.nve.no/faktaark/2021/faktaark2021_02.pdf.

[140] F. K. Tøien, J. Fagermyr, G. Treider and H. Remvang, 'IKT-sikkerhetstilstanden i kraftforsyningen 2021. (Norwegian) [On information security in power supply systems],' *The power supply must strengthen the work with ICT security*, 2021. [Online]. Available: https://publikasjoner.nve.no/eksternrapport/2021/eksternrapport2021_19.pdf.

[141] F. K. Tøien, J. Fagermyr, G. Treider and H. Remvang, 'Sikring av driftskontrollsystemer. (Norwegian) [On information security in power supply systems],' *The power supply must strengthen the work with ICT security*, 2021. [Online]. Available: https://publikasjoner.nve.no/faktaark/2021/faktaark2021_03.pdf.

[142] P. D. Leedy and J. E. Ormrod, *Practical research Planning and Design Eleventh Edition*. Pearson Custom Saddle River, NJ, USA, 2015, vol. 108.

[143] P. H. Meland, Y. F. F. Bayoumy and G. Sindre, 'The ransomware-as-a-service economy within the darknet,' *Computers & Security*, vol. 92, p. 101 762, 2020.

[144] OWASP, *Owasp top ten*, https://owasp.org/www-project-top-ten/, 2021, (accessed: 01.02.2023).

[145] S. Mathew and J. Varia, 'Overview of amazon web services,' *Amazon Whitepapers*, vol. 105, pp. 1–22, 2014.

[146] C. Paulsen, 'Glossary of key information security terms,' National Institute of Standards and Technology, Tech. Rep., 2018.

[147] S. Cybersecurity, V. Clifton and R. Hat, 'Guide to ipsec vpns,' *NIST Special Publication*, vol. 800, p. 77, 2020.

[148] K. McKay and D. Cooper, 'Nist special publication 800-52 revision 2: Guidelines for the selection, configuration, and use of transport layer security (tls) implementations,' *DOI*, vol. 10, pp. 800–52, 2017.

[149] A. DeKok and G. Weber, 'Radius design guidelines,' Tech. Rep., 2011.

[150] Juniper, *What is unified threat management?* https://www.juniper.net/us/en/research-topics/what-is-utm.html, 2023, (accessed: 05.02.2023).

[151] J. Zerbst, M. Schaefer and I. Rinta-Jouppi, 'Zone principles as cyber security architecture element for smart grids,' in *2010 IEEE PES innovative smart grid technologies conference Europe (ISGT Europe)*, IEEE, 2010, pp. 1–8.

[152] B. Bilger, A. Boehme, B. Flores, Z. Guterman, M. Hoover, M. Iorga, J. Islam, M. Kolenk, J. Koilpilla, G. Lengyel, G. Ludlow, T. Schroeder and J. Schweitzer, *Sdp specification 1.0*, 2014.

[153] H. Boyes, B. Hallaq, J. Cunningham and T. Watson, 'The industrial internet of things (iiot): An analysis framework,' *Computers in industry*, vol. 101, pp. 1–12, 2018.

[154] OWASP, *Who is the owasp® foundation?* https://owasp.org/, 2023, (accessed: 01.02.2023).

[155] CWE, *2022 cwe top 25 most dangerous software weaknesses*, https://cwe.mitre.org/top25/archive/2022/2022_cwe_top25.html, 2023, (accessed: 01.02.2023).

[156] Y. Li and Q. Liu, 'A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments,' *Energy Reports*, vol. 7, pp. 8176–8186, 2021.

[157] CWE, *Cwe-509: Replicating malicious code (virus or worm)*, https://cwe.mitre.org/data/definitions/509.html, 2023, (accessed: 01.02.2023).

[158] A. Agence National De La Securite Des Systemes D'information, *Ryuk ransomware*, https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-006.pdf, 2021, (accessed: 01.02.2023).

[159] CWE, *Cwe-89: Improper neutralization of special elements used in an sql command ('sql injection')*, https://cwe.mitre.org/data/definitions/89.html, 2023, (accessed: 01.02.2023).

[160] CWE, *Cwe category: Data neutralization issues*, https://cwe.mitre.org/data/definitions/137.html, 2023, (accessed: 01.02.2023).

[161] OWASP, *A03:2021 – injection*, https://owasp.org/Top10/A03_2021-Injection/, 2023, (accessed: 01.02.2023).

[162] CWE, *Cwe-918: Server-side request forgery (ssrf)*, https://cwe.mitre.org/data/definitions/918.html, 2023, (accessed: 01.02.2023).

[163] OWASP, *A10:2021 – server-side request forgery (ssrf)*, https://owasp.org/Top10/A10_2021-Server-Side_Request_Forgery_%28SSRF%29/, 2023, (accessed: 01.02.2023).

[164] CWE, *Cwe-79: Improper neutralization of input during web page generation ('cross-site scripting')*, https://cwe.mitre.org/data/definitions/79.html, 2023, (accessed: 01.02.2023).

[165] KirstenS, *Cross site scripting (xss)*, https://owasp.org/www-community/attacks/xss/, 2023, (accessed: 01.02.2023).

[166] U. K. Singh, C. Joshi and D. Kanellopoulos, 'A framework for zero-day vulnerabilities detection and prioritization,' *Journal of Information Security and Applications*, vol. 46, pp. 164–172, 2019.

[167] M. Albanese, S. Jajodia, A. Singhal and L. Wang, 'An efficient approach to assessing the risk of zero-day vulnerabilities,' in *2013 International Conference on Security and Cryptography (SECRYPT)*, IEEE, 2013, pp. 1–12.

[168] OWASP, *Manipulator-in-the-middle attack*, https://owasp.org/www-community/attacks/Manipulator-in-the-middle_attack, 2023, (accessed: 01.02.2023).

[169] OWASP, *Man-in-the-browser attack*, https://owasp.org/www-community/attacks/Man-in-the-browser_attack, 2023, (accessed: 01.02.2023).

[170] OWASP, *Trojan horse*, https://owasp.org/www-community/attacks/Trojan_Horse, 2023, (accessed: 01.02.2023).

[171] Mininet, *Mininet overview*, http://mininet.org/overview/, 2023, (accessed: 06.02.2023).

[172] P. S. Anton, R. H. Anderson, R. Mesic and M. Scheiern, *Finding and fixing vulnerabilities in information systems: the vulnerability assessment and mitigation methodology*. Rand Corporation, 2004.

[173] P. Bitra and C. S. Achanta, *Development and evaluation of an artefact model to support security compliance for devsecops*, 2021.

Acronyms

3D Three Dimentional. 81

ACL Access Control List. 64, 151–153, 166

AI Artificial Intelligence. viii, 55, 57, 59, 113, 115, 118, 197, 198, 317, 322

ANN Artificial Neural Networks. 197

API Application Programming Interface. vii, viii, 17, 39–42, 50, 51, 55, 59, 69, 72, 73, 81, 84, 104, 193, 196, 219, 248, 266, 282

APT Advanced Persistent Threat. 197

ARP Address Resolution Protocol. 145, 168

AWS Amazon Web Services. 74, 149, 150

BSS Business Support Systems. 43

BYOD Bring Your Own Device. 51, 67

CA Certificate Authority. 154

Capex Capital expenditures. 72

CCAM Combination Cube Analysis Model. viii, 7, 11, 14, 22, 80, 81, 84–86, 89, 91, 115–117, 142, 261

CCNA Cisco Certified Network Associate. 119, 235

CCNP Cisco Certified Network Professional. 119, 235

CCSA Check Point Certified Security Administrator R81. 119

CD Continuous Delivery. 45

CI Continuous Integration. 45, 47

CI/CD Continuous Integration and Continuous Delivery. 45, 46, 109, 196, 216, 248, 266–268, 292, 312, 315

CIS Critical Infrastructure Sectors. 3–6, 10, 15, 18–20, 32, 40, 42, 70–72, 74, 78, 97–99, 105, 110, 114, 116, 117, 141, 147, 153, 163, 164, 168, 191, 196, 198, 200, 204–206, 208, 217, 231, 271, 272, 275, 312

CLI Command-Line Interface. 37, 50, 69, 203, 204

CWE Common Weakness Enumeration. 17, 165, 166

DC Data Center. 158, 159, 161, 162

DDoS Distributed Denial of Service. 53, 57, 58, 68, 74, 75, 78, 79, 153, 167, 200, 209, 210

DevAsc DevNet Associate. 236, 253

DevNet Developer Network. 5, 60, 94, 119, 169, 171, 172, 237, 315

DevNetOps Development Network Operations. 45

DevOps Development and Operations. 43–47, 49, 55, 65, 102, 106, 108, 109, 212, 213, 217, 225, 226, 240, 241, 267, 270, 271, 292, 295, 312, 315

DevSecOps Development Security Operations. 45

DL Deap Learning. 197

DMZ Demilitarized Zone. ix, 18, 19, 26, 29, 30, 33, 69, 84, 99, 110, 148, 155–157, 163, 164, 202–205, 207, 212, 227, 228, 279

DoS Denial of Service. 68, 74, 75, 79, 147, 150, 154, 167, 200, 209, 210

EMA Enterprise Management Associates. 8, 63, 65, 94, 194, 195

FWaaS Firewall as a Service. 153

GDPR General Data Protection Regulation. 9, 10

Git Global Information Tracker. 45, 51, 196

GNS3 Graphical Network Simulator-3. 60, 71, 94, 169–171, 238, 315

GUI Graphical User Interface. 29, 31, 64, 171, 203–206

HTTP Hypertext Transfer Protocol. 155

HTTPS Hypertext Transfer Protocol Secure. 146

IaaS Infrastructure as a Service. 49, 152, 153, 192, 209, 210

IaC Infrastructure as Code. 26, 27, 84, 100, 101, 108, 175, 212, 214, 216, 219, 222, 225, 226, 232, 233, 246–248, 251, 265–268, 284–286, 302, 307

IDS Intrusion Detection Systems. 41, 53, 58, 73, 75, 77, 151, 153, 154, 156, 167, 204

IIoT Industrial Internet of Things. 3, 200

IoT Internet of Things. 73, 113, 142, 171, 172, 196, 200

IPS Intrusion Prevention Systems. 41, 73, 151, 153, 154, 156, 204

IPv4 Internet Protocol version 4. 194

IPv6 Internet Protocol version 6. 194

ISP Internet Service Provider. 64, 200, 209

IT Information Technology. 4, 8, 14, 20, 43, 44, 61, 62, 65, 84, 93–110, 112, 114, 117, 119, 143, 144, 147, 153, 163, 195, 197, 200, 211, 214–217, 220, 223, 224, 226, 227, 229–233, 235, 237–241, 243, 244, 246, 248–250, 252, 253, 255, 257–259, 261, 263–265, 267–271, 274–276, 283, 285–293, 295, 299, 300, 302, 303, 306, 311–316

ITAT Information Technology Actors Triangle. viii, 7, 82, 83, 89, 95, 109, 117, 261, 265

ITIL Information Technology Infrastructure Library. 119

JSON JavaScript Object Notation. 49, 50

KNN K-Nearest Neighbors. 197

LAN Local Area Network. 157, 158

LB Load Balencer. 72, 73, 195

LDAP Lightweight Directory Access Protocol. 152

MAC Media Access Control. 145, 168

MANO Management and Network Orchestration. 42, 43

Mbps Megabits per second. 199

MFA Multi-factor authentication. 155, 162

MitB Man-in-the-Browser. 167

MitM Man-in-the-Middle. 75, 79, 167, 168

ML Machine Learning. viii, 8, 11, 21, 22, 24–28, 33, 35, 53–60, 62, 63, 75, 77, 84, 100, 101, 104, 108, 115, 118, 142, 150, 162, 169, 170, 174, 175, 192, 194, 196–200, 209, 212, 214, 216, 219, 222, 232, 233, 246, 247, 251, 263, 264, 266, 284–286, 307

NaaS Network as a Service. 93, 94, 313, 315

NAC Network Access Control. 152, 204

NAP Network Access Protection. 152

NAPALM Network Automation and Programmability Abstraction Layer with Multivendor support. 51, 74

NAT Network Address Translation. 42, 64, 151, 158

NETCONF Network Configuration Protocol. 36, 37, 41, 50, 72, 73, 196

NetZTP Network Zero Touch Provisioning. 66, 67

NFV Network Function Virtualization. 22, 35, 42–44, 63, 192, 196–198

NGFW Next-Generation Firewalls. 150

NGFWs Next-Generation Firewalls. 153, 154, 191

NIC Network Interface Card. 40, 148, 170

NIST National Institute of Standards and Technology. 151, 191, 192

NSA Network Security Automation. viii, 4–6, 11, 15, 17, 18, 20, 22, 24–28, 34, 35, 43, 44, 51, 53, 54, 59–63, 66–69, 75, 76, 79, 84, 91, 110, 112–118, 141, 142, 144, 192, 232, 236, 238–240, 242, 244, 246, 248–250, 252, 254–260, 262–270, 272, 273, 278–280, 282–286, 288–305, 307, 308, 310

NTNU Norwegian University of Science and Technology (Norges Teknisk-Naturvitenskapelige Universitet). 114, 119, 141, 143

NTP Network Time Protocol. 37

NVE Norwegian Water Resources and Energy Directorate. 119

Opex Operational Expenditure. 72

OS Operating System. 149, 152, 153, 166, 243

OSI model Open Systems Interconnection model. ix, 10, 17, 145, 146, 149, 194

OSS Operations Support Systems. 43

OWASP Open Web Application Security Project. 17, 68, 149, 150, 165

PaaS Platform as a Service. 49, 152, 153, 192

PC Personal Computer. 19, 40, 148, 170

PCA Principal Component Analysis. 197

PDU Protocol Data Unit. 145, 146

QoE Quality of Experience. 194, 200

QoS Quality of Service. 19, 41, 72, 74, 77, 194, 199, 200

RaaS Ransomware as a Service. 147

RADIUS Remote Authentication Dial In User Service. 152

RDP Remote Desktop Protocol. 161, 162

REST Representational State Transfer. 40, 55, 72, 73, 193

RESTCONF Representational State Transfer Configuration Protocol. 36, 41, 50, 72, 73

RL Reinforcement Learning. 197

ROI Return on Investment. 9, 55, 62, 66, 72

RPC Remote Procedure Call. 72, 73

RPCs Remote Procedure Calls. 50

RQ Research Question. xiii, 1, 6, 11, 13, 14, 22, 23, 28, 29, 35, 36, 39, 42, 44, 51, 53, 59–62, 69, 74, 76, 89–91, 96–100, 102, 104, 109, 111, 112, 117, 140, 141, 144, 148, 176, 190, 192, 193, 197, 198, 200, 226, 227, 229–234, 236, 238–240, 242, 244–246, 248–250, 252, 254–260, 262–270, 272, 273, 275–280, 282, 284–286, 288–294, 296–305, 307, 308

SaaS Software as a Service. 147, 152, 153, 192, 209, 210

SCADA Supervisory Control and Data Acquisition. 3

SCM/VCM Supply Chain Management/Value Chain Management. 47

SDN Software-defined Networking. vii, viii, 21, 22, 24–27, 35, 38–43, 51–58, 62–64, 66–68, 70–79, 84, 100, 101, 104, 108, 162, 163, 166–170, 172, 174, 175, 192–201, 212, 214, 216, 219, 222, 232, 233, 246–248, 251, 264–266, 284–286, 307

SDP Software Defined Perimeter. 162, 163

SFTP Secure File Transfer Protocol. 146

SL Supervised Learning. 197

SNMP Simple Network Management Protocol. 37, 41

SOM Self-Organizing Maps. 197

SotA State-of-the-Art. viii, xiii, 1, 6–8, 11, 13, 14, 17, 20, 22–25, 27–36, 42, 44–46, 48–50, 53–58, 60–64, 66–75, 81–84, 90–92, 94, 96, 98, 102, 104, 107, 113, 115, 117, 118, 141, 142, 144, 145, 164, 165, 167–170, 174, 176, 190, 191, 200–203, 205, 228, 231, 236, 238–240, 242, 243, 246, 248, 250, 252, 255, 257–270, 273, 277, 280, 283–287, 289–294, 298–305, 307, 308, 310, 315

SQL Structured Query Language. 166

SQL Injection Structured Query Language Injection. 149, 150, 166

SSH Secure Shell. 37, 67, 146

SSL Secure Socket Layer. 152

SSL/TLS Secure Socket Layer/Transport Layer Security. 146, 152

SSRF Server-Side Request Forgery. 149, 153

SVM Support Vector Machine. 197

SWOT Strengths, Weaknesses, Opportunities, and Threats. vii, 2, 5–8, 10, 11, 14–17, 22, 26, 27, 29–34, 60, 61, 76, 79, 90, 91, 113, 115, 116, 142, 200–203, 205, 207, 208

syslog System Logging Protocol. 37

TCP Transmission Control Protocol. 146

TCP/IP Transmission Control Protocol/Internet Protocol. 145

TLS Transport Layer Security. 152

UDP User Datagram Protocol. 146

USL Unsupervised Learning. 197

UTM Unified Threat Management. 154

vApp virtual Application. 159–161

vCenter virtual Center. 159

VFs Virtual Firewalls. 153

VLAN Virtual Local Area Network. 18, 50, 73, 203

VM Virtual Machine. 21, 52, 72, 78, 153, 157, 159, 160, 192, 193

VNF Virtual Network Functions. 42, 43

VPN Virtual Private Network. 147, 152–155, 166, 204

WAF Web Application Firewall. 149, 150, 153

WAN Wide Area Network. 70, 153

Wi-Fi Wireless Fidelity. 113

XML Extensible Markup Language. 49, 50

XSS Cross-Site Scripting. 149, 150, 153, 166

YAML Yet Another Markup Language. 49, 50

YANG Yet Another Next Generation. 49, 50

ZTA Zero Trust Architecture. 21, 29, 33, 53, 54, 58, 115, 162, 163, 208–210

Appendix A

In-Depth Methodology Insights

In this appendix, we present additional information about each step in our methodology.

Problem Description and Definition of RQs

In the initial stages of this thesis, we meticulously outlined our research plan and precisely defined the problem under investigation. This process culminated in the formulation of a hypothesis. Subsequently, we developed a set of RQs aligned with the hypothesis, as detailed in Chapter 1, Section 1.7.

In light of our available resources and research capabilities, we have determined that our research approach will encompass both Qualitative Exploratory[1] and Descriptive[2] methodologies. This choice aligns with our overarching goal of assessing the validity of the initial hypothesis.

Our selected research approach is designed to facilitate the resolution of our research questions using a meticulously documented process. This documentation will be crafted in a manner accessible to our defined audience, ensuring a comprehensive understanding of the procedure and enabling the replication of the process to yield consistent results.

---

[1] A Qualitative Exploratory research method is where the researcher uses nonnumerical data and build the theory on observations [142, p. 98-102]. On the one hand, the complexity of the problem makes us follow a qualitative research method. On the other hand, this method is more suitable for our research as we don't have access to statistical and numerical data related to our topic. Also, our research is exploratory as we are investigating a problem that has not been clearly defined before now.

[2] A Descriptive research method is where we plan to research the current situation without any modification in the circumstances or any attempt to find the cause-and-effect relations of the facts [142, p. 154]. So from this aspect, we mean that our research will be descriptive.

Data Gathering Through the Study of the State-of-the-Art

We conducted a comprehensive review of the SotA to document various network security management techniques. The selection criteria for these documents prioritized the most recent articles relevant to our research topic. Additionally, our document search was guided by the keywords outlined in Chapter 1, Section 1.2, providing the foundation for our subsequent data collection processes, including interviews and addressing RQ1 and RQ2. This approach also informed our hypothesis evaluation.

Within the SotA data collection phase, we meticulously identified and cataloged works directly pertinent to our RQs, as presented in Chapter 1, Section 1.10. This step helped us streamline our research focus.

Our data-gathering efforts encompassed papers, books, and information germane to firewalls and traditional network security methods and architecture, specifically addressing RQ1[3]. We concentrated on network security methods and techniques most applicable to large-scale networks, particularly within Critical Infrastructure Sectors (CIS), which aligns with the core focus of our study. This approach was designed to prevent scope creep and ensure alignment with the problem description detailed in Chapter 1. The problem description underscores the underutilization of Network Security Automation (NSA) techniques and technologies within CIS networks.

Subsequently, we acquired data about existing NSA techniques and technologies, as well as recommendations for their implementation to address RQ2. In this context, we included a wide array of works, papers, books, and scholarly materials, all of which also suggested the incorporation of machine learning as a complementary and essential technology to enhance the efficiency of NSA. For information gathering, we extensively utilized reputable scientific databases, including Google Scholar, ScienceDirect, IEEE Xplore, Research Gate, Springer Link, OPTICA Publishing Group, IOPScience, Penn State (psu.edu), Taylor & Francis Group, Hindawi, and Gartner, to meticulously search for and retrieve the relevant documents.

Furthermore, we leveraged textbooks and study materials that were part of our curriculum at the Norwegian University of Science and Technology (Norges Teknisk-Naturvitenskapelige Universitet) (NTNU). Notably, study materials such as those authored by Morris, K. [79], Odom, W. [26], Odom, W. [115], Froom, R., & Frahim, E. [28], Teare, D., Vachon, B., & Graziani, R. [27], and Ranjbar, A. [116] were instrumental. Additionally, materials used in our professional journey to attain network-related certifications, including resources like Jackson, Chris, et al. [10] and Dahir, Hazim, et al. [17], greatly expedited our research process while

---

[3] By traditional we mean everything that is not utilizing automation techniques, and therefore, even the research on micro-segmentation network security methodology is also counted as traditional as even this method is not originally based on automation techniques, but it has the potential to be automated as we will explain in Chapter 4.

enriching our findings.

These resources are characterized by their substantial volume and could be excessively time-consuming to fully digest. Moreover, technical resources of this nature, often published by specific companies, may not be readily discoverable through research engines like Google Scholar, which we mentioned earlier as one of our search engines for the SotA. Fortunately, the direct relevance of our research to our professional responsibilities granted us access to these materials, initially studied during the pursuit of network certifications, such as those on network development, network engineering, and network automation technologies. During our resource analysis, we also explored the sources cited within the primary works under review, using them as secondary resources to supplement our SotA study.

Given the vast number of scientific articles related to network automation, we placed a premium on the most recent publications unless a paper presented unique insights crucial to our research. Furthermore, some scientific resources, while related to network automation, also extended to other technologies beyond the scope of network security and firewalls. In such cases, we decided to either exclude the resource or incorporate those containing pertinent information for our investigation. For example, Jiang, W., Strufe, M., & Schotten, H. [56] delved into ML technology in 5G network systems, while ARZO, Sisay Tadesse, et al. [6] offered insights into IoT network automation. Notably, [6] discussed challenges and opportunities associated with network automation, and [56] contained sections about ML in conjunction with network automation, both of which held relevance for our research.

Result Evaluation, Analysis, and Reflection

Likewise, we conducted an extensive evaluation and analysis of the SotA study's results. Our approach began with a systematic SWOT analysis of the network security methods elucidated earlier. Subsequently, we devised a novel model termed the Combination Cube Analysis Model (CCAM). This model was designed to visually represent the intricate landscape of the complexities in network security by delineating various dimensions that could be flexibly combined in diverse configurations. Each dimension corresponds to the results previously presented in Chapter 4.

Moreover, our findings underscore the potential for integrating diverse network security techniques within each dimension of the CCAM, thereby introducing additional complexity to the decision-making process for those tasked with configuring and implementing NSA solutions. The comprehensive analysis derived from our investigation into existing network security management and automation techniques is expounded upon in Chapter 4, providing valuable insights into the field.

Data Validation Through the Interviews and Surveys

For data validation, we employed a combination of surveys and interviews. Microsoft Forms was utilized for the surveys due to their simplicity and the absence of personally identifiable information in the questions. The survey collected general background information, such as the respondent's occupation and years of work experience, with all responses anonymized. This ensured that no individual's answers could be linked back to them, their company, or any other identifying information.

As stipulated in our pre-survey communication, once participants submitted their responses, we could not separate their contributions from the overall results unless they provided additional identifying information. Participants were also given the option to immediately download their responses in a PDF format for their records.

Similarly, our approach to interviews prioritized participant anonymity. We neither recorded nor disclosed any information that could identify individuals. Instead, we referred to quotes in a general and unidentifiable manner, such as 'an experienced IT security employee' or 'a new beginner network engineer'. This continuous anonymization ensured that no data could be traced back to specific participants or their affiliated companies.

To further protect the privacy of participants and their organizations, we refrained from disclosing the number or names of companies involved in the research. This decision was made to prevent any correlation between the answers provided and the participants' respective employers. Importantly, we had no formal agreements with these companies; individuals voluntarily participated in our research.

We conducted a comprehensive review of the regulations outlined in the Data Processor Agreement (DPA)[4], and presented by NTNU. Subsequently, we made a deliberate decision to report our research to Sikt, given that our validation method consisted of surveys and interviews. This decision was motivated by our collection of certain background information from participants, even though the surveys were promptly and thoroughly anonymized.

It is crucial to emphasize that beyond the anonymized background data we collected, we took rigorous measures to ensure that no sensitive personal information was gathered through our surveys or interviews. Furthermore, we diligently informed all participants about the strict confidentiality and anonymity protocols in place, while also communicating their rights in the research process.

In our communication with participants, the email containing the survey link included an attached PDF file outlining the ethical and legal considerations we

---

[4] Data processor agreement (DPA) mandates that individuals conducting research involving personally identifiable data must report it to Sikt in advance.

had established to safeguard their rights and data privacy (see Section 1.11 for the contents of this file).

The survey questions were divided into three parts. The first section consisted of general questions addressed to both groups of participants: scientific personnel and IT professionals. The second section was customized for each group based on their specific knowledge and experience areas, as detailed in Chapter 5.

The interview questions, as outlined in Chapter 5, Section 5.1, were formulated based on our study of the SotA in traditional network security management and NSA techniques and technologies. This approach aimed to address RQ3 and validate our research results and hypotheses. Interviews were conducted with individuals possessing significant expertise in our research area, including university professors and technical personnel with practical experience in network security solutions.

The individuals from the IT professional community, who were employed across various companies and specialized in diverse network security solutions and architectures, possessed a wealth of expertise. Their extensive competencies, including those in network architectures and network engineering, made them an ideal population for our validation process. We harnessed their extensive knowledge and experience through both surveys and interviews to underpin our validation process. The outcomes of this validation process are detailed in Chapter 5.

Conclusion

After successfully verifying the results through in-depth surveys and interviews, we meticulously assessed these findings concerning our initial hypotheses. This critical analysis allowed us to determine whether our hypotheses were substantiated, disproven, or required further justification. In cases where the hypotheses were found to be incorrect or in need of additional substantiation, we recommend a subsequent research iteration on this subject as future work. This next phase of research can incorporate new hypotheses to advance our understanding. For a detailed discussion and comprehensive conclusions, please refer to Chapter 6.

Appendix B

Glossary

This glossary will elaborate on key concepts used throughout this thesis. Its purpose is to equip readers with the essential complementary background knowledge related to the terms and concepts extracted from the SotA and employed in this thesis. This understanding will aid readers in comprehending the thesis content more effectively.

B.1 OSI Model Overview

This section explains the Open Systems Interconnection model (OSI model) model in brief. This is because we will be using the concepts related to this model in our thesis. Transmission Control Protocol/Internet Protocol (TCP/IP) which was introduced with four layers in the 1970s has evolved through the years and become the OSI model we know today with seven layers of physical, data link, network, transport, session, presentation, and application as shown in Figure B.1 [26, Chapter 1 p. 33].

In the OSI model we know today, the physical layer, which for instance, consists of cables, pins, and the medium for the transmission, is responsible for transmitting and receiving the bit streams through this channel. The second layer, data link, utilizes frame Protocol Data Unit (PDU), and it is the layer that transmits data frames based on the Media Access Control (MAC)[1] address of the connected nodes. For instance, the Address Resolution Protocol (ARP)[2] protocol which utilizes MAC addresses works with the data frames exchanged at this layer [26, Chapter 1 p. 34].

---

[1] Working on data link layer, a MAC address refers to the address allocated to each interface of a network device and rarely used as the information needed for the filtering done by the firewalls [118, p. 1]

[2] While operating at the data link layer of the OSI model, ARP protocol contributes to providing an overview of the MAC addresses of the devices and their connected IP addresses for mapping the network [26, Chapter 4].

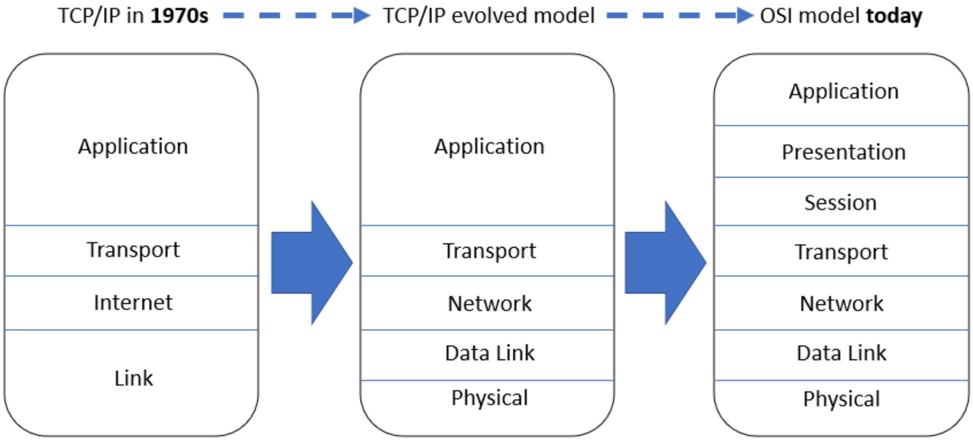


Figure B.1: Evolution of OSI model. The figure is inspired by Figure 1-15 at [26, Chapter 1 p. 33].

The third layer, network, is the layer that works with routing traffic, transmits the IP address of the interfaces, and utilizes packet PDU. Transport which is the fourth layer in the OSI model, transmits segment PDU and while working with hosts and firewalls, utilizes protocols such as Transmission Control Protocol (TCP) [3] and User Datagram Protocol (UDP) [4].

Layers five, six, and seven, the session, presentation, and application layers, utilize data PDU with protocols such as Secure Shell (SSH)[5], Hypertext Transfer Protocol Secure (HTTPS)[6], or Secure File Transfer Protocol (SFTP)[7] to work with hosts and firewalls. The functionality of these three layers, however, differs from each other. The session layer manages session communications between two nodes, while the presentation layer focuses on character encoding, encryption, decryption, or even data compression which means negotiating data formats. The application layer opens an interface to make communication between humans and the network possible at this layer [26, Chapter 1 p. 34].

---

[3] Slower than UDP, TCP connection-oriented network protocol ensures that the lost transmitted data are retransmitted [26, Chapter 5].

[4] More used for services such as video and voice streaming applications that require low latency in data packet transfer, UDP is a network protocol for the transmission of data with high efficiency and speed in contrast to TCP and does not ensure package reception [26, Chapter 5].

[5] SSH is the protocol used to provide secure access terminal for users to the network devices [26].

[6] The extension of Hypertext Transfer Protocol (HTTP), HTTPS, provides secure communication at the network layer by encryption of data using SSL/TLS protocols and operates on port 443 [26].

[7] SFTP is the protocol used to facilitate transferring of files through the network traffic in an encrypted and secure manner [26, p. 920].

B.2 Detailed Examples on Cyberattacks Targeting Critical Infrastructure Sectors

This section delves into notable instances of cyber attacks on Critical Infrastructure Sectors (CIS). Examining specific cases illustrates the vulnerabilities within these systems and underscores the imperative for advanced security measures. The presented examples include a supply chain attack on SolarWinds Orion, a cyberattack on Ukraine Power Grid, and a ransomware attack on Colonial Pipeline in the United States which are instances of large CIS networks. Each case sheds light on the urgency for novel methods, such as automation technology, to fortify the security of large networks [33].

The platform **SolarWinds** Orion provides network monitoring software for their customers. This IT administration tool for monitoring of both on-premise, SaaS, and hybrid network infrastructures was a target of a supply chain attack cybercriminals in March 2020 where 18,000 customers who utilized this monitoring software, unknowingly updated their systems with malicious payloads put into the update package [36]. The SolarWinds network monitoring tool is provided for the monitoring and administration of big networks, which means the customers were big companies who provide services in CISs, and consequently, the society that suffered from this cyberattack [36].

The cyberattack on **Ukraine Power Grid** was conducted utilizing the BlackEnergy 3 malware to target the CIS environment. This cyberattack, which took place in December 2015, caused a service outage for more than 225,000 Ukrainian people [37, p. iii-vi]. In this cyberattack, the cybercriminals, among others, utilized a Virtual Private Network (VPN) connection to access the critical infrastructure network after conducting a phishing attack through email. A phishing attack that was functional and installed the BlackEnergy 3 malware on the client device, which at the end of a cyber kill chain[8] ended with the power outage and making the systems unavailable [37, p. 9]. Another one of the several attack vectors utilized in this cyber attack was a Denial of Service (DoS) attack on their central call service [37, p. 2].

The ransomware attack on **Colonial Pipeline** which ended with the company paying $4.4 million in bitcoin to cyber criminals and still not being able to solve the encrypted systems causing more than 16,000 gas stations in the United States to fall out of service to the customers and remaining shut down in six days [31, p. 1]. This cyberattack mainly targeted the payment system which made it impossible for customers to pay and consequently not be able to purchase the product [31, p. 1]. This cyberattack at the same time is one of the instances of Ransomware as a Service (RaaS) where the cyber attackers do not need to have much knowledge about how to conduct the attack but rather they only need to order the attack and

---

[8] The series of the stages of a cyberattack to be explained is called a cyber kill chain. Defining these steps makes it easier to understand and analyze different parts of a cyberattack [37].

pay for the order, so ransomware operators will accomplish their evil requested goal [31, 143].

B.3 Traditional Network Security Technique and Technologies - Contextualizing RQ1

This section offers essential background information on traditional network security techniques and technologies to enhance the reader's comprehension. It covers topics such as IP network firewalls, basic network security strategies, Demilitarized Zone (DMZ), zone-based, micro-segmentation, and zero-trust network security architectures. These concepts serve as the foundational knowledge supporting the answers to Research Question (RQ)1.

B.3.1 IP Network Firewalls and Basic Network Security Strategies - RQ1

By IP network, we mean connecting computer devices by using Internet Protocol (IP) to make communication between them possible. These devices in an IP network could be a PC, router, switch, or even other types of devices that exist and have the potential to communicate in a network by receiving an IP address per Network Interface Card (NIC) [26].

A firewall could be software or hardware and is used to separate IP networks and control the communication between them based on the rules we determine. The rules we set could be various. For instance, we can filter network packets based on their source or destination address, their port or application type, or even other preferences we have in filtering the traffic flow [117]. There are two approaches to setting up the filtering rules. We can use whitelisting or blacklisting of the network traffic [64].

Blacklisting: Black listing is a method of filtering the network communication flow where specific resources will be registered in a list to be blocked. Other than the blocked resources, all communications are allowed to take place [64].

Whitelisting: In the whitelisting method, all communication is denied other than those specifically allowed. This means that the firewall blocks everything other than the rules applied to allow the specific communication to take place [64]. This is also called zero-trust network security architecture [39].

Firewall Structures

There are many different types of firewalls, both software and hardware, with differences in how they filter the packets. In this section, we present some of the firewall types. Dividing firewalls based on their structure, there are hardware firewalls, software firewalls, or a hybrid combination of these two. This section keeps firewall products that are the commercial side of the case explained in the footnotes to not mix them with the scientific reviews of firewall concepts.

Hardware Firewall: These are physical devices provided by different companies to be purchased and configured by the administrators. Hardware firewalls are usually beneficial for companies with a significant amount of devices and more extensive networks to protect. The advantage of using hardware firewalls is that the software that is to be installed on the physical device will have the CPU and RAM needed available on the hardware firewall and will be more optimal in functionality [67].

Software Firewall: Contrary to hardware firewalls that are provided with the computing resources needed, software firewalls will require using the CPU and RAM of the host device and need to be managed manually by an administrator. These applications need to be installed and configured to further block unwanted and allow other network traffic. Both whitelisting and blacklisting methods have been utilized to configure software firewalls [67].

Firewall Types

Dividing firewalls based on how they operate in different categories, there are host-based, application-based, and network-based firewalls explained below:

Host-based Firewalls: By host/based firewalls we mean the software firewalls that are to be installed on a host, such as on a computer or a single device. Instances of host-based firewalls are many. Here we can name Windows Security Defender[9] without extra costs after purchasing a computer device with Windows OS, and McAfee[10] with extra costs for users, as examples of host-based firewall applications. In the instances of host-based firewalls we named here, one can do extra configurations on the firewall software to filter and drop unwanted packet traffic and allow the other resources. Otherwise, they will be managed centrally by their supplier [29].

Web Application Firewalls: Web applications have since long been attractive targets for cyber-attacks such as Server-Side Request Forgery (SSRF) or injection [144]. Web application firewalls are to protect websites against cyber-attacks that target web application vulnerabilities and provide better security at the seventh Layer in the OSI model explained in Section 3.2 [29]. Some examples of web application firewalls include Azure Web Application Firewall (WAF)[11], Amazon

---

[9] Provided by Microsoft, Windows Security Defender is a host-based firewall to Windows Operating System (OS) users for protecting their computer devices against cyber threats.

[10] McAfee is mentioned here as an example for host-based firewall applications that provide security for user devices.

[11] The cloud-native application firewall Azure Web Application Firewall, protects web applications in the cloud against known security threats such as Cross-Site Scripting (XSS) or Structured Query Language Injection (SQL Injection). WAF follows Open Web Application Security Project (OWASP) Top Ten web application vulnerabilities, published yearly, to provide security for their customers'

Web Services (AWS)[12] WAF[13], F5 NGINX[14], F5 BIG-IP Advanced Web Application Firewall (Advanced WAF)[15], Citrix Web App Firewall[16], FortiWeb[17], Qualys WAF[18] [110, 121].

Network Firewalls: Network firewalls are the firewalls that secure the IP networks by using stateful traffic inspection both for ingress and egress network traffic [114]. As some of the network firewall instances in the current market, we can name FortiGate[19], Check Point Quantum[20], Cisco Secure Firewall[21], Azure Firewall[22], F5 BIG-IP Advanced Firewall Manager[23], VMware NSX Distributed Firewall[24], vSRX Series by Juniper[25], and Cisco Umbrella[26]. The firewalls that are mentioned above can be used not only for on-premise solutions but also for cloud-native and virtual solutions [110, 121, 126].

---

web applications [144].

[12] AWS applies to one of the cloud service providers which offer their services to everyone with a pay-as-you-go policy for the payments [145].

[13] AWS WAF allows one to protect their web applications by creating policies, blocking or filtering, and monitoring the network traffic. Examples of common cyber threats that this application protects against are Cross-Site Scripting (XSS) and SQL Injection briefly explained in Appendix B.

[14] F5 NGINX provides a scalable firewall solution for the security of NGINX web application instances.

[15] F5 BIG-IP Advanced Web Application Firewall (Advanced WAF) has focused on cyber security based on the OWASP Top Ten web application vulnerabilities that are published per year. As instances of their security measures, we can name defense against Denial of Service (DoS) attacks and encryption of the Layer seven data traffic to protect against man-in-the-browser attacks.

[16] Citrix Web App Firewall is a firewall for web applications. For instance, it protects against loss of data or malicious manipulation of the website. Instances of the known cyber attacks that this application protects the websites against are XSS and SQL Injection.

[17] FortiWeb is a type of WAF that protects against malicious cyber attacks by leveraging Machine Learning (ML). This is interesting regarding our work as we have focused on what applications are almost ready to leverage automation of network and firewall implementation and maintenance, and ML is one of the methods for network automation as we will explain later in this thesis.

[18] Qualys WAF provides security for web applications by being agile and patching the last security updates while it is designed to protect different virtual platforms such as VMware or Docker and applications such as WordPress or Sharepoint.

[19] FortiGate, provided by Fortinet company, is a firewall for the network of data centers, campus branches, and cloud platforms.

[20] Check Point Quantum is a network firewall that provides network protection against cyber-attacks using bidirectional stateful traffic inspection.

[21] The flexible Cisco Secure Firewall among others provides the capability to adapt, collaborate, and combine its functionalities with other related network product from other vendors such as AWS, VMware, and Azure.

[22] Azure Firewall, among others, provides threat intelligence for the security of the workloads and the protection of virtual network resources.

[23] Utilizing among others ML capabilities F5 BIG-IP Advanced Firewall Manager provides networks with protection against cyber threats including DDoS attacks which, as we discuss more in Chapter 4, is needed when utilizing automation techniques in the network.

[24] VMware NSX Distributed Firewall provides layer 7 network security by utilizing advanced threat intelligence capabilities in addition to zero-trust protection while reducing costs.

[25] Capable of providing virtual core and NGFW functionalities, vSRX Series by Juniper is a firewall product provided by Juniper company.

[26] Armed with the security protection against malware, ransomware, phishing, and botnet Cisco Umbrella is provided by Cisco company to protect the edge of the network.

Firewall Technologies

This section provides an overview of firewall technologies from the perspective that National Institute of Standards and Technology (NIST)[27] has presented in Guidelines on Firewalls and Firewall Policy [118]. One reason why we choose NIST aspect of view on this is that many of the related works we studied for this thesis point to this guide as their main resource. The other reason for that is that we find the NIST guide, despite being from 2009, as a comprehensive guide that is complete for what we need to discuss here.

There are ten different firewall technologies mentioned in NIST Guidelines on Firewalls and Firewall Policy Special Publication 800-41 Revision 1. These include Packet Filtering, Stateful Inspection, Application Firewalls, Application-Proxy Gateways, Dedicated Proxy Servers, Virtual Private Networking, Unified Threat Management (UTM), Web Application Firewalls, and firewall for Virtual Infrastructure. Here, we explain some of these firewall technologies that are useful in our coming discussions about network automation.

The filtering done by firewalls is based on what goes through the application layer, transport layer, and network layer[28]. There are many technologies that are also counted as firewalls, such as Network Address Translation (NAT)[29] which actually is a routing protocol, Intrusion Detection Systems (IDS)[30] that work for monitoring or detecting, and Intrusion Prevention Systems (IPS)[31] that is set to prevent the cyberattacks which in many cases are implemented or delivered as independent systems or applications [118].

Packet Filtering: This is the most basic functionality that each firewall delivers. Here, the filtering of the traffic is based on the packet headers. This filtering could be done by choosing to filter the IP address of the packet sender or receiver, packet type that could be TCP, UDP, or other types, or port number related to the application access to allow or deny [29]. For instance, it checks the IP address of the source and destination to decide on allowing or denying the connection. This is the same as how the Access Control List (ACL)s[32] work and is also called stateless inspection [118].

---

[27] Established in 1901, NIST is one of the U.S. physical science laboratories with a mission of advancing the technology and improving the level of life in this country.

[28] These layers are explained closer in Section 3.2.

[29] By performing translation between private and public IP addresses, NAT technology, among others, provides higher security for the network and hides the internal resources IP addresses from the outside world [27, 115, 146].

[30] The network detection tool, IDS, monitors the network and analyzes the captured traffic to detect and raise alerts when malicious or suspicious network traffic is captured [45, 146].

[31] IPS not only detects the threats to the network and resources but also actively attempts to trace, block, and stop these threats before they cause harm or reach their targets [146].

[32] ACL is applied to the lists in which we can specify what communication we allow and what we deny. There are different types of ACLs to implement based on what is needed. Instances of these are extended ACL and standard ACL [26, 115].

Stateful Inspection: In this type of technology, the firewall tracks the state of the packets and works at the network layer. In addition to what stateless packet filtering performs, it has a state table for the packets that are sent in addition to keeping track of source and destination IP addresses and source and destination ports for the packets transferred. Here the packets that are not verified as legitimate will be dropped [118].

Virtual Private Networking (VPN): VPN is a communication tunnel that encrypts the network traffic by utilizing the encryption mechanisms such as IPsec[33] or Secure Socket Layer/Transport Layer Security (SSL/TLS)[34]. The architectures used for VPN are gateway-to-gateway, such as an organization's different locations to communicate with each other, and host-to-gateway, which for instance, could be an engineer that works far from the organization's headquarters and needs to connect to the organization's resources such as different servers [118].

In the gateway-to-gateway architecture, the users located at each of the ends do not need to configure VPN, but in the host-to-gateway architecture, the user who works remotely and needs to connect to the office, for example, needs to activate VPN to be able to communicate with the organization's resources. As the authentication protocols that are used by VPN, we can name Lightweight Directory Access Protocol (LDAP)[35] or Remote Authentication Dial In User Service (RADIUS)[36] that will secure authorized access to the VPN encrypted communication channel [118, p. 7-8].

Network Access Control (NAC): NAC and Network Access Protection (NAP) check that the hosts that connect to the organization's network fulfill some requirements such as having their firewall applications updated or the necessary OS patches in place. Worth mentioning that NAC and NAP are different from ACLs where ACLs are the lists of rules that are implemented on routers or firewalls to allow or deny packet traffic. But NAC and NAP are to confirm that clients are healthy at the edge of the networks and therefore they need to have software implemented on that clients [118, p. 8-9].

Cloud Firewalls: With the evolution of cloud technologies the three possibilities Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) are provided for customers to choose among based on their needs and possibilities. By choosing each of these types of cloud service offers customers can choose how much of their systems shall be managed and secured by the ser-

---

[33] IPsec or IP Security protocol supports the security of private communication on the network while utilizing Internet Key Exchange (IKE) protocol for authentication of users [147].

[34] While being the successor to SSL, TLS contributes to the protection of user data that is sent on the internet [148].

[35] LDAP is a software which contributes to the authentication of users by utilizing certification based TLS handshake [148].

[36] RADIUS protocol is utilized for contributing to network security by Authentication, Authorization, and Accounting (AAA) of users while performing this operation centrally either by utilizing TCP or UDP protocols [149].

vice provider. In these cloud models, customers can take advantage of Firewall as a Service (FWaaS) which is how they decide to implement their firewalls for each of the cloud service models mentioned above. The firewall types in FWaaS include the traditional first-generation firewalls, Next-Generation Firewalls (NGFWs), application firewalls, and circuit-level gateways. The functionality of FWaaS is to scan and monitor inbound and outbound network traffic for providing network security [29].

Web Application Firewalls: Above, the types of WAFs were briefly explained. Here, we briefly elaborate on the technology behind the WAFs. These application firewalls are made to protect the applications from cyber attacks such as Cross-Site Scripting (XSS) or Server-Side Request Forgery (SSRF). As also mentioned above about WAFs, today there are many professional WAFs offered by different vendors to prevent cyberattacks against web applications to reduce the risk of vulnerabilities that threaten the security of the assets, the risks which otherwise could not be reduced by other types of security measures such as VPN or ACLs [118, p. 9]. WAFs are better suited and applicable to SaaS cloud models [29].

Virtual Firewalls and Firewalls for Virtual Infrastructures: With the evolution of technology, network and IT environments become more virtual rather than bare metal and on-premise solutions. With these improvements, firewalls also become more virtual. The concept of Virtual Firewalls (VFs) includes a wider context where NGFWs, WAFs, and even micro-segmentation are part of it. An instance of VFs is the virtual firewall implemented on each Virtual Machine (VM) in micro-segmentation architecture to separate and monitor communication traffic based on the security group policy implemented[37]. These VFs that are well implemented in virtual environments with VMs and different cloud service models are not equally suited for other network solutions such as for Wide Area Network (WAN) technology [29].

Further, 'Firewalls for Virtual Infrastructures' points to the state in which virtual hosts run on the top of an OS. This could be done by utilizing a hypervisor such as Hyper-V, Virtual Box, or a VMware to run VMs on top of it. Instead of the external firewall, which in this case cannot control and monitor the virtual network provided for the virtual hosts, the built-in firewalls will be utilized to control the network traffic of the virtual hosts [118].

Next-Generation Firewalls (NGFWs): By performing deep packet inspection in addition to the normal functionalities of the firewalls, NGFWs capture and block cyberattacks such as Distributed Denial of Service (DDoS) [114]. The IDS and Intrusion Prevention Systems (IPS) functionalities included in NGFWs [114, p. 4] make them better suitable for CIS infrastructure which requires high availability [9, 29].

NGFWs also are suitable for PaaS and IaaS cloud service solutions because of

---

[37] See Section B.3.4 for more explanation on this type of network security architecture.

their high functionality in providing network security [29]. Some vendors, such as Juniper, refer to NGFWs and Unified Threat Management (UTM) firewalls where the network security solution provided offers multiple network security functionalities in one solution which also will have the advantages, such as meeting many goals in one solution, and the disadvantages, such as being a single point of failure [118, p. 9] [29, 150]. NGFWs are more costly and require more management resources as the logs of IDS and IPS need to be checked and alarms need to be verified [29].

Circuit-Level Gateways: This type of firewall, which is suited to be used for VPN connection, filters network packets based on the session layer headers. Circuit-level gateways are solutions that are not expensive and provide the security of the network by verifying the TCP/UDP connection between the two hosts based on their entry table. These network security solutions alone are not enough, a fact that makes network engineers to rather prefer to use Stateful Inspection firewalls over these [29].

Application Firewalls: NIST - Guidelines on Firewalls and Firewall Policy - Special Publication 800-41 [118] refers to these types of firewalls as the solutions which can allow or block specific content in the applications such as an unwanted, or malicious email attachment, and in this way prevent cyber attack vectors such as DoS, malware, and buffer overflow[38] that can be conducted through the applications. These firewalls can also permit or reject web pages that have revoked or compromised Certificate Authority (CA)s or even unwanted contents [118].

Application-Proxy Gateways: Implemented in the application layer, these firewalls, which are also known as proxy firewalls, permit or deny the network packets based on compliance with the security policy defined. Here, the host and destination, each establish a connection with the proxy server, and their packets could be inspected by their user ID and password, or other parameters for authentication [118].

Another functionality of proxy firewalls is that the IP address of the internal hosts will be hidden from the external hosts, and they only see the public IP address when they communicate with the application proxy gateway. This type of firewall can decrypt the network packets for examination and then after that re-encrypt them before sending them to the destination. Because of these high awareness mechanisms, application-proxy gateways are slow in reading the packets which brings the need for proxy servers [118].

Dedicated Proxy Servers: These firewalls that have a close association with proxy firewalls are capable of fewer firewall functionalities. These proxy servers are provided to reduce the workload from the main firewall while logging and monitoring the network packet traffic. These could be implemented after a firewall to transfer inbound or outbound network traffic. An instance of the latter would

---

[38] For an explanation about these three types of cyber threats see Section B.5 in this appendix.

be a HTTP proxy server [118, p. 6-7].

B.3.2 Demilitarized Zone Network Security Architecture - RQ1

One of the simplest strategies for isolating the internal network from the internet, the so-called outside network, by using firewalls, is to utilize a Demilitarized Zone (DMZ) architecture. DMZ is the network area between two different firewalls. The type of firewalls will be chosen based on the network technician's preference, company[39] security policy and network security architecture.

The DMZ area, located between the external and the internal firewalls of the network, as shown in Figure B.2, has many different functionalities. On the one hand, DMZ is the area where, for instance, the company's web servers, which should be publicly available for external users, are usually located. This access is provided for them without delegating access to the internal network of the company resources. On the other hand, traps such as honeypots which are network security measures to lure cybercriminals away from their real targets, are usually placed in this DMZ area [39].

The company's remote employees, however, as shown in Figure B.2, are allowed to go through the internal firewall to access the company's internal network and its resources, utilizing VPN connection. This permission is granted to the remote users, who authenticate and authorize before accessing any company internal resource by utilizing policies configured on firewalls or other applications dedicated to this job [39, p. 19].

Figure B.2 depicts the DMZ concept. Here we have the customer in blue color, which needs to access one of the company's web servers, in this instance. The remote employee, depicted in green color, needs to utilize the company's internal network and work with internal resources that should not be available for unauthorized access. This employee will be authenticated and authorized by the functionalities of the external and internal firewalls in addition to using the VPN connection to be able to get the needed access.

Nowadays, most companies also utilize Multi-factor authentication (MFA)[40] for login authentication of their users. Following NIST SP 800-207 both VPN and MFA are zero-trust architecture strategies that today are highly adopted in every network security architecture in small, medium, or large networks. We mention it here in DMZ because these methods are highly intertwined in even this simple network security architecture. We discuss zero-trust network security architecture further in Section B.3.5, and VPN is briefly explained in the previous section, Section B.3.1.

---

[39] In this thesis, we have used the words organization, company, and enterprise interchangeably.

[40] MFA technology is utilized to authenticate users by utilizing several factors. These factors are such as a dynamic code sent to a user's mobile phone or other methods rather than just utilizing a password to log in [40].

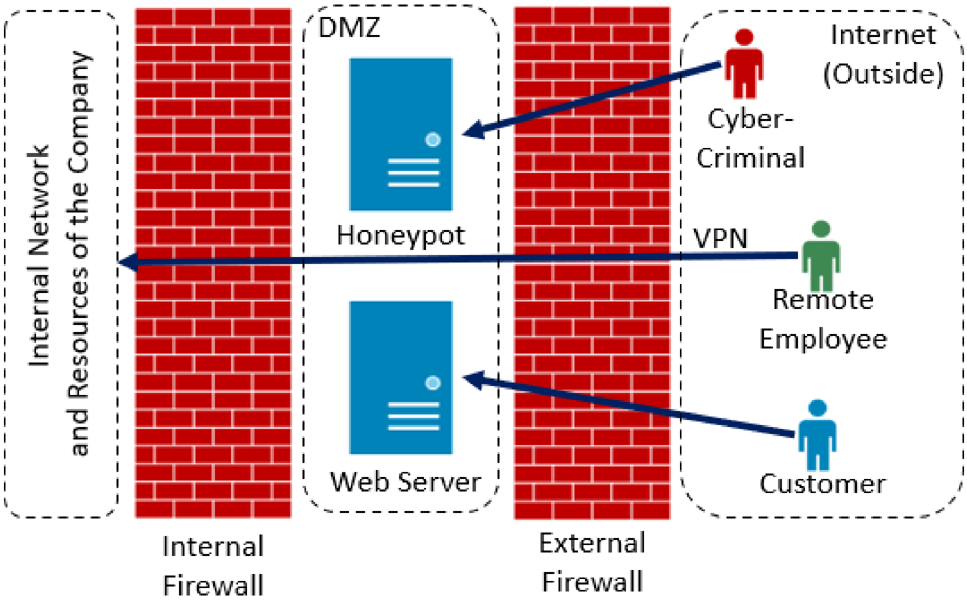


Figure B.2: Simple strategy of utilizing DMZ, also called perimeter zone, in traditional network architecture for separation of the internal network and its resources, from the external network while keeping some public resources available for public access. The figure is created by the author.

The cybercriminals, depicted in red color in Figure B.2, with malicious goals, will attempt to access the publicly available company servers, while ending on honeypot instead. This protects the essential resources from their access without them noticing it. The two-layer firewall strategy used in this simple DMZ architecture makes it possible for the company to have the resources that should be available for public users in place while at the same time protecting them by proper security measures [39][41].

B.3.3 Zone-Based Network Security Architecture - RQ1

A security architecture to separate different portions of the network is to divide it into different zones. These zones could, for instance, include DMZ, internal, and secure zones or DMZ, trusted, and management zones [39, p. 8]. All hosts in the same zone will be on the same subnet, and to communicate with other zones, firewall rules to allow this will be utilized [39, Chapter 1 p. 8-16].

An advantage of this architecture, also called defense in depth [151], is that, for instance, the hosts in the internal zones that should not have access to secure-

---

[41] DMZ and the two-layer firewall security strategy discussed here has also other functionalities. For instance, these functionalities are such as where to place IDS and IPS solutions for the protection of the network, based on the network security architecture strategy provided in each specific case [146].

or management-zone are kept separated from accessing these areas. It also gives the possibility not to allow access from the secure zone to the internet or vice versa. A disadvantage of this architecture is that zone-based network architecture is more expensive and requires more effort to implement and manage than if only a simple DMZ architecture with firewalls were utilized [39, Chapter 1 p. 11-14].

Figure B.3 shows that internal and secure zones are separated from the other zones with firewalls. DMZ located between the internal firewall connects this zone to LAN, and the external firewall connects this zone to the internet. The latter firewall controls all connections to and from the internet. In the internal and secure zone depicted in Figure B.3, we have from VM1 representing the first VM, to VMn representing the last VM located in each zone. This locating of VMs is abstract and would be practiced by giving each VM an IP address that is related to each subnet that belongs to each specific zone. Firewalls control connections to zones by allowing or denying specific connections based on their rule sets.

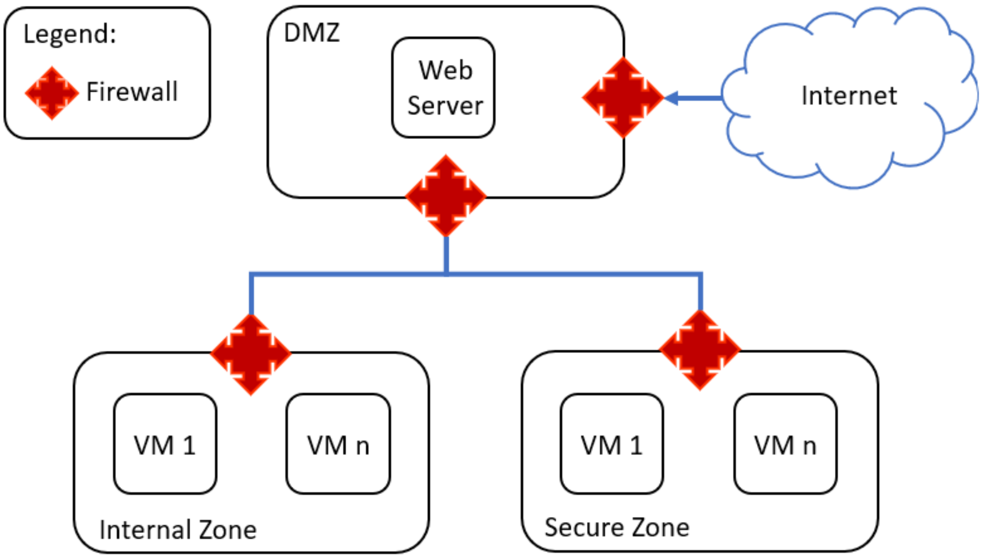


Figure B.3: Zone-based defense network security architecture. The figure is created by the author.

Here we give an example of how to allow one simple network traffic from outside to the secure zone. Say a network engineer is working remotely and needs to access a server located in the secure zone. In a zone-based network security architecture, as shown in Figure B.3, we will need to configure one rule on the external firewall of the DMZ to allow the connection from the external zone, which is the internet, to the DMZ, one rule on the internal firewall of the DMZ, and a third role on the firewall of the secure zone as in this example, the network technician wants to access a server located in this zone. Usually, when the network traffic passes different zones, there will be a need for security personnel to check and approve the zone-passing traffic before the rule can be implemented on the firewalls.

Hence, for one single access request to a specific server here we have to deploy three rules on three different firewalls manually. This means logging into each firewall, and checking if the exact rule does not exist since before or if the IP address of the source of the connection is not already included in an already existing rule with a subnet that provides the same access to the same destination. If the rule has existed since before, checking if the port requested to be opened for this connection is included in the existing rule or not. If any part of the configuration that we checked needs to be implemented, this should be done on all three firewalls to allow the requested network traffic. Table B.1 shows an example of a single firewall opening request that needs to be checked and, if needed, implemented on each of the firewalls that need to allow this communication[42].

Table B.1: The firewall rule; is to be implemented manually on the three firewalls mentioned, and to allow the network connection from an external source to a specific server located in the secure zone.

Source IP Address and mask	Security Zone	Destination IP Address and mask	Security Zone	Protocol	Application	Port
100.128.111.20/32	External	172.16.20.10/32	Secure	TCP	RDP	3389

B.3.4 Micro-segmentation Network Security Architecture - RQ1

This section explains our view of network segmentation[43] in this thesis. One of the platforms to use for network segmentation is VMware[44] [39]. As we will explain here, network segmentation architecture is a solution to providing better security in the network. This solution has rules to allow or deny northbound and southbound communications. Northbound network traffic means that the communication direction is from inside to the resources outside and southbound network traffic means any communication from outside of the local network to the Local Area Network (LAN) [39, p. 12][45]. In addition, in this network security architecture, we need to specify rules for two hosts in the same LAN to communicate with

---

[42] The IP addresses of the source and destination hosts here are to give examples and the intention is not to prove or specify if they are public or private IP addresses, nor whether the IP address of the source that comes in has used NAT for translation. We intend to establish a rule request to be implemented once on each of the three firewalls to demonstrate the amount of work needed for the configuration of each firewall opening.

[43] In this thesis, the words segmentation and micro-segmentation are used interchangeably and the same concept applies to both of them.

[44] With embedded security measures, VMware is a platform for virtualization of data centers, networks, virtual machines, and other cloud-native facilities.

[45] In the definition of northbound and southbound traffic when it comes to micro-segmentation architecture, we talk about communication between the outside and inside of the DC [39]. In other contexts, this definition points to the communication between the data plane and the centralized control plane [10]. So the concept of northbound and southbound, when used in this thesis, should be interpreted based on the context it is used in.

each other. This is because, otherwise, the local firewall on each host will deny any communication with the host.

Here one can have one to ‘n’[46] virtual Application (vApp)s on a VMware virtual Center (vCenter). vApps serve VMs as containers on each Data Center (DC). In a zero-trust[47] manner of network security implemented here, to let each VM communicate with other VMs in the same network segment and to itself, we need to set East-Westbound firewall rules. This East-Westbound network traffic is a type of network traffic that remains in DC [39, Chapter 1 p. 8-16].

For this, we need to register the VM into specific security groups that we set up. The groups are specified by tags that we can then set to the chosen VMs. As long as two VMs are in the same security group and the East-Westbound firewall rule for that group is made the hosts can communicate with each other on the ports and the protocols allowed in the specific rules. The East-Westbound firewall rule will let them communicate with each other based on what is specified in the rule set. Otherwise, there will be no connection between any hosts, even if they are located in the same network segment [39, 121].

Figure B.4 shows that several VMs located on the same vApp, on the same DC, are allocated three different tags. In this network security architecture, no VM is allowed/able to communicate with each other, other than a specific common tag is delegated to each of the VMs. In this Figure B.4, we have given both blue, red, and green tags to VM1. This makes VM1 communicate with VM2, VM3, VM4, and VMn. VMn depicts that we can have any number of VMs in this architecture. So it could be VM number 10 or VM 100 or other numbers of VM that we might have in a vApp located on a DC.

VM2 can only communicate with VM3 and VM1. This is because it has only the red tag. VM3 can communicate with VM1, VM2, and VMn. VM4 is only able to communicate with VM1, and finally, VMn can communicate with the VMs that have the same tag, the blue tag, which includes VM1 and VM3. The tags in practice, are not colors, but names we assign to different tags to be able to group the VMs. In the figure shown, we have also put two vApps on the depicted DC. But we only use one of them in the demonstration. All we show in vApp1, can also be done on other vApps on DC1 and other DCs.

---

[46] Here, with *one to ‘n’*, we mean *from one to any number*. This is also used in the figures shown.

[47] Zero-trust network security architecture implies that no network traffic packet is allowed other than it is specifically allowed by the rules specified on the firewall [39].

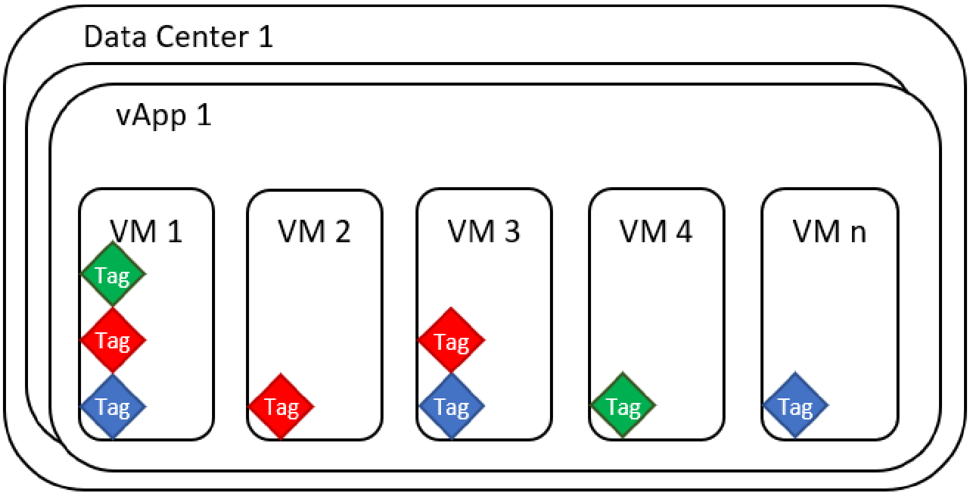


Figure B.4: Data Center, vApp, VM, and tag depicted, only VMs that have the same tag can communicate with each other. The figure is created by the author.

Further, firewall rules should be implemented to allow the flow of network traffic packets that have a specific tag specified between the hosts in addition to between the hosts and the outside network. The firewall rules that allow network traffic between the hosts located in vApps are called Eastbound and Westbound rules. Here also, security groups based on tags are used for specifying which network traffic is allowed to flow in those network portions [39].

Figure B.5 shows the first and second line of defense by micro-segmentation where the network security architecture has provided a firewall per host in addition to the main firewall for the whole network segment [39, p. 19]. Further, we give an example of East-Westbound and an example of North-Southbound firewall rule implementation from a high-level perspective, which means the process is defined holistically, to describe a picture of the complexity of the implementation. The high-level overview provided here is based on the step-by-step instructions available in NSX Administration Guide [126, Chapter 16 p. 435-460].

Example of East-Westbound firewall rule: Here we provide an example where VM1 is running a web server application and needs to launch its own web page[48]. VM1 also needs to launch a web page that is running on another web server that is VM2. Both VMs are located in the same vApp, which means that they are using the same network segment. Even though they are located in the same network segment, without the configuration of tags, security groups, and firewall rules that are needed, neither can VM1 launch its web page in a web browser, nor it can access the web page that is running on VM2. For these tasks to be accomplished,

---

[48] As we mentioned earlier in this section, for a host to be able to communicate to itself, in a micro-segmentation network security architecture, we need to allow this using tags, security groups, and firewall rules specifically

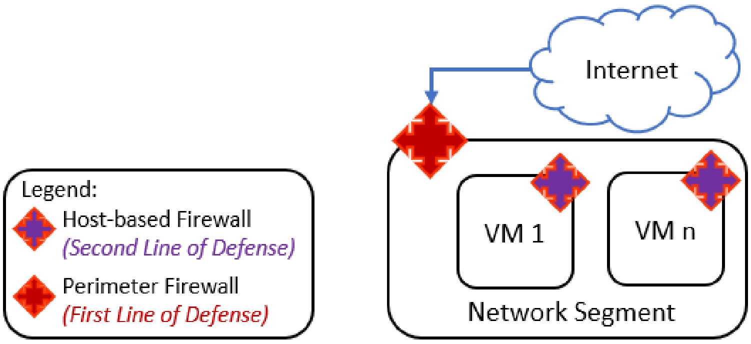


Figure B.5: First and second line of defense in micro-segmentation. The concept drawn in this figure is inspired by Figure 2.1 in [39, p. 19].

we need the following configurations to be done [126, Chapter 16 p. 435-448] [49]:

1. Define a tag. Here we choose to call this tag ‘web’.
2. Define the IP addresses of VM1 and VM2 one by one in the IP lists as objects.
3. Apply the tag ‘web’ to VM1 and the same tag to VM2. By applying the tags to the VMs, they are also added to the same security group. But we still need to configure firewall rules to allow the needed East-Westbound communications.
4. To let VM1 launch its web page, we need to set a firewall rule for it. Open a new firewall rule, under the East-Westbound tab of DC network rules, that allows VM1’s IP address as the source IP address to communicate to its IP address as the destination of the communication in addition to allowing connection on port 443 for HTTPS protocol for web applications using a TCP connection in this rule.
5. For VM1 to launch VM2’s web page, we need a new firewall rule to allow this. Open a new firewall rule, under the East-Westbound tab of DC network rules, that allows VM1’s IP address as the source IP address to communicate to VM2’s IP address as the destination IP address. This rule should also allow connection on port 443 for HTTPS protocol for web applications using a TCP connection.
6. We test both of the firewall rules that we implemented here for the two different East-Westbound network communication flows.

Example of North-Southbound firewall rule: Now a remote computer where a network engineer works needs to make a remote connection to VM1. In this example, the remote host has an IP address of 100.128.112.30/32. The network engineer needs to use Remote Desktop Protocol (RDP) with port 3389 and the TCP protocol. We need to do the following steps to implement this connection [126,

---

[49] Both East-Westbound and West-Eastbound firewall rules are applied for communication between the hosts in the same vApp on the same DC [126].

Chapter 16 p. 449-460][50]:

1. Define a tag. Here we choose to call this tag ‘mgmt’.
2. Assign this tag to VM1.
3. Make an object with the IP address of the remote host, 100.128.112.30/32, and give this object the same tag as we gave to the VM1 for this connection, the ‘mgmt’ tag. Here, we assume we already made an object with the IP address of VM1 in the previous task. If we had not done this, then an object, with VM1’s IP address, was needed to be made in the firewall IP sets.
4. Make a firewall rule under the tab of North-Southbound rules of the firewall in the DC network tab. The rule should allow the source IP address of 100.128.112.30/32 to the destination of VM1’s IP address and include RDP application on TCP port 3389.
5. We test the firewall rule that we implemented here for the North-Southbound network communication flow. The firewall rule should allow the network engineer located at the remote host to connect to VM1.

B.3.5 Zero Trust Network Security Architecture - RQ1

Another type of network security architecture Zero Trust Architecture (ZTA) focuses on continuously evaluating access and identity instead of assuming as long as access is granted, every movement is safe [113]. Essentially, the security of the network before introducing ZTA relied on the perimeter network security where everything outside was assumed unsecured, and everything inside beyond the perimeter area in the network[51] was counted secure. ZTA paradigm oversees different threats, such as the insider threat, solving the problems related to security [40, p. 13].

Therefore, the strategy of ZTA takes advantage of reevaluating the connections made in the network to give precisely the access rights to the assets that should be given in the exact time window that is necessary to be given. ZTA takes advantage of ML for the intelligence used in threat analysis [40, p. 19, 29, 30]. This network security paradigm also is based on the separation of the data plane and control plane, which is consistent with SDN automation paradigm [40, p. 9-16].

This network security strategy utilizes SDN and ML techniques for automating the processes [41], as well as for overcoming complexities when network security methods are getting more complicated [88]. ZTA contributes to other network security approaches including but not limited to micro-segmentation and Software Defined Perimeter (SDP)[52], with the latter one including and utilizing concepts

---

[50] Both North-Southbound and South-Northbound firewall rules are applied for communication between the resources on the outside and the inside of the organization network [126].

[51] Perimeter network is explained earlier in this chapter.

[52] As one of the techniques for implementation of ZTA, SDP provides encrypted transmission of data, identification of users by being able to utilize Single Sign On (SSO) and MFA techniques,

related to SDN discussed in this thesis [40, p. 11-13].

The scenarios in which ZTA network security paradigm is used include but are not limited to when a remote employee wants to access enterprise assets, such as the intranet, or the assets available on the internet through perimeter zone, the DMZ we explained above, such as web-based services. Also, inter-server communication in the organizations, communication between two enterprises, and integration of monitoring and security systems with the organization policies are other instances of ZTA use cases [113, p. 5-6].

Moreover, ZTA can be applied to different scenarios. For instance, enterprises with one or more locations that are geographically far from each other, with a single headquarters, and utilizing multiple cloud providers. In this scenario, multiple cloud providers supply secure access from one cloud provider to another for company users connecting to the cloud resources. This way ZTA provides time-limited access for employees that need to perform specific tasks for the organization and take advantage of public-facing assets when there is a need for organization[53] to control user access [40, p. 23-27].

ZTA contributes to identification, protection, detection, and response to incidents in the network. The contribution to identification is done by asset management and risk assessment. Identity management, authentication, and access control mechanisms in ZTA provide protective technology that contributes to protecting the network. The contribution to detection is accomplished by evaluating anomalies and events, continuously monitoring security, and providing detection procedures. Finally, responding to incidents ZTA contributes to containing and mitigating the incidents [113, p. 12-14].

B.4 CIS General IP Network Architecture

Today IP networks CIS connect the control systems to the external world. In the abstracted model depicted in Figure B.6, the security zones in a typical industry model of the network are shown. As the figure depicts, the main manufacturing facilities are located in the manufacturing zone separated from other parts of the industry sector and connected to them by firewalls and other security measures [153]. Thereafter, the DMZ[54] separates the enterprise zone from the manufacturing zone while it also serves some services such as security related, data historian, and some of the servers in this zone. Further, the enterprise zone, which is located between the two different DMZs, is the place where the services such as servers, databases, access points, workstations, and IT authentication servers are

---

verification of devices that connect to the network by the functionality of its controller component, and making a mutual secure connection between the user and the desired services possible by utilizing the SDP virtual gateway [152].

[53] In this thesis, the words organizations, companies, and enterprises are used interchangeably.

[54] DMZ as a network security architecture strategy is explained further in Section B.3.2.

located [153].

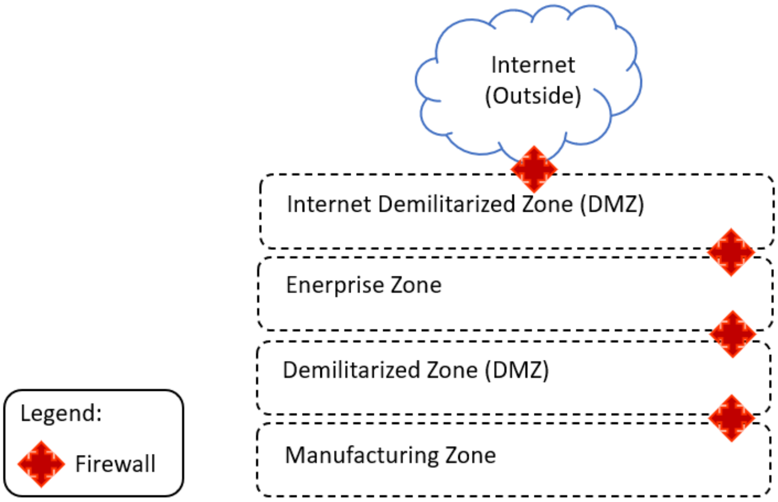


Figure B.6: Security zones in industry, depicted in layers inspired by [153].

The goal of this architecture is to separate the critical services, located in the manufacturing zone, in a safe manner from the other enterprise resources that are located in the enterprise zone between the two DMZs. The internet DMZ separates the enterprise zone from the outside which is the internet as depicted in Figure B.6. The architecture shown here is not an absolute model. Hence, the enterprises more or less use their architect and desired model of security zones to keep the critical zone of the CIS secure and separated from all unauthorized access [153]. Today CIS networks, which usually also connect different sites that are located separately in different locations, utilize IP networks for communication and management, something that makes it more difficult to keep the critical industry separate and safe from the cyber-attacks that aim to cause damage to CIS [34, 66].

B.5 Information Security Related Terms and Concepts

In this section, we explain the concepts and terms that are related to information security. The terms and concepts explained here are used in the SotA and further referred to in different parts of this thesis. These include but are not limited to the cyberattack vectors that can threaten network security. Every place where appropriate and also mentioned by the SotA, we have briefly pointed to the mitigation measures related to the specific cyber threat vector. The aim is to assist the reader in comprehension of the cybersecurity-related concepts that are utilized in our thesis out of the study of the SotA.

OWASP Top Ten

The organization Open Web Application Security Project (OWASP) has a focus on software security [154]. Every year this nonprofit organization provides a list of the Top Ten risks to application security that is made freely available to everyone to take advantage of [144]. This list differs from year to year based on the threats and incidents that have occurred each year.

Common Weakness Enumeration (CWE™) Top 25

Common Weakness Enumeration (CWE) focuses on software weaknesses and every year publishes, among others, a list of software weaknesses with a link to a detailed overview of each of them to provide the organizations and interested parties with valuable knowledge and information. They aim to help them in mitigation of the risk in for example their architecture, design, test, and production environment [155].

Worm

A worm is one of the cyberattack vectors that, when deployed on a host will replicate itself to the other hosts that the original victim is in contact with [156]. As soon as a host in a network gets infected by a worm this will very fast propagate itself to the other machines that the original victim is in contact with [157]. An example of this is the Ryuk ransomware which was a worm-type malicious software that was programmed to replicate itself to other hosts in the same network as the original host, with a specific time setup for the replication to other hosts, planned by the attacker [158].

Besides the antivirus and other technologies that can function to block such malware, one of the prevention measures pointed to by the SotA, is network segmentation as one of the recent methods that are presented to be functional and efficient in isolation of the hosts. The isolation done in this type of network security architecture is to prevent the spreading of the worm from one host to all the other hosts. This is because by segmenting the network, hosts will not be able to connect if not permitted specifically by the rules that are set on the firewalls and by the tags set on each host that make them a member of specific desired security groups[55] [1, 39].

Virus

The malicious software, virus, will be deployed on the host victim to perform adversarial activities. Unlike worms, a virus program needs the host victim to trigger it, like clicking on a malicious link, to be activated, whereas worms perform malicious attacks as a stand-alone software [156, 157].

---

[55] See also the explanation in Section B.3.4 about micro-segmentation network security architecture and the related techniques.

Injection

In cyber security, injection is known as a type of cyber-attack where the attacker injects malicious code into a program using the existing vulnerabilities in the code [159]. This type of cyber attack refers to a broad group of attack vectors [160]. Among the different types of injection attacks, we can name a few here, such as SQL Injection, no SQL, or even OS injection. Some examples of the most significant measures to prevent injection attacks are included but not limited to server-side input validation and escaping special characters for dynamic queries [161].

Server-Side Request Forgery

In this type of cyber attack, the intruder forges the request sent from the server to the client by manipulating the server-side back end. An attacker can conduct this cyber attack when for instance, the server-side permits modification of the resources [162]. This type of attack can bypass security measures such as firewall, Virtual Private Network (VPN), and Access Control List (ACL). The measures to prevent these types of cyberattacks in the network include reducing the impact of the attack by segmenting which access functionalities the remote resources are granted, and on the firewalls using whitelisting strategies such as deny by default policy to reduce these types of attacks on the network [162, 163].

Cross-Site Scripting (XSS)

CWE defines Cross-Site Scripting (XSS) in three types of attacks including reflected, stored, and DOM-Based XSS [164]. Generally explained, in an XSS cyber attack, the adversary injects malicious code into the website to access cookies, the tokens of the sessions, and the sensitive data and information that belongs to the legitimate user. A few methods to prevent these types of cyberattacks include but are not limited to filtering the input data on its arrival, encoding data on the output, using proper response headers, and finally, utilizing content security policy [165].

Zero-day Attack, Zero-day Exploit, and Zero-day Vulnerabilities

Zero-day vulnerability applies to a vulnerability that exists in the system; here we talk about network and firewall applications that are not yet patched [166]. Regarding zero-day vulnerabilities, cyber attackers usually discover these vulnerabilities before the owner of the system. Further, they use attack vectors to target zero-day vulnerabilities. Their method for targeting zero-day vulnerability is called 'zero-day exploit', and these types of cyberattacks are referred to as 'zero-day attacks' [167]. Zero-day attacks in SDN technology are yet not comprehensively investigated, and therefore there exists a high possibility of zero-day attacks when these unknown vulnerabilities get exploited [95].

DoS and DDoS Attacks

In a Denial of Service (DoS) attack, the attacker makes the target system unavailable by exhausting the resources. For instance, this could be accomplished by shutting down a server, exhausting a DHCP server to hand out all the available IP addresses, and collapsing down, or even by any means making a service unavailable to users [48].

A Distributed Denial of Service (DDoS) attack, is the same type of cyberattack as the DoS attack explained above, with a difference where the amplitude of the attacker systems is more extensive than what could have been utilized in a DoS attack. Here multiple systems are involved to attack the target system. For instance, one of the methods used to conduct a DDoS attack on a target is to utilize many malware-infected devices that are connected to the internet, called botnets, and make them simultaneously flood the victim system [81].

As we will explain in more detail in Chapter 4, SDN as a nearly new technology, has different vulnerabilities that fall in the interest of the cyber attackers to take advantage of and exploit [42]. More specifically, the control plane is mentioned by the SotA, as a bottleneck and a single point of failure for the systems utilizing network automation. The latter mentioned vulnerability in SDN architecture is pointed to by various resources in the SotA[56] [42, 98, 99, 101].

Buffer Overflow Attack

A cyberattack that exhausts the memory buffer of the storage is called a buffer overflow attack which is pointed at as a vulnerability in SDN automation technology [96]. Other resources while providing an overview of this vulnerability in SDN driven networks, suggest different approaches to mitigate it [97, 98, 100]. These resources, among others, suggest solutions such as applying IDS or *SNORT* as a signature-based IDS, for the mitigation of this vulnerability in SDN.

Man-in-the-Middle, Man-in-the-Browser, and ARP poisoning Attacks

Manipulator-in-the-middle or Man-in-the-Middle (MitM) attack applies to the cyberattack where the adversary is located between a sender and a receiver in a communication, and this intruder intercepts the data flow between the two parties that communicate with each other. In this type of cyberattack, all the communication is monitored by the attacker and can be manipulated before the legitimate parties access the data traffic [168].

Further, Man-in-the-Browser (MitB) attack is conducted in the same way as MitM attack, but with a difference that here the attacker plants a Trojan horse

---

[56] In Section 4.4.4, we will take a deeper look at the vulnerabilities in automated networks, discussed by the SotA, including the 'controller as the most vulnerable part of the SDN architecture' [101, p. 2588].

to do the work that the man in the middle was doing with the data information packets [169]. A Trojan horse, which is utilized in this type of attack, is a malicious program that looks legitimate, but it has a malicious payload that will be activated on the host to perform the adversary's planned tasks. An instance of this type of malware is the 'Security software disabler Trojan', where the malicious code will disable the security software to prepare the circumstances, where the firewall is deactivated, to further run an attack on the victim's network and hosts [170].

Resources studied in the SotA emphasize the importance of putting attention to this vulnerability in SDN driven networks and mention ARP-poisoning as one of the methods used to perform this type of cyberattacks against software defined networks [101, 102]. For instance, in an ARP-poisoning cyber attack, the attacker lures the sender and the receiver devices to use the attacker's MAC address for communicating with each other, and consequently, their data traffic goes through the attacker device, making it possible to be monitored by the MitM [102, p. 8].

Supply Chain Attack

By a supply chain, we mean, for instance, the suppliers or the service providers from the external systems that are to support an enterprise or organization with their products and services. Further, a supply chain attack points to the cyberattack vector that targets the products delivered by those third parties, which consequently, if compromised, will affect their customers' infrastructure that utilizes third-party products [38, p. 1-3]. SolarWinds, as we will explain about cyberattacks conducted against CIS companies in the coming section, is an instance of a supply chain attack [36].

B.6 Network Automation Simulation Platforms - RQ2

In contribution to Chapter 4 Section 4.3.7 in this glossary section we expand on the details of the simulation platforms.

There are many solutions to utilize when one is planning to do a test or training in a lab environment. But here, we explain some instances of the available lab environments that exist and can contribute to testing and experimenting with both traditional networks and network security automation management in the scope of our literature reviewed in the SotA. The reason why we also consider the traditional network lab environments in this section is that one needs to first learn how to set up the network in a traditional manner to acquire competency in the network domain itself before adding the knowledge and competency of the automation techniques and technologies at the top of it.

Then, when that knowledge is in place, one can take advantage of network automation techniques knowledge to the job and make the methods used in the network automated. When the network is set up, then the firewalls and security techniques can be added to make the network secure. This is why we consider both traditional network, network and network security automation management as how one can practice acquiring the competency needed by experimenting and learning.

Here the lab environments that are discussed through the SotA studied in this thesis are explained, which include Mininet, Graphical Network Simulator-3 (GNS3), Cisco Developer Network (DevNet) Sandbox, and some other lab environments that are set up by companies and universities for the practice of their employees or their students[57]. We also take a brief look at Packet Tracer as this lab is easily available, helping new beginners in network knowledge to learn and practice while having a lack of advancement, which makes it unuseful for automation practices. Finally, we mention some other helpful materials that are freely available for test and practice with network and network security automation.

Mininet

Mininet[58] network emulator is, in many cases, used and mentioned for testing and emulation environment for the theories that support and provide evidence to network automation. This is for proving the automation methods such as ML and SDN as a solution to the problems of the increasing complexity of the networks. The complexities that make the management tasks of the networks, such as monitoring, updating, and securing, more difficult [43, 76].

Megyesi, Péter, et al. [62] in 2017 and Chowdhury, Shihabur Rahman, et al. [63] in 2014 utilized Mininet for their experiments. Megyesi, Péter, et al.'s experiment was about finding a solution to the problem of monitoring and bandwidth estimation in SDN. Chowdhury, Shihabur Rahman, et al. used a Mininet testbed to experiment and propose a monitoring framework for SDN with a zero-cost model. The students at Shri Mata Vaishno Devi University and National Institute of Technology, Surat, Gujarat, India, used Mininet to do an experiment that showed the advantages of SDN as promising for network security over the traditional manner of managing networks [71].

The experiments done by different groups of researchers show that Mininet is

---

[57] We keep the instances of the lab environments mentioned here in the scope of our study of the SotA. But as you will see in the interviews in Chapter 5, the participants not only mention GNS3 as a possibility for practicing, but they also mention Virtual Internet Routing Lab (VIRL), which today is replaced with Cisco Modeling Labs (CML), and also EVE-NG. This is because many of the participants in the interviews have long years of experience in working with network and network security, and for instance, VIRL, mentioned by them, is a deprecated and old version solution of the newer version of the lab for practicing today. Still, we should remember that there are many options to choose between, and they can be combined based on everyone's needs, competency, and possibilities [11].

[58] Mininet is one of the open-source network lab environments that make experimenting with network automation techniques, using, for instance, python scripts, possible for those who are interested. This lab solution has its community and people who contribute to this open-source environment with their discussions and findings.

a proper solution to test SDN solutions for network security [68, 72]. In another research, they test ML automation techniques in a Mininet in combination with Docker containers [73]. Moreover, Mininet is utilized to simulate the automation of IP network firewalls [94]. As this open source environment is freely available, students and researchers can utilize this lab environment for research to test the desired network management methods [71].

There are some limitations to Mininet as a lab environment. For instance, the process tested in Mininet, even if the lab results are promising, needs to also be tested in a lab environment that has the characteristics of the production environment of the company to show if it works. In addition, among the network programming languages, it allows Python, which opens possibilities, but at the same time means that other automation configuration tools that can be utilized in network automation cannot be used in this lab environment. Finally, one cannot increase the CPU and bandwidth of a server, and neither can the OpenFlow switches that are not Linux-compatible run on this lab environment [72, 171].

GNS3

Of of the research groups that experimented with both Mininet and GNS3[59] used Mininet to experiment with SDN and GNS3 for testing with hardware-defined networks [72]. Moreover, studying the SotA shows that GNS3 is also made for experimenting with SDN. This is explained step by step in, for instance, Brendan Choi [11]. GNS3 provides a strong environment for experimenting with different network devices such as routers, switches, and even firewalls. The downside of this environment is that the device images are not free and need to be bought from Cisco in addition to having some complications in setting up the lab environment [11].

For instance, to experiment with SDN lab tasks in GNS3 environment, one needs to get a connection between a network card, Microsoft KM-TEST Loopback Adapter on the PC, and the cloud image in the GNS3 [11, p.462-477]. These complications, for instance, could be related to the compatibility of the hosting device, or the hardware type connected to the virtual NIC in the GNS3 [11]. The lab guides provided by the published books are also promising, but with the current speed of the evolution of the technology, even the links or guidelines get old very fast [11].

Other than this, one also needs to have a clear plan for what to test and how

---

[59] The network software emulator GNS3 is a strong lab environment for professional network technicians to take advantage of and implement training both in traditional and automation based techniques such as SDN. This emulator has a community where people can ask and answer questions about the lab environment, their problems in the lab setup, and every question that they would like to bring to the discussion. The community, however, is managed by volunteers who dedicate their time to answering the questions, but the questions could also be answered by other people who feel that they can contribute to solving a problem or explaining a topic. This way, they help each other both in the lab setup and in working with the content of the lab.

to test and configure devices which means that the technician needs to have a professional level of knowledge and experience to use the environment efficiently. Because the lab environment does not provide any instructions for the person who trains about how to lab, this requires the individual to have a level of independence and experience to take advantage of the provided lab environment. But if the competency needed is there, this lab provides a proper environment to practice and test with complex networks both when it comes to traditional and automated techniques [11].

Santyadiputra G. et al. [8] experimented with network automation by utilizing GNS3 and VirtualBox[60] for implementing the virtual environment for the testbed. Their experiment shows how network automation can contribute to managing large networks with a considerable number of network devices that need to be configured and managed in a more efficient and agile manner. VirtualBox is not the only solution for implementing the virtual environment to work with GNS3. In this regard, in some of the resources studied in this thesis and presented in Section 4.1, VMware is also used to provide the same functionality [11].

Cisco Developer Network Sandbox

Cisco Developer Network (DevNet) Sandbox[61] presetup lab with the possibility for reservation is made available by Cisco company for everyone interested in learning and practicing with automation of the network. These free lab environments make it possible to practice networking, data center, cloud, security, collaboration, open source solutions, IoT, and analytics and automation without needing the equipment set up or caring for that part. One who wishes to practice can reserve the lab sandbox environment, which is available 24/7 for everyone, or for some lab environments without even reservation, to be able to work with the chosen lab [17].

Besides the advantage of this lab which is that one does not need to set up the equipment oneself, the limitation of time and the requirement of the reservation are the drawbacks. Also, for newer beginners, who do not have much experience with network and network security automation, it would be a challenge to find the task they can learn as the lab only provides the lab environment and no scenario for practice. This makes it necessary that despite the environment being set up in forehand, one should have a plan, competency, and knowledge to be able to take advantage of Cisco DevNet Sandbox. Moreover, occurring errors can affect the reserved time for those who are using the lab environment [17].

---

[60] VirtualBox is one of the open source software virtualization tools available for whom needs to utilize it for virtualization of different tasks while the Graphical User Interface (GUI) interface of this test bed makes every experiment for both enterprises and home users much easier.

[61] Cisco Developer Network Sandbox is made available by Cisco company for everyone interested.

Other Lab Environment Instances

In addition to the lab environment for practicing with different technology solutions, which also includes network and network security automation, there are many instances where different service providers, universities, and companies have also set up their lab environments. One of the instances in this regard is Space-SDN/NFV Lab: MIRSAT[62] which is a testbed for satellite-terrestrial networks. This testbed will help to reduce the burden the complexity of the network imposes on the management of the network by providing this environment for testing and finding proper solutions. The solutions that will answer the problems where multiple factors such as IoT, 5G, wireless, and other technologies are involved in the network and affect its security. This testbed, among others, utilizes Mininet, which we have explained earlier in this section.

Packet Tracer?[63]

For acquiring competency in working with traditional networks[64], Packet Tracer is an environment suggested by Cisco. This environment works fine as long as one does not need to involve network automation. One needs to be a member of Cisco Networking Academy courses to be able to utilize this lab environment. This will also not provide any practice in working with firewalls or combining the practice of network devices with the firewalls that are implemented for this. The lab setup, however, is straightforward and appropriate for new beginners who need to learn the basic network concepts from the very start to the level of professional networking [26].

Other Helpful Materials for Learning and Practicing Network Automation

To make it easier to utilize network automation, companies such as Cisco and Juniper provide some helpful materials. A few instances include free available DevNet courses[65], for newcomers to network automation, libraries that provide template codes for automation tests, such as bubo[66] or Jinja2[67], and comprehens-

---

[62] MultI-layer awaRe SDN-based testbed for SAtellite-Terrestrial networks (MIRSAT) is a testbed set up by the university of Luxembourg for practicing with network automation SDN solutions to help the progress of virtualization and softwareization of the networks.

[63] The reason why we use a question mark beside Packet Tracer as the title is that we mean this training platform is under a question mark, and we want to explain why no one can utilize it for training regarding network automation techniques and technologies.

[64] Here, by the traditional network, we mean networks that are not automated in any manner but rather every task and configuration is managed manually by logging into the network device and managing the desired job.

[65] Some companies, such as Cisco, provide both free courses such as DevNet or free webinars to encourage network engineers to manage the tasks of the network programmatically.

[66] bubo is a repository which everyone can fork and run their automation tests in a sandbox.

[67] Jinja2 provides free available documented templates that can generate HTML pages, Unix/Linux configuration files, and not least configuration files for network devices. These templates, which are written in Python programming language, are to make the utilization of network

ive information on their websites about how to work with and utilize automation techniques and technologies. Additionally, other pre-written codes such as Ansible Modules[68], are also available for network professionals to reuse, rather than starting from scratch.

As we also explain in Section 4.4.2, this is substantial due to the progress of this process as network professionals need to build their automation skills and experience. Also, we assume that one of the essential parameters besides motivation is to have access to lab environments that are advanced enough to let everyone practice the automation of network and network security solutions.

---

automation even more accessible for those who are professional in networking but lack knowledge in professional programming.

[68] Pre-written codes such as Ansible Modules are made available for network professionals to raise productivity and make working with network automation easier for everyone.

Appendix C

Criteria Used to Categorize the State-of-the-Art

The criteria for categorizing the resources studied in the SotA are presented in this Appendix. These categorizations are to make our work with the resources easier and finding the information needed through them during the work on this research more feasible for us. The criteria presented below consist of 14 questions which are further answered in Table D.1 in Appendix D. We, however, could have defined more questions and made the content of Table D.1 more granular. But this was not necessary as what we have defined here was enough for us to accomplish our research and reach our goals. The following criteria are defined to register the relevance and support of each resource to our research needs. These are referred to as 'C' followed by the number of each question mentioned below, in TableD.1. We have also referred to these criteria using the mentioned method in Table 4.1 in Section 4.1.

1. Is the resource **related** to network automation?
2. Is the resource using or mentioning Software-defined Networking (SDN) with any of programming languages such as Python (P)[1], automation tools such as Ansible (A)[2], or Other programming languages (O) as a solution to network automation? (The answer Yes to this question means that the resource does not emphasize a specific programming language but mentions SDN as a solution.)
3. Does the resource discuss change management, including updates and upgrades, in traditional networks as a **challenge**?
4. Does the resource suggest Machine Learning (ML) as one solution to network security automation?
5. Does the resource point out the challenge related to **multi-vendor** solutions

---

[1] For Python see Section 4.3.4.

[2] For Ansible see Section 4.3.4.

utilized in the networks?

6. Does the resource discuss network **segmentation** as a solution to the complexity of network security and architecture?
7. Does the resource discuss the importance of the **competency** in network automation techniques among the network engineers who manage the network's daily tasks?
8. Does the resource discuss Cost (C) and Limitations (L) that SDN might bring into the systems leveraging it?
9. Does the resource discuss the relation between raising security in networks or handling security challenges by leveraging SDN techniques and technologies? (It discusses the Inadequacies (I) of SDN on the security of the network, its Positive (P) effect, Both (B), or Neither (No). Yes means, it points at securing the network by leveraging SDN without discussing any positive or negative effect of it)
10. Does the resource give an overview of network security automation methods? (ML means: Yes, an overview of ML methods for automation is provided, SDN means: Yes, the resource gives an overview of SDN as the automation method, IaC means: Yes, the resource gives an overview of Infrastructure as Code (IaC) related technologies and methods which are related to SDN.)
11. Does the resource provide a taxonomy of the network security automation techniques presented?
12. Does the resource put light on Advantages (A), Disadvantages (D), Threats (T), and Opportunities (O) regarding the network security automation techniques presented?
13. Does the resource present the use case customized to each network security automation technique presented?
14. Does the resource discuss traditional network technologies, techniques, and/or architecture?

Appendix D

Table Utilized to Work with the State-of-The-Art

The table utilized in our work with the literature reviewed in the SotA is presented in this appendix. The categorization of the resources and the method we used here was to help us in managing our review of the SotA. The reason why we have attached this table in this appendix to our thesis is to show the method we have used in working with the resources. In Table D.1, presented below, we have categorized the resources based on the criteria we have defined to help us in this research. These criteria are presented in Appendix C. We could have defined more criteria for categorizing these resources, but what we have defined here was enough for us to reach our goal.

These resources have helped us to find answers to RQ1, RQ2, and RQ3. The relation of each resource to the RQs is presented in the last column of the table, with the title RQ. Some of the resources also, as specified in Table D.1, are at the same time related to more than one of the RQs. The year of the publication of each resource is presented next to this column. In this table, the number connected to each resource presented in Bibliography is presented beside their titles. Further, the capital letter 'C' stands for 'Criteria' and is followed by the number of each criterion explained in Appendix C. The abbreviation 'Nr' stands for 'Number' and is just for ordering in the table for all resources based on the row numbers. This row number is NOT referred to in any place in this thesis.

Table D.1: The categorization the literature reviewed in the state-of-the-art based on the defined criteria

Nr	Title	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	Year	RQ
1	Introduction to Python Network Automation [11]	Yes	PO	Yes	No	No	No	Yes	No	No	No	No	No	No	No	2021	2
2	Machine learning for network automation: overview, architecture, and applications [44]	Yes	Yes	Yes	Yes	Yes	No	No	No	Yes	ML	Yes	No	No	No	2018	2
3	5G network slicing using SDN and NFV: A survey of taxonomy, architectures, and future challenges [1]	Yes	Yes	Yes	No	No	Yes	No	No	No	SDN	No	No	Yes	No	2020	2
4	Cisco Certified DevNet Associate DEVASC 200-901 Official Cert Guide [10]	Yes	PAO	Yes	No	Yes	No	Yes	C	P	SDN	No	No	Yes	No	2020	2
5	A survey of machine learning techniques applied to software-defined networking (SDN): Research issues and challenges [45]	Yes	Yes	Yes	Yes	No	No	No	CL	Yes	ML SDN	Yes	AD	Yes	No	2019	2
6	A Survey of Network Automation for Industrial Internet-of-Things Towards Industry 5.0 [46]	Yes	Yes	Yes	No	No	No	No	CL	No	No	No	AO	No	No	2022	2
7	Automation of network simulation: Concepts related to IPv4 and IPv6 convergence [12]	Yes	No	Yes	No	No	No	Yes	No	No	No	No	No	No	No	2019	2
8	Towards security automation in software-defined networks [5]	Yes	P	Yes	Yes	No	Yes	Yes	C	P	ML	Yes	AO	No	No	2022	2

Continued on the next page

Table D.1 – Continued from the previous page

Nr	Title	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	Year	RQ
9	A Survey of Deployment Solutions and Optimization Strategies for Hybrid SDN Networks [47]	Yes	O	Yes	No	No	No	Yes	CL	B	SDN	No	AD	Yes	No	2019	2
10	Hybrid SDN Networks: A Survey of Existing Approaches [13]	Yes	Yes	No	No	No	No	Yes	CL	Yes	No	No	AO	No	No	2018	2
11	Emerging DDoS attack detection and mitigation strategies in software-defined networks: Taxonomy, challenges, and future directions [48]	Yes	P	Yes	Yes	No	Yes	No	L	B	ML SDN	Yes	AO	No	No	2021	2&3
12	Network Automation Using Python [49]	Yes	P	Yes	No	Yes	No	Yes	C	B	SDN	No	ADO	No	No	2020	2&3
13	A Theoretical Discussion and Survey of Network Automation for IoT: Challenges and Opportunity [50]	Yes	Yes	Yes	Yes	No	No	No	C	Yes	ML SDN	No	AO	No	No	2021	2&3
14	SDN in wide-area networks: A survey [14]	Yes	Yes	No	No	No	No	No	L	B	No	No	AD	No	No	2017	2
15	A Comprehensive Survey: Benefits, Services, Recent Works, Challenges, Security, and Use Cases for SDN-VANET [51]	Yes	P	Yes	No	No	No	No	C	Yes	SDN	No	A	Yes	No	2020	2&3
16	Interfaces, attributes, and use cases: A compass for SDN [111]	Yes	Yes	Yes	No	Yes	No	No	No	B	SDN	No	AD	Yes	No	2014	2

Continued on the next page

Table D.1 – Continued from the previous page

Nr	Title	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	Year	RQ
17	Considerations for Software Defined Networking (SDN): Approaches and use cases [52]	Yes	Yes	No	No	No	Yes	No	CL	P	SDN	No	AO	Yes	No	2013	2
18	The Future of Data Center Network Automation - February 2022 EMA Research Report [15]	Yes	Yes	Yes	No	No	No	Yes	CL	B	No	No	ADO	No	No	2022	2&3
19	User fears and challenges in the adoption of network automation [16]	Yes	Yes	Yes	No	No	No	Yes	CL	B	No	No	AD	No	No	2022	2&3
20	DevSecOps: Security Expertise a Key to Automated Testing in CI/CD Pipeline [53]	Yes	No	Yes	No	No	No	No	No	No	No	No	AO	No	No	2020	2&3
21	Tactical network automation with Net-ZTP and one shot [7]	Yes	No	Yes	No	No	No	No	No	No	No	No	AO	Yes	No	2019	2
22	The Role of Artificial Intelligence for Network Automation and Security [54]	Yes	Yes	Yes	Yes	No	No	No	No	P	No	No	AO	No	No	2018	2
23	Accelerating materials development via automation, machine learning, and high-performance computing [55]	Yes	No	No	Yes	No	No	No	No	No	No	No	No	No	No	2018	2
24	Machine learning-based framework for autonomous network management in 5G systems [56]	Yes	Yes	Yes	Yes	No	Yes	No	C	Yes	ML	No	AO	Yes	No	2018	2

Continued on the next page

Table D.1 – Continued from the previous page

Nr	Title	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	Year	RQ
25	Zero Touch Management: A Survey of Network Automation Solutions for 5G and 6G Networks [57]	Yes	Yes	Yes	Yes	No	No	No	No	No	ML	Yes	AO	Yes	No	2022	2
26	Network Automation and Abstraction using Python Programming Methods[58]	Yes	P	Yes	No	Yes	No	No	No	P	No	No	AO	No	No	2017	2
27	Handbook of Computer Networks and Cyber Security (Chapters 13, 14, and 15) [59]	Yes	P	Yes	No	Yes	No	No	L	B	No	No	AD TO	Yes	No	2020	2&3
28	Incremental switch deployment for hybrid software-defined networks [60]	Yes	Yes	Yes	No	No	No	No	CL	No	No	No	No	No	No	2016	2
29	A survey: Typical security issues of software-defined networking [61]	Yes	Yes	Yes	No	No	Yes	No	C	B	SDN	No	TO	No	No	2019	2&3
30	Challenges and solution for measuring available bandwidth in software-defined networks [62]	Yes	P	Yes	No	No	No	No	No	No	No	No	No	No	No	2017	2
31	A theoretical discussion and survey of network automation for IoT: Challenges and opportunity [6]	Yes	Yes	Yes	Yes	No	No	No	C	P	SDN	No	AO	No	No	2021	2&3
32	PayLess: A Low-Cost Network Monitoring Framework for Software Defined Networks [63]	Yes	O	No	No	No	No	No	C	P	No	No	A	No	No	2014	2

Continued on the next page

Table D.1 – Continued from the previous page

Nr	Title	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	Year	RQ
33	Mastering Python Networking: Your one-stop solution to using Python for network automation, programmability, and DevOps [2]	Yes	PAO	Yes	No	No	No	Yes	No	Yes	SDN	No	AO	Yes	No	2020	2
34	CCENT/CCNA ICND1 100-105 Official Cert Guide [26]	No	No	No	No	No	No	No	No	No	No	No	No	No	Yes	2017	1
35	CCNA Routing and Switching ICND2 200-105 Official Cert Guide [115]	No	No	No	No	No	No	No	No	No	No	No	No	No	Yes	2017	1
36	Implementing Cisco IP Switched Networks (SWITCH 300-115) [28]	No	No	No	No	No	No	No	No	No	No	No	No	No	Yes	2014	1
37	Implementing Cisco IP Routing (ROUTE 300-101) [27]	No	No	No	No	No	No	No	No	No	No	No	No	No	Yes	2014	1
38	Troubleshooting and Maintaining Cisco IP Networks (TSHOOT 300-135) [116]	No	No	No	No	No	No	No	No	No	No	No	No	No	Yes	2015	1
39	The Firewall [117]	No	No	No	No	No	No	No	No	No	No	No	No	No	Yes	2022	1
40	Design and implementation of SDN-based proactive firewall system in collaboration with domain name resolution [64]	Yes	Yes	Yes	No	No	No	No	No	P	No	No	AO	No	No	2018	2
41	The analysis of firewall policy through machine learning and data mining [65]	Yes	Yes	Yes	Yes	No	No	No	L	No	ML	No	ADO	No	No	2017	2
42	Next-generation firewall for network security: a survey [114]	No	No	No	No	Only vendors	No	No	No	No	No	No	No	No	Yes	2018	1

Continued on the next page

Table D.1 – Continued from the previous page

Nr	Title	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	Year	RQ
43	Software-defined networking firewall for industry 4.0 manufacturing systems [66]	Yes	Yes	Yes	No	No	No	No	No	P	SDN	No	AO	Yes	No	2018	2
44	Analysis of performance and efficiency of hardware and software firewalls [67]	Yes	Yes	Yes	No	No	No	No	No	P	No	No	AO	No	Yes	2017	1&2
45	Firewall best practices for securing smart healthcare environment: A review [29]	No	No	No	No	No	Yes	No	No	No	No	No	No	No	Yes	2021	1
46	Building firewall over the software-defined network controller [68]	Yes	P	Yes	No	No	No	No	No	P	No	No	AO	Yes	No	2014	2
47	The analysis of firewall policy through machine learning and data mining [69]	Yes	No	No	Yes	No	No	No	CL	No	ML	No	No	No	No	2017	2
48	Zero Trust Networks with VMware NSX [39]	Yes	P	No	No	No	Yes	No	No	No	No	No	No	No	Yes	2019	1
49	Network Programmability and Automation: Skills for the Next-Generation Network Engineer [70]	Yes	PAO	Yes	No	No	No	Yes	C	P	SDN	No	AD	No	No	2018	2
50	Guidelines on Firewalls and Firewall Policy Special Publication 800-41 [118]	No	No	No	No	No	No	No	No	No	No	No	No	No	Yes	2009	1
51	Performance analysis of proposed network architecture: OpenFlow vs. traditional network [71]	Yes	P	Yes	No	No	No	No	No	P	SDN	No	AO	No	No	2016	2

Continued on the next page

Table D.1 – Continued from the previous page

Nr	Title	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	Year	RQ
52	Comparison for the Hardware Defined Networks vs the Software Defined Networks Environments for IPv6 When Applied to the Backbone of the Advanced Network REUNA [72]	Yes	Yes	Yes	No	No	No	No	L	B	SDN	No	No	No	No	2021	2
53	Lightweight testbed for machine learning evaluation in 5G networks [73]	Yes	P	Yes	Yes	No	Yes	No	C	P	ML SDN	No	AO	No	No	2019	2
54	Towards ML-based Management of Software-Defined Networks [74]	Yes	P	Yes	Yes	No	No	No	C	P	ML SDN	No	AO	Yes	No	2021	2
55	RPA-RA: A resource preference aware routing algorithm in software-defined network [75]	Yes	Yes	Yes	No	No	No	No	No	P	SDN	No	A	No	No	2015	2
56	Software-defined networks: a comprehensive approach [76]	Yes	P	Yes	No	Yes	No	Yes	CL	B	No	No	AD TO	Yes	No	2016	2&3
57	Using machine learning for cognitive Robotic Process Automation (RPA) [77]	Yes	P	No	Yes	No	No	No	No	Yes	ML	No	A	No	No	2020	2
58	Machine-learning techniques for detecting attacks in SDN [78]	Yes	Yes	Yes	Yes	No	No	No	L	B	ML	No	AT	No	No	2019	2
59	Infrastructure as code: managing servers in the cloud [79]	Yes	PAO	Yes	No	No	No	Yes	CL	No	IaC	No	No	No	No	2016	2
60	SAFE: SDN-assisted framework for edge–cloud interplay in secure healthcare ecosystem [35]	Yes	Yes	Yes	No	No	No	No	No	P	SDN	No	AO	Yes	No	2019	2

Continued on the next page

Table D.1 – Continued from the previous page

Nr	Title	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	Year	RQ
61	Modern API Development with Spring and Spring Boot: Design highly scalable and maintainable APIs with REST, gRPC, GraphQL, and the reactive paradigm [80]	Yes	Yes	Yes	No	No	No	Yes	No	P	SDN IaC	No	A	No	No	2021	2
62	Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges [81]	Yes	Yes	No	No	No	No	No	L	B	SDN	No	AD TO	Yes	No	2016	2&3
63	Security risk assessment for SDN-enabled smart grids [34]	Yes	Yes	No	No	No	No	No	No	P	No	No	O	No	No	2019	2&3
64	A survey and a layered taxonomy of software-defined networking [82]	Yes	P	Yes	No	No	No	No	C	B	SDN	Yes	AD O	Yes	No	2014	2
65	Impacts of blockchain in software-defined Internet of Things ecosystem with Network Function Virtualization for smart applications: Present perspectives and future directions [83]	Yes	Yes	Yes	Yes	No	No	Yes	No	B	SDN	No	AD	Yes	No	2023	2
66	Software-defined networking: A comprehensive survey [43]	Yes	Yes	Yes	No	Yes	No	No	CL	B	SDN	No	AO	Yes	No	2014	2&3

Continued on the next page

Table D.1 – Continued from the previous page

Nr	Title	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	Year	RQ
67	The effectiveness of Automatic Network Administration (ANA) in network automation simulation at Universitas Pendidikan Ganesha [8]	Yes	PA	Yes	No	Yes	No	No	C	P	SDN	No	AO	No	No	2021	2
68	Network Automation Cookbook: Proven and actionable recipes to automate and manage network devices using Ansible [84]	Yes	PA	Yes	No	Yes	Yes	Yes	No	P	SDN	No	A	Yes	No	2020	2
69	Practical Network Automation: Leverage the power of Python and Ansible to optimize your network [85]	Yes	PA	Yes	No	Yes	No	Yes	C	P	SDN	No	AO	Yes	No	2017	2
70	Zero Trust Architecture NIST SP 800-207 [40]	Yes	Yes	No	Yes	No	Yes	No	No	Yes	No	No	No	No	Yes	2020	1&2
71	Distributed SDN control: Survey, taxonomy, and challenges [86]	Yes	P	No	No	No	No	No	No	No	SDN	Yes	A	Yes	No	2017	2
72	A comprehensive survey: Benefits, services, recent works, challenges, security, and use cases for sdn-vanet [87]	Yes	P	No	Yes	No	No	No	C	B	ML SDN	No	AO	Yes	No	2020	2
73	Implementing a zero trust architecture [113]	No	No	No	Yes	No	Yes	No	No	No	No	No	No	No	Yes	2020	1
74	Automation and Orchestration of Zero Trust Architecture: Potential Solutions and Challenges [88]	Yes	Yes	Yes	Yes	No	Yes	No	No	Yes	No	No	No	No	Yes	2022	1&2

Continued on the next page

Table D.1 – Continued from the previous page

Nr	Title	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	Year	RQ
75	Survey on Zero-Trust Network Security [41]	Yes	Yes	Yes	Yes	No	Yes	No	No	Yes	No	No	No	No	Yes	2020	1&2
76	Impact of Network Automation [89]	Yes	A	Yes	No	No	No	No	No	P	No	No	AO	Yes	No	2018	2
77	Introducing programmability and automation in the synthesis of virtual firewall rules [90]	Yes	Yes	Yes	No	No	No	No	No	P	SDN	No	AO	Yes	No	2020	2&3
78	Fortress: an efficient and distributed firewall for stateful data plane SDN [91]	Yes	Yes	Yes	No	No	No	No	L	Yes	SDN	No	AO	Yes	No	2019	2&3
79	Formal verification of SDN-based firewalls by using TLA+ (2020) [92]	Yes	Yes	Yes	No	No	No	No	No	Yes	SDN	No	A	No	No	2020	2&3
80	Survey on application programming interfaces in software-defined networks and network function virtualization [93]	Yes	P	Yes	No	No	No	No	No	P	Yes	Yes	AO	Yes	No	2021	2&3
81	Evaluation of four SDN controllers with firewall modules [94]	Yes	P	Yes	No	Yes	No	No	C	P	SDN	No	AO	Yes	No	2020	2&3
82	DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges [42]	Yes	Yes	Yes	No	Yes	No	No	CL	B	No	No	ADTO	No	No	2021	2&3
83	Zero-Day Attack Detection and Prevention in Software-Defined Networks [95]	Yes	P	Yes	No	No	No	No	No	B	No	No	ADTO	No	No	2019	2&3

Continued on the next page

Table D.1 – Continued from the previous page

Nr	Title	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	Year	RQ
84	Research on LDoS Attack Detection and Defense Mechanism in Software Defined Networks [96]	Yes	Yes	No	No	No	No	No	L	I	No	No	DT	No	No	2020	2&3
85	Vulnerability Assessment and Analysis of Software-Defined Networking using a Virtual Testbed [97]	Yes	Yes	No	No	No	No	No	L	I	No	No	DT	No	No	2022	2&3
86	An intelligent software-defined networking controller component to detect and mitigate denial of service attacks [98]	Yes	Yes	No	No	No	No	No	L	I	No	No	DT	No	No	2021	2&3
87	Taxonomy of DDoS Attacks in Software-Defined Networking Environment [99]	Yes	Yes	No	No	No	No	No	L	I	Yes	No	DT	No	No	2019	2&3
88	IQR-based approach for DDoS detection and mitigation in SDN [100]	Yes	P	No	No	No	No	No	L	I	No	No	DT	No	No	2022	2&3
89	Solutions to Vulnerabilities and Threats in Software Defined Networking (SDN) [101]	Yes	Yes	No	No	No	No	No	L	I	No	No	DT	No	No	2020	2&3
90	Man in The Middle Attacks on Software Defined Network [102]	Yes	P	Yes	No	No	No	No	L	I	No	No	DT	No	No	2023	2&3
91	Kubernetes Cookbook: Practical solutions to container orchestration [103]	Yes	PAO	Yes	No	No	No	Yes	No	P	SDN	No	AO	Yes	No	2018	2

Continued on the next page

Table D.1 – Continued from the previous page

Nr	Title	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	Year	RQ
92	Transition to SDN is HARMLESS: Hybrid architecture for migrating legacy ethernet switches to SDN [104]	Yes	PO	Yes	No	Yes	No	No	CL	B	No	No	AO	Yes	No	2020	2
93	Cisco Certified DevNet Professional DEVCOR 350-901 Official Cert Guide [17]	Yes	PAO	Yes	No	No	Yes	Yes	CL	B	SDN	No	AO	Yes	No	2023	2
94	Enterprise cloud-native automation [105]	Yes	Yes	Yes	No	Yes	No	Yes	No	P	IaC	No	AO	No	No	2022	2
95	Management and Orchestration of Edge Computing for IoT: A Comprehensive Survey [106]	Yes	Yes	Yes	Yes	No	No	No	CL	No	ML	No	A	Yes	No	2023	2
96	Formal specification and verification of firewall using TLA+ (2017) [107]	Yes	Yes	Yes	No	No	No	No	No	P	No	No	A	No	No	2017	2
97	Microservices: How to make your application scale [108]	Yes	O	No	No	No	No	No	No	No	IaC	No	A	Yes	No	2018	2
98	Mastering Azure Machine Learning Perform large-scale end-to-end advanced machine learning in the cloud with Microsoft Azure Machine Learning [109]	Yes	No	No	Yes	No	No	No	C	No	ML	No	A	Yes	No	2020	2
99	A generalized flow for B2B sales predictive modeling: An azure machine-learning approach [110]	Yes	P	No	Yes	No	No	No	No	No	ML	No	O	No	No	2020	2

Continued on the next page

Table D.1 – Continued from the previous page

Nr	Title	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	Year	RQ
100	Mitigating malicious packets attack via vulnerability-aware heterogeneous network devices assignment [112]	No	No	Yes	No	No	No	No	C	No	No	No	T	No	Yes	2020	1&3

Appendix E

Review of a Selection of Resources in the SotA

In this appendix, we present a more comprehensive review of a selection of the resources studied in the SotA. These resources suggest and use different methods and technologies. The presentation here is divided into three main subsections each of which discusses the related resources to one of the three RQs. In some of these subsections, more granular divisions are made to make it more presentable. Some category divisions are approximate as one resource can, at the same time, be related to different categories. The categories used in this section are to provide a more comprehensible overview.

Resources Related to RQ1

This section presents a selection of the resources studied in the SotA that are to assist us in answering RQ1, which is related to the existing network security techniques and technologies such as firewalls in different forms, the existing knowledge related to network management, and the different network security architectures.

Traditional Network Management Knowledge

Odom, Wendell in CCENT CCNA ICND1 100-105 Official Cert Guide [26] and CCNA Routing and Switching ICND2 200-101 [115] explains all around network concepts and setup for who is on their way to work on IP networks. In these two books, however, there is not even one sign about network automation concepts. This is despite the book DEVASC 200-901 Official Cert Guide [10] being published only three years after the publication of the ICND1 and ICND2 books from Odom, Wendell. This huge difference shows us how quickly network development is moving towards utilizing automation techniques.

This also applies to the books published by the same publisher but other authors, Cisco for professional network engineers, Implementing Cisco IP Switched Networks (SWITCH 300-115) [28], Implementing Cisco IP Routing (ROUTE 300-101) [27], and Troubleshooting and Maintaining Cisco IP Networks (TSHOOT 300-135) [116]. Despite these network professional books being enriched with network-related knowledge, none of these, which were published in 2014-2015, has any sign about automation concepts in networks which is another proof that network deployment is evolving faster toward automation of the processes.

Traditional Firewalls

Different types of firewalls, including both first and next generation are reviewed in one of the surveys studied in the SotA [114, p. 1-4]. The mentioned survey also sheds light on the advantages and functionalities of different types of firewalls in addition to the need and necessity of the NGFWs. Providing an overview of the cyber attack vectors, this resource explains why NGFWs is the answer to the existing threats in cyberspace. Comparing the four generations of firewalls, this work highlights the extra functionalities of NGFWs.

The above-mentioned resource also makes a comparison between traditional and NGFWs in addition to comparing different firewall types based on their vendors [114, p. 4-6]. Despite the comparison between different vendor products, this resource does not point out the challenges the variety of the different existing firewall products in the market will bring to the management of network security. On the other hand, it points to the functionality of each solution provided by each vendor, which is a useful starting point to see the advantages of each of the discussed firewall products.

One of the resources studied in this research focuses on the implementation of the firewalls in CIS networks instances, such as healthcare sectors [29]. This resource brings to light the importance of network security with firewalls on top of it in the healthcare network environment and provides an overview of best practices in this context. The paper enumerates different types of firewalls in the healthcare sector in addition to security challenges in this environment and the vulnerabilities of the firewalls. This work emphasizes the importance of legitimate users' access to healthcare data in the health sector and highlights that unauthorized access should be prohibited in the healthcare network and data environment.

Another resource studied in the SotA, provides an overview of different firewall technologies and network architectures [118]. This NIST published resource, also enumerates firewall policies and how to plan and implement the firewalls. The resource was last updated in 2009, which lacks the newer network security technology and architecture-related information. The reason why we have reviewed this resource is that some of the other resources that we have utilized in this thesis, such as Anwar, R. W., Abdullah, T., & Pastore, F. [29] refer to NIST's publication [118] as their resource which makes it a secondary resource for us.

The other reason for reviewing this NIST associated resource is that this is the last publication we found from NIST about firewalls.

Resources Related to RQ2

This section briefly presents a selection of the resources studied in the literature review. These resources are to answer and assist us in finding the answer to RQ2 about raising the efficiency, resilience, and security of the network by utilizing network automation techniques and technologies. We present some of the resources that have contents closer to the concept of SDN, ML, and finally, those resources that present experiments with lab environment related to NSA.

Resources More Closer to Software Defined Networking

Focusing on the 5G mobile network, the different technologies used to enable 5G network slicing are discussed [1]. The technologies reviewed include SDN, Traffic management applications for stateful SDN data plane, NFV, Multi-access Edge Computing (MEC), Cloud/fog computing, Network hypervisors, VMs, and finally containers. The cloud computing discussed here includes heterogeneous infrastructures such as SaaS, PaaS, and IaaS where customer company chooses the environment based on their needs.

Different vendors, such as Microsoft Azure, Amazon Web Services (AWS), and Google Compute Engine, that provide cloud computing services for customers are enumerated, and hypervisor as a solution for network virtualization is explained without paying attention to the complexities of multi-vendor supports for applications and services bring to the customers [1, p. 13].

Some challenges related to this topic, from the aspect of the end user and the tenant, are discussed [1, p. 30-33]. For instance, one of the challenges mentioned is about costs related to different business models and economic challenges related to these models, such as Business to Business (B2B), Business to Customer (B2C), or Business to Business to Customer (B2B2C), or the challenges related to the security of the network that escalates the complexity of the already existing cyber security challenges when slicing the network.

A comprehensive overview of what are the different elements and requirements of SDN in a level that is required for development associate network engineers to manage are provided [10]. The readers are provided with a broad range of basic knowledge and concepts about network development so that they can make themselves familiar with network development [10]. When it comes to automation languages, however, the overview given by the same resource about the usage of Puppet, as a tool related to network automation, is extremely short.

This shortage also applies to the other network programming languages or automation tools used for automation, such as Ansible and Chef [10, Chapter 15-p. 759-773]. Here, however, it is put more focus on explaining Python and different platforms used for different phases of automation operations. The reason for this might be that the book is made for beginners' level who need to take the first step to make themselves familiar with network and automation concepts and elements. Despite that, readers who need to practice automation techniques to achieve a feeling of mastery in network automation suffer as the book does not provide a holistic lab from the start to the end of a complete process. This resource is mainly provided to help students pass the DevNet Associate theoretical exam, as the book itself also mentions [10, Chapter 15-p. 56-57].

Some authors even go further than only automating network operations and also focus on automating security mechanisms in SDN [5]. This resource is closer to what RQ2 asks about. The reason why automation should be done, not only in operation tasks but also in the security of the network, is also explained. They mention the problem of the growth of the network while the complex tasks shall be managed manually by network administrators. At the same time, the authors shed light on the vulnerability of manual task management being error-prone, which is one of the problems we have pointed out in Section 1.4.

The network architecture where zero trust and micro-segmentation are utilized to provide a higher level of security is presented [39]. They also discuss zone-based defense network architecture, as a less secure network security architecture compared to micro-segmentation, but more secure than the traditional manner of implementing firewalls and other requirements of network security. VMware NSX[1] is the platform used for explaining this network architecture, which makes running VMs on this platform closer to applications.

The importance of network security automation is emphasized by this resource and the possibilities in VMware for utilization of Representational State Transfer (REST) Application Programming Interface (API)[2] for incorporation of automation tools is mentioned [39, p. 23-25]. This book also shows how tasks such as creating firewall rules, creating security groups, and adding members to these security groups can be automated [39, Chapter 6].

Choi B. in [11] goes step-by-step through the learning of Linux programming, Python programming, set up of the GNS3 lab, and then executing the automation labs by using Python programming code scripts. This book is a valuable guide for every learner who wishes to get hands-on with network automation. One thing to mention is that with the rapid change and advancement of technology and the related documentation made available on different websites that the book refers to, many of the links and references have already become non-functional.

This is despite the mentioned book [11] being written in 2021. So the learners need to work on the solutions and adapt the book's references to the market's up-

---

[1] Underlying hardware independent, VMware NSX makes it possible for both containers, VMs, and physical hosts to run on this platform.

[2] REST API is explained in Section 4.3.4.

dated solutions. Noteworthy, however, as the writer of the book also emphasizes, is that earning and practicing programming skills, here Python being referred to, plays a significant role in being able to raise one's proficiency not only in the automation of the network but also for opening the doors in one's carrier path to many new and more exciting possibilities. A slightly similar work is provided by Milios G. [49], where one can follow the guides provided step by step to practice hands-on and learn about network automation using Python programming language and its libraries.

Some resources compare the two approaches to managing networks. [71]. These two approaches include traditional management of networks and SDN based management of networks. The motivation for this work is mentioned to be the increasing complexity of the network by adding hosts, nodes, and typologies in addition to different technologies that enable communications, which makes the management of the networks even more difficult and infeasible. This work has utilized Mininet to test their theory and concludes with SDN as the solution to this problem.

Connecting this part to SDN, they give an overview on where in SDN is ML applied. This includes the classification of the traffic, routing optimization, the prediction of Quality of Service (QoS)/Quality of Experience (QoE), resource management, and security [45, p. 403-416]. Among the challenges discussed related to SDN, the need for high-quality training data sets, the need to make all network switches SDN-aware by using a distributed multi-controller platform, and the lack of intelligence in switches' data planes are mentioned. The latter challenge is mainly imposed because switches only send data they receive to the controller, which makes the attackers take advantage of this vulnerability and overload the controller [45, p. 416-421].

The importance of the expertise of the network engineers, who manage the daily tasks of the network, and the need to leverage automation techniques is discussed [12]. This resource presents the simulation of network automation for the transition between IPv4[3] and IPv6[4]. Comparing this transition process, they conclude that it can be done much faster and with less cost by using automation techniques.

Shamus McGillicuddy as the vice president of the research in their research report [15], puts light on the importance of network automation. The annual report of EMA that in 2021 had more focus on reporting the state of data center networking in 2022 had a focus on the future of data center network automation. Their research report includes participants from many large companies and is a

---

[3] Internet Protocol version 4 (IPv4) refers to the 32-bit addressing method used on our devices to connect to the web while it operates at the network layer of the OSI model [26, Chapter 21].

[4] While IPv4 was getting exhausted, the 128-bit length method of addressing devices, Internet Protocol version 6 (IPv6), came which among others will save us from the problem of running out of IP addresses [26, Chapter 28].

comprehensive report.

We don't count the EMA report [15] as a total white paper, nor do we look at it as a total scientific paper. This is because the report is sponsored by other large IT technology-provider companies such as RedHat, VMware, Juniper, Nokia, IP Fabric, and Gluware. Therefore, we refer to their research result in combination with other scientific papers where appropriate. More interesting is that EMA has changed focus totally to evaluate network automation in large companies and reflect on the result of the research on that. This also proves that there is a reason to write this thesis and focus on this topic.

The book 'Handbook of Computer Networks and Cyber Security' in [59, Chapter 13 p. 313-337] discusses SDN usage regarding automation of firewall and Load Balencer (LB). This chapter explains components of SDN and compares traditional and SDN-based applications. It takes a look at four different automation models in the background and explains the difference between proactive and reactive SDN controllers. Different SDN controllers with their various programmatic languages are mentioned. This is interesting for us as we are trying to find out if using different applications from different vendors will cause extra challenges in network security. This chapter of this resource provides a small testbed called Mininet.

The mentioned chapter also discusses the two strategies of whitelisting[5] and blacklisting[6] in addition to explaining SDN-firewall and its usage. [59, Chapter 13 p. 333] introduces LB and the need to SDN management approach in traditional LBs. Finally, this chapter of the book discusses SDN related challenges and the application areas of this technology [59, Chapter 13 p. 335-334]. In Chapter 14 of the book 'Handbook of Computer Networks and Cyber Security' [59, Chapter 14 p. 340-378] which is about issues, solutions, and future directions in SDN data plane security, in addition to explaining SDN components, an analysis of SDN security, including a vulnerability assessment, a taxonomy of cyber attacks against SDN, an overview of the literature related to SDN security, and an overview of control plane and data plane security is provided.

Some resources, such as one of the surveys, set the focus on having hybrid solutions by deploying both traditional and SDN solutions for network automation [47, p. 1483-1504]. Despite mentioning the advantages of having a hybrid solution for network deployment, this resource also uncovers the disadvantages of deploying this type of solution. In the hybrid solutions, mixing traditional and SDN techniques, error-prone deployment processes, risk of inconsistencies, and complexity are mentioned as challenges. The resource points out use cases for hybrid SDN technology in addition to deployment strategies for hybrid networks [47, p. 1497-1503]. Further, the structure of hybrid SDN and the deployment solutions

---

[5] Whitelisting strategy in firewall rule implementation is an approach to not allow any traffic besides those defined as allowed in the firewall rules [59, Chapter 13 p. 331].

[6] Blacklisting strategy in firewall rule implementation is about allowing all traffic through the firewall besides those that are forbidden by setting up specific firewall rules [59, Chapter 13 p. 331].

in each part of this structure is explained. Last but not least, it sheds light on security improvement in addition to budget and economic challenges as a consequence of this solution.

Challenges related to the cost of network automation by using SDN solutions have also been paid attention to [60]. This resource suggests using the given budget and deploying the least number of SDN switches, mentioning that all network flows need to go through at least one SDN switch. In a simulation provided in this resource, they claim to be able to control 95% of the network flows by consuming only 10% of the given upgrading budget.

Some resources pay attention to the security challenges in SDN and suggest solutions to the security issues mentioned in their work [61]. Providing a list of the security issues in SDN, their work points out attack vectors, security defense technology, and the suggested security methods for each of the abstracted layers in SDN. The review of the security issues in SDN automation technology in this resource is considerable for us as we need to see both opportunities and threats related to automation techniques to evaluate them properly and give a holistic view in our analysis.

Putting light on the increase of the network complexity by improvement of the technology some resources point to moving toward a smart world with smart IoT and smart CIS, including but not limited to smart city, agriculture, transport, and healthcare [6]. This resource points out the importance of reducing the cost and amount of work moving toward networks that manage themselves automatically. This article introduces the work the European Telecommunication Standardization Institute (ETSI) has done to Generic Autonomic Network Architecture (GANA) related to SDN, NFV[7], ML, and other network automation-related technologies.

Some resources suggest utilizing Ansible to simplify network automation [70]. This book also explores various tools and technologies, including programming languages like Python and Linux, which are relevant choices for network automation. It further explains how to handle source code using Git as an effective method for Continuous Integration and Continuous Delivery (CI/CD)[8].

Additionally, the cited resource as [70] mentions different data formats and data models used in network automation tasks, such as YAML, XML, and JSON. The book also touches on network APIs, including the Network Configuration Protocol (NETCONF) and HTTP-based APIs, which are vital for network automation. The book sheds light on the importance of organizational management in developing a strategy for implementing network automation[9].

---

[7] For an explanation about NFV see Section 4.3.3.

[8] You will find the explanation about Git and CI/CD in Section 4.3.4.

[9] While YAML is a data serialization format, XML and JSON are data interchange formats. For more explanation about YAML, XML, JSON, NETCONF, and API see Section 4.3.4.

Machine Learning

One of the resources evaluates both ML, Reinforcement Learning (RL), and Deap Learning (DL) as the Artificial Intelligence (AI) techniques contributing to reactive security solutions, while it points at NFV, network segmentation, cyber deception, moving target defense, and blockchain as proactive solutions for security [5, p. 76]. While the resource pays attention to cyber security threats such as Advanced Persistent Threat (APT), and the need for more IT security professionals, the proactive security techniques are pointed at to be leveraged for reducing the exploitable surface for cyber attacks. Among the open problems mentioned, the urgency and need for automation of security are explained while the statistics made available by Cisco's report are used as the base for their arguments [5, p. 78].

In [45], the authors present how to leverage ML to improve SDN as a technique for network automation. They provide a taxonomy of SDN based on ML and give an overview of the SDN workflow. Going through ML algorithms Supervised Learning (SL), Unsupervised Learning (USL), Semi-supervised Learning, and USL and deep-diving in different ML algorithms, they also present the shortcomings and the advantages of each ML algorithm they discuss [45, p. 397-403], which can assist us in finding the answer to RQ2.

Leveraging ML in SDN architecture is also mentioned by other resources [74]. Here, it is to shed light on the inefficiencies of traditional network management techniques where the results and processes are error-prone, troubleshooting mechanisms and performance are poor, and monitoring processes are inefficient. This resource provides solutions in data collection with SDN utilizing ML effectiveness to experiment with complex tasks.

There are also suggestions about utilizing six different ML based algorithms to analyze firewall rule anomalies [69]. Based on the experiment, they provide a risk analysis and conclude that ML is useful for finding firewall anomalies. They also emphasize that due to the number of firewall rules to be analyzed by the algorithms, it is needed to reduce and justify the number of rules to be analyzed, in addition to considering the fact about hardware capacity needed for being able to process a significant amount of logs produced by firewalls.

Considering fiber optic communication, some resources pay specific attention to ML as a solution to the challenges of network demands [44, p. 128-130]. They point out the time-consuming difficulties in the management of network implementation and maintenance. They present four ML families including Semi-supervised, SL, USL, and RL with the three latter as the main methods. In SL family they explain three ML algorithms including K-Nearest Neighbors (KNN), Artificial Neural Networks (ANN), Support Vector Machine (SVM). In USL family the algorithms presented include K-Mean Clustering, Principal Component Analysis (PCA), and Self-Organizing Maps (SOM). Finally, in RL family they present the Q-Learning algorithm. All mentioned methods are presented in their work as being relevant for network automation.

Further, they in [44, p. 130-132] discuss several evaluation strategies for ML algorithms including evaluation from data aspects and performance aspects. Network probes, sensors, network logs, control signaling, and network management data are mentioned as sources for data collection for ML-driven network operations where static, dynamic, text, and multidimensional data are the categories of the data types collected. When it comes to SDN, it emphasizes that for ML to work effectively it needs to be integrated into the software code for network automation. This resource even mentions that one complexity that exaggerates the challenge of network change management is related to the fact that networks are managed by multi-vendor and multi-layer solutions [44, p. 134].

Another resource focuses on how ML can effectively be utilized in the automation of network management [74], but this resource does not research to what degree the automation is utilized in CIS companies, or if it is seldom utilized, what is the reason for that. As long as our research shows, the same applies to some other works done with a focus on how to automate or utilize automation techniques in network security while they do not pay any attention to the importance and lack of competency among network engineers in this field. They neither focus on the role of the management in this relation. These types of resources, which are many, are still related to our research when it comes to providing an overview of automation techniques to answer RQ2.

The first chapter of the book Artificial Intelligence for Autonomous Networks [54, Chapter 1-p. 2-21] not only discusses automation by SDN but also takes one step longer and brings the topic of the autonomous network into the discussion. This chapter starts with presenting a history of the network from the beginning where Morce code was invented by Samuel Morce and his assistant in 1837. It explains the improvements done in the network circuits until the time when the network traffic increases exponentially. This has taken place between the years 2007 and 2016, but the article emphasizes that the amount of network traffic which already has increased by 250,000% will continue to grow which shows the exponential speed of network expansion.

The same resource mentions that the legacy packet processing systems are no longer delivering enough flexibility, automation, and elasticity that is needed in network management and that the only way for responding to the growing needs is to establish SDN together with NFV to manage the overwhelming load of network traffic [54]. They further explain AI and its relation to SDN as a perfect connection [54, Chapter 1-p. 10]. The result of this connection is said to be an autonomous network. The opportunities of having ML, AI, and SDN are enumerated with among others a strong effect on the improvement of network security [54].

Experiment with Lab Environments

The lightweight containerized lab environment for testing ML is presented as a network automation method [73]. This resource points to network automation as a solution for reducing operational costs in addition to human errors, caused by the manual implementation of network configurations. It is mentioned that the Mininet lab environment is an answer to the problems researchers have in testing ML solutions for network automation. Their test method and combination of containers, SDN, and ML to prove the ability of network automation in predicting the real-time bandwidth is impressive [73].

Another resource utilizes Mininet and GNS3 to implement and compare the two approaches in network management [72]. They use Mininet to experiment with SDN, and GNS3 is utilized for using the traditional method of network management. The result of their emulation shows that SDN uses less time for transition, processing, and convergence time, and uses fewer resources in comparison with the traditional manner of managing network resources. The result does not hide the disadvantage of SDN compared to the hardware-defined network which is higher bandwidth usage. For instance, this is demonstrated when the SDN tested in Mininet had a 13,977.97 Mbps bandwidth usage while this number for hardware-defined networks was 2.95 Mbps.

Another research group experiments in the Mininet testbed to find a PayLess solution in a monitoring model in SDN [63]. The reason for focusing on the monitoring framework, as they mention, is that this is an essential task from both perspectives of security and maintenance in the network. They explain that monitoring can give overhead. What they try to do is to provide a programming model for this task to overcome this challenge. They explain the PayLess architecture setup and test their hypothesis in a Mininet testbed to request statistics from the network.

One of the resources reviews challenges related to SDN approach for network automation for providing QoS related services [62]. Pointing at the separation between the control plane and the data plane in SDN, it explains the complexities introduced into network management by this separation. This work provides a simulation of SDN using Mininet[10] virtual testbed to validate their proposed technique for measurement of the available bandwidth. This resource also discusses errors and limitations of SDN and Openflow and suggests solutions to these.

---

[10] Mininet is a virtual testbed that uses the Python programming language for simulation of SDN with minimum needs for lab equipment. In this type of lab environment, one can simulate every switch, router, and host by code scripts. This virtual testbed has a Mininet Community that provides documentation and improvements on this solution for testing and training on network automation [62, 63, 72].

Resources Relate to RQ3

This section presents a selection of the literature reviewed that will help us map the answers to RQ3. These are to assist us with key factors that affect the adoption of network security automation techniques in organizations. Some examples of such key factors include cost, vendor lock-in, and challenges related to network automation. Other instances of such documents that answer our third RQ include the documents that explain SWOT characteristics, limitations, and opportunities related to network automation.

One of the resources puts light on SDN utilization in CIS IP network infrastructure and reviews the risks related to this solution [34]. This paper reviews different types of cyber attacks on CIS IP network and the goals that cybercriminals want to achieve. It also points to SDN as a solution that brings limitless opportunities in how to secure CIS gigantic network where, at the moment, according to their claim, no other security solution exists. An instance of lack of security is mentioned to be in securing ISPs against DoS attacks.

The relation of SDN to IIoT in industry 4.0[11] is discussed in one of the resources in the SotA [46]. Here, the motivation for network automation in industry 5.0[12] and its advantages are enumerated in addition to enumerating industry 4.0 flaws and shortcomings. The correlation of IIoT network automation to the standard IEEE P2668[13] is explained in addition to defining what is expected from network automation. Their definition emphasizes that network automation can be self-configuring, self-optimizing, self-protecting, and self-healing. The article presents network automation as the only potential solution for the needs required for industry 5.0 with also a reduction in operating costs [46, p. 2065].

Discussing the challenges, the above-mentioned resource puts light on the improvement of the technology where 5G and Industry 4.0 will be replaced with 6G and Industry 5.0. Here, it talks about ‘Green’ IIoT by Harmonization of energy efficiency and QoS/QoE. Also, it talks about receiving ‘real-time feedback from users via sensors’ by improving human-robot collaboration [46, p. 2075]. Another challenge mentioned in this article is related to security and privacy. This challenge comes up when improving technology towards 6G-based Industry 5.0 and when having heterogeneous network devices. In this relation, it is mentioned that we can experience higher cyber attack risk to our network assets.

One of the resources, in addition to pointing at the positive sides of leveraging SDN in the automation of network, puts light on the effect of this technology and the related strategies for mitigation of DDoS cyber attacks [48, p. 6]. From the aspect of IT security, strategies such as blockchain, ML, network segmentation,

---

[11] Industry 4.0 refers to including communication and IT technology into industry [46].

[12] Industry 5.0 refers to where the focus is more set on how customers experience the services delivered with a more human-centric priority [46].

[13] IEEE P2668 refers to the standard set for IoT where among others the formats for IoT Maturity Index (IDex) are specified [46, p. 2065].

honeynets, and SDN architecture are suggested as useful countermeasures. They review both inadequacies and the advantages of SDN for the security of the network.

The discussions in another one of the resources imply that the characteristics of SDN, such as scalability, automation, and contribution to workflow, improve the security of the network [48, p. 4-5]. They mention that at the same time, there are weaknesses that we should be aware of. These also expand new opportunities for future research. According to this resource, the security-related challenges in SDN devices include limitation of memory, centralization of the controller as a point of failure, distributed controllers having security issues, and the vulnerability of the communication channel between the controller and the device.

Another resource studied in the SotA, provides an overview of the changes applied to traditional network routing by introducing SDN approach in networks [76]. In addition, this resource sheds light on the challenges that organizations are facing in the transition from traditional networking approaches to software-defined networking. Also, inadequacies in the networks, that do not have network automation applied, in addition to OpenFlow limitations are explained.

The work of the above-mentioned resource is interesting for our research where we are going through the definition of SDN and OpenFlow, and more specifically when we work on SWOT analysis of the application of network security automation technology to the traditional network management architecture. Moreover, the mentioned resource's discussions about the efficiency and characteristics of SDN in automation of firewalls, the related use cases, limitations, and benefits of network automation are also interesting and useful to our research [76].

Appendix F

Comprehensive SWOT Analysis of Traditional Network Security Management Characteristics - RQ1

In this appendix, we offer an extensive examination of the characteristics associated with traditional network security architectures and firewall management. To maintain the thesis's conciseness, we have presented specific details regarding these techniques and technologies in Appendix B.

The SWOT analysis presented here assesses four types of traditional network security techniques and technologies discussed in the SotA reviewed during this research. These encompass traditional firewalls and DMZ network security architecture, zone-based network architecture, micro-segmentation network security architecture, and zero trust network security architecture.

Since these traditional techniques and technologies are well-established, comprehensive information on them is available in Appendix B. In this section, we furnish a thorough SWOT analysis of these four network security architectures, while a summary of this analysis is provided in Chapter 4[1].

F.1 SWOT Analysis of Traditional Firewalls and DMZ Network Security Architecture - RQ1

IP network firewalls are elaborated on in Appendix B in detail. That appendix includes how the security strategies of black listing and white listing work, what

---

[1] To better understand our discussion on network security, please refer to Section 3.3.

are the firewall structures, different firewall types, different firewall technologies, and how traditional network security and firewalls are managed.

Following the study of the SotA, in traditional network security and firewall management, the network technician has to do the tasks manually. For instance, this could be accomplished by using the Command-Line Interface (CLI) per network device, such as a layer three (L3) switch or a router to set up the desired settings, or by utilizing the Graphical User Interface (GUI) of the firewall application for implementation or update of firewall rules. Regarding the firewalls, the rules need to be implemented one by one. When it comes to setting up routers and switches, while manually managed, the fastest way to do that is to use the commands that include, for instance, a range of interfaces so that one does not need to implement or update interfaces one by one[2]. Without automation technology, one still needs to log into and manage devices manually [5, 27, 28, 71][3].

Appendix B, is where we also presented Demilitarized Zone (DMZ) as a more uncomplicated network security architecture strategy in more detail. For raising the security of the network, the DMZ could be complicated by adding the technologies that would be utilized in this perimeter zone. In comparison with the other network security architectures, such as zone-based defense network security architecture, micro-segmentation, and zero-trust network security strategy, however, it still is simpler and, in a way, utilized as a subset of those more complicated network security architectures. Below, we delve into a SWOT analysis of firewalls and DMZ network security architecture when managed through traditional manual methods:

Strengths

1. Firewalls applications are easy to set up and utilize because of their GUI-based interface [118, 120].
2. Less competency and experience are needed for managing firewall rules, as those who work with the firewall applications will learn the application by utilizing their GUI interface [118, 120].
3. Firewalls GUI-based platforms make it easy to add new security rules, both for allowing or denying network traffic [118, 120].
4. Firewall applications, as explained in Appendix B, make complicated security functionalities easy and available to users. These functionalities include but are not limited to different firewall types, such as host-based, Web application firewalls, and network firewalls; different structures, such as hard-

---

[2] A reminder is in order here regarding our definition of network security, as outlined in Section 3.3. This definition encompasses security measures such as shutting down unused interfaces, isolating unused VLANs within a black hole VLAN, and incorporating various other security measures into the network security framework.

[3] Within this SWOT analysis, where we make use of several resources to substantiate our reasoning, these referenced resources harmonize with each other. This signifies that, collectively, they reinforce the findings presented by the SWOT analysis.

ware or software firewalls; different types of technologies, such as packet filtering, stateful inspection, VPN, NAC, and different types of cloud firewalls available in different platforms [118].

5. DMZ network security architecture, while separating external and internal networks, makes organizational resources available for public access while keeping internal resources safe from unauthorized access [123, 124].
6. DMZ network security architecture providing a network zone where services such as IDS, IPS, and honeypots can be placed for raising the security of the network [123, 124].

Weaknesses

1. In larger networks, while thousands of rules implemented on different firewalls and different configurations implemented on the network exist, it is difficult and cumbersome to manage, update, and trace incidents while managed manually (traditional network security management) [76].
2. Cost of the firewall applications, and other network security-related services, imposed on companies utilizing those provided by vendors and third parties [43].
3. While fewer skills are needed to manage GUI-based firewall applications, more network professionals are needed to manage network security in larger networks, such as in data centers or CIS networks, consequently raising network management costs [2, 120].
4. DMZ while being good security protection for smaller networks, as one single network security architecture would be inadequate for protecting larger networks' security and need application of more security measures to protect network and network resources [39, 40].

Opportunities

1. Single hosts can take advantage of firewall applications that provide them with sufficient security coverage [118].
2. While firewall applications are GUI-based and can be managed both by GUI and CLI interfaces, their management will need a less expert level of competency and network experience, hence bringing less cost when it comes to hiring skilled personnel who would manage those firewalls. This is because lower salaries and consequently lower costs for skills per person will be needed [43, 120, 121, 126].
3. DMZ network security architecture and GUI-based firewall applications are simpler than other more complicated network security architectures, some of which we will explain later in the coming sections, and more appropriate to manage for companies with the need for the management of smaller networks' security [123, 124].

Threats

1. DMZ network security architecture and firewall applications, alone as the network security strategy, would be insufficient to cover the needs of network and network resources' protection in larger networks. Because in larger networks, such as in CIS or data centers networks, more security measures are needed in addition to the fact that handling thousands of firewall rules manually would be unmanageable, which brings less security and control in the network [2, 40, 76, 90, 92, 93].
2. Without a more secure architecture strategy, having firewalls with many rules, especially in large networks such as in CIS networks, is a nightmare to manage manually and brings more complexity and insecurity to the management of the network security [76, 90, 92, 93].
3. Manually managing firewall applications in large networks with tens of thousands of security rules in the firewalls is a cumbersome and challenging task for network owners. This difficulty can consequently cause remaining thousands of deprecated unmanaged rules in the network firewalls, making it easier for adversaries to reconnaissance, take advantage of zero-day vulnerabilities, and compromise the network [2, 42, 76, 90, 92, 93].
4. Firewall applications, delivered by vendors and third parties, compromise customers' network security when being targeted in cyber attacks such as supply-chain or the malicious payloads as also explained in Section 3.4 [36].

F.2 SWOT Analysis of Zone-based Network Security Architecture - RQ1

This section presents the SWOT analysis of zone-based network security architecture. As elaborated about this type of network security strategy in Appendix B, utilizing zone-based network security architecture provides more satisfactory security for large networks, such as CIS networks; while by utilizing this network security architecture, we are adding a higher level of complexity to the network security. Following the study of the SotA, this higher level of complexity, while being managed manually, will result in the characteristics that we present here in the following SWOT analysis:

Strengths

1. To a degree easy to implement the network architecture and the new firewall rules because of the utilization of the GUI-based interface of firewalls [39].
2. Because the network security is managed by the GUI infrastructure of the firewalls managing this type of network security architecture does not require very high expertise in network management [125].
3. Providing higher security for the network and network resources compared with network security architecture which only utilizes DMZ and firewall applications [122].

Weaknesses

1. While thousands of rules exist difficult to manage, update, and trace incidents in network and network security resources, including firewalls [76, 90, 92].
2. Utilizing more firewall components will raise the cost of the applications that vendors provide for network security and firewalls [120].
3. The architecture utilized in network security will be more complex in larger networks [2, 76].
4. Very fast reaching a point that thousands of firewall rules exist without being able to go through every rule for check and deletion of the rules that no longer are in use, consequently, growth of security holes in network and firewalls while being managed manually. [76, 90, 92, 93].
5. Decreasing network security while traditionally managed because of the growth of the uncontrolled existing holes in the firewalls, consequently making an avalanche effect of uncontrolled existing holes in the network security and firewalls [42, 76, 90, 92, 93].
6. Vendor and vendor security dependent because of broadly utilizing vendor products such as firewalls in the network [42, 76, 90, 92, 93].

Opportunities

1. Zone-based network security architecture is based on zone division of network portions, which allows making and keeping some zones more secure as needed in larger networks [151].
2. Easy to manage for companies with smaller networks because of the GUI-based firewall [39].
3. Compared to more complicated network security architectures; and as long as GUI-based firewalls are used, and the network is not very large, there is less need for highly skilled and experienced network personnel to manage network security which consequently brings a lower cost for acquiring skills by the network owner company [39, 43].

Threats

1. While more suitable and needed for CIS and other large networks, more difficult to trace logs and incidents while managed manually [42, 76, 90, 92, 93]
2. Higher degree of vulnerability imposed to the network as it is more difficult to update and have an overview when above thousands of rules and network configurations are deployed [76]
3. Reduced security because deprecated rules and configurations exist that are difficult to find and delete while manually managing network configurations and firewalls [42, 76, 90, 92, 93].
4. Easier for adversaries to compromise the network because of the existence

of many deprecated unmanaged rules and configurations on both network and firewalls [42, 76, 90, 92, 93].

F.3 SWOT Analysis of Micro-Segmentation Network Security Architecture - RQ1

Segmentation, or micro-segmentation, as also reviewed in Appendix B, is a network security architecture that provides a zero-trust security model for more satisfactory cyber hygiene. This network architecture can utilize firewalls, DMZ, and zone-based defense network security architectures. Micro-segmentation, which brings a higher level of security to the network, at the same time, will impose a higher level of complexity in the network security architecture compared to the previously mentioned network security measures in this chapter. The SWOT analysis of this network security architecture is presented below:

Strengths

1. GUI-based firewall and network security management platform make it easier to work with rules and network configurations [39, 121].
2. GUI-based configurations require fewer programming skills, reducing skills required compared to if it had a programmatic interface [126].
3. GUI-based applications make the addition of rules easier and provide GUI-based overview [126].
4. Because of zero trust network architecture, providing higher security than no zero trust [39].

Weaknesses

1. Adding a higher level of complexity to both network architecture and network management that requires more skilled personnel to manage network security [90].
2. Exponential growth of security rules makes it less manageable and less security for companies with thousands of rules configured for the security of the networks; exponential avalanche effect of uncontrolled existing holes in the network security and firewalls while being managed manually [90].
3. The transmission from old network infrastructure to micro-segmentation architecture becomes more difficult if done manually [76].
4. While thousands of rules exist difficult to manage, update, and trace incidents [90].
5. Cost of the applications that are provided by the vendor for network security and firewalls [126].
6. Vendor and vendor security dependent [126].
7. In gigantic networks like CIS networks, very fast reaching a point where thousands of firewall rules exist without being able to go through every

rule for check and deletion of deprecated rules; exponential growth of the holes in network security and firewalls while managing manually [90].

Opportunities

1. By providing a zero trust architecture reducing the possibilities of a cyber attack such as warm getting spread fast from machine to machine; reducing cyber attack success possibility with better cyber hygiene [39].
2. While combined with zone-based network security architecture, which divides the network into internal, secure, or other desired zones[4], it provides a higher level of security [39].
3. A network security architecture based on micro-segmentation of network chunks where no host is allowed to communicate to other hosts other than we specifically set a rule for it, raising internal network security [39].
4. This network security architecture is also manageable for companies with smaller networks because of GUI-based security platforms [39].

Threats

1. While micro-segmentation is more suitable and needed for CIS and gigantic networks, it is more difficult to trace logs and incidents while manually managed [90].
2. More difficult to update and have an overview when more than thousands of rules and network configurations are deployed [90].
3. Reduced security because deprecated rules and configurations exist that are difficult to find and delete while manually managing network configurations and firewalls [127, 128].
4. Easier for the adversary to compromise the network because of the existence of many deprecated rules and configurations on both network and firewalls [127, 128].

F.4 SWOT Analysis of Zero Trust Network Security Architecture - RQ1

While Zero Trust network security architecture, more discussed in detail in Appendix B, brings a higher level of security for the network and network resources, this security strategy will also introduce a higher level of complexity to the network and network security management. This is because this network security architecture will be applied beside and to the other network security measures that are needed in the enterprise networks [40]. The SWOT analysis of the Zero Trust Architecture (ZTA) is presented below:

Strengths

---

[4] For an explanation of Zone-based network security architecture, please refer to Appendix B.

1. Providing information security and resilient in policies by implementing ZTA which consequently reduces the misuse of stolen credentials by cyber criminals [40, p. 29].
2. Preventing the motion of compromised accounts or resources through the network. ZTA will not permit access if the credentials that are compromised do not manage to authorize [40, p. 29].
3. Quickly detecting and responding to the attacks that are conducted by misusing stolen credentials [40, p. 29].
4. Protecting the sensitive enterprise resources from insider threat and compromised accounts and employees [40, p. 29].
5. Providing the ability to combine and utilize ML techniques to analyze the network traffic that is encrypted, which will help to classify the information gathered; and recognize the malicious traffic to further remediate [40, p. 30].

Weaknesses

1. ZTA decision process without logging and audit could be vulnerable to mistakes in the configuration of rule changes which could be done mistakenly by the policy administrator and policy engine [40, p. 28].
2. Vulnerable to attack vectors such as Mirai botnets[5] [40, p. 28]. Vulnerable to DoS and DDoS attack vectors targeting ISPs [40, p. 28].
3. Vulnerable to root high jacking [40, p. 28].
4. Containing a single point of failure as Policy Engine (PE) and Policy Administrator (PA) are the single point to approve all permissions and rules [40, p. 28].
5. Possibility to accidentally turn off the PE or PA if implemented based on cloud services such as SaaS or IaaS [40, p. 28].
6. Vulnerable to the result of cyber attacks such as phishing and social engineering where vulnerable accounts are compromised [40, p. 29].
7. The information gathered by ZTA analytical engines are interesting targets to cyber attackers if not protected by strong access policies [40, p. 30].

Opportunities

1. Combining with different network security techniques such as micro-segmentation and perimeter-based network security architectures to achieve higher security for the enterprise network [40].
2. Expanding the possibilities to work remotely in a safe manner with organization resources by providing strong security while the employees of the organization can access the resource remotely in a secure manner [40, p. 23-27].
3. Raising possibilities to take advantage of different cloud service providers

---

[5] This attack vector is not limited to ZTA paradigm [40, p. 28].

by providing access control while enterprise employees need to access IaaS and SaaS cloud services directly or by accessing them through another cloud service provider [40, p. 23-27].

4. Secure communications between different enterprises which raises opportunities for inter-collaboration between them [40, p. 23-27].
5. Assuring policy compliance for organizations which otherwise could have been more difficult to achieve [113].
6. Reduction of the attack surface by combining with network security architectures such as micro-segmentation, and utilizing Multi-Factor Authentication (MFA), Identity Access Management (IAM), and Zero Trust Network Access (ZTNA) security measures [40].

Threats

1. Disruption of enterprise operation by policy unproved changes to rules [40, p. 28].
2. Interception and block of the network traffic to policy administrator or policy engine from some of all of the user accounts in the enterprise network by a cyber attacker [40, p. 28].
3. Enterprise network disruption, assets not being available even if access granted by PA, or loss of connectivity while DoS or DDoS attacks taking place [40, p. 28].
4. Insider attack still can compromise the assets protected by ZTA [40, p. 29].
5. Reconnaissance of the information gathered by the management tools in ZTA where the cyber attacker can gain valuable information about what accounts are more interesting and worth compromise [40].

Appendix G

Survey Questions

As mentioned in Chapter 5 Section 5.2, a solid version of the questions utilized in the surveys is presented in this appendix. This includes both general questions, scientific personnel group-specific questions, and IT professionals group-specific questions presented in Appendix G. You will also find each question presented where the results of the survey are provided in Section H.

General Questions

The general questions, enumerated below, are asked first at the start of the survey from both groups of participants. It will take between **5 to 10** minutes to fulfill the following **20** general questions.

1. Have you read and agreed to consent to our declaration about the ethical and legal considerations regarding data privacy and confidentiality you received through email for proceeding with this process?
2. Which of these describes your current job/position?
   - Professor at University
   - Network Engineer
   - Manager in an IT company with experience in the IP network and/or firewalls
   - Director in an IT company with experience in the IP network and/or firewalls
   - Network technical architect
   - Other positions
3. Which of these areas do you have knowledge or familiarity with?
   - Network traditional manner (for instance, CCNA, CCNP)
   - Network firewalls
   - Network security
   - Network automation

  - DevOps and IaC
  - Programming knowledge and/or experience/hands-on
  - All of the above
  - None of the above

4. Are you familiar with the traditional way of implementing and maintaining network firewalls?
5. Are you familiar with the concept of the Demilitarized Zone (DMZ) in network security architecture?
6. Are you familiar with the concept of zone-based network security management architecture?
7. Are you familiar with the concept of micro-segmentation in network security architecture?
8. Are you familiar with the concept of zero-trust network security architecture?
9. Are you familiar with/have utilized any of the following automation methods for network and network security management?
   - Software-defined Networking (SDN)
   - Machine Learning (ML)
   - Infrastructure as Code (IaC)
   - Other automation techniques
   - No
10. Do you see network automation competency as a useful product and knowledge in today's market?
11. Do you have any certification related to traditional network and network security management (such as CCNA, CCNP, or any firewall certificate)?
12. Open Question: If you have any certification related to traditional network and network security management (such as CCNA, CCNP, or any firewall certificate), please specify. (not mandatory to answer)
13. Do you have any network automation-related certification (such as DevAsk or certifications in automation programming languages such as Python or others)?
14. Open Question: If you have any network automation-related certification (such as DevAsk or certifications in automation programming languages such as Python or others), please specify. (not mandatory to answer)
15. Are you familiar with/have you utilized any network automation lab environment?
16. Open Question: Please specify which network automation lab environment you have used for work and/or practice. (not mandatory to answer)
17. Do you see benefits in utilizing automation techniques and technologies in network and network security?
18. When thinking about the organizations that already are utilizing manual processes for the management of network and network security solutions, it is suggested by the studied resources in our research work that teamwork

in a DevOps manner would help programmers to work with network personnel to automate the existing network and network security infrastructure (Resources are available in the thesis).
**The teams can consist of professionals with different competencies or different teams with different competencies working together in a DevOps manner.*
Do you agree that DevOps manner of teamwork in the organizations will help automate the existing network and network security solutions? (Alternative answers: Yes, No, I don't know)

19. Utilizing a diversity of hardware, software, techniques, and technologies has made the situation requiring and complex when automating network and network security tasks and processes.

    Do you think avoiding diversity and utilizing standardization of techniques and technologies, as much as possible, will help to make it more practical, less complex, easier, and faster to automate the network and network security solutions?
    Alternative answers:

    - Yes, the benefits of automation will compensate for the vulnerability of homogeneity that will be imposed on the system by the degree of standardization and reduction/avoidance of diversity and reduce the complexity of the system, which is a winning factor for the security of the systems.
    - Yes, but it will introduce other security challenges into the network as we will face the vulnerability of homogeneity in the network design/architecture. So we need to have some flexibility and balance in solutions when standardizing the solutions.
    - No
    - I don't know

20. As mentioned above, one solution could be to utilize teams with team members who are professionals in different fields or different teams with different professionalities to work together in a DevOps manner.
    Do you agree with the claim that it is the organization- and team-leader skills in team-building, encouragement in learning and skills-building, and leadership of teams that determine the progress of improvement in automating network and network security?

Questions to Scientific Personnel at Universities

In this section, you will see **31** questions, among which four are 'not mandatory'.
This part will take a total of **20-25 minutes** to answer.
We encourage you to also, even briefly, answer the 'not mandatory' questions.
This will help us in our research result evaluation.

21. Do you teach/have you been teaching traditional network management

techniques and technologies to students?
We assume that universities that teach traditional network management techniques and technologies to students also encourage and inform students about taking certifications in this relation. Your positive answer to this question will also confirm this fact.
By 'traditional', we mean all the methods and technologies that are managed manually and not automated.

22. Do you teach/have you been teaching techniques and technologies related to the following automation methods to your students:
    - Software-defined Networking (SDN)
    - Machine Learning (ML)
    - Automation using Infrastructure as Code (IaC)
    - Any other automation techniques and technologies
23. Open Question: If you answered 'Any other automation techniques and technologies' to the above question, please mention the name of these methods here:(not mandatory to answer)
24. From 0 to 10, how many years of experience in working as scientific personnel concerning IT knowledge do you have?
    (*Each number below represents a multiply of 2. For instance, if you have 20 years or more experience, you choose 10)
25. As much as you know, do your students utilize the knowledge they gain related to network security automation techniques and technologies when they start working for companies?
26. Do you think it is necessary to have network automation as part of the study of the students of Information Technology (IT)?
27. Open Question: Please briefly explain the reason for the answer you gave to the above question below:(mandatory to answer)
28. Open Question: Network automation using automation configuration tools, such as Ansible, and programming languages like Python, and different platforms, in addition to various platforms and technologies, such as SDN, ML, and IaC, are suggested by many academic researchers.
    Why do you think these technologies are/are not used in today's knowledge learning by universities for teaching and nurturing knowledge in network security automation? (mandatory to answer)
29. Open Question: Is there any subject specifically focusing on network automation techniques and technologies for students working on their Bachelor's or Master's degree at the university where you are a member of the scientific personnel? (mandatory to answer)
30. Do students, who specialize in network or network security subjects such as CCNA, CCNP, etc., have the chance to choose subjects that help them to learn about certification-related topics such as Development Associate (DevAsc) where the focus is on automating network and network security processes by utilizing network automation techniques and technologies?

31. Open Question: If you answered 'Yes' to the question above, please write the name of the subjects that you mean to help students learn about and get hands-on with network automation. (not mandatory to answer)
32. Do you introduce and mention the existence of network and network security automation knowledge and technologies to your IT students and encourage them to follow the path and be curious about it?
33. Regarding what was asked in your first group-specific question, we assume that students who study network or network security subjects are encouraged to get ready and take the certification exams provided by different companies, for instance, Cisco certifications in CCNA and CCNP. Do you also encourage them to take certifications in network automation techniques and technologies?
34. In case you answered yes to the questions above, which are about existing and teaching network and network security automation to students at the university you work for:
    Regarding the students who have graduated and started working for the companies;
    Do you think/know if they do utilize/have utilized their knowledge in network automation in their work?
35. According to your knowledge and experience, do you think there is a gap between what students learn and what they can utilize of the knowledge related to network automation gained during their education when they start working?
    (*If you mean that they don't gain knowledge related to network automation during their study, this means that there is not a gap, and your answer should be 'No' to this question, but if otherwise, then the answer should be 'Yes' to this question)
36. According to your knowledge and experience, is what you teach students related to network automation techniques and technologies far ahead or far behind what they are required, need to know, and should manage within their working life?
    Alternatives:
    - What we teach them in **network automation techniques and technologies**, is far behind what they need in their future working life
    - What we teach them in **network automation techniques and technologies**, far ahead of what they need in their future working life
    - When it comes to utilizing **network automation techniques and technologies**, it is a nice and good sync between what we teach them at university and what they need to work with, in their future working life
37. In research conducted through many papers, books, and related works to network and network security automation, we can see a considerable amount of academic work done in this area, but we also see that the industry is util-

izing manual techniques to manage their network and network security. Do you see and agree that there is a gap between the level of academic research done in this area and the level of utilization of their results in the industry?

38. Open Question: If your answer to the above question was ’Yes’, please briefly mention the reason you think the gap between these two areas, the industry, and the academic research in the context of network and network security automation exists. (not mandatory to answer)
39. Assuming that academic research is far ahead when it comes to researching network and network security automation techniques and technologies, and industry is far behind when it comes to utilizing the latest and newest results produced by academia in this knowledge area.
    Do you agree that for teaching new IT students, the university utilizes the materials published by the industry, which is far behind the newest academic research results?
    Alternatives answers:
    - Yes, we utilized the famous published books and materials by the industry
    - No, what we teach the students is based on academic work and the last and the newest research results
    - Both, we always combine both the literature published by the industry and the results from the academic work by students and staff at the university
    - We sometimes use both, sometimes only the books and materials published by industry companies such as Cisco or Juniper concerning network and network security
    - We don’t teach them network and/or network security automation. This is not in the focus area of what we teach them!
40. Does the university you work for offer any subject directly related to Machine Learning (ML)?
41. As much as you know, how many subjects related to ML does the university you work for offer to the students who study network and information security?
    Alternatives answers:
    - No subjects related to ML
    - Ten or more subjects/study topics related to skill building and gaining knowledge in ML are offered to students
42. Does the university you work for offer any subject directly related to Software-defined Networking (SDN)?
43. Does the university you work for offer any subject directly related to Infrastructure as Code (IaC)?
44. Does the university you work for offer any subject directly related to Software development and CI/CD?

45. The way you see it when the IT students finish their education at the university you work for, do they have enough knowledge, experience, and confidence to utilize automation techniques in practice in network and network security?
46. Do you or other university personnel teach and train IT students in team working to acquire competencies in team working process and skills?
47. Are Python and Ansible, which are mentioned by the state-of-the-art studied in our research, among the automation configuration tools that the school/university you work for teaches to the students?
    Alternative answers:
    - Python Yes, but Ansible No
    - Ansible Yes, but Python No
    - Both of them, Yes, and comprehensively
    - Both of them, Yes, but with limitations
    - No, neither of them
48. A DevOps manner of teamwork is suggested by many resources, studied in our research, to help organizations that are utilizing manual manner of the network and network security management to automate the existing network and network security infrastructure.
    In the subjects offered to the IT students, who take network and network security lines of study at the university you work for, do they learn about teamwork in a DevOps manner?
    - Yes, comprehensively
    - Yes, but with limitations
    - No
    - I don't know
49. Critical Infrastructure Sectors (CIS) include companies such as the Emergency Services Sector, Energy Sector, Hospitals, Financial Services Sector, etc.

    As much as you know, what percentage of the students who graduated from the study lines related to network and network security at the university you work for start/have started working for CIS companies' network and network security?
    (*Where 0 means 0% and not likely, and 10 means 100% and very likely)
50. In your opinion, introducing automation as one or more study subjects to the students that study network and or network security will benefit their future approach to solving the problems when they start working for the companies?
    Alternative answers:
    - Yes, this is a good idea; we should have more automation-related knowledge and study subjects available for the students. This will help them

  to take advantage of automation knowledge in their future work and have a positive perspective on it. But we are not ready for it yet... maybe in the future...
  - Yes, absolutely, and we are looking into it with a positive viewpoint. It will give them and their employer many benefits when they start their work for companies
  - No; the students already have challenges in learning the basics of network and network security. Putting more challenges on them to learn to automate solutions will only make the study more difficult for them!

51. Open Question: Do you have any comment on why there is nothing/little/too much network and network security automation-related knowledge offered for learning at the university you work for?
    (*You decide if the degree of it is nothing, little, or too much) (not mandatory to answer)

Questions to Network Professionals Who Work in Organizations

In this section, you will see **34** questions, among which four are 'not mandatory'. This part will take a total of **20-25 minutes** to answer.
We encourage you to also, even briefly, answer the 'not mandatory' questions. This will help us in our research result evaluation.
The questions asked from network professionals, including network engineers, managers, directors, and technical architects, are as follows:

21. Do you directly work/have worked with network and/or network security? (Yes, No)
22. Critical Infrastructure Sectors (CIS) include companies such as the Emergency Services Sector, Energy Sector, Hospitals, Financial Services Sector, etc. In your IT career, which is what we have in mind here, do you work/have been working for any CIS company's network and/or network security?
23. As a network professional, do you also work/have worked with different firewall management solutions as part of your work in the network? (Yes, No)
24. Differentiation makes it more challenging to manage and automate network and network security solutions such as firewalls, etc. Usually, companies use different products from different vendors to manage this task.
    When you work/have been working with network and network security for organizations, did you have to utilize different platforms from different vendors? (Yes, No)
25. From 0 to 10, how many years of experience working with network or network security do you have?
    (*Each number below represents a multiply of 2. For instance, if you have 20 years or more experience, you choose 10)
26. Do you have competency and experience in network and network security

automation that, with a safe and confident feeling, lets you immediately start to utilize automation techniques in the infrastructure you work with now? (Yes, No)

27. Do you use/have used any form of automation techniques in practice when you work with network security,
    or
    do you manage/have managed networks and firewalls using the traditional manner, such as utilizing the GUI of the different networks and firewalls? (Alternative answers are: Not at all, Partly automation methods, Totally automation methods)
28. From 0 to 10 how much do you use automation methods in network security?
    (*Where 0 means 0% and not at all, and 10 means 100% and Total automation methods are used - the answer is in percentage)
29. What do you see as the reason for the percentage you give?
    - Lack of competency
    - Lack of proper equipment
    - Lack of organizational budget that can support it
    - Lack of proper training for network professionals
    - Difficulty in revoking changes that are implemented by automation techniques through the network security and network security
    - Existing difficulties in understanding the collaboration between automation tools and other platforms
    - The organization or its customers are not ready for changes coming to the networks by automation techniques and technologies
    - Network security automation requirements are not defined or clarified
    - The leadership of the organization or its customer is not ready to accept the change to utilizing automation in network security
    - Difficulties in adopting automation of network security will impact customer satisfaction in a negative manner
    - People don't trust automation techniques and tools yet
    - The impact of change imposed on performance by automated processes will make them fear accepting it
    - The legacy technology is not compatible with the changes imposed by network automation or to utilize APIs for automation
    - None of the answers above
30. What network automation techniques are you able to utilize?
    (SDN, ML, or IaC, or Neither)
    (You can choose multiple answers)
31. What network automation techniques do you practice in your daily work?
    (SDN, ML, or IaC, or Neither)
    (You can choose multiple answers)
32. Do you think it is easy to use network automation in network and network

security jobs?

33. How close in the future do you think we will be utilizing network automation methods actively? (Alternative answers: Far in 10 years or more, Close in five years, Very close in two years)
34. Have your organization provided or supported training in IT fields related to your profession/work area in a way that you feel it becomes easier to utilize network automation in practice?

    - Yes, very much
    - No, not at all
    - Partly with financial support, but training on my own

    *By supporting training, we mean providing you with labs and other materials needed for skills building, such as courses, etc.
35. Is certification and official qualifications a motivating factor for you for trying harder to achieve higher competency in IT in general, and if your organization requires, in network and network security automation? (Yes, No)
36. Do you see the support of their organization's management and leadership about the progress of each IT project and specifically automating the network security infrastructures, having a significant effect on the progress of the automation process?
37. IT staff needs to learn and do training to acquire network automation skills and knowledge needed in the organizations.
    Do you think supporting and encouraging IT staff by management in this relation will have a significant effect on the progress of knowledge building in favor of organizations' projects?
38. Where you have been working/do work today with network and network security infrastructure and solutions, is it/has it been possible to collaborate across teams to accomplish organizational objectives, learn and share knowledge and competencies, and achieve automated solutions for network and network security?
39. Do you agree when it comes to achieving network and network security automation goals, collaboration across teams and between IT professionals with different competencies, in addition to knowledge sharing, is the way to go and not organizational silos? Alternative answers:

    - Yes, I agree with this claim
    - No, I don't agree; separating different types of employees in organizations will have good results for automation as well
40. Which of the following success factors do you agree affects the progress of network security automation in organizations? (multiple answers)

    - Providing training for network personnel to build their experience in network security automation
    - Increasing budget needed to fill the gap of lack of the budget to phase out legacy devices that are not automation-compatible

- Hiring new skilled personnel in network security automation
- Supporting and encouraging the existing network personnel to build their knowledge in network automation
- Providing practical hands-on labs for network personnel to build skills in network automation
- Encouraging learning of other vendors' solutions in network security and network security automation
- Aligning middle management with network security automation goals in different projects of the organization
- Building and supporting teams of programmers and network engineers that work together in a DevOps manner
- None of the above

41. Open Question: Regarding the above question, do you have any other factors in mind to suggest? (not mandatory to answer)
42. Which of the following factors do you agree affect why network security automation projects can fail in organizations?
    - Lack of plan for the needed budget and cost of network security automation project
    - Lack of the right strategy for network security automation by project leaders
    - Stakeholders' and organizations' fears and resistance against the automation of network security processes and tasks
    - All of the above
    - None of the above
43. Open Question: Regarding the above question, do you have any other factors in mind to suggest? (not mandatory to answer)
44. Do you fear that if you automate tasks, they could end up collapsing and avoid introducing network automation in the system because of this fear?
45. Are you more comfortable doing tasks manually or by automation in network and network security infrastructures? (Alternative answers: Manually, By automation, Partially of each (both manual and automated))
46. From 0 to 10, what percentage of the network tasks do you think can be automated? (From 0% to 100%)
    (*Where 0 means 0% and none of the tasks, and 10 means 100% and all of the tasks. For instance, if you mean 50%, you can choose 5)
47. Which automation-related tools have you worked with or are more familiar with? (Alternative answers: Python (programming language), Ansible (automation tool), and Other programming languages for network automation.)
    (You can choose multiple answers)
48. Open Question: If you answered 'Other programming languages' to the question above, please mention their names. (not mandatory to answer)
49. Do you feel fear in utilizing automation in network and network security

where you work?

50. Do you feel confidence and trust in addition to sufficient knowledge and competency to automate network security jobs where you work?
51. Do you feel confident and trust in addition to sufficient knowledge and competency to fix errors and mistakes and easily revoke tasks that need to be fixed after automation where you work?
52. Do you think at the point we are at the current time, customer tickets will take too long to solve when the issues are related to the automation of the tasks?
53. Do you think automation of the procedures and tasks will raise the security of the network?
    Alternative answers:
    - Yes, but it will impose new challenges to the security of the network
    - Yes, but it will impose new challenges to the management of the network and network security
    - I agree to both of the above solutions
    - Yes, and the benefits of the automation of the processes and tasks in network and network security infrastructure will compensate for the disadvantages it will impose on the system
    - No, it will only impact our work with network and network security negatively and impose more complexity on the system resulting in less security
54. Open Question: Network automation using automation configuration tools, such as Ansible, Python, and different platforms in addition to technologies, such as SDN, ML, and IaC, are suggested by many academic researchers. Why do you think these technologies are/are not used in today's solutions for network security automation? What do you see as the reason for that?

We appreciate your participation *in this interview/survey. Your answers help us in the investigation of the existing gap we research in our Master's thesis.*

When you send in this form, you will not be able to do the survey again. Therefore, we kindly ask you only to click the* ***send-in* *button when you are sure that all the answers you want to apply are given.*
Best Regards;

Appendix H

Comprehensive Review of Survey Results

In this appendix, we present the survey results obtained from two distinct participant groups mentioned earlier in this chapter: scientific personnel and IT professionals. Our surveys comprised a total of 31 participants, including six scientific personnel and 25 IT professionals. We begin by unveiling responses to the general questions, which were identical for both groups. Subsequently, we delve into the responses from scientific personnel regarding group-specific questions, followed by the insights provided by IT professionals in response to their specific set of questions.

H.1 General Questionnaire Responses

The responses to the general questions, common to both participant groups, are presented in this section.

General Question Number 1

Question: Have you read and agreed to consent to our declaration about the ethical and legal considerations regarding data privacy and confidentiality you received through email for proceeding with this process?

The Reason for Asking This Question: To ensure the participants' rights and data privacy were respected and that they were informed about this, the first condition for participating in the survey and interviews was to inquire about their awareness, as stated in the information we provided to them[1].

Reference to Research Question: This question is informative and related to

---

[1] The legal and ethical considerations, which were provided to participants in PDF format, are detailed in Section 1.11.

compliance with data privacy norms and declarations.

Reference to What in SotA Results We Validate: Neither, this question is to assure compliance of our investigation with rules and regulations.

Result Facts: Everybody has unanimously answered 'Yes' to this question.

Analysis: We assume that everyone who answered 'Yes' and took part in the survey and interviews is well-informed about their rights as outlined in our declaration.

General Question Number 2

Question: Which of these describes your current job/position?

- Professor at University
- Network Engineer
- Manager in an IT company with experience in the IP network and/or firewalls
- Director in an IT company with experience in the IP network and/or firewalls
- Network technical architect
- Other positions

The Reason for Asking This Question: To register participants' backgrounds and assess the validity of our results.

Reference to Research Question: Background registration question.

Reference to What in SotA Results We Validate: Neither, this question is to evaluate the participants' work experience.

Result Facts: As presented in Figure H.1, we had four people who answered that they work as professors at the university, one person who answered network engineer, and one who answered other positions.

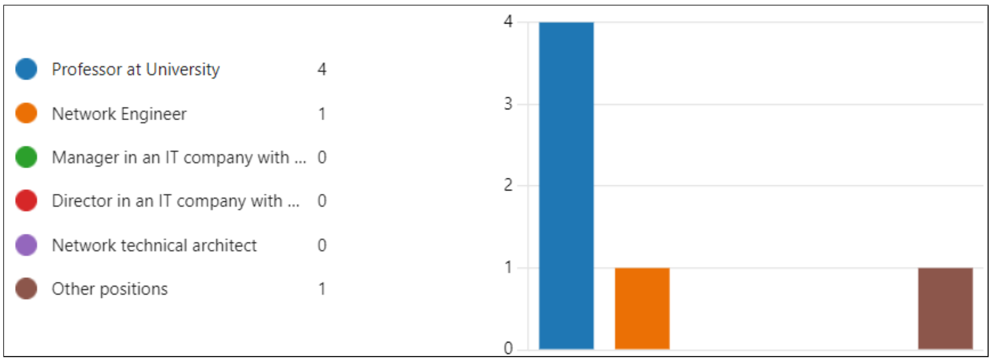


Figure H.1: Scientific personnel survey answer to question 2

Among the IT professionals participating in the survey, as presented in Figure H.2, we had 16 people who answered network engineer, six who answered network technical architect, and three who answered other positions.

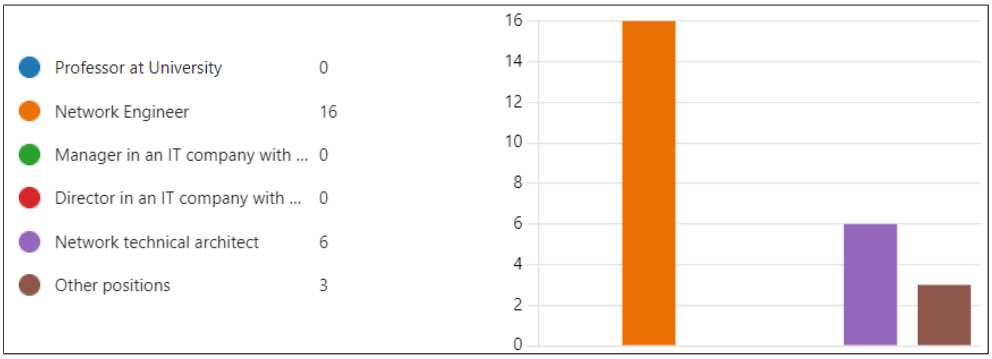


Figure H.2: IT professional survey answer to question 2

Analysis: The majority of participants hold jobs or positions that are relevant to the information required for our investigation.

General Question Number 3

Question: Which of these areas do you have knowledge or familiarity with?

- Network traditional manner (for instance, CCNA, CCNP)
- Network firewalls
- Network security
- Network automation
- DevOps and IaC
- Programming knowledge and/or experience/hands-on
- All of the above
- None of the above

The Reason for Asking This Question: To register participants' backgrounds and assess the validity of our results.

Reference to Research Question: Background registration question.

Reference to What in SotA Results We Validate: Neither, this question is to evaluate the participants' knowledge area and competence.

Result Facts: Here we observe various knowledge areas among scientific personnel. As presented in Figure H.3, the majority know network security and programming, most of them have knowledge of traditional network techniques and technologies, and some of them have knowledge of and familiarity with network firewalls, network automation, and other areas.

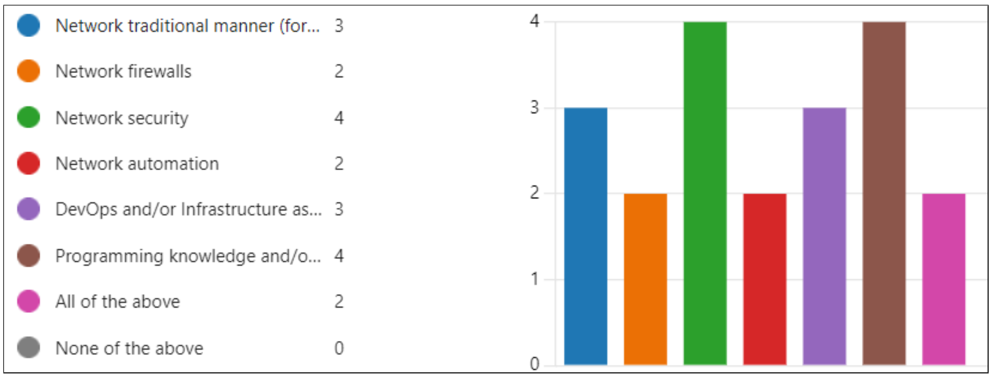


Figure H.3: Scientific personnel survey answer to question 3

Among IT professionals, most are familiar with traditional network management, firewalls, and security. As presented in Figure H.4, half of the participants have knowledge and familiarity with network automation techniques and technologies, and below half of them know DevOps, IaC, and programming languages. About one-third report that they know all the areas that are mentioned here.

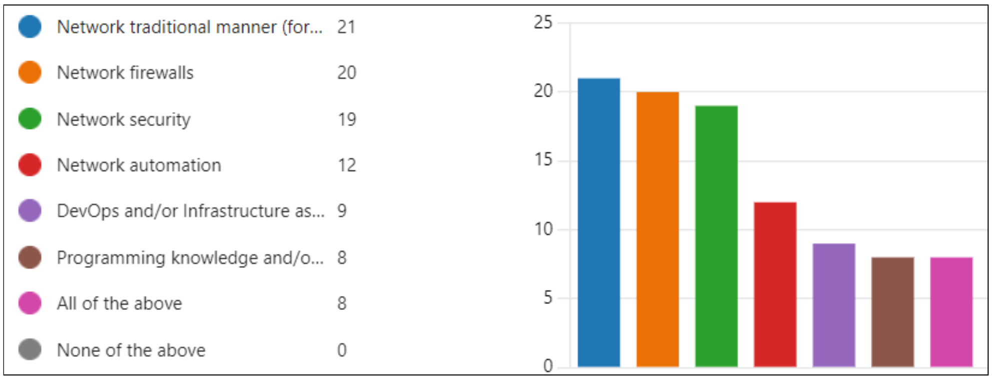


Figure H.4: IT professional survey answer to question 3

Analysis: The extensive knowledge and competence within both groups of participants lead us to assume that the responses gathered through our investigation are highly reliable.

General Question Number 4

Question: Are you familiar with the traditional way of implementing and maintaining network firewalls?

The Reason for Asking This Question: To confirm the participant's familiarity with this technology and to align with their job and experience area, we verified whether this technology is actively utilized in the field of network security.

Reference to Research Question: RQ1

Reference to What in SotA Results We Validate: Traditional network security techniques, technologies, and architecture [26–29, 39–41, 67, 88, 112–118].

Result Facts: In answer to this question, five out of six scientific personnel report that they are familiar with the traditional way of implementing and maintaining network firewalls, as presented in Figure H.5, while this number among IT professionals includes all of them, as presented in Figure H.6.

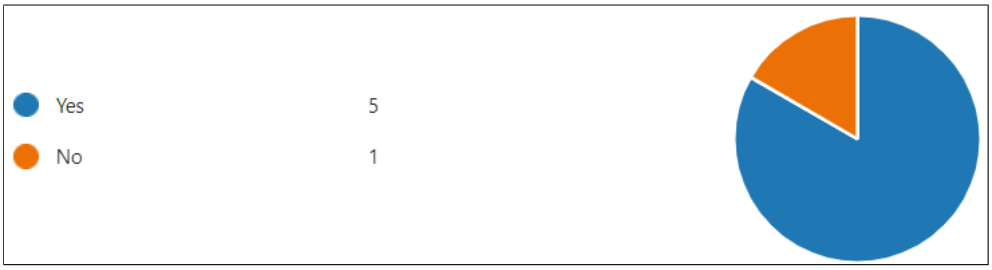


Figure H.5: Scientific personnel survey answer to question 4

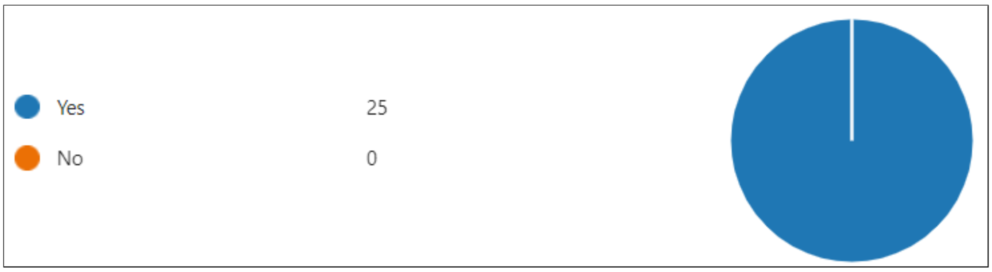


Figure H.6: IT professional survey answer to question 4

Analysis: As indicated by the responses, 96.7% of the participants are well-versed in traditional network firewall implementation and management.

General Question Number 5

Question: Are you familiar with the concept of the Demilitarized Zone (DMZ) in network security architecture?

The Reason for Asking This Question: To confirm the participant's familiarity with this network security architecture, in line with their job roles and experience as verified in the background registration questions, we validated the practical utilization of this security strategy in network protection.

Reference to Research Question: RQ1

Reference to What in SotA Results We Validate: Traditional network security techniques, technologies, and architecture [26–29, 39–41, 67, 88, 112–118].

Result Facts: Here, all the participants from both groups answered 'Yes' to this question, as shown in Figure H.7 and Figure H.8.

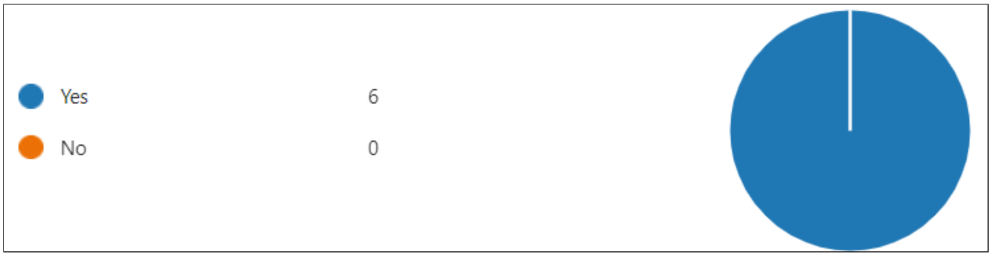


Figure H.7: Scientific personnel survey answer to question 5

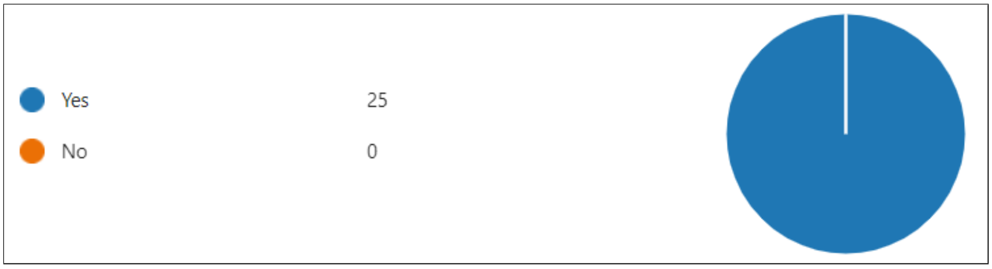


Figure H.8: IT professional survey answer to question 5

Analysis: When all participants unanimously indicate their familiarity with this type of network security architecture, it strongly suggests that DMZ is indeed one of the most recognized and frequently used network security architectures. This finding reaffirms the information we presented regarding DMZ in our results.

Furthermore, when considering the responses to questions number 2 and 54, we can confirm that not all participants are employed by large companies with extensive networks. It's worth noting that one of the responses to question 54 highlights the presence of participants from small or medium-sized companies, as indicated by the following statement:

"In my environment, we have such a limited amount of devices that automation in the setup on the network devices does not make much sense."

This insight indicates that DMZ is utilized across networks of varying sizes, including those in small, medium, and large companies. This finding aligns with our observations from the review of the SotA literature.

General Question Number 6

Question: Are you familiar with the concept of zone-based network security management architecture?

The Reason for Asking This Question: To confirm participants' familiarity with this type of network security architecture and align it with their job roles and experience, we assessed whether this security strategy is actively employed in practice to secure their networks.

Reference to Research Question: RQ1

Reference to What in SotA Results We Validate: Traditional network security techniques, technologies, and architecture [26–29, 39–41, 67, 88, 112–118].

Result Facts: As shown in Figure H.9, 83% among scientific personnel, and as shown in Figure H.10, and 96% among IT professionals answered 'Yes' to this question.

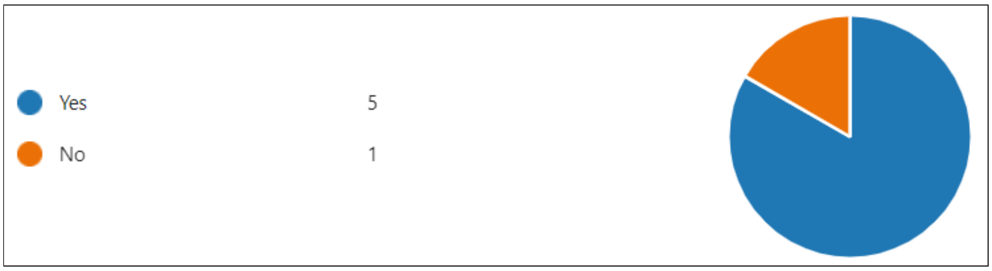


Figure H.9: Scientific personnel survey answer to question 6

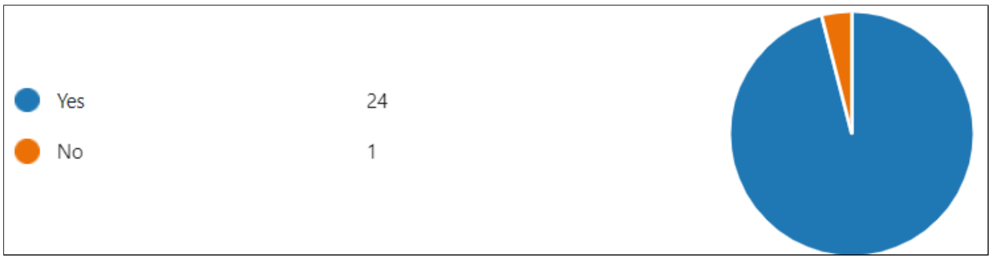


Figure H.10: IT professional survey answer to question 6

Analysis: The responses gathered for this question reveal that within both groups of participants, the majority are acquainted with the concept of zone-based network security management architecture. Building on the insights gained from the analysis of question number 5, we can reasonably infer that a significant proportion of small, medium, and large networks incorporate zone-based network security architecture into their practices. This confirmation aligns with the findings from our literature review about this network security strategy.

———————General Question Number 7———————

Question: Are you familiar with the concept of micro-segmentation in network security architecture?

The Reason for Asking This Question: To validate participants' familiarity with this specific network security architecture and to align it with their job roles and experience, we assessed the practical implementation of this security strategy in securing their respective networks.

Reference to Research Question: RQ1

Reference to What in SotA Results We Validate: Traditional network security techniques, technologies, and architecture [26–29, 39–41, 67, 88, 112–118].

Result Facts: Here, we observe 67% of scientific personnel confirm familiarity with micro-segmentation network security architecture, shown in Figure H.11, while as presented in Figure H.12 this percentage among IT professionals is 88%.

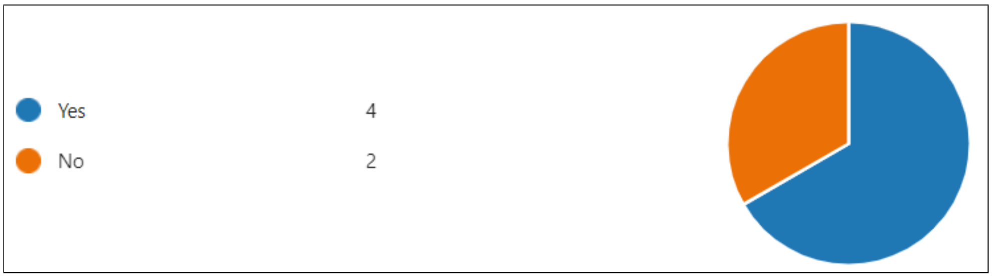


Figure H.11: Scientific personnel survey answer to question 7

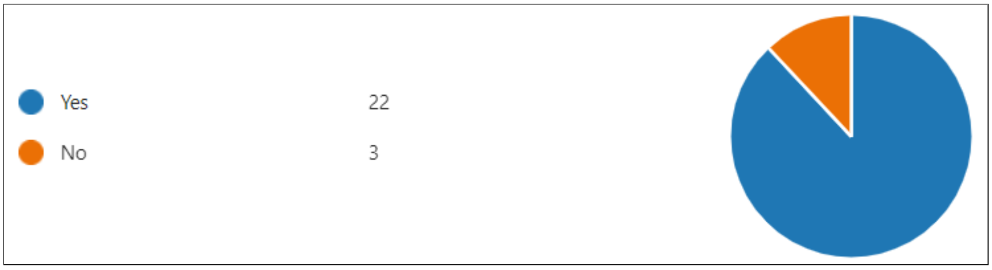


Figure H.12: IT professional survey answer to question 7

Analysis: In total, it is evident that 83.9% of participants responded with 'Yes' to this question, indicating that a majority, though not all, of the companies they are affiliated with, have employed this specific network security architecture to some extent. This suggests that, despite the inherent complexity associated with this security strategy in network architecture, they are actively implementing it in their networks. These findings further corroborate the insights obtained from our literature review on the adoption of this more intricate network security strategy.

General Question Number 8

Question: Are you familiar with the concept of zero-trust network security architecture?

The Reason for Asking This Question: To confirm participants' familiarity with this type of network security architecture and to align it with their job roles and experience as validated in the background registration questions, we assessed the practical utilization of this security strategy in securing their networks.

Reference to Research Question: RQ1

Reference to What in SotA Results We Validate: Traditional network security techniques, technologies, and architecture [26–29, 39–41, 67, 88, 112–118].

Result Facts: As shown in Figure H.13, all the scientific personnel confirmed familiarity with this concept, while among IT personnel, we have a majority of 80% that was familiar with this concept, presented in Figure H.14.

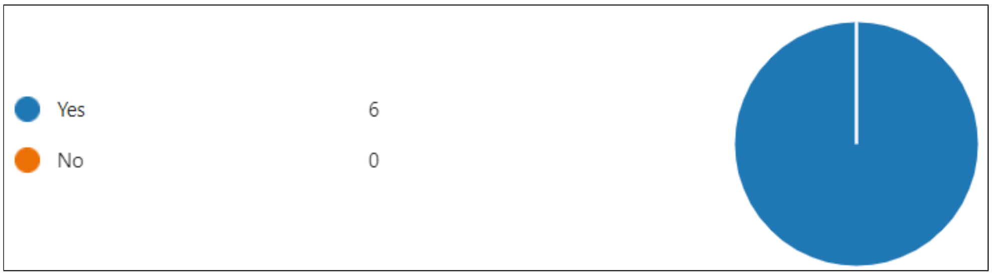


Figure H.13: Scientific personnel survey answer to question 8

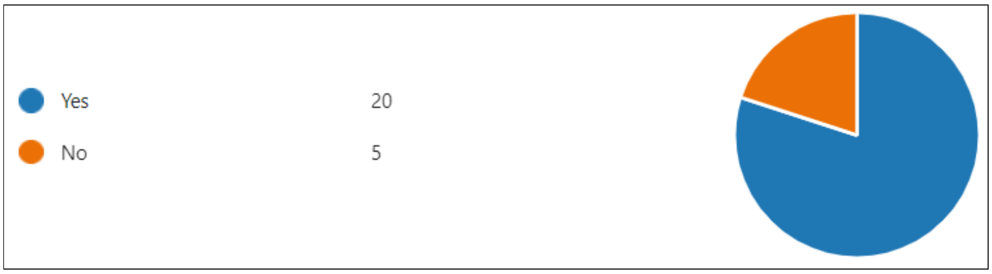


Figure H.14: IT professional survey answer to question 8

Analysis: Based on the provided responses, it is evident that all individuals within the scientific personnel category confirm their familiarity with the zero-trust network security strategy. Among IT professionals, the response rate is consistent with the findings from the group-specific question 22, where 76% of them affirmed their experience in managing CIS and large company networks. This comparison suggests a correlation between the 80% of IT professionals in this question and the 76% in question 22, indicating that a substantial proportion of those working with large networks, including CIS networks, are well-versed in zero-trust network security architecture.

In total, 83.9% of all participants provided affirmative responses to this question, signifying a significant adoption of this network security strategy within network security architecture. This finding aligns with our observations from the SotA literature study.

General Question Number 9

Question: Are you familiar with/have utilized any of the following automation methods for network and network security management?

- Software-defined Networking (SDN)
- Machine Learning (ML)
- Infrastructure as Code (IaC)
- Other automation techniques
- No

The Reason for Asking This Question: To confirm participants' familiarity with any of these network automation technologies, following their job roles and experience as verified in the background registration questions, we assessed the practical application of this security strategy in securing their networks.

Reference to Research Question: RQ2

Reference to What in SotA Results We Validate: NSA techniques and technologies such as SDN, ML, and IaC [1, 2, 5, 6, 8, 10, 17, 35, 43–45, 47–52, 56, 57, 61, 65, 66, 69–75, 77–87, 90–94, 99, 103, 105, 106, 108–111].

Result Facts: As shown in Figure H.15, 50% of scientific personnel knew about Software-defined Networking (SDN), while as shown in Figure H.16, this percentage among IT personnel was 72%. In total, from both groups, 67.7% of the participants express familiarity with SDN. 16.6% of scientific personnel, only 1 person, and 12% of IT personnel, only 3 person, express familiarity with Machine Learning (ML), which gives a total of 12.9% of all the participants.

66.7% of scientific personnel were familiar with Infrastructure as Code (IaC), while this percentage among IT personnel was 60%. Altogether, we have 61.3% of the total participants who express familiarity with IaC. In total, 22.6% of the participants confirmed that they are also familiar with other automation techniques. We also have 16% of IT professionals that express absolutely 'No' familiarity with network automation techniques mentioned here or other automation techniques.

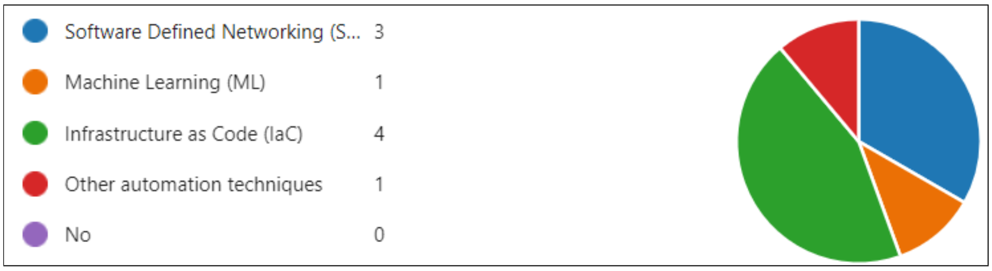


Figure H.15: Scientific personnel survey answer to question 9

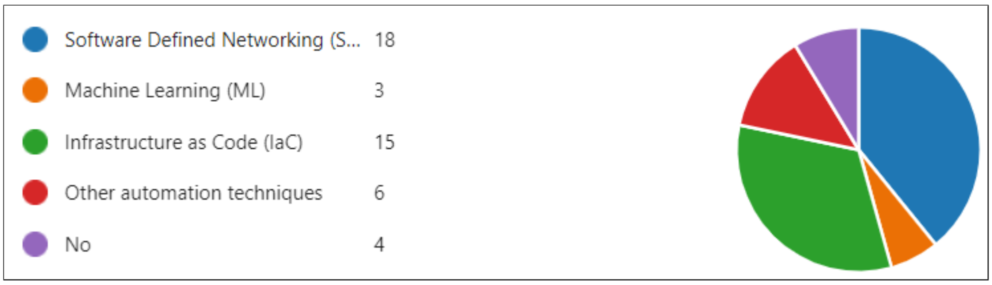


Figure H.16: IT professional survey answer to question 9

Analysis: Up to this point in the survey, we have received confirmation from the majority of participants that they possess knowledge of traditional network and network security techniques and technologies. This widespread awareness among participants adds credibility to our research findings.

The results obtained in this section indicate that SDN is more prevalent among IT professionals. Conversely, Infrastructure as Code (IaC) appears to be more commonly employed among scientific personnel, with a notably high adoption rate. However, ML knowledge is relatively scarce and infrequently encountered among both groups of participants.

It is worth noting that all scientific personnel exhibit an understanding of one or more automation techniques and technologies presented in the survey questions, underscoring the breadth of their knowledge in this area.

General Question Number 10

Question: Do you see network automation competency as a useful product and knowledge in today's market?

The Reason for Asking This Question: We posed this question to assess the participants' perspectives and attitudes toward automation technology, operating on the premise that individuals tend to invest their efforts in endeavors they deem advantageous. (It's worth noting that the reasons behind perceiving something as beneficial can vary, although we are not exploring those reasons in this particular question.)

Reference to Research Question: RQ2 and implicitly RQ3

Reference to What in SotA Results We Validate: Network security automation techniques and technologies and their affecting factors [2, 5, 10–13, 15–17, 47, 49, 70, 76, 79, 80, 83–85, 105].

Result Facts: As presented in Figure H.17, one scientific personnel, counted as 17%, answered 'No' to this question, while as shown in Figure H.18, 8% of the IT professionals answer 'No' to this question.

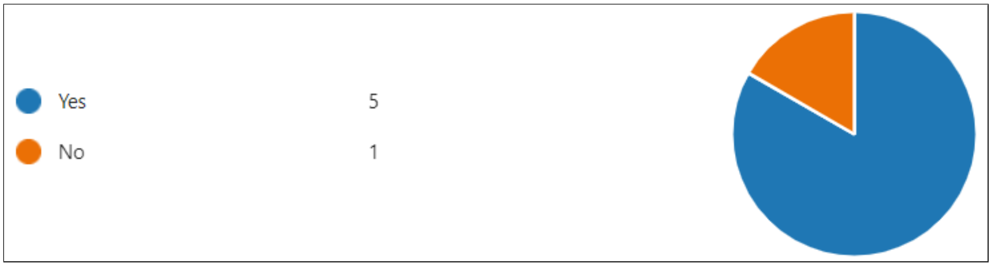


Figure H.17: Scientific personnel survey answer to question 10

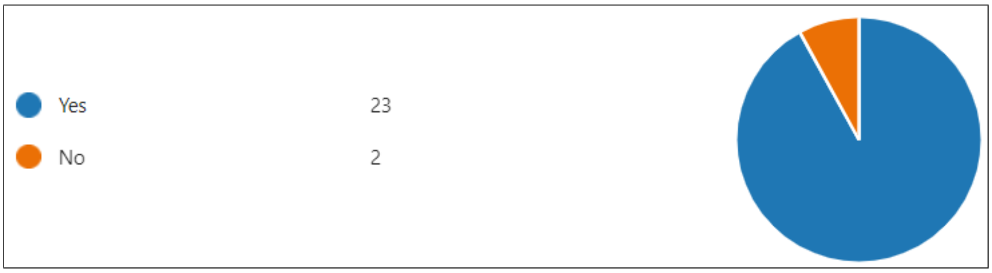


Figure H.18: IT professional survey answer to question 10

Analysis: In total, 90% of participants from both groups have confirmed the perceived benefits of network automation competency, considering it a valuable asset and knowledge in today's market.

——————General Question Number 11 and 12——————

Question 11: asked if they have any certification related to traditional network and network security management (such as CCNA, CCNP, or any firewall certificate).
Question 12: which was to expand the answers given to question 11, was an open question that asked if the participant has any certification related to traditional network and network security management (such as CCNA, CCNP, or any firewall certificate); please specify. (Not mandatory to answer)

The Reason for Asking This Question: Here, we ascertained the distribution of participants holding various types of certifications in network and network security, which serve as an official validation of their competency levels in these domains. Additionally, we assessed participants' motivation and interest in pursuing certifications related to traditional network and network security management techniques and technologies. This evaluation enables us to draw comparisons with the results obtained for network automation techniques and technologies and derive meaningful conclusions from the data.

Reference to Research Question: RQ1 and implicitly background registration question

Reference to What in SotA Results We Validate: Traditional network security techniques and architecture, and also evaluating the participants' knowledge area and competence [26–29, 39–41, 67, 88, 112–118].

Result Facts: In answer to questions number eleven, 50% of scientific personnel, as shown in Figure H.19, answered 'Yes' to this question. In the open question number twelve, the scientific personnel who responded that they have certification specified Cisco Certified Network Associate (CCNA), Cisco Certified Network Professional (CCNP), and Google Contact Center Artificial Intelligence (CCAI) as their certifications.

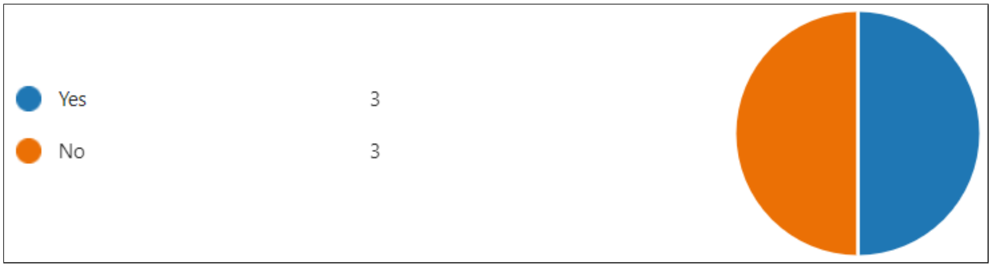


Figure H.19: Scientific personnel survey answer to question 11

Among IT professionals who answered question number eleven, as shown in Figure H.20 and Figure H.21, 72% specified that they had related certifications such as CCNP Enterprise, CCNP Security, Multiple CCNA, CCNP Routing and Switching, CCNP Service Provider, as their certifications.

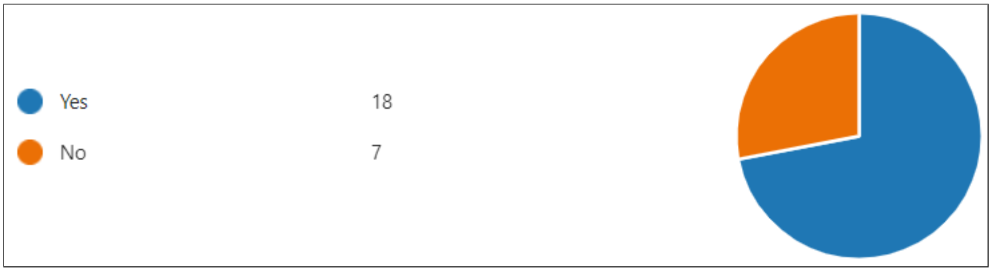


Figure H.20: IT professional survey answer to question 11

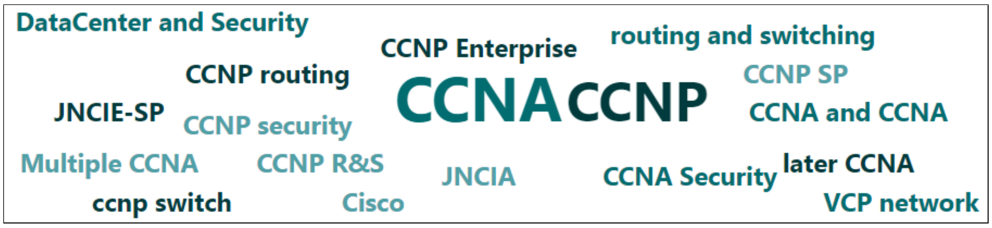


Figure H.21: IT professional survey answer to question 12, where ten respondents (40%) answered CCNA to this question

Analysis: The gathered responses allow us to confirm the accuracy of our findings as outlined in the SotA and discussed in Chapter 4 regarding certifications. Moreover, they validate that participants in both groups are deeply committed to skill development and actively seek official evidence of their competencies through the acquisition of the mentioned certifications.

General Question Number 13 and 14

Question 13: asked whether they have any network automation-related certification (such as DevAsk or certifications in automation programming languages such as Python or others).
Question 14: which was to expand on the answers given to question 13, was an open question that asked if the participant has any network automation-related certification (such as DevAsk or certifications in automation programming languages such as Python or others); please specify. (not mandatory to answer)

The Reason for Asking These Two Questions: Here, we verified participants' certifications related to network automation techniques and technologies, as these certifications serve as official proof of their level of competency. We also assessed participants' motivation and interest in obtaining network automation-related certifications. The answers received enable us to compare their progress in knowledge and competency in network automation techniques and technologies with the results of previous similar questions related to traditional network competency, allowing us to conclude.

Reference to Research Question: RQ2, and implicitly RQ3 and background registration question

Reference to What in SotA Results We Validate: NSA techniques and technologies, their affecting factors, and also evaluate the participants' knowledge area and competence [1, 2, 5, 6, 8, 10–17, 34, 35, 39–52, 54, 56–68, 70–108, 110, 111].

Result Facts: In answer to question thirteen, as shown in Figure H.22, we can see that none of the scientific personnel have any network automation-related certification, while in answer to question 14, two of them nevertheless mention having some network automation-related certifications such as DevAsc or other certifications in automation programming languages such as in Python.

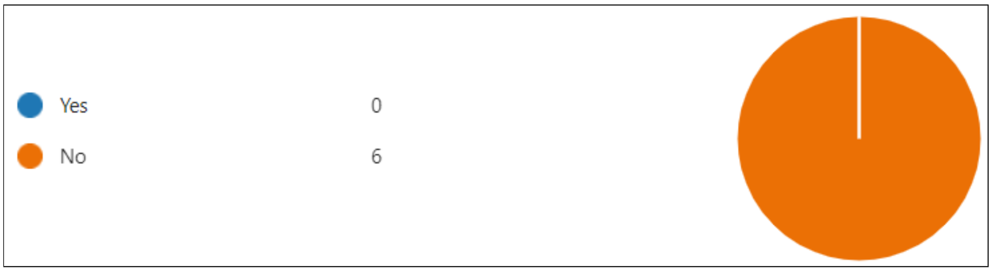


Figure H.22: Scientific personnel survey answer to question 13

This is while the answers that were given to question number thirteen by the IT professionals imply that 24% have earned some network automation-related certifications as presented in Figure H.23, where observe many participants, in answer to question 14, have answered that they among others have DevNet Associate certification. The answers that are given by IT professionals about what certifications related to network automation they have earned are demonstrated in Figure H.24.

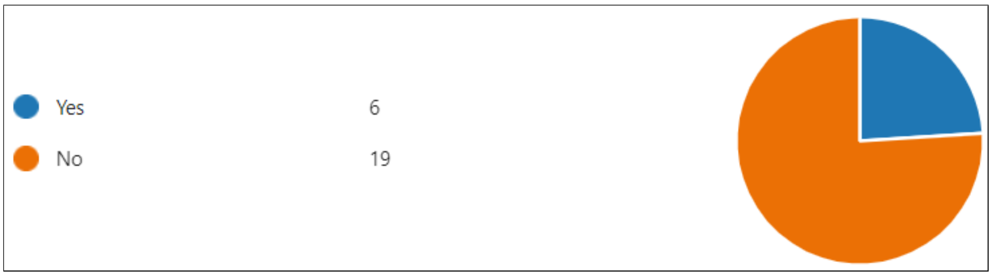


Figure H.23: IT professional survey answer to question 13

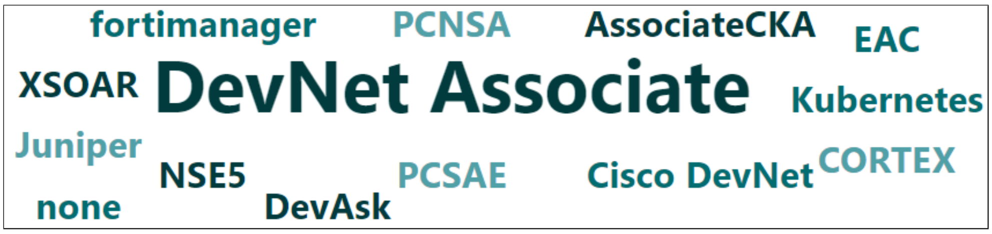


Figure H.24: IT professional survey answer to question 14 where seven people have, among others, mentioned DevNet Associate as their network automation-related certifications

Analysis: Based on the responses to questions 13 and 14, it appears that IT professionals actively working within organizations and industry networks are more engaged in skills development and certifications related to network and network security automation compared to scientific personnel dedicated to university teaching.

General Question Number 15 and 16

Question 15: asked if they are familiar with/have utilized any network automation lab environment.
Question 16: which was related to the previous question, asked them to specify which network automation lab environment they have used for work and/or practice. (not mandatory to answer)

The Reason for Asking These Two Questions: With this question, we gauge participants' competency levels and assess the prevalence and accessibility of automation lab opportunities. By requesting details about the specific network automation lab environments they have utilized for practical work, we aim to validate the information obtained during the study of the SotA.

Reference to Research Question: RQ2, and implicitly RQ3 and background registration question

Reference to What in SotA Results We Validate: NSA techniques and technologies, their affecting factors, and also evaluating the participants' knowledge area and competence [2, 5, 10–13, 15–17, 47, 49, 63, 70, 72, 76, 79, 80, 83–85, 105].

Result Facts: In answer to question number 15, as Figure H.25 presents, only one scientific personnel answered 'Yes', mentioning OpenStack as the lab environment in answer to question 16. This is while the answer 'Yes' to question 15 among IT professionals, as shown in Figure H.26, includes 56% of respondents.

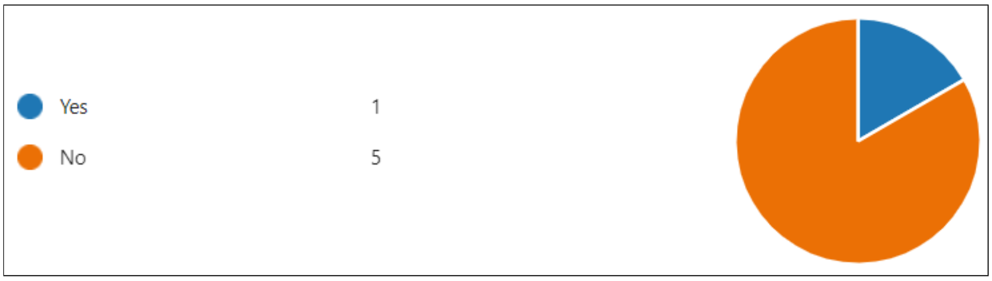


Figure H.25: Scientific personnel survey answer to question 15

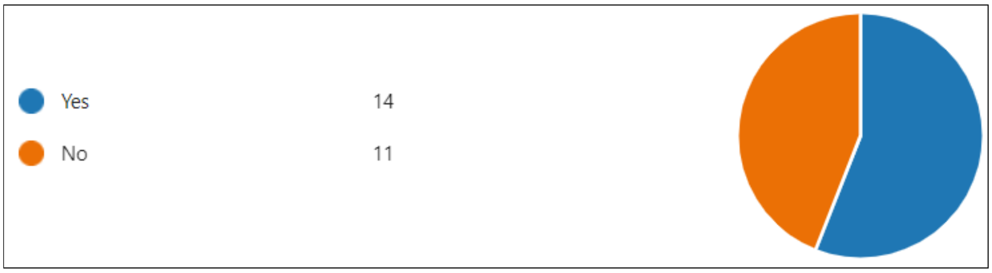


Figure H.26: IT professional survey answer to question 15

The lab environments GNS3, Ansible, Python and Terraform, EVE-NG, CML, and container labs, as shown in Figure H.27, are among the answers given by IT professionals to question number 16 which asked them to specify which network automation lab environment they have used for work and/or for practice.

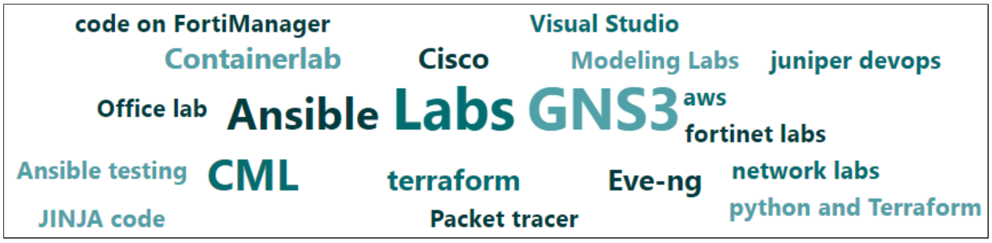


Figure H.27: IT professional survey answer to question 16

Analysis: The answers provided to question 15 imply that those who work with networks of different companies have more hands-on experience and training with network and network security automation environments than the scientific personnel who are more concerned with the teaching stuff. This will make us assume that IT professionals know more about what is more practical when they answer coming questions about the application of automation techniques and technologies to network security or when it comes to the existing challenges related to the existing network security infrastructure we ask about. Hence, we assume high validity in the answers received from IT professionals in this regard. Moreover, the answers received about the lab environments validate our findings from the SotA.

———General Question Number 17———

Question: Do you see benefits in utilizing automation techniques and technologies in network and network security?

The Reason for Asking This Question: We posed this question to both ascertain the disparity in perspectives between the two distinct participant groups on this topic and to implicitly assume whether they are inclined to employ this technology in their work, regardless of their practical roles.

Reference to Research Question: RQ3

Reference to What in SotA Results We Validate: Factors affecting NSA and related work resources [1, 2, 5–8, 10–17, 34, 35, 40–112].

Result Facts: In answer to question number 17, As Figure H.28 presents, there is one person among scientific personnel, representing 16.7%, who answers 'No' to this question, while as shown in Figure H.29, IT professionals unanimously answer 'Yes' to this question.

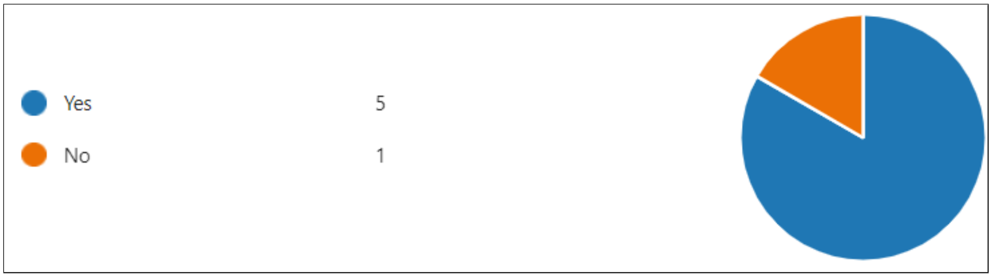


Figure H.28: Scientific personnel survey answer to question 17

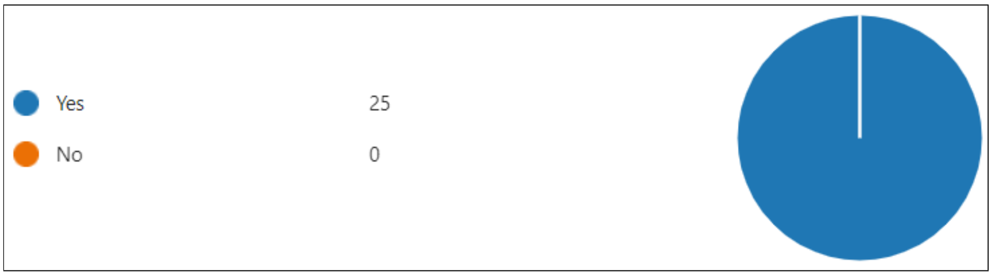


Figure H.29: IT professional survey answer to question 17

Analysis: While the majority of participants recognize the benefits of using network automation techniques and technologies in network and network security, the unanimous response from IT professionals to this question implies their unwavering belief in the advantages of network automation for network and network security management.

General Question Number 18

Question: Do you agree that DevOps manner of teamwork in the organizations will help automate the existing network and network security solutions? (Alternative answers: Yes, No, I don't know)

The Reason for Asking This Question: Here, we ascertained whether participants working with networks in organizations and industry have encountered the DevOps approach to teamwork as a beneficial process for automating network and network security solutions, to corroborate the research findings with those from the SotA analysis. This also aimed to determine whether they perceive teamwork and DevOps as influential factors in the success of network security automation progress.

Reference to Research Question: RQ3

Reference to What in SotA Results We Validate: Factors affecting NSA and related work resources [1, 2, 5–8, 10–17, 34, 35, 40–112].

Result Facts: Regarding the answers given by scientific personnel, as Figure H.30

presents, 50% of them choose to answer that they don't know about this being helpful. At the same time, two people respond that they don't agree, and only one agrees with the statement mentioned in the question. Concerning the answers given by IT professionals to this question, as shown in Figure H.31, 8% of them disagree with the statement mentioned in the question, while 20% choose that they don't know about this. Finally, 72% of them answer 'Yes', which means that they believe a DevOps manner of teamwork in the organizations will help to automate the existing network and network security solutions.

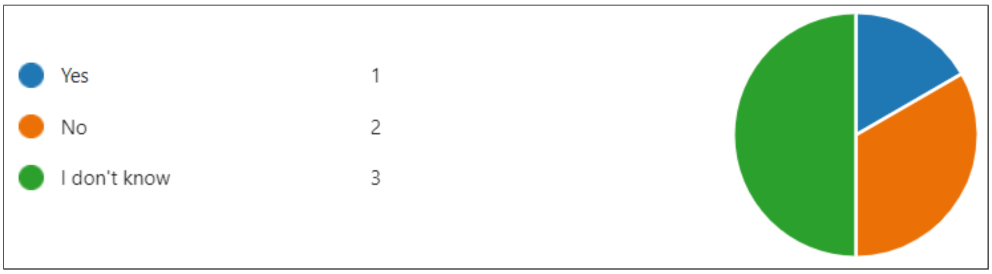


Figure H.30: Scientific personnel survey answer to question 18

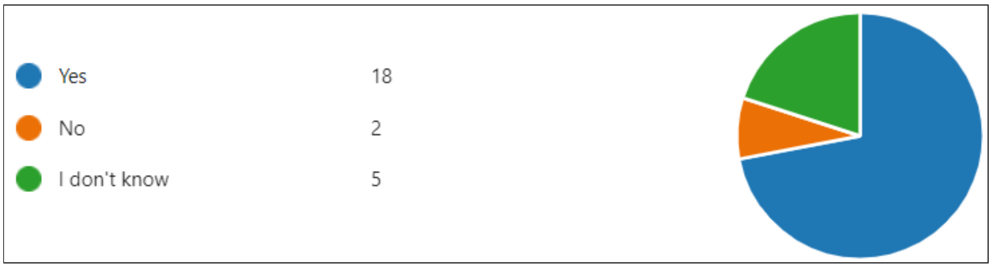


Figure H.31: IT professional survey answer to question 18

Analysis: From the responses received to this question, we speculate that the 72% of IT professionals who agree with the statement mentioned in the question may be among those who have experience working with large networks, as indicated by 76% of them in their responses to question 22. Their answers also lead us to assume that substantial projects require more teamwork. Nevertheless, the answers received here show that the ratio among IT professionals who actively work with networks and believe in a DevOps manner of teamwork for the success of automation of the existing networks is significantly higher than those who believe in this among scientific personnel.

General Question Number 19

Question: Do you think avoiding diversity and utilizing standardization of techniques and technologies, as much as possible, will help to make it more practical, less complex, easier, and faster to automate the network and network security solutions? Alternative answers:

- Yes, the benefits of automation will compensate for the vulnerability of homogeneity that will be imposed on the system by the degree of standardization and reduction/avoidance of diversity and reduce the complexity of the system, which is a winning factor for the security of the systems.
- Yes, but it will introduce other security challenges into the network as we will face the vulnerability of homogeneity in the network design/architecture. So we need to have some flexibility and balance in solutions when standardizing the solutions.
- No
- I don't know

The Reason for Asking This Question: Here, we sought participants' opinions on addressing the complex problem identified in our research. To explore their preferences, we proposed potential solutions and used reverse psychology techniques. Given that the SotA suggests standardization and homogeneity as vulnerabilities in network security architecture [112, 172], we inquired whether participants would consider embracing some degree of standardization and homogeneity in their network security practices to enhance security through automation techniques and technologies and whether they deemed this goal feasible.

Reference to Research Question: RQ3

Reference to What in SotA Results We Validate: Factors affecting NSA [2, 5–8, 13–17, 34, 35, 42, 43, 45–54, 56–59, 61, 63–68, 70, 71, 73–78, 80–87, 89–112].

Result Facts: Here, the answers given by scientific personnel, as presented in Figure H.32, shows that one person chose that they don't know about this, two of them decided that they agree with the statement mentioned in the question, but it will introduce other security challenges into the network as we will face the vulnerability of homogeneity in the network design/architecture. Hence, we need to have some flexibility and balance in solutions when standardizing the solutions.

Finally, the resting 50% of them chose they agree that the benefits of automation will compensate for the vulnerability of homogeneity that will be imposed on the system by the degree of standardization and reduction of diversity and that this will reduce the system's complexity, which is a winning factor for information security.

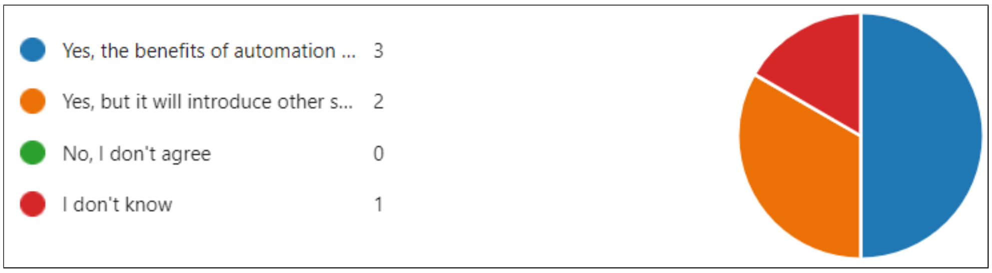


Figure H.32: Scientific personnel survey answer to question 19

Among IT professionals' answers to this question, as Figure H.33 presents, 16% of them stated that they don't know about this being helpful, 8% do not agree with the statement mentioned in this question, 28% of them chose that they agree, but it will introduce other security challenges into the network as we will face the vulnerability of homogeneity in the network design/architecture. Hence, we need to have some flexibility and balance in solutions when standardizing the solutions.

Finally, 48% of them answered that they agree that the benefits of automation will compensate for the vulnerability of homogeneity that will be imposed on the system by the degree of standardization and reduction of diversity and that this will reduce the complexity of the system, which is a winning factor for information security.

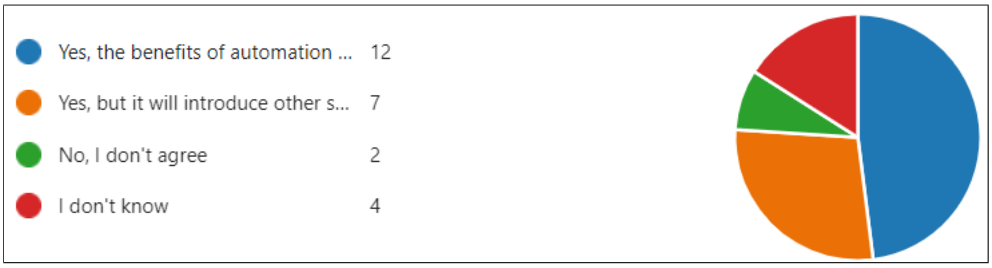


Figure H.33: IT professional survey answer to question 19

Analysis: Based on the responses to this question, it is evident that the majority agrees that the benefits of automating network processes and tasks outweigh the potential vulnerability of homogeneity resulting from standardization and reduced diversity. The concept of standardization and reduced diversity in technologies, suggested by the SotA [112], aims to simplify system complexity[2].

Regardless of the feasibility of our suggestions, we assume the participants who chose 'Yes' expressed a desire for improved security and efficiency in their network environment, even if it involves some level of standardization and homogeneity. We also assume that those who selected 'I don't know' indicate a recognition of the need for a change in network security management but may have reservations about whether our proposed solutions are the right approach.

General Question Number 20

Question: Do you agree with the claim that it is the organization- and team-leader skills in team-building, encouragement in learning and skills-building, and

---

[2] It's worth noting that we refer to the 'reduction' of diversity rather than its 'removal,' as complete homogeneity can also introduce vulnerabilities to the system, as highlighted in the SotA literature. For example, avoiding total homogeneity ensures that if one Operating System (OS), such as Windows, is targeted by cybercriminals, the presence of other diverse OS options, like Linux, can provide system resilience, preventing a complete system collapse [112].

leadership of teams that determine the progress of improvement in automating network and network security?

The Reason for Asking This Question: Here we wanted to evaluate if they agree with the organization- and team-leader skills in team-building, encouragement in learning and skills-building, and leadership of teams as an affecting factor in determining the progress of improvement in automating network and network security.

Reference to Research Question: RQ3

Reference to What in SotA Results We Validate: Factors affecting NSA and related work resources. We also wanted to validate our findings presented in the summary of the results [2, 5–8, 13–17, 34, 35, 42, 43, 45–54, 56–59, 61, 63–68, 70, 71, 73–78, 80–87, 89–112].

Result Facts: Here, as Figure H.34 presents, among the scientific personnel, 67% agree to this claim, while among IT professionals, as shown in Figure H.35, we have 84% who agree to this.

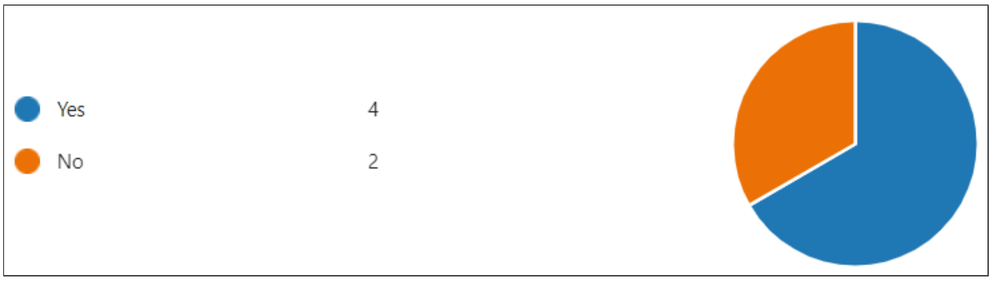


Figure H.34: Scientific personnel survey answer to question 20

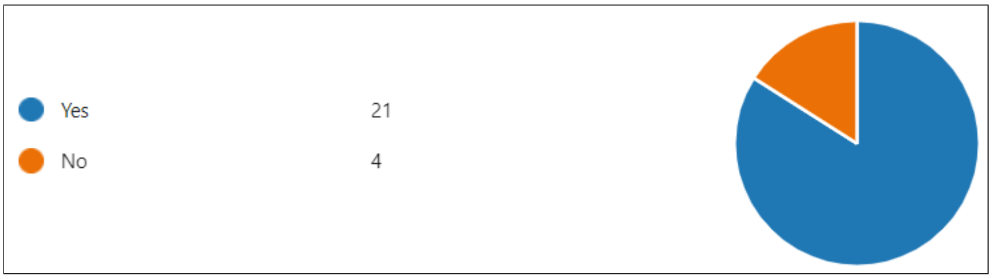


Figure H.35: IT professional survey answer to question 20

Analysis: Based on the responses to this question, 80.6% of all participants from both groups agree that organizational leadership, along with their skills in team building and encouragement in learning and skills development, plays a crucial role in determining the success and progress of network automation in their projects.

End of General Questions

H.2 Scientific Personnel Answers to Group-Specific Survey

This section presents the responses to group-specific questions from scientific personnel at the same university who are involved in teaching students.

Scientific Personnel - Question Number 21

Question: Do you teach/have you been teaching traditional network management techniques and technologies to students?
We assume that universities that teach traditional network management techniques and technologies to students also encourage and inform students about taking certifications in this relation. Your positive answer to this question will also confirm this fact.
By ‘traditional’, we mean all the methods and technologies that are managed manually and not automated.

The Reason for Asking This Question: This question was asked to both registers if the participants from the scientific personnel group have experience in teaching these topics and also to validate if the mentioned topics in this question are being studied at universities, which means that the learning of the mentioned topic is in progress.

Reference to Research Question: RQ1 and implicitly background registration of participants

Reference to What in SotA Results We Validate: Traditional network security techniques and architecture, and also evaluating the participants’ knowledge area and competence [26–29, 39–41, 67, 88, 112–118].

Result Facts: As shown in Figure H.36, 67% of the scientific personnel answered ‘Yes’ to this question.

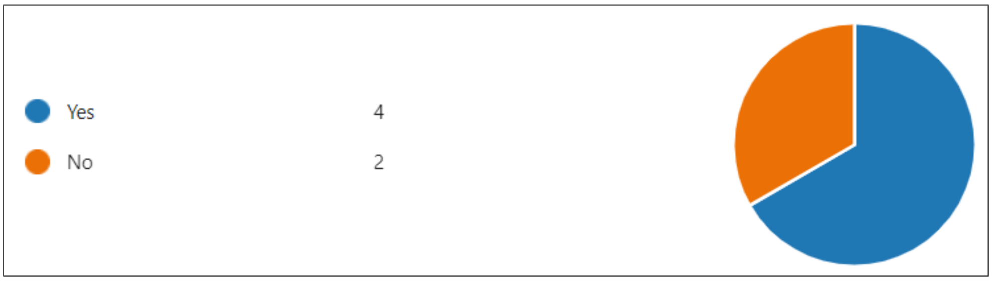


Figure H.36: Scientific personnel survey answer to question 21

Analysis: The answers received through this question indicate that traditional network techniques and technologies are introduced to the IT students at the university.

Scientific Personnel - Question Number 22

Question: Do you teach/have you been teaching techniques and technologies related to the following automation methods to your students:

- Software-defined Networking (SDN)
- Machine Learning (ML)
- Automation using Infrastructure as Code (IaC)
- Any other automation techniques and technologies

The Reason for Asking This Question: Both to register if the participant is involved in teaching automation techniques, which tells us to what ratio the participants are involved in teaching network automation to their IT students, and to determine what automation techniques and technologies are mainly studied to IT at universities. This was to verify the gap existing between what automation techniques the university teaches, what is utilized in organization and industry, and what is suggested by solution and equipment providers to find if this is affecting the progress of NSA. This was also to verify the automation techniques and technologies we have registered through the study of the SotA.

Reference to Research Question: RQ2, and implicitly RQ3 and background registration of participants

Reference to What in SotA Results We Validate: NSA techniques and technologies, their affecting factors, and also evaluating the participants' knowledge area and competence [1, 2, 5–8, 10, 13–17, 34, 35, 42–54, 56–59, 61, 63–87, 89–112].

Result Facts: As shown in Figure H.37, we observe that 22% of the scientific personnel have taught their students automation techniques and technologies such as SDN and other automation techniques. A higher percentage of 33% have been teaching their students IaC, and despite the sector diagram showing that 22%, which means 2 of them, have not been teaching any automation techniques and technologies to their students; by taking a deeper look at the details of the answers, we can see that only one of them has not been teaching any automation-related knowledge to their students, which means the majority of them are teaching students.

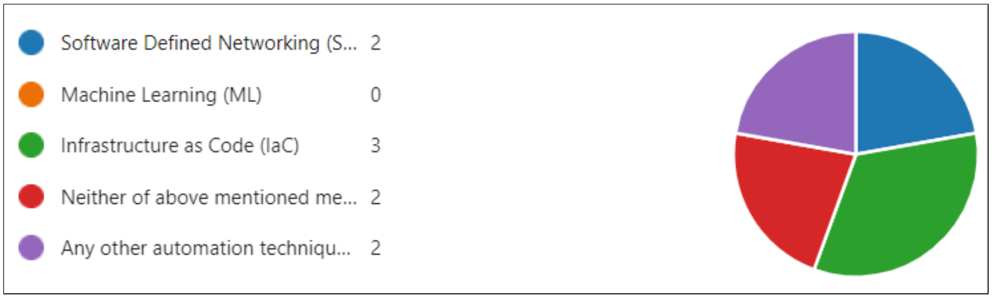
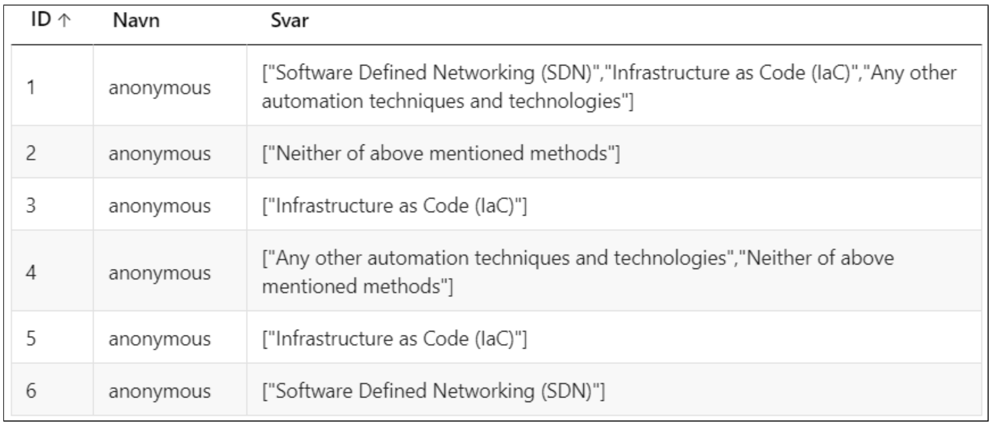


Figure H.37: Scientific personnel survey answer to question 22

This is because, as presented in Table H.1, one of them, who has answered Yes’ to the other automation techniques mentioned in this question, has also chosen neither of the above, which also makes sense. This means that not SDN, ML, or IaC, but ‘Any other automation techniques and technologies’. The participants answer which automation techniques they talk about in the next question.

Table H.1: Scientific personnel survey answer to question 22 in table format with details of each answer



ID ↑	Navn	Svar
1	anonymous	["Software Defined Networking (SDN)","Infrastructure as Code (IaC)","Any other automation techniques and technologies"]
2	anonymous	["Neither of above mentioned methods"]
3	anonymous	["Infrastructure as Code (IaC)"]
4	anonymous	["Any other automation techniques and technologies","Neither of above mentioned methods"]
5	anonymous	["Infrastructure as Code (IaC)"]
6	anonymous	["Software Defined Networking (SDN)"]

Analysis: It is interesting to consider that ML has not been a subject of study to students at all while as mentioned in Section 4.1, about 24% of the resources studied in this research work suggested utilization of ML and 90% of those resources suggested to combine ML with SDN to raise security resilience. This is while out of question 21, we know that 4 out of 6 scientific personnel who have participated in the survey have been teaching traditional network management techniques and technologies to university students.

Scientific Personnel - Question Number 23

Question: If you answered ‘Any other automation techniques and technologies’ to the above question, please mention the name of these methods here:(not mandatory to answer)

The Reason for Asking This Question: To specifically find out what automation techniques and technologies are studied to IT at universities to verify the gap existing between what automation techniques university teaches, with what is utilized in organization and industry, and what is suggested by solution and equipment providers. This was also to verify what automation techniques and technologies we have registered through the study of the SotA.

Reference to Research Question: RQ2 and implicitly RQ3

Reference to What in SotA Results We Validate: NSA techniques and technologies and their affecting factors [1, 2, 5–8, 10, 11, 13–17, 34, 35, 39–54, 56–68, 70–112].

Result Facts: In answer to this question, some participants mentioned Scripting using bash, PowerShell, and Python as any other automation techniques and technologies they have been teaching to the students. They also have mentioned Network administration toolkits, Scripted configuration deployment, Templated configuration, Business logic integration, Configuration Management integration, and Network management software as other automation techniques that they are or have been teaching to the students.

Analysis: This shows us what they teach IT students at universities about network automation techniques and technologies has a slightly different direction than what solution and equipment providers, such as Cisco and Juniper, suggest in their publications, as explained in Chapter 4. We can see the university has a stronger tendency to IaC methods with a CI/CD cycle with much focus on coding and programming skills. In contrast, as the review of the SotA has shown us, solution and equipment providers are more focused on SDN and API utilization with more focus on utilizing predefined templates to solve the lack of programming competency in the network operation, as mentioned in Chapter 4 Section 4.4.

———————Scientific Personnel - Question Number 24 ———————

Question: How many years of experience in working as scientific personnel in relation to IT knowledge do you have?

The Reason for Asking This Question: To register participants' backgrounds and evaluate the validity of our results.

Reference to Research Question: Background registration question.

Reference to What in SotA Results We Validate: Neither, evaluating the participants' knowledge area and competence.

Result Facts: Here, four answered that they have 20 years or more experience teaching university students, one answered 14, and the last person answered eight years of experience.

Analysis: This gives a high validity to our survey, as the people who participated in our investigation confirm having many years of experience in teaching students at university, and we assume that due to their valuable long experience in their work, we can highly count on their answers.

Scientific Personnel - Question Number 25

Question: As much as you know, do your students utilize the knowledge they gain related to network security automation techniques and technologies when they start working for companies?

The Reason for Asking This Question: To verify the gap existing between what students learn out of the knowledge they have acquired at university and what in practice is utilized in organizations and industries related to network automation techniques and technologies. This was to verify if the competency acquired helps the students who start working after graduation utilize their network automation competency.

Reference to Research Question: RQ2 and implicitly RQ3

Reference to What in SotA Results We Validate: NSA techniques and technologies and their affecting factors [1, 2, 5–8, 10, 11, 13–17, 34, 35, 39–54, 56–68, 70–112].

Result Facts: As presented in Figure H.38, all the participants unanimously answered 'Yes' to this question.

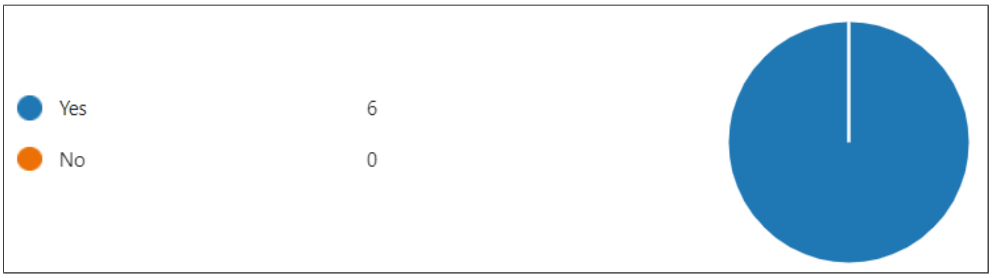


Figure H.38: Scientific personnel survey answer to question 25

Analysis: The answers received in this question indicate that the knowledge taught to students at university is practical and syncs with what they need further in their careers.

Scientific Personnel - Question Number 25

Question: Do you think it is necessary to have network automation as part of the study of the students of Information Technology (IT)?

The Reason for Asking This Question: This was to investigate the viewpoint of scientific personnel on the necessity of network automation, assuming that we put effort into what we believe in, which makes it an affecting factor in the success of the progress of learning process of network security automation at the universities, which is the step before work starts for IT students.

Reference to Research Question: RQ2 and implicitly RQ3

Reference to What in SotA Results We Validate: NSA techniques and technologies and their affecting factors [1, 2, 5–8, 10, 11, 13–17, 34, 35, 39–54, 56–68, 70–112].

Result Facts: As Figure H.39 presents, one participant answers 'No' to this question. In contrast, the rest of the participants responded 'Yes'; they see it as necessary to have network automation as part of the study of the IT students.

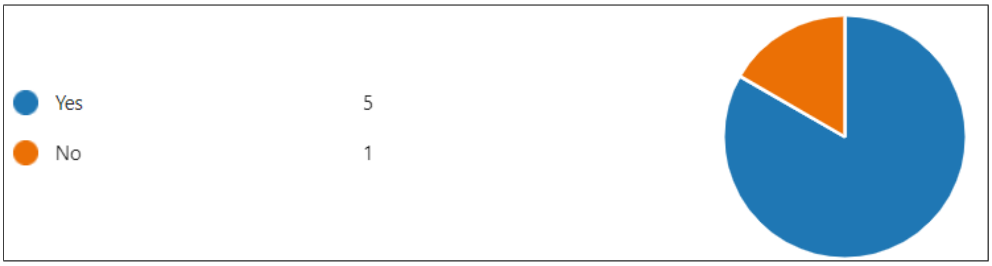


Figure H.39: Scientific personnel survey answer to question 26

Analysis: The answers here show most of them believe in the necessity of teaching network automation to their IT students. Hence, following their answers, we assume that they pave the way and show their support to IT students in this regard.

Scientific Personnel - Question Number 27

Question: Please briefly explain the reason for the answer you gave to the above question.

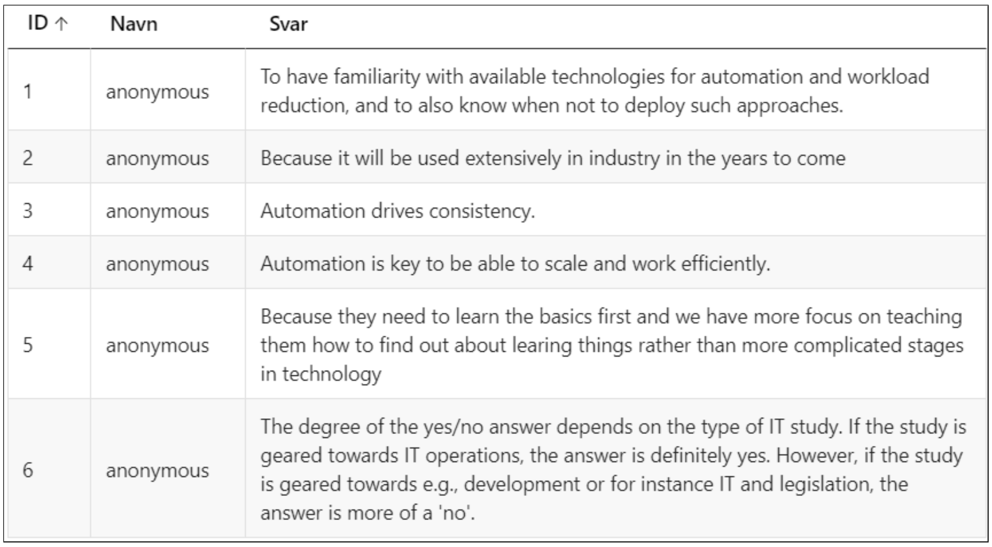
The Reason for Asking This Question: To validate the rationale behind the response provided in the previous question, which aids us in gaining a deeper understanding of their beliefs. This will also confirm the findings we have explored in the SotA about the necessity of automating network and network security solutions from the scientific personnel point of view.

Reference to Research Question: RQ2 and implicitly RQ3

Reference to What in SotA Results We Validate: NSA techniques and technologies and their affecting factors [1, 2, 5–8, 10, 11, 13–17, 34, 35, 39–54, 56–68, 70–112].

Result Facts: Reviewing the answers received to this open, not mandatory question, as Table H.2 presents, we assume that the answer number 5 is connected to the answer 'No', given in the previous question. The rest of the responses we assume have a connection to the 'Yes' answers to the previous question. This is because answer number 5 solidly sets its focus on the process of teaching students the basics of technology rather than jumping to the more complicated stages, which is the automation of those essential tasks and processes. This is understandable, and we see it as a 'process-oriented' reasoning.

Table H.2: Scientific personnel survey answer to question 27



ID ↑	Navn	Svar
1	anonymous	To have familiarity with available technologies for automation and workload reduction, and to also know when not to deploy such approaches.
2	anonymous	Because it will be used extensively in industry in the years to come
3	anonymous	Automation drives consistency.
4	anonymous	Automation is key to be able to scale and work efficiently.
5	anonymous	Because they need to learn the basics first and we have more focus on teaching them how to find out about learing things rather than more complicated stages in technology
6	anonymous	The degree of the yes/no answer depends on the type of IT study. If the study is geared towards IT operations, the answer is definitely yes. However, if the study is geared towards e.g., development or for instance IT and legislation, the answer is more of a 'no'.

The other answers, which were closer to those who answered ‘Yes’ to question 26, explained their reasoning as *‘Automation drives consistency’*, *‘Automation is key to be able to scale and work efficiently’*, *‘Because it will be used extensively in the industry in the years to come’*, *‘To have familiarity with available technologies for automation and workload reduction and also to know when not to deploy such approaches’*, and finally *‘The degree of the yes/no answer depends on the type of IT study. If the study is geared toward IT operations, the answer is definitely yes. However, if the study is geared towards, e.g., development or, for instance, IT and legislation, the answer is more of a ‘no”*, which seems more ‘result-oriented’ and focuses on the outcome rather than the learning process, which is also understandable.

Analysis: From the answers received in this question, we assume that scientific personnel has different viewpoints on the topic asked about in this and the previous question, and their priorities vary as here we can see two distinct trends in their reasoning. One that we called ‘process-oriented’ reasoning and the other one that we called ‘result-oriented’ reasoning. While we can see that their focus is on how to give the best study path to the students, the variety of their viewpoints on the teaching strategy makes it difficult for us to conclude.

Scientific Personnel - Question Number 28

Question: Network automation using automation configuration tools, such as Ansible, and programming languages like Python, and different platforms, in addition to various platforms and technologies, such as SDN, ML, and IaC, is suggested by many academic researchers[3]. Why do you think these technologies are/are

---

[3] See Chapter 4.

not used in today's knowledge learning by universities for teaching and nurturing knowledge in network security automation?

The Reason for Asking This Question: To confirm whether they believe these technologies are employed in the knowledge-learning process at universities and the reasons behind their positive or negative responses. This will help identify and validate the factors influencing the success of network automation skills development for IT students.

Reference to Research Question: RQ2 and implicitly RQ3

Reference to What in SotA Results We Validate: NSA techniques and technologies and their affecting factors [1, 2, 5–8, 10, 11, 13–17, 34, 35, 39–54, 56–68, 70–112].

Result Facts: In answers received to this open question, we observe the answers such as *'They are used because they are industry standards in many places'*, *'I believe they all are taught and not reached, depending on the program focus'*, *'It will become too complicated for our students who are just starting to learn different IT techniques and technologies'*, and finally, *'If they are not, it is probably a question of balancing included content. There are so many areas it is 'important to cover' that it is impossible to cover them all. In other words, it all boils down to the type of IT study and the corresponding prioritization of topics to include'*.

Analysis: From the answers received in this question, we can see that despite the variety in responses, all of them point to the fact that what they teach the students at universities depends on their study program and will be justified about each study program's goals. Hence, we assume that automation techniques and technologies for network and network security are not necessarily prioritized to be included in the IT students' study programs but are included if relevant for the specific study program.

Scientific Personnel - Question Number 29

Question: Is there any subject specifically focusing on network automation techniques and technologies for students working on their Bachelor's or Master's degree at the university where you are a member of the scientific personnel?

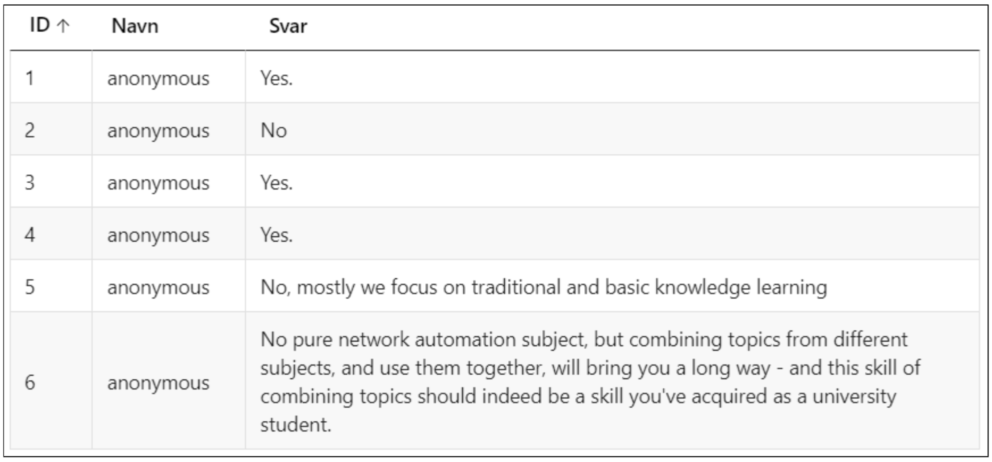
The Reason for Asking This Question: This was conducted to investigate whether universities contribute to knowledge learning and skills development for IT students. Additionally, we aimed to examine the role of competency and skills development, as mentioned in the SotA, as a factor affecting the success of progress in network security automation.

Reference to Research Question: RQ2 and implicitly RQ3

Reference to What in SotA Results We Validate: NSA techniques and technologies and their affecting factors [1, 2, 5–8, 10, 11, 13–17, 34, 35, 39–54, 56–68, 70–112].

Result Facts: Here, three of the scientific personnel answered 'Yes', while three others answered 'No' followed with some complementary sentences as *'No, mostly* *we focus on traditional and basic knowledge learning'*, and *'No pure network automation subject, but combining topics from different subjects, and use them together, will bring you a long way - and this skill of combining topics should indeed be a skill you've acquired as a university student'*, mainly pointing at skills building and the process of learning rather than the specific related topics.

Table H.3: Scientific personnel survey answer to question 29



ID ↑	Navn	Svar
1	anonymous	Yes.
2	anonymous	No
3	anonymous	Yes.
4	anonymous	Yes.
5	anonymous	No, mostly we focus on traditional and basic knowledge learning
6	anonymous	No pure network automation subject, but combining topics from different subjects, and use them together, will bring you a long way - and this skill of combining topics should indeed be a skill you've acquired as a university student.

Analysis: From the answers received, we cannot conclude precisely. This is because we are receiving different answers from scientific personnel who work at the same university, where half of them reject, and the other half confirm. We interpret this as they see different subjects as related to network automation and have different viewpoints on what is relevant and counted as automation techniques and technologies. Hence, this does not give us a precise conclusion. From their answers, we can only confirm that they focus extensively on skills-building and the learning process.

Scientific Personnel - Question Number 30

Question: Do students, who specialize in network or network security subjects such as CCNA, CCNP, etc., have the chance to choose subjects that help them to learn about certification-related topics such as DevNet Associate (DevAsc) where the focus is on automating network and network security processes by utilizing network automation techniques and technologies?

The Reason for Asking This Question: This question was posed to assess whether IT students studying at universities have the opportunities to acquire knowledge and skills in network automation techniques and technologies, thereby better preparing them for their future careers. Additionally, it was used to review this parameter as a factor influencing the possibilities of skills development in network security automation during the validation of our results.

Reference to Research Question: RQ2 and implicitly RQ3

Reference to What in SotA Results We Validate: NSA techniques and technologies and implicitly their affecting factors [2, 5, 10–13, 15–17, 47, 49, 70, 76, 79, 80, 83–85, 105].

Result Facts: As shown in Figure H.40, 67% of the participants answer 'No' to this question, which means that the students cannot choose network automation-related topics to work on their skills-building in this relation, while 33% answered 'Yes' which means that the students do have this chance at their university.

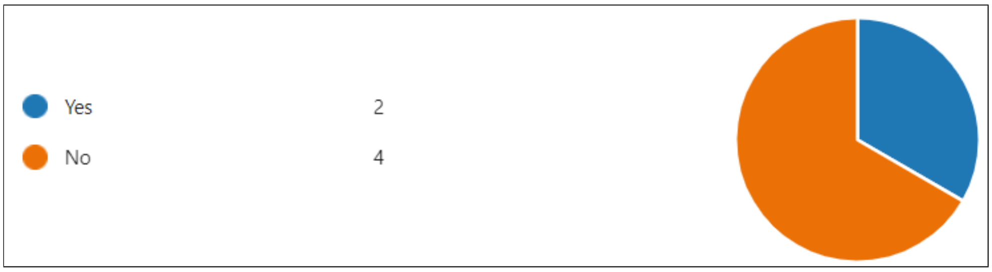


Figure H.40: Scientific personnel survey answer to question 30

Analysis: In this question, same as the answers to the previous question, we have received both no and yes as responses, and as we do not have an overview of which participants answered yes or no, we cannot make a solid conclusion on this. We, however, from the answers, can assume that based on what each of the participants counts as related to automation techniques and technologies, most of them reject that this chance which was explained in the question, is offered to the students at their university.

Scientific Personnel - Question Number 31

Question: If you answered 'Yes' to the question above, please write the name of the subjects that you mean to help students learn about and get hands-on with network automation.

The Reason for Asking This Question: The same as the reason explained in the reasoning for question 30.

Reference to Research Question: RQ2 and implicitly RQ3

Reference to What in SotA Results We Validate: NSA techniques and technologies and implicitly their affecting factors [2, 5, 10–13, 15–17, 47, 49, 70, 76, 79, 80, 83–85, 105].

Result Facts: Here, we received two answers that we assume correspond to the two who answered 'Yes' in the previous question. One of them states *'I hope it's part of the network management courses at IIK.'*[4] and the other one explains that *'University subjects beyond those offered in connection with Cisco Networking Academy*

---

[4] IIK mentioned here points at Institutt for Informasjonssikkerhet og Kommunikasjonsteknologi

are not geared toward certifications, but geared toward learning and understanding. As such, some subjects give "certification-related" content, but that is not the focus and/or goal. This does, to a degree, also apply to the Network Professional level subjects'.

Analysis: From the first answer received here, we cannot see a concrete response where the study program can specifically be mentioned. This is because the respondent says they assume or hope that there is such a study program. Furthermore, the second response indicates that the emphasis is on students' learning and understanding. This suggests to us that this answer implicitly conveys that automation techniques are not the primary focus; instead, it is the learning process that holds greater significance.

Scientific Personnel - Question Number 32

Question: Do you introduce and mention the existence of network and network security automation knowledge and technologies to your IT students and encourage them to follow the path and be curious about it?

The Reason for Asking This Question: This was to verify whether they make their students familiar with the knowledge existing about network automation techniques and technologies, and also, because the competency of the IT personnel is mentioned as one of the affecting factors in the progress of network security automation by the SotA, to verify if the scientific personnel contribute to this progress.

Reference to Research Question: RQ2 and implicitly RQ3

Reference to What in SotA Results We Validate: NSA techniques and technologies and implicitly their affecting factors [1, 2, 5, 6, 8, 10, 11, 13–17, 34, 35, 39–52, 54, 56–68, 70–108, 110, 111].

Result Facts: As presented in Figure H.41, 83% of the scientific personnel who participated in the survey answered 'Yes' to this question.

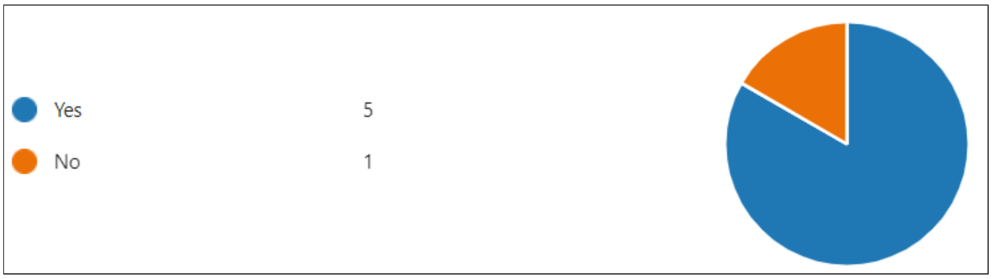


Figure H.41: Scientific personnel survey answer to question 32

Analysis: We assume that familiarity and introducing knowledge to students as

---

in Norwegian, which in English means Department of Information Security and Communication Technology.

a factor is essential because as soon as the students get familiar with a concept, they can dig into it if they find it interesting, and develop their skills, as also one of the scientific personnel has mentioned in their answer to question 27. The responses to this question show that most of the scientific personnel introduce network security automation to their students.

Scientific Personnel - Question Number 33

Question: Regarding what was asked in your first group-specific question, we assume that students who study network or network security subjects are encouraged to get ready and take the certification exams provided by different companies, for instance, Cisco certifications in CCNA and CCNP. Do you also encourage them to take certifications in network automation techniques and technologies?

The Reason for Asking This Question: This aimed to verify whether scientific personnel indeed play a role in encouraging and motivating students to pursue certification in network automation techniques and technologies. This will also confirm their efforts in motivating and building competency, factors that influence the progress of network security automation.

Reference to Research Question: RQ2 and implicitly RQ3

Reference to What in SotA Results We Validate: NSA techniques and technologies and implicitly their affecting factors [2, 5, 10–13, 15–17, 47, 49, 70, 76, 79, 80, 83–85, 105].

Result Facts: As shown in Figure H.42, we have a majority of 83% who answered 'No' to this question.

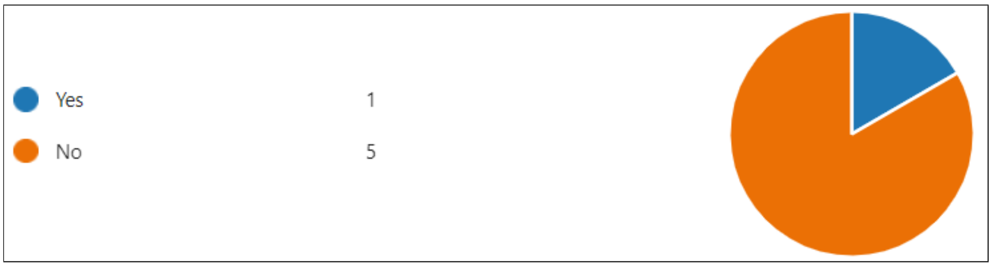


Figure H.42: Scientific personnel survey answer to question 33

Analysis: Here, we also assume the reasoning for this is the same as mentioned in the previous question, where we pointed at the answer given to question 27, as one of the scientific personnel mentioned that *'Because they need to learn the basics first and we have more focus on teaching them how to find out about learning things rather than more complicated stages in technology'*. This answer explains many other answers received through this survey. Based on this viewpoint, we assume that university has their focus on teaching students how to learn and not the more advanced steps that naturally arrive when they start working for the organizations after they graduate, such as taking related certifications.

Scientific Personnel - Question Number 34

Question: In case you answered yes to the questions above, which are about existing and teaching network and network security automation to students at the university you work for, regarding the students that have graduated and started working for the companies; do you think/know if they do utilize/have utilized their knowledge in network automation in their work?

The Reason for Asking This Question: As a factor affecting the progress of network security automation, implied by the SotA, is competency and skills building of IT personnel, we investigated how universities contribute to the progress of this factor.

Reference to Research Question: RQ2 and implicitly RQ3

Reference to What in SotA Results We Validate: NSA techniques and technologies and implicitly their affecting factors [2, 5, 10–13, 15–17, 47, 49, 70, 76, 79, 80, 83–85, 105].

Result Facts: Here, 4 participants answered that they have answered 'No' to the previous question, while 2 of them responded 'Yes' to this question.

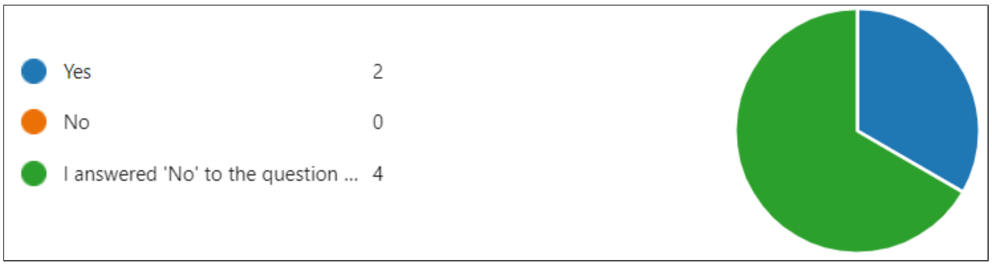


Figure H.43: Scientific personnel survey answer to question 34

Analysis: This question was mentioned regarding the previous question, question 33, where we asked if they encourage the students to take certifications in network automation techniques and technologies. The answer 'Yes' given to this question means they confirm that the students utilize their knowledge in network automation in the work they start after graduation, which is received from most of the participants, including one-third of the participants. We assume those who said 'No' to this question see it from the automation techniques perspective as this is what the question is related to, which corresponds to the answers received in question 30.

Scientific Personnel - Question Number 35

Question: According to your knowledge and experience, do you think there is a gap between what students learn and what they can utilize of the knowledge related to network automation gained during their education when they start working?

(*If you mean that they don't gain knowledge related to network automation during their study, this means that there isn't a gap, and your answer should be 'No' to this question, but if otherwise, then the answer should be 'Yes' to this question)

The Reason for Asking This Question: As a factor affecting the progress of network security automation, implied by the SotA, is competency and skills building of IT personnel, we investigated how universities contribute to the progress of this factor.

Reference to Research Question: RQ2 and implicitly RQ3

Reference to What in SotA Results We Validate: NSA techniques and technologies and implicitly their affecting factors [2, 5, 10–13, 15–17, 47, 49, 70, 76, 79, 80, 83–85, 105].

Result Facts: As Figure H.44 presents, 33% pointed that there is a gap as explained in the question, while the majority of 67% suggested that no gap exists in this regard.

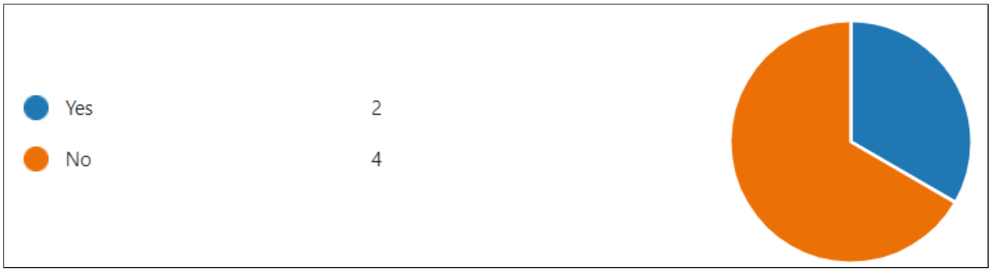


Figure H.44: Scientific personnel survey answer to question 35

Analysis: From the answers given to this question, we assume that most of the scientific personnel are satisfied with the content offered through the study programs to IT students and see no gap between what they teach students and what is needed in their future working environment. Some of them, however, disagree and mean that, indeed, there is a gap between what students receive as the content of their study programs and what they need in their future work. The variety of their answers makes it difficult to make a solid conclusion and is, to a high degree, dependent on what is each viewpoint on the result of the study programs.

Scientific Personnel - Question Number 36

Question: According to your knowledge and experience, is what you teach students related to network automation techniques and technologies far ahead or far behind what they are required, need to know, and should manage within their working life?
Alternatives:

- What we teach them in **network automation techniques and technologies**, is far behind what they need in their future working life

- What we teach them in **network automation techniques and technologies**, far ahead of what they need in their future working life
- When it comes to utilizing **network automation techniques and technologies**, it is a nice and good sync between what we teach them at university and what they need to work with, in their future working life

The Reason for Asking This Question: Same as mentioned in the previous question, as a factor affecting the progress of network security automation, implied by the SotA, is competency and skills building of IT personnel, we investigated how universities contribute to the progress of this factor.

Reference to Research Question: RQ2 and implicitly RQ3

Reference to What in SotA Results We Validate: NSA techniques and technologies and implicitly their affecting factors [2, 5, 10–13, 15–17, 47, 49, 70, 76, 79, 80, 83–85, 105].

Result Facts: As presented in Figure H.45, all the participants unanimously choose the answer which states that when it comes to utilizing network automation techniques and technologies, it is a proper sync between what we teach them at university and what they need to work with, in their future working life.

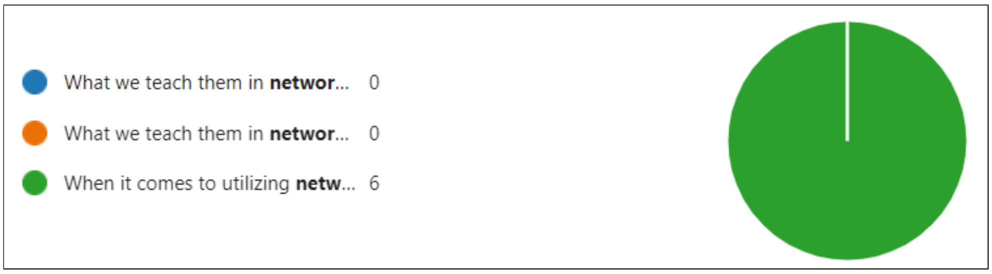


Figure H.45: Scientific personnel survey answer to question 36

Analysis: The answers received to this question show that all the scientific participants unanimously agree that what students receive today in their study program is what competency and knowledge they need to start in their future working environment.

Scientific Personnel - Question Number 37

Question: In research conducted through many papers, books, and related works to network and network security automation, we can see a considerable amount of academic work done in this area, but we also see that the industry is utilizing manual techniques to manage their network and network security.
Do you see and agree that there is a gap between the level of academic research done in this area and the level of utilization of their results in the industry?

The Reason for Asking This Question: Here, we wanted to know if the scientific personnel confirm what we have observed by studying the SotA in this research work, which was what the question was asking about.

Reference to Research Question: RQ2 and implicitly RQ3

Reference to What in SotA Results We Validate: NSA techniques and technologies and implicitly their affecting factors [2, 5, 10–13, 15–17, 47, 49, 70, 76, 79, 80, 83–85, 105].

Result Facts: As presented in Figure H.46, 83% of the participants agree with the state mentioned in this question.

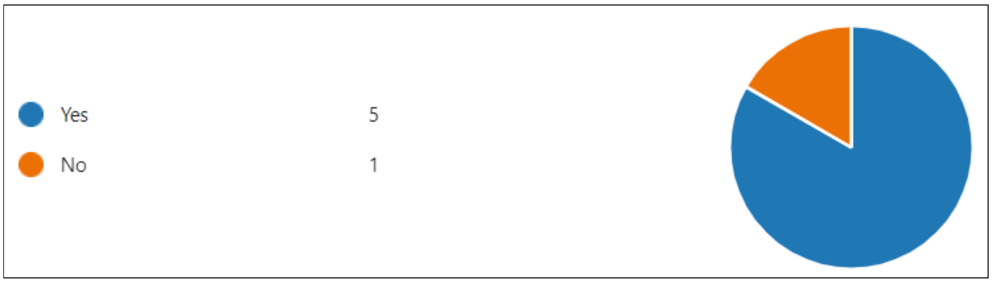


Figure H.46: Scientific personnel survey answer to question 37

Analysis: Based on the responses received from the participants, we can confirm that the majority of them agree that the gap we observed between what academic research has achieved in the field of network security automation, on one hand, and the practical utilization of their results by the industry, on the other hand, does indeed exist. This gap was identified through our examination of the SotA.

Scientific Personnel - Question Number 38

Question: If your answer to the above question was 'Yes', please briefly mention why you think the gap between these two areas, the industry and the academic research in the context of network and network security automation, exists. (not mandatory to answer)

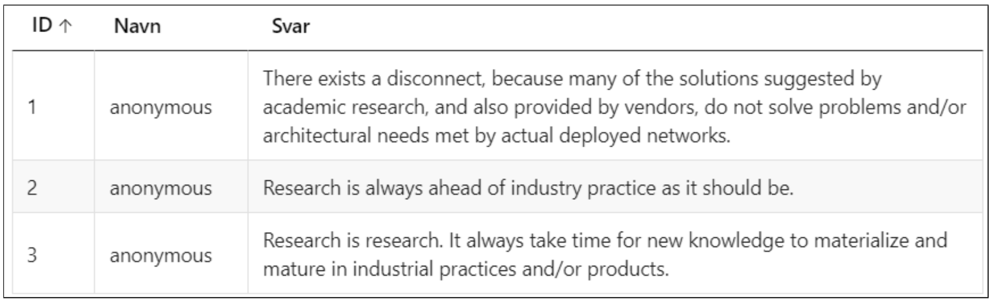
The Reason for Asking This Question: Here, we wanted to examine the viewpoint of those who confirmed that the mentioned gap exists, about the reason, they associate it with.

Reference to Research Question: RQ2 and implicitly RQ3

Reference to What in SotA Results We Validate: NSA techniques and technologies and implicitly their affecting factors [2, 5, 10–13, 15–17, 47, 49, 70, 76, 79, 80, 83–85, 105].

Result Facts: As presented in Table H.4, one participant answers that *'This is because research is always ahead of industry practice as it should be'*, while the other one answers that *'Research is research. It always takes time for new knowledge to materialize and mature in industrial practices and/or products'*. The third answer given to this question mentions, *'There exists a disconnect, because many of the solutions suggested by academic research, and also provided by vendors, do not solve problems and/or architectural needs met by actually deployed networks'*.

Table H.4: Scientific personnel survey answer to question 38



ID ↑	Navn	Svar
1	anonymous	There exists a disconnect, because many of the solutions suggested by academic research, and also provided by vendors, do not solve problems and/or architectural needs met by actual deployed networks.
2	anonymous	Research is always ahead of industry practice as it should be.
3	anonymous	Research is research. It always take time for new knowledge to materialize and mature in industrial practices and/or products.

Analysis: From the answers received, we assume that they associate it with the parameter of time, where they mention academic research is always ahead and it takes time for the industry to find and adopt the proper solutions provided to their environments. They also point at the fact, which also is mentioned by the SotA, that solutions suggested by academia or by the vendors do not always match what is needed in the industry. It is noteworthy that here, the participants, very naturally, point to the three actors that we have verified in our research and introduced as ITAT in the CCAM summary, in Chapter 4.

Scientific Personnel - Question Number 39

Question: Assuming that academic research is far ahead when it comes to conducting research on network and network security automation techniques and technologies, and industry is far behind when it comes to utilizing the latest and newest results produced by academia in this knowledge area.
Do you agree that for teaching new IT students, the university utilizes the materials published by the industry, which is far behind the newest academic research results?
Alternatives answers:

- Yes, we utilized the famous published books and materials by the industry
- No, what we teach the students is based on academic work and the last and the newest research results
- Both, we always combine both the literature published by the industry and the results from the academic work by students and staff at the university
- We sometimes use both, sometimes only the books and materials published by industry companies such as Cisco or Juniper concerning network and network security
- We don't teach them network and/or network security automation. This is

not in the focus area of what we teach them!

The Reason for Asking This Question: Here we wanted to investigate if what students receive through the study program is the newest and latest existing knowledge, as competency and skills building is mentioned as a factor that affects the progress of network security automation success by the SotA. In the previous question, we confirmed through the answers given by the participants that industry is indeed behind what academia finds and provides to society. Here, we put the question from the other perspective and wanted to know whether the study material that universities use to teach students is what the industry produces. Also, here, putting some level of bias in the question is to use reverse psychology so if they disagree with what the question states, they choose the opposite answer, which starts with 'No' and further elaborates on it.

Reference to Research Question: RQ2 and implicitly RQ3

Reference to What in SotA Results We Validate: NSA techniques and technologies and implicitly their affecting factors [2, 5, 10–13, 15–17, 47, 49, 70, 76, 79, 80, 83–85, 105].

Result Facts: As Figure H.47 presents the answers given here, 50% of the participants agreed that they use both, they always combine both the literature published by the industry and the results from the academic work by students and staff at the universities, and 50% agree that they sometimes use both, sometimes only the books and materials published by the industry companies such as Cisco or Juniper concerning network and network security.

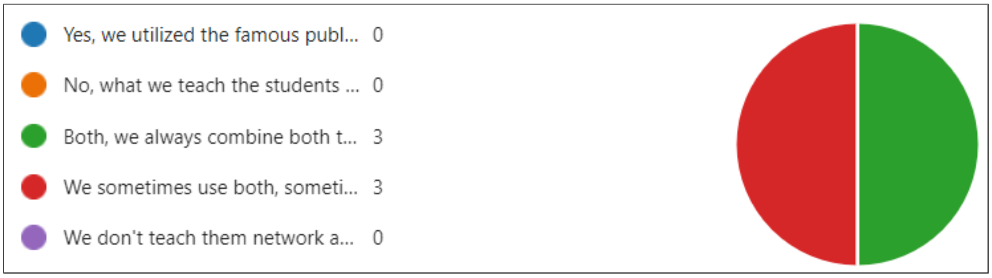


Figure H.47: Scientific personnel survey answer to question 39

Analysis: Based on the responses received here, we can confirm that scientific personnel do take this factor into account when selecting study materials for their programs. They choose a combination of materials from both industry and academia to impart the latest knowledge to their students. However, the specific selection of study materials, we assume, depends on each individual's circumstances and priorities.

———————Scientific Personnel - Question Number 40 ———————

Question: Does the university you work for offer any subject directly related to

Machine Learning (ML)?

The Reason for Asking This Question: Skills building is identified as a significant factor affecting the progress of Network Security Automation (NSA) in the SotA. This question was posed to confirm whether universities provide knowledge and skills development related to the technology mentioned in this question to IT students and to evaluate its impact on this process. Specifically, this question aims to validate this assertion, as approximately 20% of the SotA sources reviewed in this research recommend the utilization of ML in NSA.

Reference to Research Question: RQ2 and implicitly RQ3

Reference to What in SotA Results We Validate: NSA techniques and technologies and implicitly their affecting factors [5, 40, 41, 44, 45, 48, 50, 54–57, 62, 65, 69, 73, 74, 77, 78, 83, 87, 88, 106, 109, 110, 113].

Result Facts: Here we see a majority of 83% answers 'Yes' to this question.

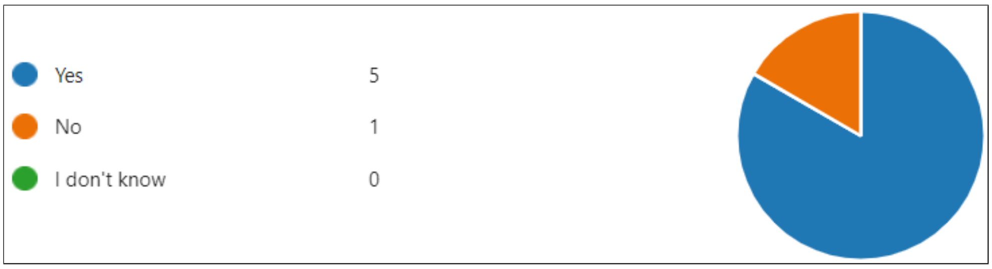


Figure H.48: Scientific personnel survey answer to question 40

Analysis: The scientific personnel who answer this question all work at the same university. Hence, observing one person say 'No' while the others confirm 'Yes' to this question makes us assume that their understanding of subjects related to ML is not the same. Hence, we cannot give a concrete conclusion despite most of them saying 'Yes'. However, this shows that they have different views on what is related to ML. The variety in answers could also be related to their overview of the topics offered to the students by their university.

Scientific Personnel - Question Number 41

Question: As much as you know, how many subjects related to ML does the university you work for, offer to the students who study network and information security?
Alternatives answers:
- No subjects related to ML
- Ten or more subjects/study topics related to skill building and gaining knowledge in ML are offered to students

The Reason for Asking This Question: Skills building is mentioned as an affecting factor for the progress of the success of network security automation by the

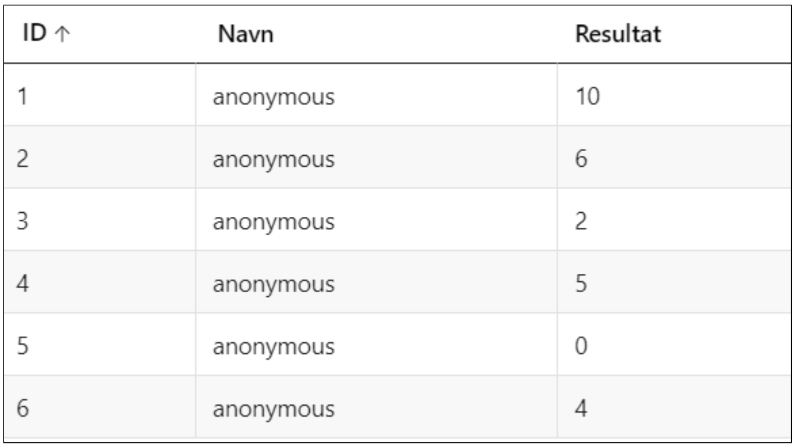
SotA. This question was asked to investigate closer to what degree the universities provide knowledge and skills building to IT students related to the technology mentioned in this question and to review it as an affecting factor for this process. Specifically, because ML is recommended by about 20% of the SotA studied in this research to be utilized in network security automation.

Reference to Research Question: RQ2 and implicitly RQ3

Reference to What in SotA Results We Validate: NSA techniques and technologies and implicitly their affecting factors [5, 40, 41, 44, 45, 48, 50, 54–57, 62, 65, 69, 73, 74, 77, 78, 83, 87, 88, 106, 109, 110, 113].

Result Facts: As presented in Table H.5 the answers given to this question were various.

Table H.5: Scientific personnel survey answer to question 41



ID ↑	Navn	Resultat
1	anonymous	10
2	anonymous	6
3	anonymous	2
4	anonymous	5
5	anonymous	0
6	anonymous	4

Analysis: Here, because of the variety of the answers received to this question, it is not easy for us to conclude their answers. We can see one person answering zero, one answering six, and the other ten, which reduces the validity of the answers received in this question mainly because they all work at the same university. Hence, the same conclusion applies to this question as the previous question, where we see this variety of answers because of what they think applies to ML or because of their different overview on the offered topics by their university. In any way, one thing is more apparent to us now, and that is ML being less known and more ambiguous to people, which points to the factor of complexity.

Scientific Personnel - Question Number 42

Question: Does the university you work for offer any subject directly related to Software-defined Networking (SDN)?

The Reason for Asking This Question: Skills building is identified as a factor influencing the progress of Network Security Automation (NSA) in the SotA. This question was posed to verify whether universities offer knowledge and skills development related to the technology mentioned in this question to IT students and to assess its impact on this process. Specifically, this question aims to confirm this assertion since 81% of the SotA sources studied in this research recommend the utilization of SDN in NSA.

Reference to Research Question: RQ2 and implicitly RQ3

Reference to What in SotA Results We Validate: NSA techniques and technologies and implicitly their affecting factors [1, 2, 5, 6, 8, 10, 11, 13–17, 34, 35, 39–52, 54, 56–68, 70–108, 110, 111].

Result Facts: As shown in Figure H.49, we observe one person answers 'No', and another person responds that they don't know about this. This is while 67% answer 'Yes' to this question.

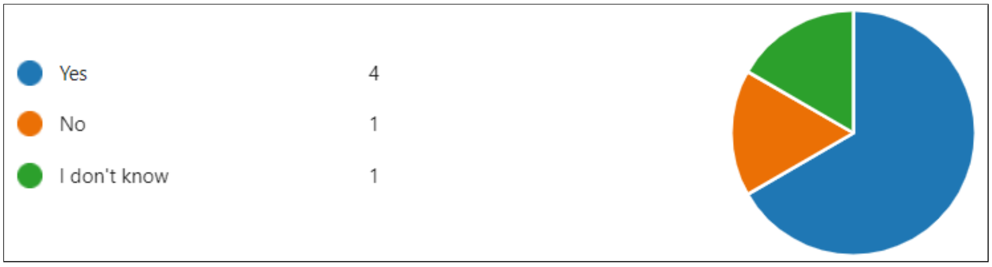


Figure H.49: Scientific personnel survey answer to question 42

Analysis: Regarding the variety of the answers received here, which are from scientific personnel working at the same university, we see it difficult to conclude. Again here, we assume that they have different understandings about what applies to the concept of Software-defined Networking (SDN). This verifies our results, pointing at various actors, explained in Chapter 4 in the figure that shows ITAT, having different ways of defining NSA solutions and providing their way of knowing about this. This fact also verifies our findings about the challenges, such as complexity and the lack of a standard definition for technologies related to network and network security automation, explained in Chapter 4.

Scientific Personnel - Question Number 43

Question: Does the university you work for offer any subject directly related to Infrastructure as Code (IaC)?

The Reason for Asking This Question: Skills building is identified as an influencing factor in the progress of Network Security Automation (NSA) in the SotA. This question was asked to verify whether universities offer knowledge and skills development related to the technology in question to IT students and to assess its impact on this process. Specifically, this question aims to confirm this assertion since the SotA sources studied in this research recommend the utilization of IaC in NSA.

Reference to Research Question: RQ2 and implicitly RQ3

Reference to What in SotA Results We Validate: NSA techniques and technologies and implicitly their affecting factors [1, 2, 5, 6, 8, 10, 17, 35, 43–45, 47–52, 56, 57, 61, 65, 66, 69–75, 77–87, 90–94, 99, 103, 105, 106, 108–111].

Result Facts: As shown in Figure H.50, one person expresses that they don't know about this, while the resting 83% answer 'Yes' to this question.

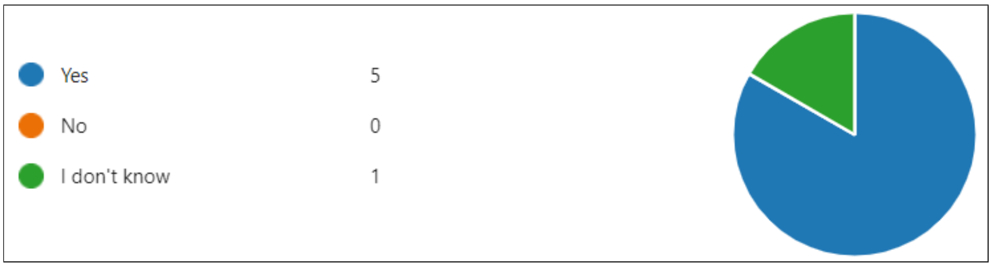


Figure H.50: Scientific personnel survey answer to question 43

Analysis: Here, we received a more solid answer than what we received to the previous question. Hence, we assume that there exists a more explicit definition about Infrastructure as Code (IaC) among scientific personnel, which results in the answers received here. Still, having one person from the same university rejecting this makes us assume that, some ambiguities about the definition of what they see as IaC exist. We assume this is also related to the complexity and the lack of a standard definition for technologies related to network and network security automation, explained in Chapter 4. Regarding the majority who confirm their university offers the knowledge related to IaC to students, we assume this means that the universities have more focus on coding and programming skills than the API related network automation models such as SDN or even ML.

Scientific Personnel - Question Number 44

Question: Does the university you work for offer any subject directly related to software development and CI/CD?

The Reason for Asking This Question: As software development and CI/CD is mentioned by many of the resources studied in the SotA, presented in Chapter 4, related to network and network security automation, here we wanted to investigate if this is also paid attention to by university, which is dedicated to knowledge and competency enhancement for students.

Reference to Research Question: RQ2 and implicitly RQ3

Reference to What in SotA Results We Validate: NSA techniques and technologies and implicitly their affecting factors [1, 2, 5, 6, 8, 10, 17, 35, 43–45, 47–52, 56, 57, 61, 65, 66, 69–75, 77–87, 90–94, 99, 103, 105, 106, 108–111].

Result Facts: As presented in Figure H.51, 50% answers 'Yes' to this question, while 33% express not knowing the answer, and one person answers ‘No’ to this.

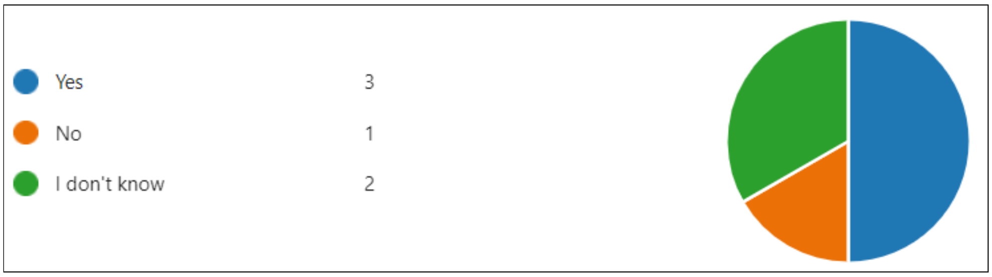


Figure H.51: Scientific personnel survey answer to question 44

Analysis: The answers received here in this question match what we have received from scientific personnel in answer to question number three, where 50% of them confirmed to know DevOps and IaC as CI/CD, following what is provided in the SotA, also taught in the same stack with IaC [70, 79]. Hence, we assume a connection here and that scientific personnel who know IaC are also involved and have an overview of their university providing subjects that are directly related to software development and CI/CD to their students. At the same time, the variety of the answers received here makes us assume this result again to a degree, pointing to the complexity and lack of a standard definition for technologies related to network and network security automation, explained in Chapter 4.

Scientific Personnel - Question Number 45

Question: The way you see it when the IT students finish their education at the university you work for, do they have enough knowledge, experience, and confidence to utilize automation techniques in practice in network and network security?

The Reason for Asking This Question: Directly addressing network and network security, our investigation here aims to verify whether what students learn at university in this context supports their future career needs and assess if universities positively impact the competency of IT students. This inquiry stems from the recognition of competency as a significant factor in this regard, as highlighted in the SotA [2, 10, 11, 17, 26–28, 115, 116].

Reference to Research Question: RQ2 and implicitly RQ3

Reference to What in SotA Results We Validate: NSA techniques and technologies and implicitly their affecting factors [2, 5, 10–13, 15–17, 47, 49, 70, 76, 79, 80, 83–85, 105].

Result Facts: As presented in Figure H.52, everybody unanimously answered ‘Yes’ to this question.

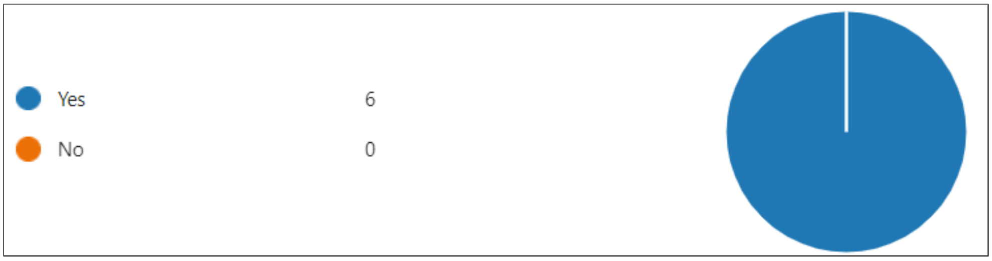


Figure H.52: Scientific personnel survey answer to question 45

Analysis: In the answers to this question, like what we received to question 25, all the scientific personnel agreed that what they offer of knowledge in network and network security to students is providing students with enough experience and confidence in their future career. Hence, from both of these answers and the other answers to similar questions received, we assume that they agree on this. Thus we assume that universities are doing what is possible to do to support students and make them ready for their future career needs.

Scientific Personnel - Question Number 46

Question: Do you or other university personnel teach and train IT students in team working to acquire competencies in team working process and skills?

The Reason for Asking This Question: As highlighted in the SotA presented in Chapter 4, network automation necessitates programming skills, and the utilization of IaC, for example, requires collaborative teamwork in a CI/CD context [70, 79]. Consequently, we investigated to verify whether universities actively contribute to teamwork skills development among students. This inquiry seeks to confirm whether universities support this critical factor in the development of skills for future IT professionals.

Reference to Research Question: RQ2 and implicitly RQ3

Reference to What in SotA Results We Validate: NSA techniques and technologies and implicitly their affecting factors [2, 5, 10–13, 15–17, 47, 49, 53, 70, 76, 79, 80, 83–85, 105].

Result Facts: As the results of the answers given to this question are presented in Figure H.53, the same unanimity with 'Yes' as the chosen answer is received in this question.

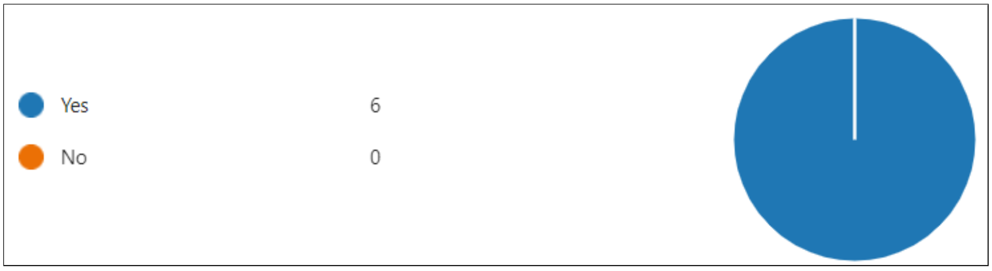


Figure H.53: Scientific personnel survey answer to question 46

Analysis: Here, all the participants unanimously confirm that the university supports skills building in teamwork for the students, which verifies that IT students that start working for different companies are already trained to be able to collaborate and accomplish their jobs by working in teams.

Scientific Personnel - Question Number 47

Question: Are Python and Ansible, which are mentioned by the state-of-the-art studied in our research, among the automation configuration tools that the university you work for taught to the students?
Alternative answers:

- Python Yes, but Ansible No
- Ansible Yes, but Python No
- Both of them, Yes, and comprehensively
- Both of them, Yes, but with limitations
- No, neither of them

The Reason for Asking This Question: To investigate more closely the extent to which programming skills related to network automation, which, as mentioned in the SotA, are heavily based on utilizing the Python programming language and Ansible automation tools [2, 11, 70], are supported by universities.

Reference to Research Question: RQ2 and implicitly RQ3

Reference to What in SotA Results We Validate: NSA techniques and technologies and implicitly their affecting factors [1, 2, 5, 6, 8, 10, 11, 13–17, 34, 35, 39–52, 54, 56–68, 70–108, 110, 111].

Result Facts: As Figure H.54 presents, we observe that various answers are received to this question. 33% of participants confirm that 'Both of them, Yes, but with limitations'. Another 33% confirm that 'Python Yes, but Ansible No'. One person confirmed that 'Both of them, Yes, and comprehensively', and finally, one person chose the answer which is 'No, neither of them'.

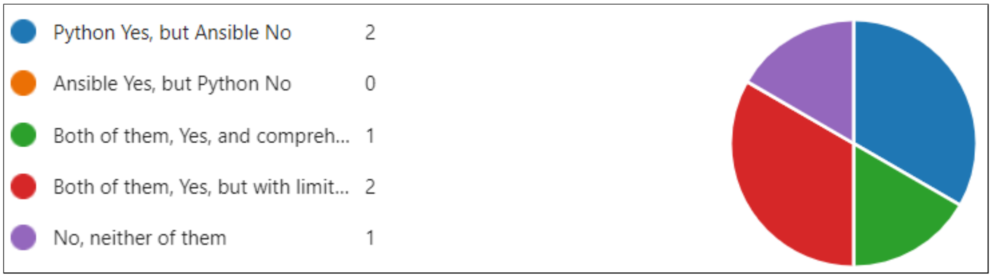


Figure H.54: Scientific personnel survey answer to question 47

Analysis: Because of the variety of the answers received in this question from scientific personnel who work at the same university, it is difficult for us to conclude based on their responses. The answers received to this question make us assume that either the participants have different overviews of what is provided by their university related to what the question asks for, or they have different understandings of what defines the programming languages mentioned in this question.

Either way, we assume this is a sign of the complexity and lack of a standard definition for technologies related to network and network security automation, as explained in Chapter 4. This is because the scientific personnel participating in this survey, verified in questions three and 24, have comprehensive knowledge and long experience in their job.

———————Scientific Personnel - Question Number 48 ———————

Question: A DevOps manner of teamwork is suggested by many resources, studied in our research, to help organizations that are utilizing manual manner of the network and network security management to automate the existing network and network security infrastructure.
In the subjects offered to the IT students, who take network and network security lines of study at the university you work for, do they learn about teamwork in a DevOps manner?

- Yes, comprehensively
- Yes, but with limitations
- No
- I don't know

The Reason for Asking This Question: To verify if the suggestion made in the SotA, regarding it being an essential factor for the success of network automation projects, is also supported by universities.

Reference to Research Question: RQ2 and implicitly RQ3

Reference to What in SotA Results We Validate: NSA techniques and technologies and implicitly their affecting factors [2, 5, 10–13, 15–17, 47, 49, 53, 70, 76, 79, 80, 83–85, 105].

Result Facts: As shown in Figure H.55, we have 33% that chose the answer 'Yes, comprehensively', while the same percentage chose the answer 'Yes, but with limitations', and still the same percentage of participants chose that they don't know the answer to this.

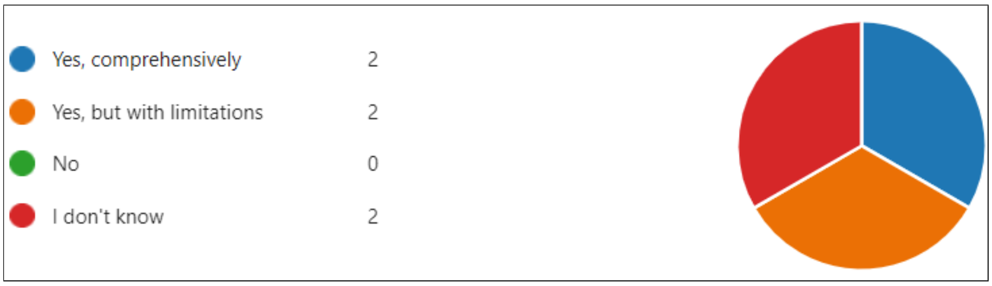


Figure H.55: Scientific personnel survey answer to question 48

Analysis: The answers received here make us assume the participants have different viewpoints on what is DevOps or different knowledge about what their university provides to students. The variety of the answers received makes it difficult for us to conclude whether their university supports what the question investigates. We assume that this is a sign of the complexity and lack of a standard definition for technologies related to network and network security automation, explained in Chapter 4. This assumption is about their level of knowledge and experience verified in the answers to questions three and 24.

Scientific Personnel - Question Number 49

Question: Critical Infrastructure Sectors (CIS) include companies such as Emergency Services Sector, Energy Sector, Hospitals, Financial Services Sector, etc. As much as you know, what percentage of the students who graduated from the study lines related to network and network security at the university you work for start/have started working for CIS companies' network and network security?

The Reason for Asking This Question: To evaluate the validity of our results about and whether the knowledge provided to IT students at universities is attracted by and related to what large companies need.

Reference to Research Question: Registering the background facts about their students based on the participants' knowledge.

Reference to What in SotA Results We Validate: Neither, this question is to register background information about the facts.

Result Facts: In answer to this question, three participants confirmed that this applies to 50% of their students; one participant answered 40%; another participant answered 30%; and finally, the last participant answered 10%.

Analysis: From the answers received, we can see that participants have different responses to what this question asks them. We assume that this could be related to the study program they work for as each study program could have a different relation to the future work the graduates get. So their study program could answer this question differently based on their results. Either way, we can see that something between 10% to 50% is suggested by the participants which means to some degree this is a fact that their students will start working for CIS companies after their graduation.

Scientific Personnel - Question Number 50

Question: In your opinion, introducing automation as one or more study subjects to the students that study network and/or network security will benefit their future approach to solving the problems when they start working for the companies? Alternative answers:

- Yes, this is a good idea; we should have more automation-related knowledge and study subjects available for the students. This will help them to take advantage of automation knowledge in their future work and have a positive perspective on it. But we are not ready for it yet... maybe in the future...
- Yes, absolutely, and we are looking into it positively. It will give them and their employer many benefits when they start their work for companies
- No; the students already have challenges in learning the basics of network and network security. Putting more challenges on them to learn to automate solutions will only make studying harder for them!

The Reason for Asking This Question: Here we investigated what is their viewpoint about including automation techniques and technologies in the future more than before to see the future path at universities and how they affect the progress of skills building in automation techniques in the future.

Reference to Research Question: RQ2 and implicitly RQ3

Reference to What in SotA Results We Validate: NSA techniques and technologies and implicitly their affecting factors [2, 5, 10–13, 15–17, 47, 49, 53, 70, 76, 79, 80, 83–85, 105].

Result Facts: As presented in Figure H.56, 50% of the participants chose the answer which is 'No, the students already have challenges in learning the basics of network and network security. Putting more challenges on them to learn to automate solutions will only make the study more difficult for them!', 33% chose the answer which is 'Yes, absolutely, and we are looking into it with a positive viewpoint. It will give them and their employer considerable benefits when they start their work for companies, and one person chose the answer which is 'Yes, this is a good idea, we should have more automation-related knowledge and study subjects available for the students. This will help them to take advantage of automation knowledge in their future work and have a positive perspective on it. But we are not ready for it yet... maybe in the future...'.

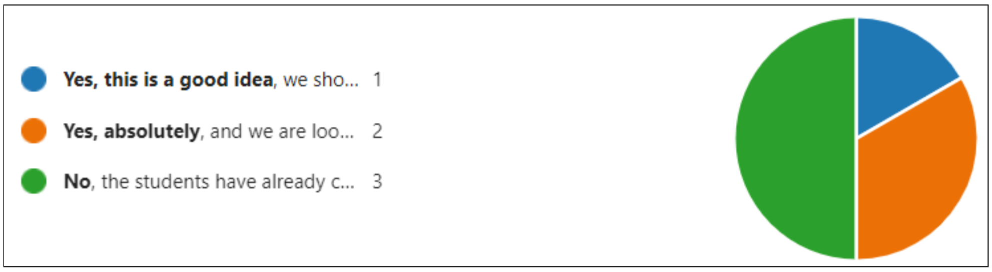


Figure H.56: Scientific personnel survey answer to question 50

Analysis: As shown in the results, the perspectives they have on this issue are various. Hence, we cannot for sure make a conclusion in which direction the university is moving to. Will they see the inclusion of automation techniques and technology as necessary and possible in the study programs they offer, or will they continue the same path that they have now, which we assume is to focus on basics and the more essential skills building, based on their answers, can't be answered for certain. Thus, we can't speculate which way they will choose to go in the future based on the various answers received here.

———Scientific Personnel - Question Number 51 ———

Question: Do you have any comment on why there is nothing/little/too much network and network security automation-related knowledge offered for learning at the university you work for?
(*You decide if the degree of it is nothing, little, or too much)
(Not mandatory to answer)

The Reason for Asking This Question: Here, we wanted to let the participants openly discuss what they thought regardless of what we had planned to ask. This was because in the previous questions, we had planned answers and they had to choose the solutions among them. This could help us see the perspectives that they might have in mind but we have not verified them mentioned through the SotA.

Reference to Research Question: RQ2 and implicitly RQ3

Reference to What in SotA Results We Validate: NSA techniques and technologies and implicitly their affecting factors [2, 5, 10–13, 15–17, 47, 49, 53, 70, 76, 79, 80, 83–85, 105].

Result Facts: Here we received one answer, which is the following: '*Including some content related to automation in network and -security subjects is essential. Even if the types of automation developed by academic research and the types pushed by vendors are not the types used, there will always be a level of automation in real-world networks of significant scale. It is also important not to lock the content to* *certain technologies or vendors, as this knowledge will quickly become obsolete. It is far more important to teach general concepts and the ability to learn and adapt. And it is important to keep this at a level that does not overwhelm the students, as the burden of learning is already quite high.'*

Analysis: From the first part of the answer received, we assume this verifies our results related to the necessity of utilizing automation techniques in large networks, and from the second part of it, we assume that scientific personnel at universities are concerned with teaching students the knowledge that is not bounded to a specific technology or vendor, but rather, without overwhelming the students with the existing complexity in different technologies. They focus on the learning process and teach students how to adopt different techniques when they work on their own.

End of Scientific Personnel Group-specific Questions

H.3 IT Professionals' Answers to Group-Specific Survey

This section presents the answers given to the group-specific questions by IT professionals who daily work with large networks in the organizations and their customers' organizations' networks.

IT Professionals - Question Number 21

Question: Do you directly work/have worked with network and/or network security? (Yes, No)

The Reason for Asking This Question: To register participants' backgrounds and evaluate the validity of our results.

Reference to Research Question: Background registration question.

Reference to What in SotA Results We Validate: Neither, this question is to evaluate the level of validity of the answers we will receive from the participants which will be evaluated based on their relevant experience.

Result Facts: As Figure H.57 presents, all the participants unanimously confirm that they have experience working with network and/or network security.

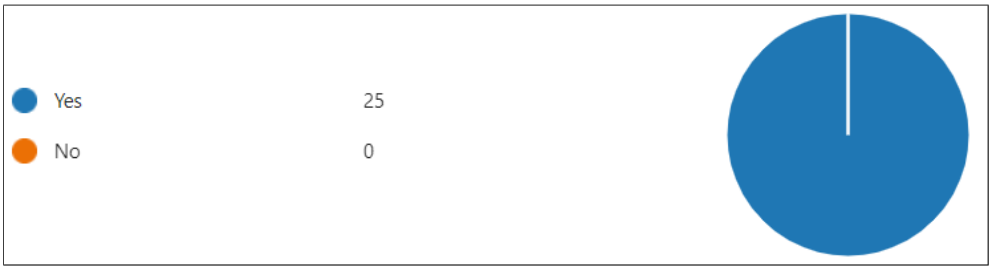


Figure H.57: IT professional survey answer to question 21

Analysis: We assume this means that the participants have knowledge and experience in what they answer the survey questions.

——————IT Professionals - Question Number 22 ——————

Question: Critical Infrastructure Sectors (CIS) include companies such as the Emergency Services Sector, Energy Sector, Hospitals, Financial Services Sector, etc. In your IT career, which is what we have in mind here, do you work/have been working for any CIS company's network and/or network security?

The Reason for Asking This Question: To register participants' backgrounds and evaluate the validity of our results.

Reference to Research Question: Background registration question and RQ1

Reference to What in SotA Results We Validate: This question is to evaluate the level of validity of the answers we will receive from the participants which will be evaluated based on their relevant experience. Also, Traditional network security techniques and architecture [26–29, 39–41, 67, 88, 112–118].

Result Facts: As Figure H.58 shows, a majority of 76% confirmation by answering 'Yes' to this question.

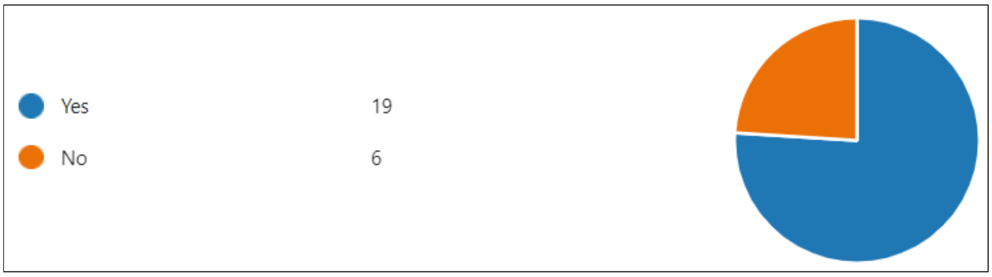


Figure H.58: IT professional survey answer to question 22

Analysis: With the majority of participants having IT career in CIS company's networks and/or network security we will have this factor as a base in mind when analyzing the answers given to the other questions.

——————IT Professionals - Question Number 23 ——————

Question: As a network professional do you also work/have been working with different firewall management solutions as part of your job in the network? (Yes, No)

The Reason for Asking This Question: To register participants' backgrounds and evaluate the validity of the answers received through our investigation.

Reference to Research Question: Background registration question and RQ1

Reference to What in SotA Results We Validate: Traditional network security techniques, technologies, and architecture [26–29, 39–41, 67, 88, 112–118].

Result Facts: As Figure H.59 presents, a majority of 92% of participants answers 'Yes' to this question

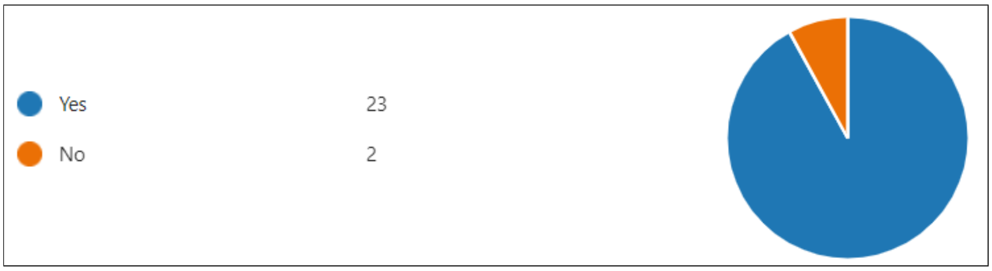


Figure H.59: IT professional survey answer to question 23

Analysis: The answer to this question raises the validity of the answers received through the survey and interviews as it proves that the majority of the IT professionals that participated in the investigation have an understanding of the existing solutions and problems regarding IP firewalls in the field.

IT Professionals - Question Number 24

Question: Differentiation makes it more challenging to manage and automate network and network security solutions such as firewalls. Usually, companies use different products from different vendors to manage these tasks.
When you work/have been working with network and network security for organizations, did you have to utilize different platforms from different vendors? (Yes, No)

The Reason for Asking This Question: To register participants' backgrounds in what they know and evaluate the validity of our results. Here, our intention was not to put a bias in the questions, but instead, we wanted to evaluate their point of view about this theory based on their practical experience, as their answers could even prove quite the opposite side of the case.

Reference to Research Question: Background registration question and RQ1 and RQ3

Reference to What in SotA Results We Validate: Traditional network security techniques, technologies, and architecture [8, 10, 26–29, 39–44, 49, 58, 59, 67, 76, 84, 85, 88, 94, 104, 105, 111–118].

Result Facts: As Figure H.60 shows, a majority of 84% among participants have experienced that organizations utilize different platforms provided by different vendors in their network environment which consequently requires different competency for the management of the different networks and network security platforms.

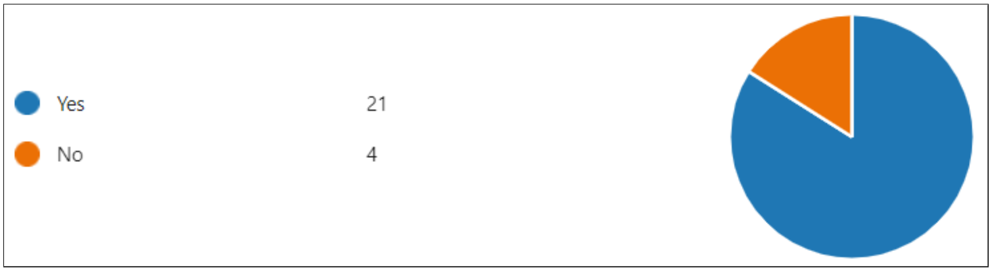


Figure H.60: IT professional survey answer to question 24

Analysis: The answers received in this question verify that even though differentiation makes it more challenging to manage and automate network and network security solutions such as firewalls, companies still use different products from different vendors to manage network security tasks. The responses received here validate the existence of the factor about different products from vendors being in use in each network. This also validates the factor we have registered as complexity through the study of the SotA when enterprises are to review their systems to make a plan and a strategy for automation of their network security solutions.

IT Professionals - Question Number 25

Question: How many years of experience working with network or network security do you have?

The Reason for Asking This Question: To register participants' backgrounds and evaluate the validity of our results. Here, we intended to evaluate how much experience the survey participants have to be able to further evaluate the validity of the responses received.

Reference to Research Question: Background registration question in addition to RQ1.

Reference to What in SotA Results We Validate: This question is to evaluate the participants' knowledge area and work experience. Also, Traditional network security techniques and architecture [26–29, 39–41, 67, 88, 112–118].

Result Facts: In answer to this question as presented in Figure H.61, seven participants, representing 25% of the sector diagram, confirmed that they have 20 or more years of related experience, we had two participants with 18 years of related experience, two with 16 years, three with 14 years, one with twelve years, four with ten years, one with eight years, two with six years, and finally, three with two years of related experience in the mentioned field. We can also see that 80% of them have more than eight years of related experience in working with traditional networks or network security.

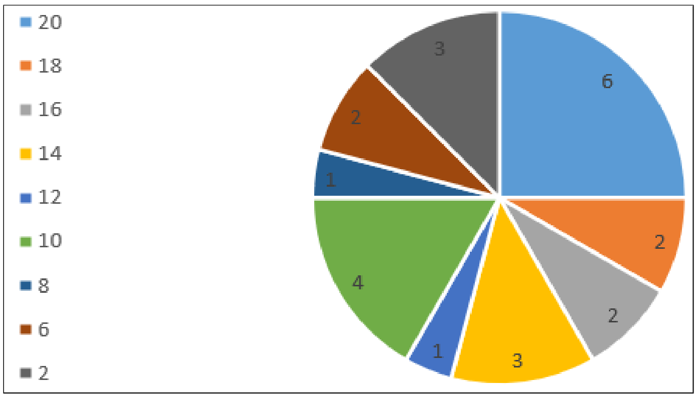


Figure H.61: IT professional survey answer to question 25. The numbers on the sectors present the number of people who apply to the specific sector, and the numbers on the left side, connected with each color, present the number of years of experience in working with network and network security techniques and technologies. We have removed number four, representing four years of experience, as there was no response received in that sector.

Analysis: With 80% having above eight years of related experience in working with traditional networks and network security, from this point of view, we assume a high validity in the answers received and that most of the participants know what we are asking about and have many years of experience in this regard. Yet, here we still have not included the factor of experience in automation techniques and technologies.

IT Professionals - Question Number 26

Question: Do you have competency and experience in network and network security automation that, with a safe and confident feeling, lets you immediately start to utilize automation techniques in the infrastructure you work with now? (Yes, No)

The Reason for Asking This Question: To register participants' backgrounds and evaluate the validity of our results.

Reference to Research Question: Background registration question and RQ2

Reference to What in SotA Results We Validate: NSA techniques and technologies [1, 2, 5, 6, 8, 10, 11, 13–17, 34, 35, 39–52, 54, 56–68, 70–108, 110, 111].

Result Facts: As shown in Figure H.62, we receive the answer 'Yes' from 52% of participants, which almost includes only half of the participants in the survey.

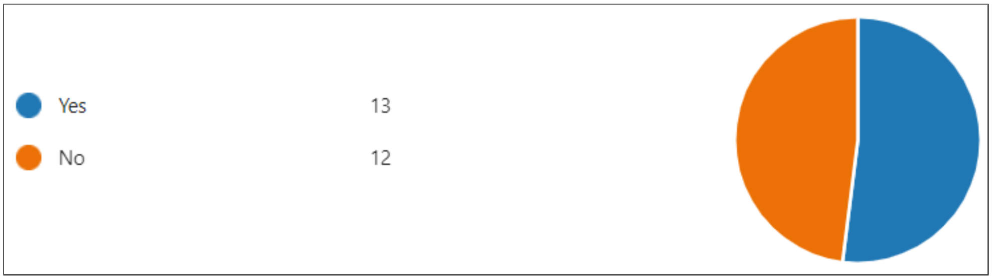


Figure H.62: IT professional survey answer to question 26

Analysis: Receiving confirmation from 52% of participants in this question is, although we know from their answers to the previous questions, that the participants in this survey are highly experienced in network and network security, and all of them, confirmed in question 21, have been or are working with network and/or network security solutions.When they don't have the competency, even if it is planned to automate the network, they can't perform automation. We now know that all of them know basic network security techniques and technologies such as firewalls and DMZ, 76% have been working in large networks, 80% of them have more than eight years of experience, and yet, only about half of them have competency and experience in network security automation.

IT Professionals - Question Number 27

Question: Do you use/have used any form of automation techniques in practice when you work with network security, or do you manage/have managed networks and firewalls using the traditional manner, such as utilizing the GUI of the different networks and firewalls? (Alternative answers are: Not at all, Partly automation methods, Totally automation methods)

The Reason for Asking This Question: To register what method the participant can utilize for working with network and network security, either traditionally or modern and automatically.

Reference to Research Question: RQ1 and RQ2

Reference to What in SotA Results We Validate: Traditional network security techniques, technologies, and architecture in addition to NSA techniques and technologies [1, 2, 5, 6, 8, 10, 11, 13–17, 26–29, 34, 35, 39–52, 54, 56–68, 70–108, 110–118].

Result Facts: As Figure H.63 presents here, one participant confirms utilizing automated methods. Despite the answers received here being quite exciting to see, it still is a minority, as the majority of 84% responded that they partially utilize automation methods. Finally, there is also a minority of 12%, who answer that they do not utilize automation techniques and technologies at all.

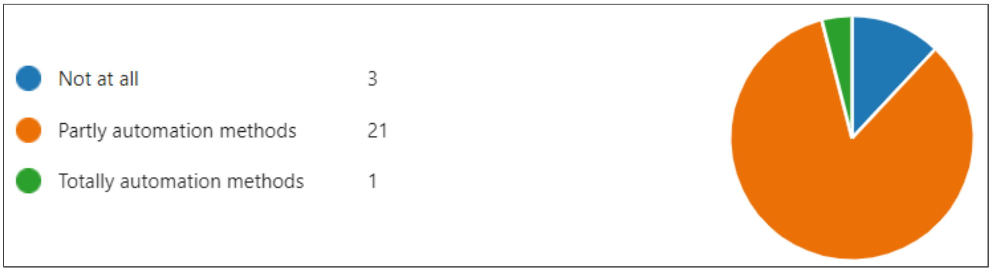


Figure H.63: IT professional survey answer to question 27

Analysis: We evaluate the answers received to this question, such as 84% responding that they partially utilize automation methods as realistic, because, from the study of the SotA, we know that the first step for companies which have their network and network security already in place and established, is, to begin with, a hybrid solution to take practical steps towards automation of their network and network security solutions [47].

We also should express how surprising it is to notice that a majority of 84% are utilizing network automation techniques and technologies in their daily work with network and network security. This is more than what we expected, as in the answers to previous questions, such as question 26, we confirmed that only 52% of the participant expressed that they feel they can utilize automation techniques and technologies in their daily job with safe and confident feelings.

IT Professionals - Question Number 28

Question: How much do you use automation methods in network security?

The Reason for Asking This Question: To validate our findings related to automation of network security in this research and further connect the answer given to this question to the findings out of the other questions for concluding.

Reference to Research Question: RQ2 and RQ3

Reference to What in SotA Results We Validate: NSA techniques and technologies and implicitly their affecting factors [1, 2, 5–8, 10, 11, 13–17, 34, 35, 39–54, 56–68, 70–112].

Result Facts: As presented in the bar chart shown in Figure H.64, we can see that about 52% of the participants utilize network automation 20% to 40%, and 68% of the participants utilize it something between 10% to 50%.

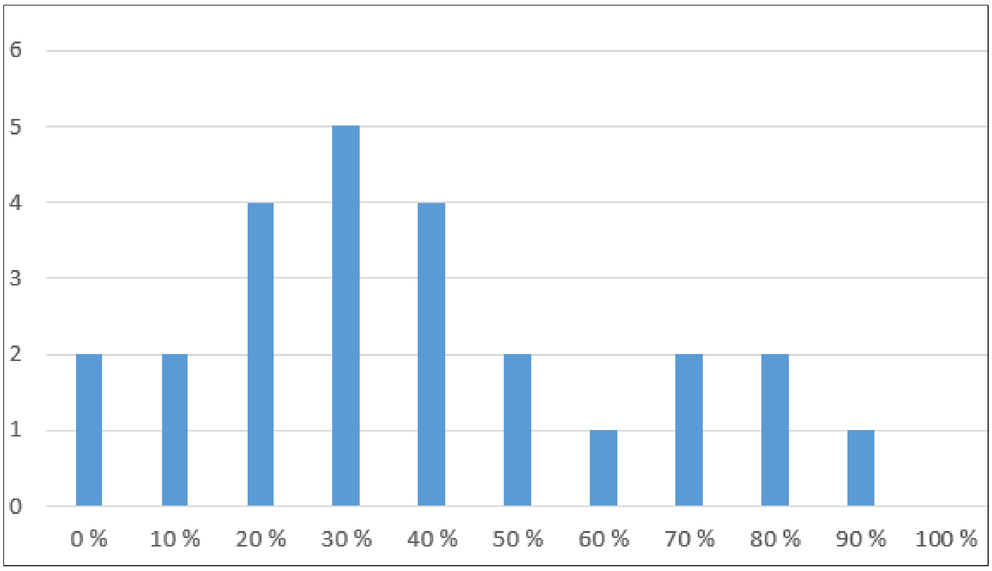


Figure H.64: IT professional survey answer to question 28. The bars in the bar chart represent the number of people utilizing network automation, also marked vertically. The percentage of their utilization of these techniques is shown in the horizontal axis in this figure.

Analysis: The answers received to this question are various. This makes it difficult for us to make a concrete conclusion. At the same time, from the bar chart, we can see that about half of the participants utilize automation, something between 10% to 50%, which makes us assume it can be interpreted as partially utilizing network automation techniques and technologies. Something that slightly corresponds to the findings from the answers to the previous question, where 84% confirmed partially utilizing automation techniques.

To find a closer match to the previous question, if we review how many of them utilize network automation between 10% to 70%, which corresponds to 80% of the participants, we have a slightly closer match with the answers received in question 27. Yet, still, it depends on our definition of partially. Do we mean 10% to 50% as 'partially', or do we define 'partially' as 10% to 70%? Hence, as we have not set a clear definition for what we exactly mean by 'partially', as mentioned here, it is difficult to conclude this.

IT Professionals - Question Number 29

Question: What do you see as the reason for the percentage you gave in question 28, above?

- Lack of competency
- Lack of proper equipment
- Lack of organizational budget that can support it

- Lack of proper training for network professionals
- Difficulty in revoking changes that are implemented by automation techniques through the network security and network security
- Existing difficulties in understanding the collaboration between automation tools and other platforms
- The organization or its customers are not ready for changes coming to the networks by automation techniques and technologies
- Network security automation requirements are not defined or clarified
- The leadership of the organization or its customer is not ready to accept the change to utilizing automation in network security
- Difficulties in adopting automation of network security will impact customer satisfaction in a negative manner
- People don't trust automation techniques and tools yet
- The impact of change imposed on performance by automated processes will make them fear accepting it
- The legacy technology is not compatible with the changes imposed by network automation or to utilize APIs for automation
- None of the answers above

The Reason for Asking This Question: To validate our findings related to automation of network security in this research and further connect the answer given to this question with the findings out of the other questions for concluding.

Reference to Research Question: RQ3

Reference to What in SotA Results We Validate: Factors affecting NSA [2, 5–8, 13–17, 34, 35, 42, 43, 45–54, 56–59, 61, 63–68, 70, 71, 73–78, 80–87, 89–112].

Result Facts: Here, the participants could choose as many alternatives as they thought would apply. As presented in Figure H.65, the most voted reasons included lack of proper training for network professionals, network security automation requirements are not defined or clarified, and the legacy technology is not compatible with the changes imposed by the network automation to utilize APIs for automation.

We had many people agreeing with the reasons being related to the lack of competency, lack of organizational budget that can support it, the leadership of the organization or its customers not being ready to accept the change imposed by utilizing automation in network security, the organization or its customers' environments are not prepared for changes coming to the networks by automation techniques and technologies, and finally, that people don't trust automation techniques and tools yet.

Fewer people agree that the reason is related to lack of proper equipment, difficulty in revoking changes that are implemented by automation techniques through the network and network security, existing difficulties in understanding the collaboration between automation tools and other platforms, and the impact of change imposed on performance by automated processes will make them fear accepting it.

No participant voted that difficulties in adopting automation of network security will negatively impact customer satisfaction as a reason for this problem, and we also had three people who did not agree with any of the above-mentioned reasoning.

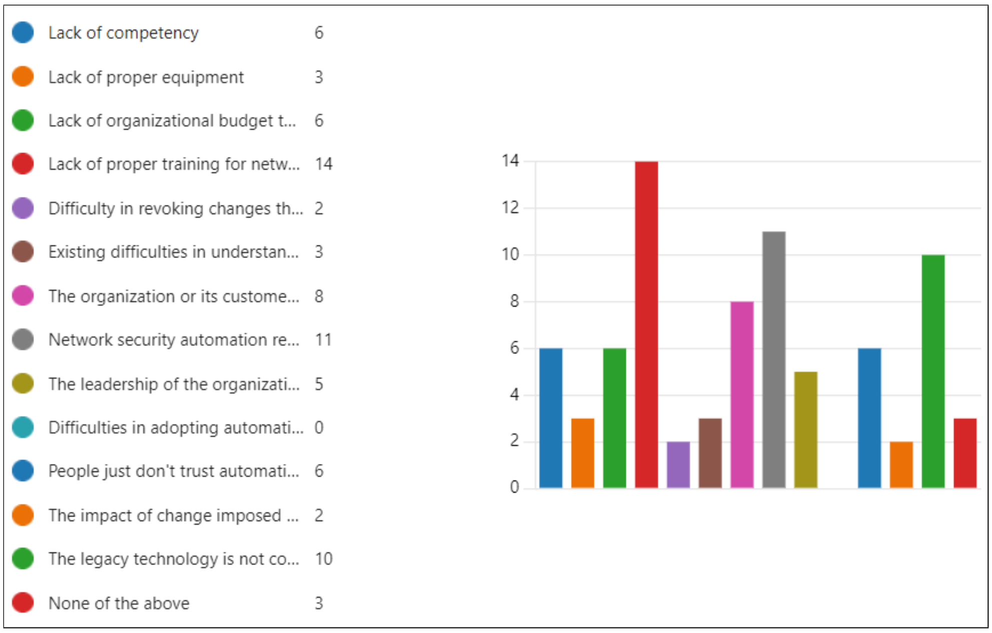


Figure H.65: IT professional survey answer to question 29

Analysis: The results received here imply that the participants mostly agreed with the lack of proper training, lack of clarified definition for NSA requirements, and incompatibility of legacy devices with the needed changes as the most significant reasons for how much they can utilize automation methods in network security. These impacting factors have also been mentioned by the SotA presented in Chapter 4.

Furthermore, we can confirm that reasons such as a lack of competency, insufficient budgets in organizations for NSA-related projects, leadership issues, and the unpreparedness and lack of trust of the organization's customers and their network environments regarding the changes imposed by NSA are also verified as highly valid reasons by the IT professionals, which were also mentioned in the resources reviewed in the SotA in our research.

Moreover, the validity of impacting factors such as lack of proper equipment, difficulty in revoking changes, difficulties in understanding the collaboration between automation tools and other platforms, and impact of change imposed on performance by automated processes, which also were pointed to by the SotA studied in this research, are also approved by the participants. No participant, although, accepted the reasons related to the negative impact of the changes on customer satisfaction as a relevant reason for how much they use automation methods in network security.

Here we had three people who did not choose any of the reasons mentioned in the question, which nearly corresponds with what we received in the responses to question 27, where three did not use automation at all. Hence, from this, we can assume that those who did not choose any of the reasons in answer to question 29 are those people who also confirm not using automation techniques at all. This makes us assume those participants who have voted on the reasons mentioned in this question are, in fact, those who answered in question 27 that they partially, or as in one instance utilize network automation techniques and technologies for managing networks and firewalls, which gives a higher validity in the answers received to this question.

IT Professionals - Question Number 30

Question: What network automation techniques are you able to utilize? (Alternative answers: SDN, ML, or IaC, or Neither) Multiple answers can be chosen.

The Reason for Asking This Question: To register participants' capabilities in utilizing network automation techniques and technologies and evaluate the validity of our results.

Reference to Research Question: RQ2, and implicitly RQ3 and background registration question.

Reference to What in SotA Results We Validate: NSA techniques and technologies and implicitly their affecting factors [1, 2, 5–8, 10, 13–17, 34, 35, 42–54, 56–59, 61, 63–87, 89–112].

Result Facts: As shown in Figure H.66, we had one person who confirms having competency in utilizing ML. This is a minority of 3% of the participants, while we also have 11% who confirm not being able to utilize any network automation technique or technologies. Figure H.66 also shows that 47% of participants confirm being able to utilize SDN techniques and technologies in their work, and the competency in utilizing IaC techniques and technologies is 39% among them.

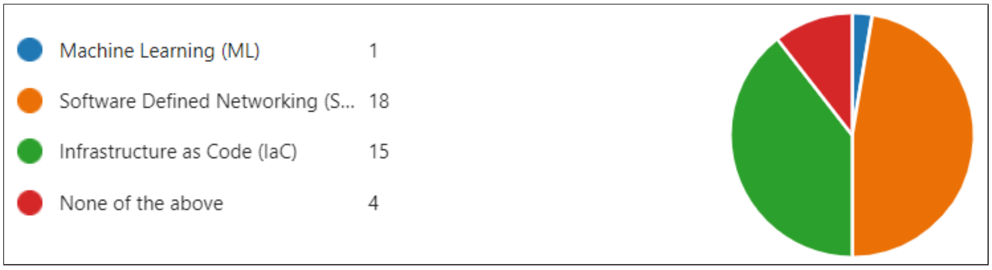


Figure H.66: IT professional survey answer to question 30

Analysis: From the results received, we can see most of IT professionals are engaged in utilizing SDN, fewer utilizing IaC, and only one person have the competency and use ML. 11% confirm that they are not able to use any of these three network automation-related competencies. Compared to what we received in answers to questions 27 and 29, we assume that three out of four who choose 'None of the above' are those who don't use network automation techniques at all and speculate that one person probably utilized an automation technique that exists and yet, not mentioned through the SotA studied in this thesis.

IT Professionals - Question Number 31

Question: What network automation techniques do you practice in your work daily? (Alternative answers: SDN, ML, or IaC, or Neither) Multiple answers can be chosen.

The Reason for Asking This Question: To assess what today's network enables them to utilize [5] compared to their confirmed capabilities with network automation techniques and technologies, as established in the previous question, and to further validate our results

Reference to Research Question: RQ2, and implicitly RQ3

Reference to What in SotA Results We Validate: NSA techniques and technologies and implicitly their affecting factors [1, 2, 5–8, 10, 13–17, 34, 35, 42–54, 56–59, 61, 63–87, 89–112].

Result Facts: Figure H.67 shows that there is one person who confirmed utilizing ML, 42% utilize SDN, and 33% utilize IaC automation technique in their work. 22%, utilize no one of these automation techniques in their work at all.

---

[5] When we talk about 'what the environments allow them to do here' we are pointing at what the infrastructures and the existing network materials' compatibility are with the modern technologies such as what is required to automate network security. For a discussion about these factors, please see Chapter 4, for instance, where we explain these factors more specifically in Section 4.4.

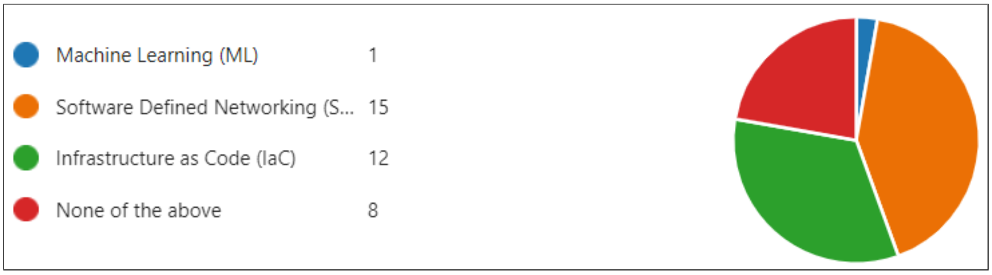


Figure H.67: IT professional survey answer to question 31

Analysis: This question is different from the previous one which asked about what automation techniques they know about. Here we ask what they use in practice, as one might know something, but for any reason, not have the possibility to utilize it in their work. The results of question 30 and 31 together with what we saw in the answers given to question 29 makes us assume that not every problem related to network automation is associated with the competency of the IT professionals.

Following these results, we assume that the one person who confirmed knowing about ML in the answer to question 30, is also the person who confirms utilizing this technology in their work. Fewer people than those who confirmed to know SDN methodology utilize it in their working environments, and fewer people than those confirming to know IaC methodology utilize it in practice. The number of people who do not utilize any of the three automation techniques and technologies mentioned in this question has doubled compared to the answers received in question 30.

We can see people who know some of those automation techniques but don't utilize them in their working environment. This makes our assumptions about the impacting factors related to leadership and organizational culture in utilizing these technologies and the competency of the IT personnel stronger and is assumed as proof of the hypothesis mentioned in Chapter 1.

IT Professionals - Question Number 32

Question: Do you think it is easy to use network automation in network and network security jobs?

The Reason for Asking This Question: To investigate participants' beliefs concerning network automation techniques and technologies, both when it depends on what they can do, and when it depends on what the environments allow them to do. This was mentioned by the SotA as affecting factors on the progress of network security automation in large networks [2, 15, 16].

Reference to Research Question: RQ2, and implicitly RQ3

Reference to What in SotA Results We Validate: NSA techniques and technologies and implicitly their affecting factors [1, 2, 5–8, 10, 13–17, 34, 35, 42–54, 56–59, 61, 63–87, 89–112].

Result Facts: 56% answered 'Yes' to this question as shown here in Figure H.68.

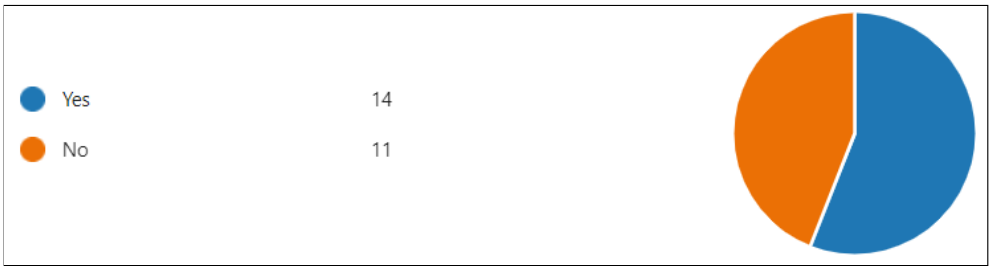


Figure H.68: IT professional survey answer to question 32

Analysis: This question is related to what we studied in the SotA about the fear of utilization of network automation techniques and technologies in practice among IT professionals [16]. It also tells us about their assessment regarding the topic brought up here. We also want to remind you that, 80% of the participants in this investigation have more than 8 years of related experience to our research, so we assume their beliefs expressed here as highly reliable.

Hence, from the responses here, we can see that about half of them believe it is easy to adopt network automation techniques into network security tasks and processes. Adding this to what we already know from the responses received to question 22 which shows that 76% of them work or have been working in large networks, again makes us assume an association between the impacting factors related to leadership and organizational culture and the progress of automation of network security stronger, and we assumed it as proof of the hypothesis mentioned in Chapter 1.

IT Professionals - Question Number 33

Question: How close in the future do you think we will be utilizing network automation methods actively? (Alternative answers: Far in 10 years or more, Close in five years, Very close in two years)

The Reason for Asking This Question: The reason why we asked this question is that they are familiar with network and network security in the production environment of numerous companies where they have been working for many years, confirmed through previous questions. This question is essential because, referring to the answers given to question number 21, we already know that all the participants work daily or have been working before with network and/or network security techniques and technologies.

By adding the answers given to question 25, which was to evaluate their experience in working with network and network security, we confirmed that 80% of the participants have above eight years of experience in this relation. So their answer to this question is assumed as highly reliable and will verify our results related to existing network automation techniques and technologies on the one hand, and the factors that affect the success of their progress in large networks on the other hand.

Reference to Research Question: RQ2, and implicitly RQ3

Reference to What in SotA Results We Validate: NSA techniques and technologies and implicitly their affecting factors [1, 2, 5–8, 10, 13–17, 34, 35, 42–54, 56–59, 61, 63–87, 89–112].

Result Facts: As Figure H.69 presents, 52%, which is about half of them, predict that this will take place in close future in about five years, 36% of them predict that this will take place in a very close future in two years, and finally, 12% predict that this will not take place sooner than 10 years.

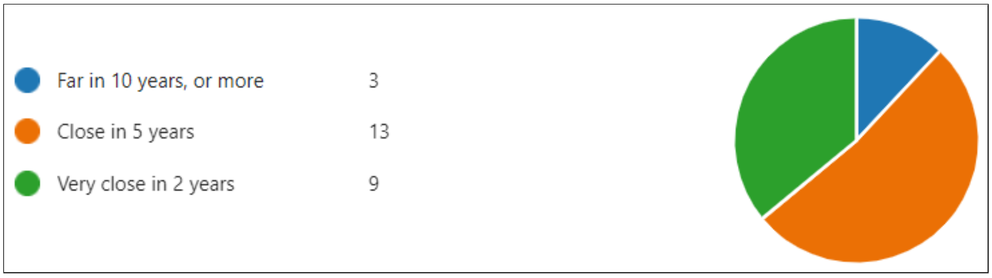


Figure H.69: IT professional survey answer to question 33

Analysis: By comparing the answers received here with the answers given to the previous question, where also 52% of them agreed that it is easy to use automation techniques in network security jobs, we can assume that here also the same people are agreeing with the changes and automation of network security taking place in a close future in five years. We also have many people who mean that it is very close to us and these changes will take place to make network security efficient in two years which is very soon.

Also, we have three people who mean that these changes will take place in more than ten years. We could relate these three people with those who answered that they don't use network automation at all in answer to question 27 to assume those people's answers, who work daily with network automation more realistically. But we can not say it for sure, as the answers to the survey are given anonymously, and we don't know exactly if these three people are those and speculate on that basis. What we are sure about is that the majority confirms that the changes related to automating network security are about to take place in something between two to five years from now.

IT Professionals - Question Number 34

Question: Have your organization provided or supported training in IT fields related to your profession/work area in a way that you feel it becomes easier to utilize network automation in practice?

- Yes, very much
- No, not at all
- Partly with financial support, but training on my own

*By supporting training, we mean providing you with labs and other materials needed for skills building, such as courses and other activities.

The Reason for Asking This Question: This question is posed to confirm the factors that influence the adoption of automation techniques and technologies in network security. This inquiry stems from the recognition in the SotA that skills building and training are essential for the competency development of IT personnel.

Reference to Research Question: RQ3

Reference to What in SotA Results We Validate: Factors affecting NSA [2, 5–8, 10–17, 34, 35, 42, 43, 45–54, 56–59, 61, 63–68, 70, 71, 73–87, 89–112].

Result Facts: As shown in Figure H.70, 16% answered that their organization both financially and practically supports their skills development by providing them with training and labs, 56% confirm that their organization supports them financially in their training related to their job while doing the activity on their own. Finally, 28% answered that their organization in neither way endorses this.

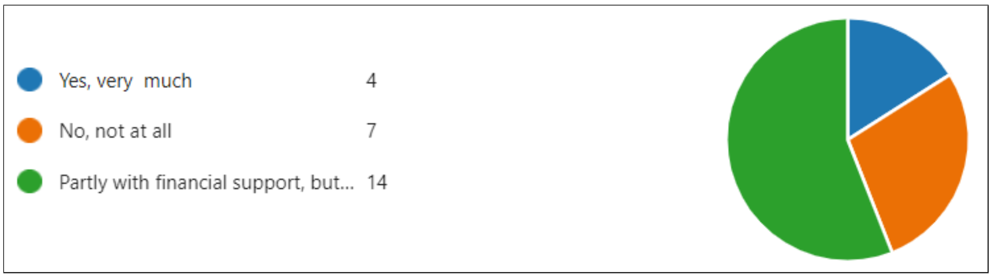


Figure H.70: IT professional survey answer to question 34

Analysis: In the answer to question 35, we see that certification and official qualifications are confirmed as a motivating factor by about half of the IT professionals. In question 13, we observed that 24% of them also confirmed having network automation-related certifications, and in question 11, 50% of them confirmed having certifications related to traditional network and network security knowledge and competency. This verifies what we have discussed about motivation factors and the effect of the support of the management in this relation, to the progress of skills development. This factor was also confirmed both by the answers received here in the survey and the interviews, in addition to the SotA, as a significant factor in the progress of network security automation.

IT Professionals - Question Number 35

Question: Is certification and official qualifications a motivating factor for you to try harder to achieve higher competency in IT in general, and if your organization requires, in network and network security automation? (Yes, No)

The Reason for Asking This Question: This question is posed to confirm the role of motivation, as mentioned in the SotA, as an impacting factor in enhancing competence related to the progress of projects involving the adoption of automation techniques and technologies in network security.

Reference to Research Question: RQ3

Reference to What in SotA Results We Validate: Factors affecting NSA [2, 5, 10–13, 15–17, 47, 49, 70, 76, 79, 80, 83–85, 105]

Result Facts: As Figure H.71 presents, 52% of them answer 'NO' to this question, while 48% of them find certification and the official qualification requirements as a motivating factor for skills building and training to acquire better competency related to their job.

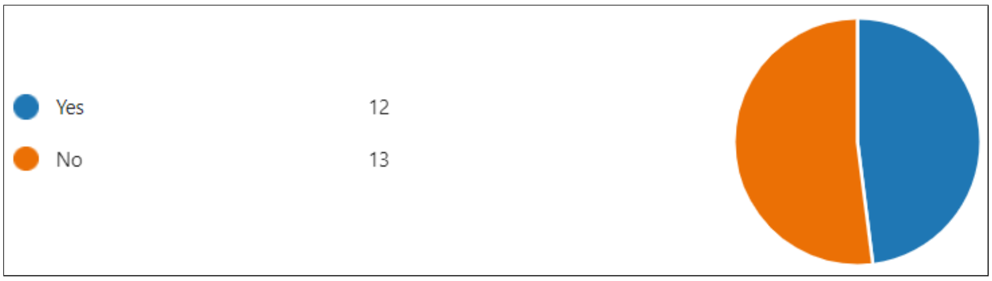


Figure H.71: IT professional survey answer to question 35

Analysis: About half of the IT professionals confirm that certification and official qualifications are motivating factors for them to work harder and acquire more related competencies. This to a high degree verifies our discussions about the certifications, provided by solution and equipment providers in addition to what organizations internally provide to their employees, being motivating for IT professionals in Chapter 4.

IT Professionals - Question Number 36

Question: Do you see the support of the organization's management and leadership about the progress of each IT project and specifically automating the network security infrastructures, having a significant effect on the progress of the automation process?

The Reason for Asking This Question: To verify the affecting factors mentioned by the SotA.

Reference to Research Question: RQ3

Reference to What in SotA Results We Validate: Factors affecting NSA [2, 5, 10–13, 15–17, 47, 49, 70, 76, 79, 80, 83–85, 105]

Result Facts: Figure H.72 shows that 88% of the participants agree that the support of the organization's management and leadership in this relationship is significantly influential, while we also have a minority of 12% who refuse to see this as a noteworthy factor in this regard.

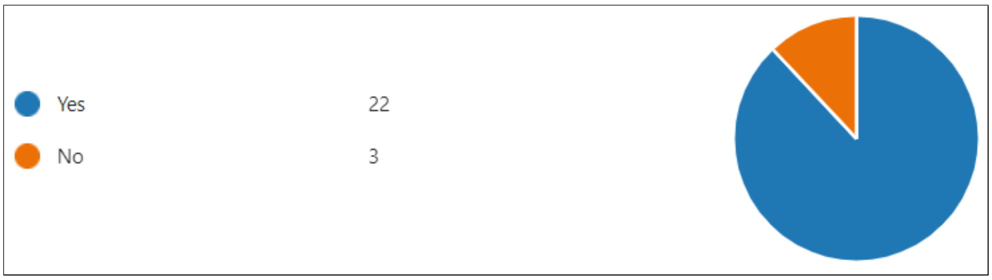


Figure H.72: IT professional survey answer to question 36

Analysis: Here, we would like to recall that in answer to question 22, we found that 76% of the participants had experience with network and network security environments in large networks. This could be related to why a close ratio to the result in question 22, confirms that the support of management and leadership is needed to reach the progress of the heavy projects mentioned here in question 36. This is significant for us as the study of the SotA confirms that the smaller networks might not have many jobs related to the network and network security management, while large networks are in absolute need of automating the tasks and processes [2].

IT Professionals - Question Number 37

Question: IT staff needs to learn and do training concerning acquiring network automation skills and knowledge needed in the organizations [11, 17]. Do you think supporting and encouraging IT staff by management in this relation will have a significant effect on the progress of knowledge building in favor of organizations' projects?

The Reason for Asking This Question: To verify the affecting factors mentioned by the SotA.

Reference to Research Question: RQ3

Reference to What in SotA Results We Validate: Factors affecting NSA [2, 5, 10–13, 15–17, 47, 49, 70, 76, 79, 80, 83–85, 105]

Result Facts: As Figure H.73 shows, 92% of participants answer 'Yes' to this question.

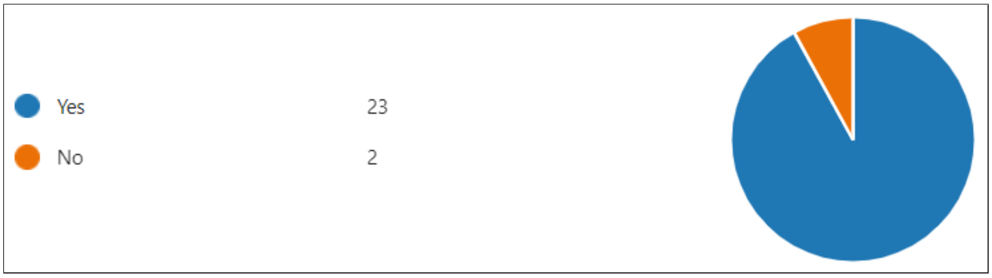


Figure H.73: IT professional survey answer to question 37

Analysis: Again here, we would like to draw a connection to what we also mentioned in analyzing the answers given to questions 36 and 22. In question 22, we have registered that 76% of participants have experience working for large networks. In question 36, 88% of them confirmed that the support of IT projects, and more specifically automation of network security projects, by management of the organization, have a significant effect on their progress. In addition, the responses received here regarding the necessity of management support in encouraging IT staff to acquire network automation skills will strengthen our understanding of the criticality of this factor and validate our findings. It will also provide evidence supporting the hypothesis mentioned in Chapter 1.

IT Professionals - Question Number 38

Question: Where you have been working or work today with network and network security infrastructure and solutions, is it/has it been possible to collaborate across teams to accomplish organizational objectives, learn and share knowledge and competencies, and achieve automated solutions for network and network security?

The Reason for Asking This Question: To corroborate our findings and validate the factors mentioned in the SotA, we also want to emphasize a connection to what the SotA suggests as a work method for automation jobs, projects involving programming, and organizational collaborations. The SotA discourages organizational silos while strongly recommending DevOps and CI/CD teamwork approaches [10, 17, 79].

Reference to Research Question: RQ2 and RQ3

Reference to What in SotA Results We Validate: NSA techniques and technologies and their affecting factors [2, 5–8, 13–17, 34, 35, 42, 43, 45–54, 56–59, 61, 63–68, 70, 71, 73–78, 80–87, 89–112, 173].

Result Facts: As shown in Figure H.74, 68% answered ‘Yes’ to this question.

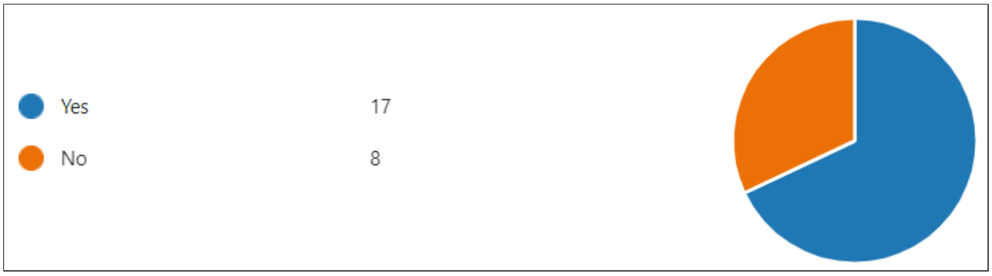


Figure H.74: IT professional survey answer to question 38

Analysis: Through the answers received here, we assume slightly the same population of 76% of the participants in our investigation, who have experience from great projects and large networks, see the necessity of teamwork more than the IT professionals who have not been involved in large networks and their projects. As in large network projects, more work and more teamwork are needed, which is not that crucial in smaller networks [2]. Hence, the answers received here to a high degree prove our findings from SotA.

IT Professionals - Question Number 39

Question: Do you agree regarding achieving network and network security automation goals, collaboration across teams and between IT professionals with different competencies, and knowledge sharing is the way to go and not organizational silos? Alternative answers:

- Yes, I agree with this claim
- No, I disagree; separating different types of employees in organizations will have good results for automation as well

The Reason for Asking This Question: To verify our findings and the affecting factors on the progress of NSA mentioned by the SotA.

Reference to Research Question: RQ2, and implicitly RQ3

Reference to What in SotA Results We Validate: NSA techniques and technologies and their affecting factors [2, 5–8, 13–17, 34, 35, 42, 43, 45–54, 56–59, 61, 63–68, 70, 71, 73–78, 80–87, 89–112, 173].

Result Facts: As Figure H.75 shows, 88% of participants agree with this claim and answered 'Yes' to this question.

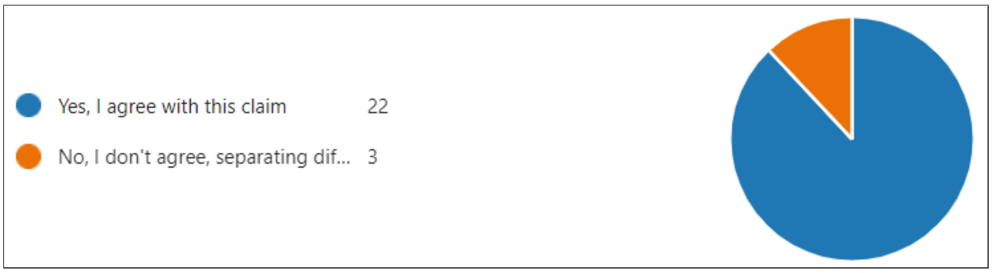


Figure H.75: IT professional survey answer to question 39

Analysis: Concerning the responses received to this question, we can, to a high degree, verify that teamwork is a vital success vector for the progress of NSA.

IT Professionals - Question Number 40

Question: Which of the following success factors do you agree affects the progress of network security automation in organizations? (multiple answers)

- Providing training for network personnel to build their experience in network security automation
- Increasing budget needed to fill the gap of lack of the budget to phase out legacy devices that are not automation-compatible
- Hiring new skilled personnel in network security automation
- Supporting and encouraging the existing network personnel to build their knowledge in network automation
- Providing practical hands-on labs for network personnel to build skills in network automation
- Encouraging learning of other vendors' solutions in network security and network security automation
- Aligning middle management with network security automation goals in different projects of the organization
- Building and supporting teams of programmers and network engineers that work together in a DevOps manner
- None of the above

The Reason for Asking This Question: To verify our findings about affecting factors from the SotA.

Reference to Research Question: RQ3

Reference to What in SotA Results We Validate: Factors affecting NSA [2, 5–8, 13–17, 34, 35, 42, 43, 45–54, 56–59, 61, 63–68, 70, 71, 73–78, 80–87, 89–112, 173].

Result Facts: As shown in Figure H.76, the factors such as providing training for network personnel to build their experience in network security automation, supporting and encouraging existing network personnel to develop their knowledge in network automation, and providing practical hands-on labs for network personnel to build skills in network automation are significantly voted on by the participants.

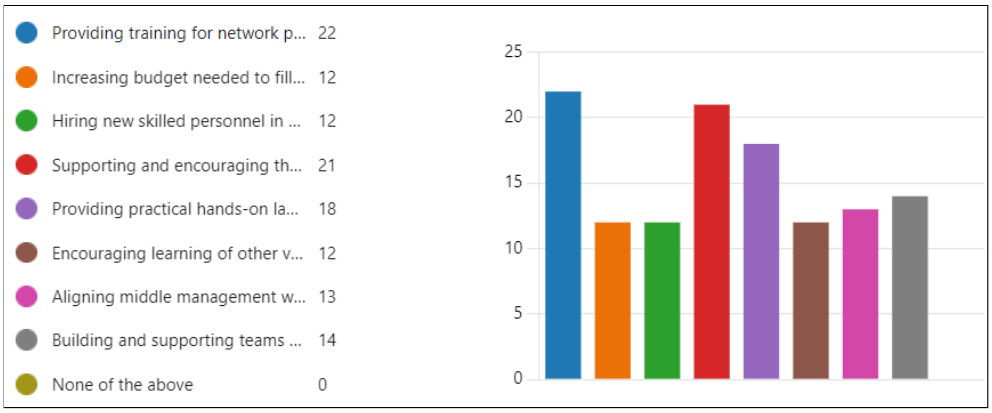


Figure H.76: IT professional survey answer to question 40

Thereafter, factors such as increasing the budget needed to fill the gap of lack of the budget to phase out legacy devices that are not automation compatible, hiring new skilled personnel in network security automation, encouraging the learning of other vendors' solutions in network security and network security automation, aligning middle management with network security automation goals in different organization projects, and finally building and supporting teams of programmers and network engineers that work together in a DevOps manner are also voted on.

Analysis: As we see no participant this time has chosen the 'None of the above' answer, we assume that all the above-mentioned factors that are voted on are more or less experienced by the participants in the survey to be influential in this relation. Hence, we conclude that at least half or more than half of the participants agree with all the mentioned factors as influential regarding the progress of NSA.

Three of these factors, however, are voted on by 72% to 88% of the participants. These factors point to supporting and encouraging the existing network personnel to build their knowledge in network automation, providing practical hands-on labs for network personnel to build skills in network automation, and providing training for network personnel to develop their experience in network security automation with the most votes received. These three factors make us assume the desired and need of the IT professionals in learning and skills building, which makes our assumptions about the correctness of the hypothesis related to the need for the support of the leadership for the progress of NSA even stronger.

IT Professionals - Question Number 41

Question: Regarding the above question, do you have any other factors in mind to suggest? (not mandatory to answer)

The Reason for Asking This Question: To investigate affecting factors related to the success of the process of the NSA.

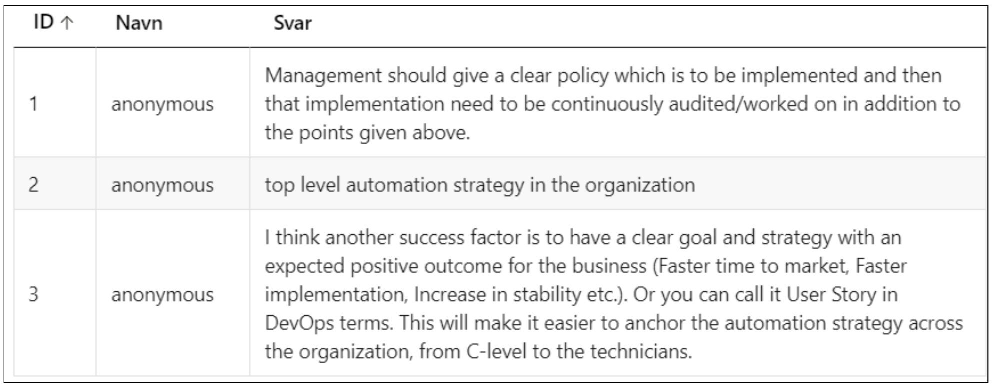
Reference to Research Question: RQ3

Reference to What in SotA Results We Validate: Factors affecting NSA [2, 5–8, 13–17, 34, 35, 42, 43, 45–54, 56–59, 61, 63–68, 70, 71, 73–78, 80–87, 89–112, 173].

Result Facts: Here we received three answers shown in Table H.6, which are as followings:

- *'Management should give a clear policy which is to be implemented, and then that implementation needs to be continuously audited/worked on in addition to the points given above.'*
- *'Top level automation strategy in the organization.'*
- *'I think another success factor is to have a clear goal and strategy with an expected positive outcome for the business, such as faster time to market, faster implementation, increased stability, etc. Or you can call it User Story in DevOps terms. This will make it easier to anchor the automation strategy across the organization, from C-level to the technicians.'*

Table H.6: IT professional survey answer to question 41



ID ↑	Navn	Svar
1	anonymous	Management should give a clear policy which is to be implemented and then that implementation need to be continuously audited/worked on in addition to the points given above.
2	anonymous	top level automation strategy in the organization
3	anonymous	I think another success factor is to have a clear goal and strategy with an expected positive outcome for the business (Faster time to market, Faster implementation, Increase in stability etc.). Or you can call it User Story in DevOps terms. This will make it easier to anchor the automation strategy across the organization, from C-level to the technicians.

Analysis: In the three factors mentioned here by participants, we see they emphasize adding factors such as management's clear policy and the top-level strategy of the organization to the list that we provided in the previous question, question number 40. We assume their emphasis on these factors as proof of the correctness of our hypothesis.

IT Professionals - Question Number 42

Question: What factors, among the following, do you believe contribute to the failure of network security automation projects in organizations?

- Lack of plan for the needed budget and cost of network security automation project
- Lack of the right strategy for network security automation by project leaders
- Stakeholders' and organizations' fears and resistance against the automation of network security processes and tasks
- All of the above
- None of the above

The Reason for Asking This Question: To investigate affecting factors related to the success of the process of the NSA.

Reference to Research Question: RQ3

Reference to What in SotA Results We Validate: Factors affecting NSA [2, 5–8, 13–17, 34, 35, 42, 43, 45–54, 56–59, 61, 63–68, 70, 71, 73–78, 80–87, 89–112, 173].

Result Facts: As Figure H.77 shows, most participants emphasize on lack of the right strategy for network security automation by project leaders and thereafter, the lack of a plan for the needed budget and cost of network security automation projects, and finally, stakeholders' and organizations' fears and resistance against the automation of network security processes and tasks.

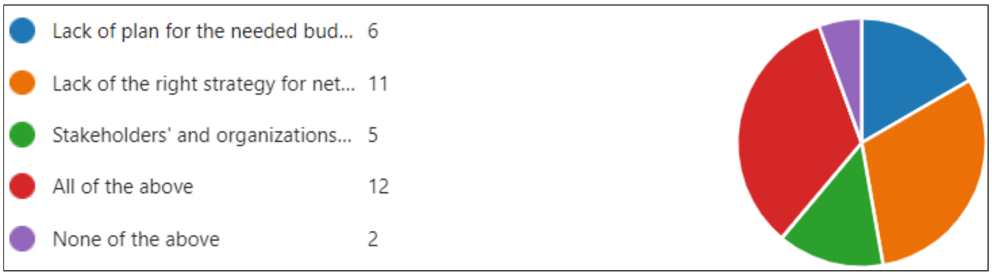


Figure H.77: IT professional survey answer to question 42

Analysis: Here, we suspect that some participants have both chosen one of the three first factors and the one which approved all the three factors above. Hence, it is difficult to make a precise conclusion based on the answers received. One assumption, however, could be made related to the most voted factor here, which points to the lack of the right strategy for network security automation by project leaders, something that also proves the correctness of our hypothesis mentioned in Chapter 1.

IT Professionals - Question Number 43

Question: Regarding the above question, do you have any other factors in mind to suggest? (not mandatory to answer)

The Reason for Asking This Question: To investigate affecting factors related to the success of the process of the NSA.

Reference to Research Question: RQ3

Reference to What in SotA Results We Validate: Factors affecting NSA [2, 5–8, 13–17, 34, 35, 42, 43, 45–54, 56–59, 61, 63–68, 70, 71, 73–78, 80–87, 89–112, 173].

Result Facts: Here we received six answers which are shown in Figure H.78 where responders, among others, mentioned automation, time, policy, and strategy as significant factors to take into account.

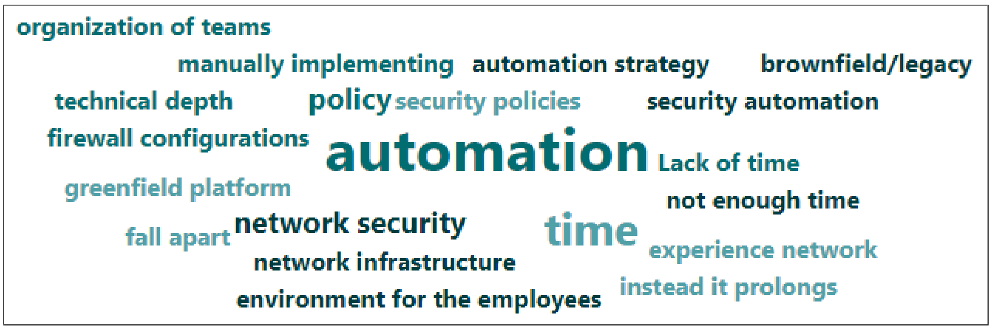


Figure H.78: IT professional survey answer to question 43

Analysis: The previous question was asking about what the participants think is the reason why NSA projects fail. Here, we would like to highlight the factor of 'time' in different contexts is mentioned. Also, 'team' and environment for employees are other factors we can see mentioned here by the participants. Finally, the factor of 'strategy', which is related to the leadership of the organizations, is also pointed to. 'Time', which is related to planning for the project by the leadership, 'team', which is managed by team leaders, and 'strategy', which is made to planning by the leadership of the organizations, all are factors that we consider as proof of the hypothesis mentioned in Chapter 1.

IT Professionals - Question Number 44

Question: Do you fear that if you automate tasks, they could end up collapsing and avoid introducing network automation in the system because of this fear?

The Reason for Asking This Question: To validate our findings concerning the affecting factors on the success of NSA projects. This was prompted by our discovery of resources in the SotA that discussed this aspect and our subsequent research in this regard [15, 16].

Reference to Research Question: RQ3

Reference to What in SotA Results We Validate: Factors affecting NSA [15, 16]. Also taking a step further in the investigation they have done.

Result Facts: In answer to this question, we can see a majority of 88% that confirmed NOT having fear and avoidance concerning utilizing automation techniques and technologies in the environments.

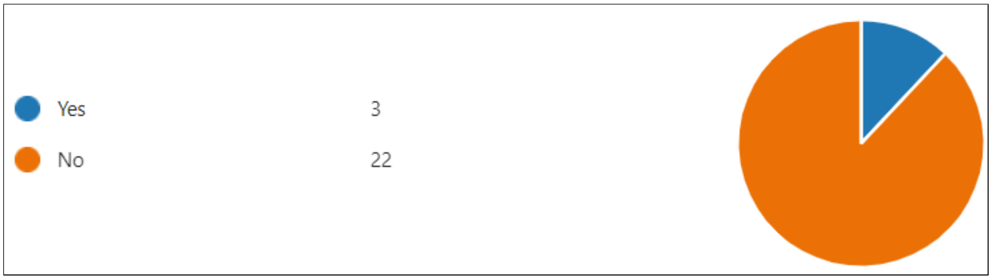


Figure H.79: IT professional survey answer to question 44

Analysis: The majority responding 'No' to the factors of fear and avoidance in this question rejects the assumption about fear of automation of the tasks among most of the IT professionals and makes us assume that the problem could be more related to the lack of proper management, as the right leadership of the projects can justify 'team', 'time', and the right 'strategy', as the participants have mentioned in answer to the above open questions.

IT Professionals - Question Number 45

Question: Are you more comfortable doing tasks manually or by automation in network and network security infrastructures? (Alternative answers: Manually, By automation, Partially of each (both manual and automated))

The Reason for Asking This Question: To confirm whether automation techniques and technologies genuinely alleviate the burden of manual tasks for IT professionals and to corroborate the findings from the SotA study.

Reference to Research Question: RQ2 and implicitly RQ3

Reference to What in SotA Results We Validate: NSA techniques and technologies and their affecting factors [1, 2, 5, 6, 8, 10, 11, 13–17, 34, 35, 39–52, 54, 56–68, 70–108, 110, 111].

Result Facts: Here, as shown in Figure H.80, we can see 68% vote for both manual and automated as a hybrid manner, which is also suggested by some of the resources studied in the SotA [47]. We also have 12% who feel more comfortable in having all tasks automated. Finally, 20% still feel more comfortable doing tasks manually.

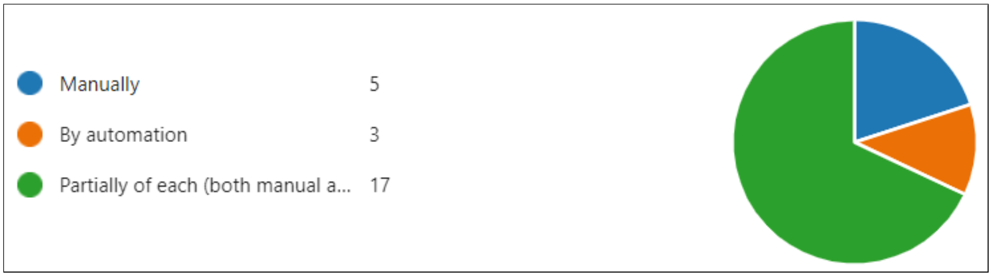


Figure H.80: IT professional survey answer to question 45

Analysis: Here, we can see that there are different opinions among IT professionals who work or have experience in working with network and network automation tasks, and not everybody prefers to do all the tasks fully automated. We also have a high voting rate on the hybrid solution of the NSA, which verifies the results based on the SotA.

IT Professionals - Question Number 46

Question: What percentage of the network tasks do you think can be automated?

The Reason for Asking This Question: To validate the findings from the SotA study. This question focuses on the possibilities IT professionals see in network environments, rather than their capabilities or preferences.

Reference to Research Question: RQ2 and implicitly RQ3

Reference to What in SotA Results We Validate: NSA techniques and technologies and their affecting factors [1, 2, 5, 6, 8, 10, 11, 13–17, 34, 35, 39–52, 54, 56–68, 70–108, 110, 111].

Result Facts: The bar chart shown in the Figure H.81, presents the answers given to this question where we have 60% of the participants who think that between 50% to 70% of the network tasks can be automated, while 80% of them means that something between 40% to 80% of tasks can be automated.

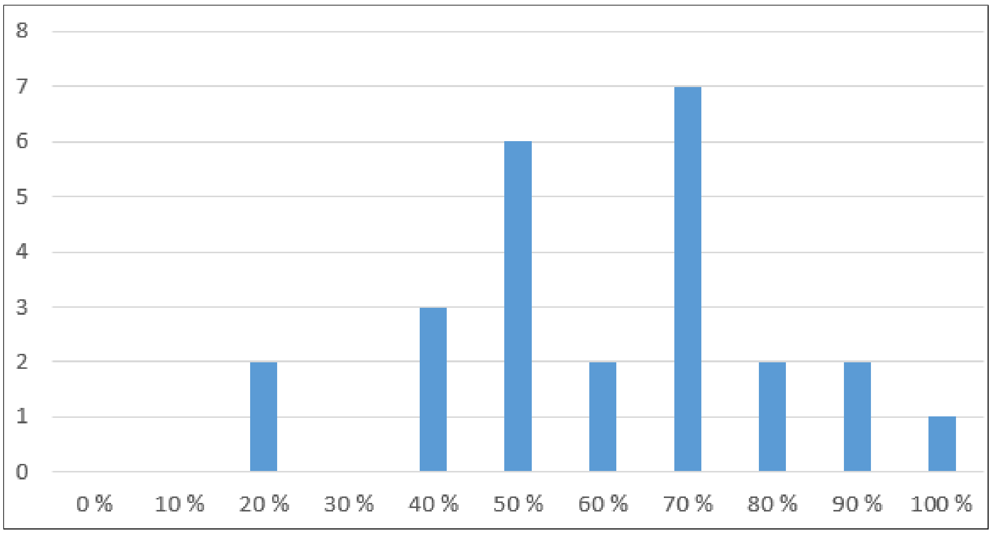


Figure H.81: IT professional survey answer to question 46

Analysis: The answers received here are various, and we assume that this variation in the answers indicates the complexity of the problem. Yet, we can interpret that the answers received here imply that most of them point to a hybrid manner of NSA where something between 40% to 80% of tasks can be automated. This also is proof of what we have studied through the SotA about hybrid solutions for NSA.

IT Professionals - Question Number 47

Question: Which automation-related tools have you worked with or are more familiar with? (Alternative answers: Python (programming language), Ansible (automation tool), and Other programming languages for network automation.) Multiple answers can be chosen.

The Reason for Asking This Question: To register participants' backgrounds and evaluate the validity of our results.

Reference to Research Question: RQ2, and implicitly background registration question

Reference to What in SotA Results We Validate: NSA techniques and technologies [1, 2, 5, 6, 8, 10, 11, 13–17, 34, 35, 39–52, 54, 56–68, 70–108, 110, 111].

Result Facts: Most of the participants confirm being familiar with or have been working with Python programming language. The number of people who confirm have been using or are familiar with Ansible is slightly lower than those who know Python. Many can additionally use other programming languages.

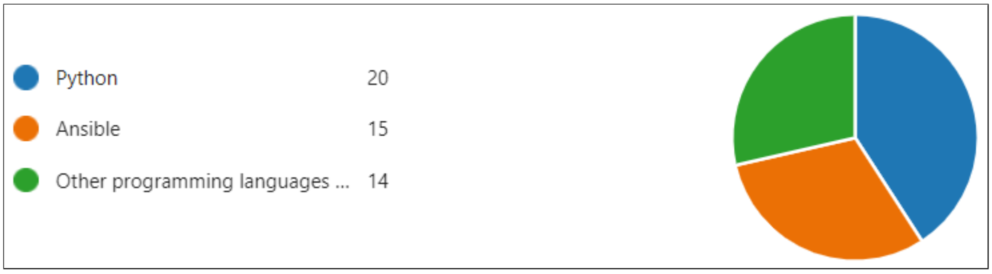


Figure H.82: IT professional survey answer to question 47

Analysis: From the received answers, it is clear that IT professionals who work daily with network and network security are indeed familiar with Python and Ansible automation configuration tools introduced in the SotA. Furthermore, it is evident that many of the participating IT professionals also possess knowledge of other programming languages.

IT Professionals - Question Number 48

Question: If you answered 'Other programming languages' to the question above, please mention their names. (not mandatory to answer)

The Reason for Asking This Question: To register participants' backgrounds and evaluate the validity of our results.

Reference to Research Question: RQ2, and implicitly background registration question

Reference to What in SotA Results We Validate: NSA techniques and technologies [1, 2, 5, 6, 8, 10, 11, 13–17, 34, 35, 39–52, 54, 56–68, 70–108, 110, 111].

Result Facts: As shown in Figure H.83, we can see participants not only mention IaC tools like Terraform, scripting languages such as Perl and Bash, but also automation tools like Puppet, and programming languages like CTL, C#, Visual Basic, Go, Ruby, and PowerShell.

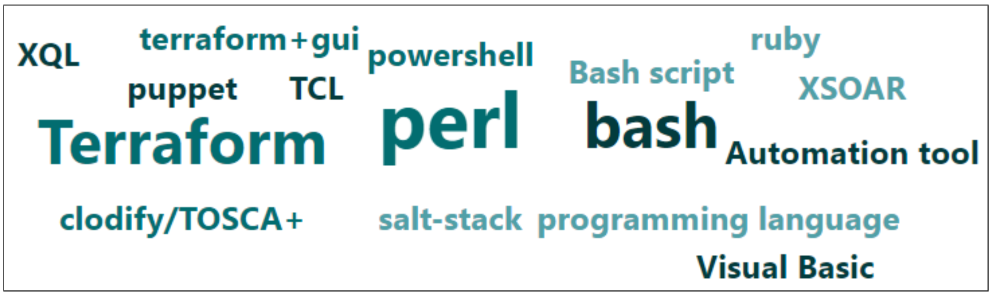


Figure H.83: IT professional survey answer to question 48

Analysis: Based on the responses to this question, we can confirm that many other automation and programming tools mentioned in the SotA, such as Puppet, Terraform, Perl (with the latter being the most frequently mentioned), PowerShell, Bash scripts, Go, CTL, Visual Basic, and other relevant languages, are indeed known to IT professionals. The SotA also highlights the usefulness of these tools in NSA-related roles and IT-related jobs

IT Professionals - Question Number 49

Question: Do you fear utilizing automation in network and network security where you work?

The Reason for Asking This Question: To validate the findings from the SotA and the influencing factors on the success of NSA projects, we posed this question. It differs from question 44, where we specifically inquire about any apprehensions they might have regarding the utilization of automation technology in their workplace. This distinction separates concerns related to the act of using automation technology from concerns about potential network issues resulting from such usage, as explored in question 44. We included the question about their fear of automation based on our literature review, which revealed references in the SotA that highlighted this factor's impact on the progress of NSA [15, 16].

Reference to Research Question: RQ3

Reference to What in SotA Results We Validate: Factors affecting NSA [15, 16]. Also taking a step further in the investigation they have done.

Result Facts: As shown in Figure H.84, 76% answered that they do NOT fear utilizing automation in network and network security where they work.

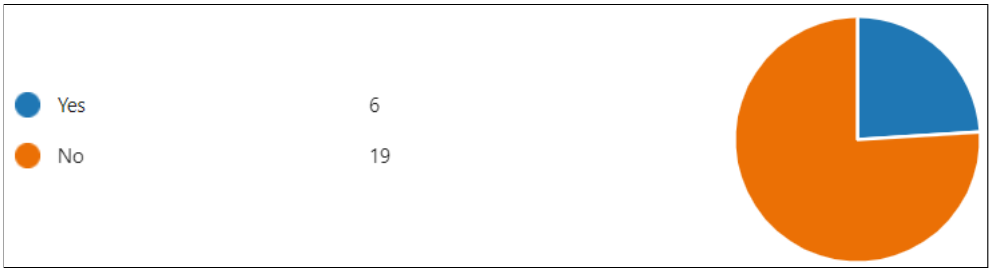


Figure H.84: IT professional survey answer to question 49

Analysis: The result here was very close to the result of the answers given to question 44 if not totally the same. Comparing the answers received in this question and in question 44, the responses received here show 24% having a fear of using automation in the network environment where they work, while only 12% fear that network processes and tasks will end up collapsing if they automate it. Fewer people believe processes and tasks in networks will collapse if they automate them, while more people fear using automation where they work. Hence, this makes us assume that fear of using automation where they work could be related to factors other than damaging the processes and tasks solely because of the use of automation techniques.

IT Professionals - Question Number 50

Question: Do you feel confidence and trust in addition to sufficient knowledge and competency to automate network security jobs where you work?

The Reason for Asking This Question: To validate the findings from the SotA and explore the factors influencing the success of NSA projects. While this question shares similarities with questions 44 and 49, it focuses specifically on trust and confidence arising from sufficient training and experience [15, 16].

Reference to Research Question: RQ3

Reference to What in SotA Results We Validate: Factors affecting NSA [15, 16]. Also taking a step further in the investigation they have done.

Result Facts: In answer to this question, as shown in Figure H.85, we have 68% confirmation about having trust and confidence in addition to sufficient knowledge and competency to utilize automation techniques in their jobs.

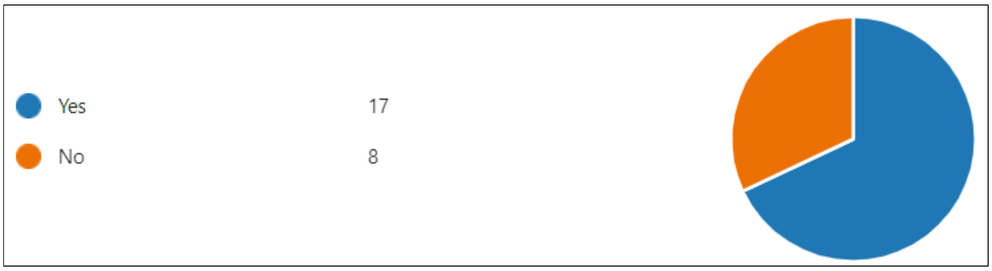


Figure H.85: IT professional survey answer to question 50

Analysis: The answers we receive here are precisely the same as those given to question 38, where we asked about team collaboration possibilities in the organization where the participant works. The team collaboration asked in question 38 was related to achieving automated solutions for network and network security. This makes us assume that there should be a substantial relationship between teamwork results on the one hand and the confidence and trust created in team members who accomplished the tasks together on the other hand. This strengthens our assumptions about teamwork as an affecting factor for the success of NSA projects in the organizations.

IT Professionals - Question Number 51

Question: Do you feel confident and trust in addition to sufficient knowledge and competency to fix errors and mistakes and easily revoke tasks that need to be fixed after automation where you work?

The Reason for Asking This Question: To validate the findings through the SotA [15, 16], and the affecting factors on the success of NSA projects.

Reference to Research Question: RQ3

Reference to What in SotA Results We Validate: Factors affecting NSA [15, 16]. Also taking a step further in the investigation they have done.

Result Facts: In answer to this question, as shown in Figure H.86, we have 68% confirmation about having trust and confidence in addition to sufficient knowledge and competency in fixing errors and problems that can be raised when automating tasks.

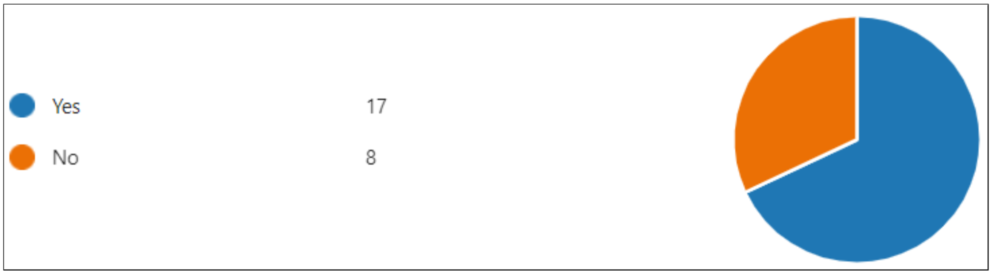


Figure H.86: IT professional survey answer to question 51

Analysis: While here focusing on the ability to fix errors and problems that can be raised when automating tasks, the answers received here in this question are precisely the same as what we received in the previous question, question 50, which makes the assumption mentioned there about the relationship between teamwork, and the confidence and trust in their competency and skills more potent.

——————— IT Professionals - Question Number 52 ———————

Question: Do you think at the point we are at the current time, customer tickets will take too long to solve when the issues are related to the automation of the tasks?

The Reason for Asking This Question: To validate the findings through the SotA [15, 16], and the affecting factors on the success of NSA projects.

Reference to Research Question: RQ3

Reference to What in SotA Results We Validate: Factors affecting NSA [15, 16]. Also taking a step further in the investigation they have done.

Result Facts: As shown in Figure H.87, we can see that 69% of the participants reject this reasoning.

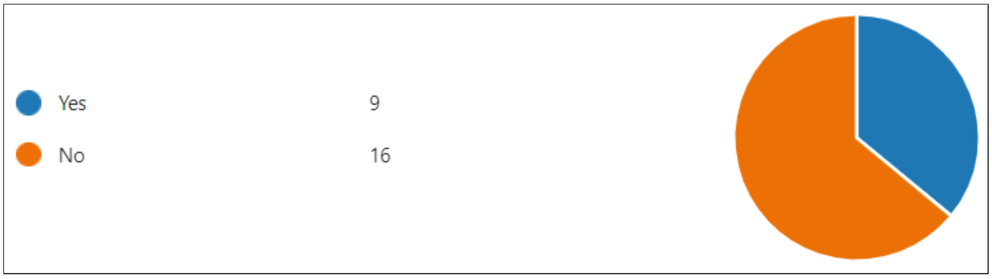


Figure H.87: IT professional survey answer to question 52

Analysis: We assume a relationship between the ability to fix errors related to automation tasks, mentioned in question 51, and solving customer tickets related to automation tasks. Noticing that the responses received to questions 51 and 52, mirror each other, we also assume that these two factors are two sides of the same coin and another proof of this relation.

Also, relating the previous question with the assumption we had about the relationship between teamwork on the one hand and confidence and trust in their results on the other hand, we see a connection to the same thread of the relationship between the parameters of teamwork, confidence, and trust of team members in the utilization of automation techniques and technologies in network and network security, not having a fear of errors raised because of the tasks that are automated, and finally having confidence in fixing mistakes and errors while consequently not letting related customer tickets taking too much time to fix.

IT Professionals - Question Number 53

Question: Do you think automation of the procedures and tasks will raise the network's security? Alternative answers:

- Yes, but it will impose new challenges to the security of the network
- Yes, but it will impose new challenges to the management of the network and network security
- I agree to both of the above solutions
- Yes, and the benefits of the automation of the processes and tasks in network and network security infrastructure will compensate for the disadvantages it will impose on the system
- No, it will only impact our work with network and network security negatively and impose more complexity on the system resulting in less security

The Reason for Asking This Question: There are numerous resources discussed in Chapter 4 Section 4.1, addressing the enhancement of security through the use of automation techniques and technologies in network and network security environments. Consequently, we aimed to investigate how IT professionals, drawing from the experience mentioned in their responses to questions 21 to 25, approach this question and what their perspective is on the issue. Also, to validate the SotA, the solutions suggested in this question are referenced by the resources presented in Chapter 4.

Reference to Research Question: RQ3

Reference to What in SotA Results We Validate: Factors affecting NSA [1, 2, 5–8, 10–17, 34, 35, 39–112].

Result Facts: As shown in Figure H.88, we have 11 participants who agree with both point one, which states 'Yes, but it will impose new challenges to the security of the network' and point two, which states 'Yes, but it will impose new challenges to the management of the network and network security'. Some participants only agree with one of these two points.

We also have six people who agree with the state which is 'Yes, and the benefits of the automation of the processes and tasks in network and network security infrastructure will compensate for the disadvantages it will impose on the system', and a few who choose to be skeptical to what automation techniques can contribute to network security and choose the last solution which is 'No, it will only impact our work with network and network security negatively and impose more complexity on the system resulting in less security'.

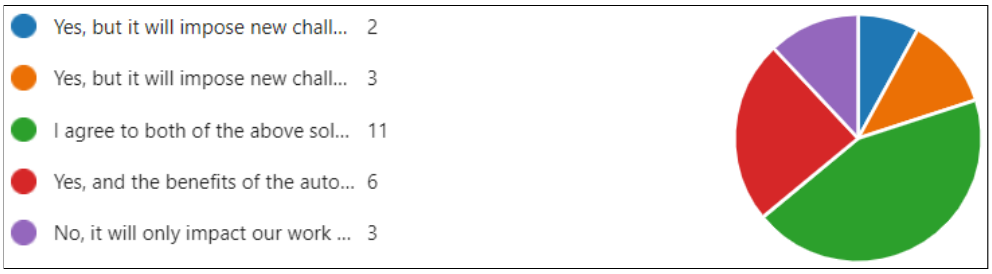


Figure H.88: IT professional survey answer to question 53

Analysis: 64% of the participants agree that NSA will raise the resilience of network security, but at the same time, it either imposes challenges on the security of the network or the management of the network, or both of these factors. We have only 24% who agree that the benefits of NSA will compensate for the disadvantages it will impose on the system. Finally, there is also a minority who believe that NSA will only harm network security while imposing more complexity on the network infrastructure.

IT Professionals - Question Number 54

Question: Network automation, facilitated by automation tools like Ansible and programming languages such as Python, in conjunction with different platforms and technologies like SDN, ML, and IaC, is suggested by many academic researchers, as discussed in Chapter 4 Section 4.1. Why do you think these technologies are/are not used in today's solutions for network security automation, and what do you see as the reason for that?

The Reason for Asking This Question: To verify the findings through the SotA and the affecting factors on the success of NSA projects. Here, we wanted to receive more open opinions, thoughts, and viewpoints from the participants regarding the way they see the problem and its solutions.

Reference to Research Question: RQ3

Reference to What in SotA Results We Validate: Factors affecting NSA [2, 5–8, 10, 13–17, 34, 35, 42–54, 56–61, 63–87, 89–112, 114].

Result Facts: In this last question, which was open and not mandatory, we received 21 answers. Here, in addition to the demonstration shown in Figure H.89, we present the answers received to this last question. Each answer is represented in a bullet point with the sentences quoted directly, and in the same way, they were written for the sake of keeping them safe from our assumptions.

- *"For the individual host/device, using IaC as an initial way of configuring the baseline/initial state of the firewall/ACLs, etc., is straightforward. Using IaC becomes a problem when the host/device needs to change from the baseline or just change in general. In general, I experience that there are many ways of doing the same thing when using IaC, and when there is not a clear policy/definition on how we do things, then it becomes difficult to audit the system/network as a whole. Examples of this are if a system/device is configured to allow a subnet in on an interface, depending on which IaC you use, removing that access is not necessarily easy without manual intervention.*
  Most IaC (in my experience) need a relatively simple script to check for access permissions that should be there but need additional relatively complex logic to check for or remove existing access permissions that should not be there. Since the point of IaC is to get things done quickly and easily to replicate on other systems, the additional time it takes to create rigorous network automation that is easy and logical to audit is not prioritized. In short. I have trust in IaC setting up the host. I do not trust IaC changing an already installed/initiated host unless I know the script has been made to take that into account.
  For whole systems/networks, using IaC is good; it works, but substantial efforts need to be placed into programming the network automation part, which I feel often is generalized down to the bare essentials, meaning opening up for subnets, hosts, ports, etc., but not enough time is spent checking for things that should not be there. Often this comes down to getting work done and moving on to the next thing that needs doing."
- *"I think it is too early, and network automation is still "new" in many people's eyes."*
- *"In my environment, we have such a limited amount of devices that automation in the setup on the network devices doesn't make much sense."*

- *“Everybody does not have a "Sandbox" large enough to test and check out their automation in practice before deploying it.”*
- *“I think SDN is becoming widely used because it is the easiest to get started with in my experience, and it requires no programming skills to use basic functions in many cases, for instance, when using Cisco DNA Center. IaC, in my experience, is used a bit, but I feel most people are using it on a small scale at this time, for instance, "unimportant" environments, single applications, etc.”*
- *“Lack of competency, legacy solutions”*
- *“Automation using IaC is often synonymous with cloud environments. On-prem is a kind of legacy to automation. ML is still viewed by many as relatively new. SDN states that the whole mindset around networking is changing. Not IP and port anymore but rather applications.”*
- *“Based on experience, network security automation might not add much value, instead, it prolongs the time needed to perform tasks vs. manually implementing changes.”*
- *“Industry is always behind; academic research is easier than doing it in practice with CIS network services in mind.”*
- *“I think that this feature is still new and needs more time to be mature as some of those automation languages are constantly changing; also, Network engineers are not prepared to do these kinds of tasks as they don ́t have formation. Regarding organizations, it could be a huge change, and so it will be a huge budget needed to update their network appliances and resources in general. The usual method for companies to update is to exhaust the end-of-life date of the appliances.”*
- *“Lack of knowledge of programming possibilities among experienced network engineers and the resistance towards the change of work habits/ways.”*
- *“Many factors can delay technology adoption and new task performance methods. This includes culture shift, and generally, more experienced engineers take longer to support methods that change the work tasks are performed, especially if things have been effective. It also requires a large investment and culture shift from the business due to the costs involved. It all boils down to trust.”*
- *“The automation solutions are not much in use due to the lack of commitment from management in organizations and lack of competency in network teams.”*
- *“For experienced network professionals, it might be a big step to change their daily way of work for many years. However, by facilitating these resources, even the experienced resources can see benefits and overcome the seemingly heavy start. As for younger network professionals, I believe we are seeing an increased use of tools named above.”*
- *“Because the error percentage is still high, and automation cannot solve some specific topics/tasks.”*
- *“I think they are used in today’s solutions in my company.”*
- *“Network technicians don’t want to learn automation.”*
- *“Competency”*
- *“High upfront investment in time and money. Licensing cost is prohibitively*

high for many solutions, such as Cisco DNA Center Organizations expect Operation teams to automate without dedicated time and resources. While understaffing might be alleviated by automation, it's very difficult to do so when teams are struggling to keep up with the day-to-day workload. Also, introducing automation tools should reduce the likelihood of human error, but it also increases the impact, i.e., Facebook killing all their systems with a BGP change, or the numerous Cloudflare incidents where similar things happened."

- *"Where these tools are used, it is because they provide a more effective and stable way to operate a network platform. Where they are not used could be because of complex legacy systems where automation is challenging or the lack of maturity in the organization for working with automation tools and processes. Especially processes are important in succeeding with an automation strategy."*
- *"Complexity"*

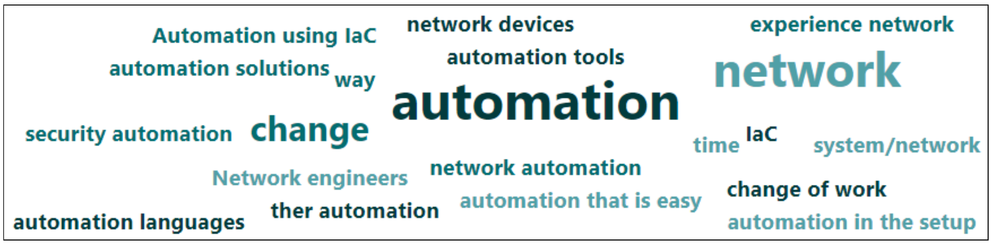


Figure H.89: IT professional survey answer to question 54

Analysis: The responses to this question, while confirming that there is a lack of automation in today's network security, suggest different solutions to this problem. First, concerning the answers applied, we assume they confirm the problem stated in Chapter 1 exists. Second, we can see their proposed solutions to answer the question point to what we have found through the SotA. For instance, they mention different affecting factors such as complexity, lack of competency, legacy solutions in the network environments that are not compatible with automation techniques and technologies, and lack of support of NSA by the management of the organizations. Hence, their answers verify what we presented in Chapter 4.

End of IT Professionals Group-specific Questions

Appendix I

In-Depth Review of the Interviews

This appendix presents a brief outcome of the interviews conducted with network professionals who work for different companies, one of the network team leaders in a large IT consulting company, and one of the scientific personnel who works at a university.

I.1 Interviews with the IT Network Professionals

In the interviews conducted, we have mainly asked two questions from network professionals to map the relationship between the utilization of automation techniques and technologies in network and network security by them and the strategies their organizations or their organization's customers take in network and network security management when it comes to automating network and network security tasks and processes. The questions mentioned in the interviews were presented in the beginning sections of this chapter. Here we present a brief version of the interview outcomes.

One of the interviewees who also had a Ph.D. educational degree mentioned:

> *"The variety of components used in the network and network security of the organizations, the rapid change of these components, and different needs in the network of different organizations are some of the factors that make it difficult for us to provide a standard solution for every organization's network and network security automation." "The best is to standardize network automation solutions to be able to offer it to all customers, but the complexity of the network solutions which are in use today, the variation of components utilized in network and network security solutions, and the difference between the networks of different organizations make it almost impossible for us to provide a standard solution for network and network security automation."*

Another interviewee with more than 20 years of professional working experience with different network and network security solutions, who also utilizes self-produced Python code scripts to automate network security and management tasks, mentioned:

> *"If we are going to utilize network automation in our work, it needs to be a teamwork in the same manner in which program developers work with CI/CD cycle of Development and Operations (DevOps) and the operation needs to be supported by the leaders and managers in the company, and in conjunction with mission, vision, and values of the organization."*

A senior network engineer with several years of working experience with different organizations' network management and network security solutions mentions:

> *"We are living in the stone age of network and network security management. All tasks we manage in the network of CIS companies are done manually, firewall rules are implemented one by one for each host or subnet, and there exist thousands of rules in the firewalls that we even don't have time or work capacity to go through and update or delete. This manual manner of network security management, which comes from both legacy products that can't cooperate with automation technologies used by different organizations' networks, in addition to our lack of competency in network automation, lack of attention, time, and willingness from managers of Network Operations of different organizations we work for makes the network tasks being cumbersome to manage and network security being like a colander with a lot of holes. Unfortunately, it is like we live in the stone age of network management and network security."*

A network engineer with more than ten years of experience in working with IT systems, who also utilizes automation techniques in network and network security tasks daily, explained:

> *"In my opinion network automation is not only the configuration of the network, troubleshooting, or even operation. But first, the automation will cost more, but then when automation procedures are implemented, and when it gives benefits, we observe the value. Not many of us can code, but we need to be developers to do automation. Many templates can be used. In any way, competency is needed to automate.*
> *We would like to automate network infrastructure because this gives consistent, scalable, error-free, and not least, a lot of fun in our work. Automating network infrastructure will also contribute to integrating it with other IT stacks and the good thing is that it is solid among different vendors. When having many repetitive tasks we need to automate the tasks. This helps us to deliver our work results more effectively, and while having less error. This also reduces the complexity of the system configurations. The reduction of complexity in the systems is more user-friendly with our technicians as the users."*

I.2 Interview with a Network Team Leader

Anonymous interview with one of the leaders[1] in one of the large companies that deliver IT consulting to their customers.

Us: First, we explained that we have the traditional networks that IT professionals should manage and have competency in, and then build their network automation competency above that. However, the organizations are different and have different network environments, infrastructures, and needs. So, there is a large variety in their solutions for network and network security management. So, we have concluded that the complex picture in front of us to solve exists of a large variety and choices to make and various problems to solve.

Network Team Leader's answer: *"Organizations need to buy network services from someone. This is what we call Network as a Service (NaaS). There are so many different platforms and many different ways they manage network and network security because the different organizations build the solutions themselves. That is why it is the way it is now! This is the way you just explained which is when no one solution matches all of the customers who are managing large networks."*

Us: Here we explained what we have in mind regarding the Rubik's Cube that we explain in Chapter 4 Section 4.5 to this leader to hear the opinion on this idea.

Network Team Leader's answer: *"As you explain the situation as a Rubik's Cube, matching the right and proper options on the Rubik's Cube that you described, is the consulting company's task to do for their customers. The task is to play with this Rubik's Cube that you compared in the exemplification and find the best solution that matches each customer as each customer is unique and has different needs. The solutions delivered can be standardized to some degree, but not very much, so the solutions delivered cannot be completely standardized.*
Many consulting companies have this task. The task of turning the bricks in the exemplified 'Rubik's Cube' and finding the right solution for each customer. So, the final solution we say for large companies is NaaS. This solution is to employ an IT consulting company that accomplishes the work for them. Otherwise, if they do it themselves, it will end up in a mess which makes automation of the network and network security extremely cumbersome. Meanwhile, the theoretical solutions provided by academia are not very useful in what we deliver to the customers in this process. We need to see what is possible to do in practice, not what is theoretically best to do."

---

[1] As discussed in a previous footnote in Chapter 3, when we refer to 'leaders', we are addressing individuals situated at higher levels within organizational hierarchies who make significant decisions. On the other hand, when we mention 'managers', we are specifically referring to leaders responsible for overseeing IT professional teams and guiding their day-to-day activities. Thus, in this context, we are discussing a leader who supervises managers responsible for leading network teams in their daily operations.

I.3 Interview with a Scientific Personnel

This section presents the interview we had with one of the scientific personnel at a university, who also had experience working as a network engineer for some large companies. Hence, the experiences discussed here relate to network and network security in both university and organizational and industry environments.

"I have experienced that the work done by employees who end their work career will be difficult for new employees to take over. This is because they have used automated techniques that are familiar to them, but not documented. So the new employees prefer to do the work rather than manually. I agree that the competency of IT personnel in automating network and network security tasks is crucial for companies. Sometimes even not many IT personnel are needed. A few IT personnel who can automate the needed and repetitive tasks are enough to fix the issues, set a start to the system, and then the job is done! Then the network and the related systems will continue to work without needing many people to manage it. Network administrators with programming knowledge will use scripting in languages such as Python and Perl to automate tasks. I also have experienced that if the people who know how these scripts and tools function leave, there is a risk of a knowledge vacuum.

In the industry, I have experienced that large companies utilize automation of network and network security tasks and processes comprehensively, while this is much less utilized in medium or small companies. There is also an issue which is related to the employees who work with networks but are not interested in programming. This could also be the opposite way, which means those who can program are not interested in working with networks and network security solutions. Experienced network administrators will use base configurations and templates, regardless of network size, and that scripting is common in large-scale networks.

Regarding the challenges when a company needs to utilize network security automation, it is complicated. It means assuming a company decides to automate part or most of its network security tasks, there are many ways to do that. Besides different techniques and technologies that exist, which should match the needs and possibilities of the company, the industry has its way of suggesting how the process and tasks should be done, while solution and equipment providers, such as Cisco and Juniper have their way of doing that. Not least, academia suggests its way of processing and utilization of technologies for automating network management tasks. So we have three different parties with three completely different ways of solutions for how to automate network security.

When it comes to platforms and possibilities that are available for training and skills building in the automation of network and network security techniques and technologies, there are many different possibilities. As a scientific personnel who works actively and educates students in network and network security-related topics, I am aware that there is an easier available tool which is Packet Tracer. This tool,

however, gives nothing to skills building in this relation.
GNS3 exists also as a solution for the training of the network personnel to build automation-related skills, but neither this solution is free for those who want to practice. They will have to buy the products to be able to practice network automation with GNS3 environment. In addition to this, even if they get access to the training application and everything required, there is a need for a scenario that can help them in the first stages of learning so they can further grow up and find the way through. This also applies to the virtual labs that are provided by Cisco or other solution and equipment providers such as Virtual Internet Routing Lab (VIRL).

When it comes to how much we teach our students about network automation, yes, we mention it in general, but our focus is mostly on teaching them how to find out different ways of learning rather than teaching them something like Developer Network (DevNet). When our students are educated, following what I know, 10% of those who work for small and medium enterprises utilize network automation in their future work after graduating from our university, while this number is higher when it comes to the students who work for large enterprises.
I agree that maybe we should have made available some topics such as DevNet for our students, but our focus is not on how much students can remember things by heart to be able to pass certifications exams, as they will have the possibility for that when they start working for companies. Our focus is on teaching them how to learn different things and grow in the learning process, while we sometimes also mention some hints about network automation generally."

I.4 Brief Summary of the Interviews

In the interviews, a diverse range of perspectives emerged on how to address the identified problem. One IT professional, holding a high educational degree, stressed the importance of standardizing solutions for customers. Another seasoned IT professional, with extensive experience in network and network security, recommended a collaborative DevOps approach, leveraging CI/CD as a solution.

A senior network engineer candidly characterized the current state of network and network security management as the *'stone age of network and network security management'*, highlighting the urgency of our investigation. An experienced network engineer underlined the crucial need for network professionals to acquire competence in automation techniques, aligning with our findings in the SotA literature regarding the efficacy of automation in network scaling, albeit with an initial cost investment.

A network team leader advocated NaaS as a viable solution for organizations managing large networks, challenging the idea of standardization as the sole remedy for addressing the diversity in technology solutions.

Furthermore, an interview with a scientific expert who has experience both as an IT professional in large companies and as a university educator revealed a focus on teaching students how to find solutions rather than imparting specific solutions. This pedagogical strategy aligns with the rapid technological advancements in various fields. The expert also endorsed the problem under investigation and emphasized the utility of templates as catalysts for addressing it.

This diversity of opinions from professionals and educators underscores the complex nature of the challenges discussed in Chapter 4, Section 4.5, and highlights the existing variety of solutions adopted by different customers in their network and network security infrastructures.

Appendix J

Experimenting with Artificial Intelligence

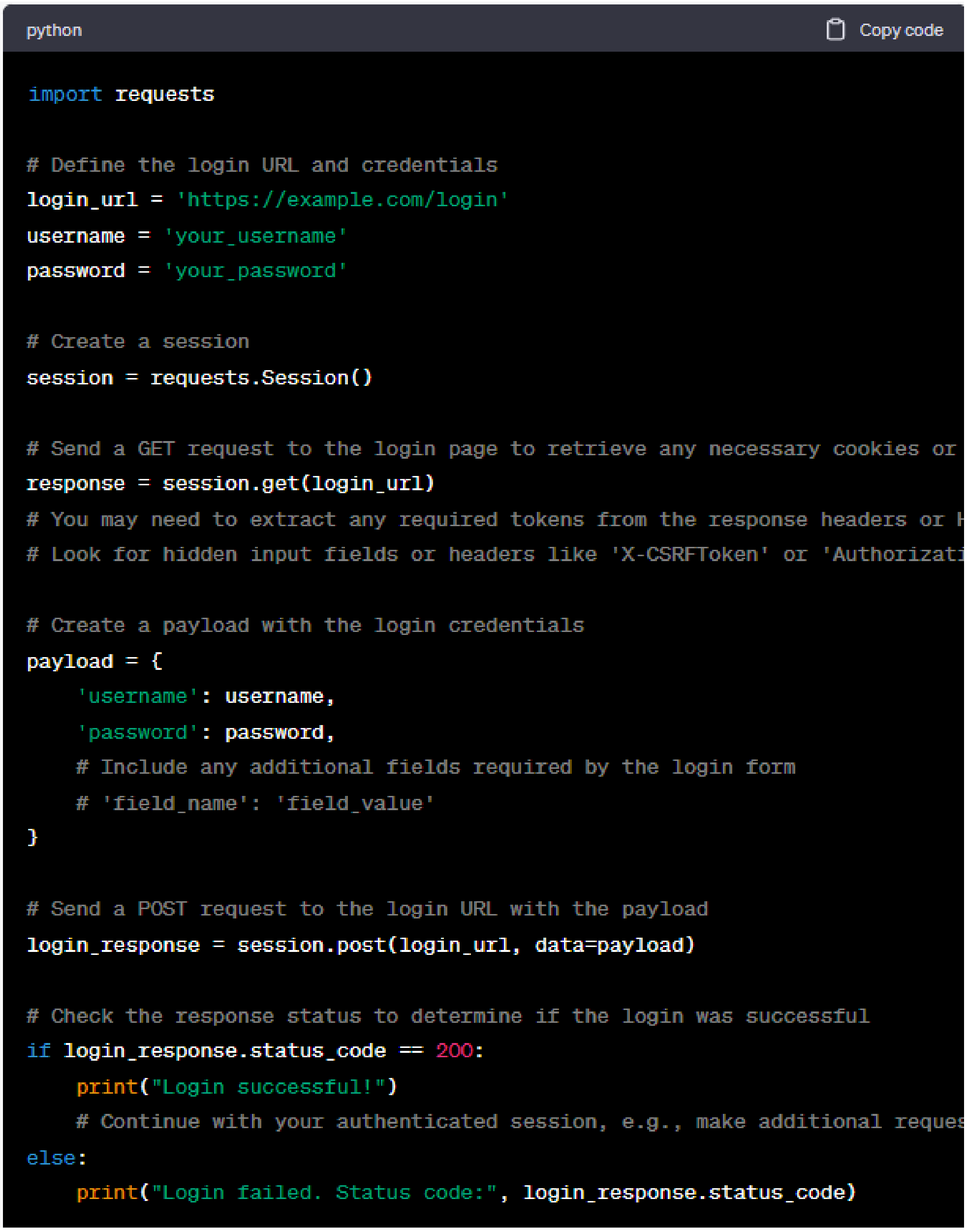
To experiment with ChatGPT, we tested a simple task to be solved by utilizing the supporting knowledge this open AI provides to everyone. For this reason, we asked ChatGPT to make a Python code for us that logs in to a specific web page. Hence, the questions asked here are just to experiment with open AI and are not meant to provide a solution to network automation related to this thesis. Concludingly, the following experiment shows that taking advantage of AI to develop scripts for automation of specific network and firewall tasks will not be far from what we experimented with here.

Question asked: Make a Python code.

ChatGPT answer: Certainly! What would you like the code to do? Please provide some details and requirements so I can create the code that fits your needs.

Question asked: Log in to a web page.

ChatGPT answer: To log in to a web page using Python, you can utilize the *requests* library. Here's an example code that demonstrates how to log in to a web page by sending a POST request with the login credentials:



```python
import requests

# Define the login URL and credentials
login_url = 'https://example.com/login'
username = 'your_username'
password = 'your_password'

# Create a session
session = requests.Session()

# Send a GET request to the login page to retrieve any necessary cookies or
response = session.get(login_url)
# You may need to extract any required tokens from the response headers or
# Look for hidden input fields or headers like 'X-CSRFToken' or 'Authorizati

# Create a payload with the login credentials
payload = {
    'username': username,
    'password': password,
    # Include any additional fields required by the login form
    # 'field_name': 'field_value'
}

# Send a POST request to the login URL with the payload
login_response = session.post(login_url, data=payload)

# Check the response status to determine if the login was successful
if login_response.status_code == 200:
    print("Login successful!")
    # Continue with your authenticated session, e.g., make additional reques
else:
    print("Login failed. Status code:", login_response.status_code)
```

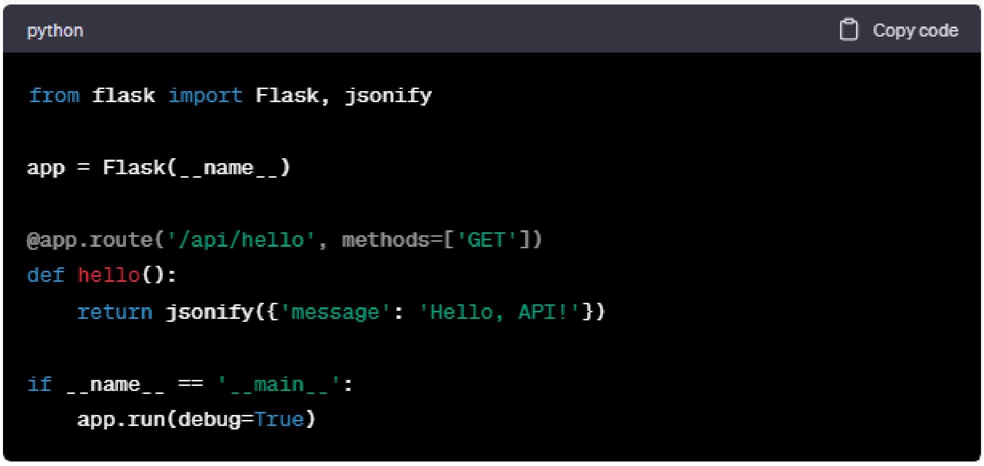
Figure J.1: Python code for login to a web page provided by AI

ChatGPT answer: Please note that the specific implementation may vary depending on the target website's authentication mechanism. You may need to inspect the HTML source code of the login page and adjust the code accordingly to handle any additional form fields, cookies, or tokens required for successful authentication. Additionally, ensure that you have the *requests* library installed. You can install it via *pip install requests*.

Question asked: How to open Python API?

ChatGPT answer: To open a Python API, you typically need to create a web server using a framework such as Flask or Django. Here's an example using Flask, a lightweight web framework:

1. Install Flask: You can install Flask by running *pip install flask* in your command prompt or terminal.
2. Create a Python file (e.g., *api.py*) and add the following code:

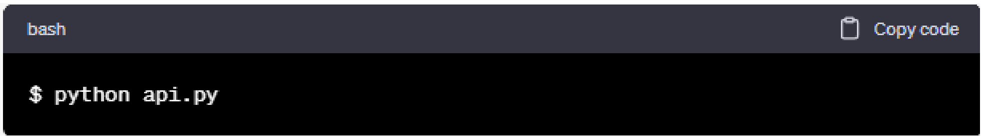


```python
from flask import Flask, jsonify

app = Flask(__name__)

@app.route('/api/hello', methods=['GET'])
def hello():
    return jsonify({'message': 'Hello, API!'})

if __name__ == '__main__':
    app.run(debug=True)
```

Figure J.2: Python code suggested by AI for how to open a Python API

In the above code, we import the Flask class from the *Flask* library and create a Flask application instance called *app*. We then define a route */api/hello* using the *@app.route* decorator, specifying that it only responds to *GET* requests. When a request is made to this route, the *hello* function is called, which returns a JSON response using *jsonify*.

3. Save the file and run it:



```bash
$ python api.py
```

Figure J.3: Python code suggested by AI about how to run a Python script

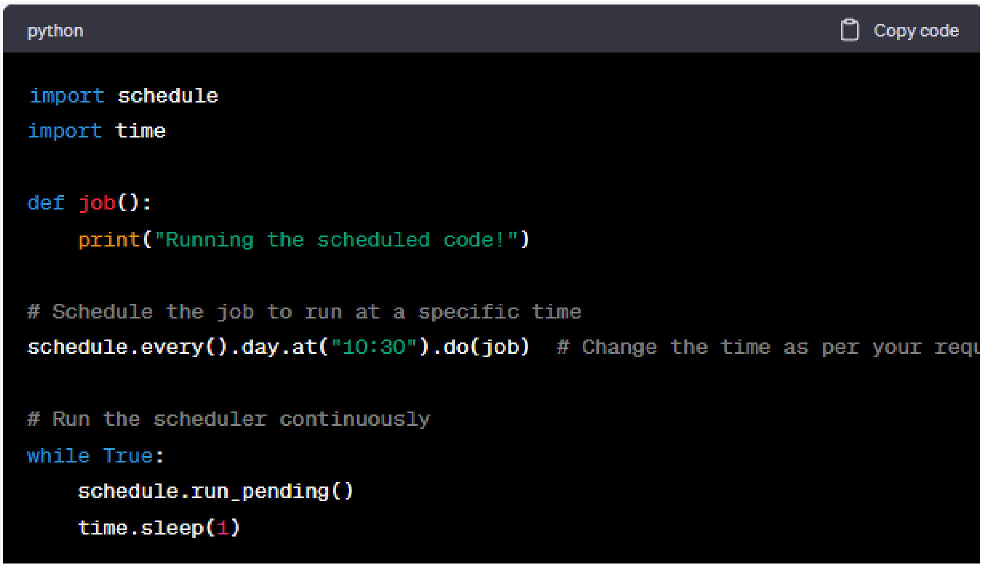
4. Your API should now be running on *http://localhost:5000*. You can test it by opening a web browser and visiting *http://localhost:5000/api/hello*. You should see a JSON response with the message "Hello, API!".

This is a basic example; you can expand upon it to create more complex APIs with additional routes and functionality. Flask provides many features for handling request data, routing, and serving static files, among others. You can refer to the Flask documentation for more information on how to build APIs with Flask: https://flask.palletsprojects.com/

Question asked: How to run a code at a specific time?

ChatGPT answer: To run a code at a specific time in Python, you can use the *schedule* library. Here's an example that demonstrates how to schedule and execute a function at a specific time:

1. Install the *schedule* library by running *pip install schedule* in your command prompt or terminal.
2. Create a Python file (e.g., *scheduled_code.py*) and add the following code:



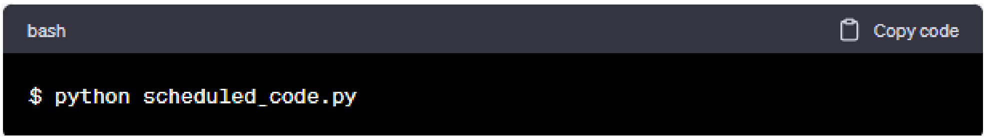
```python
import schedule
import time

def job():
    print("Running the scheduled code!")

# Schedule the job to run at a specific time
schedule.every().day.at("10:30").do(job)  # Change the time as per your requ

# Run the scheduler continuously
while True:
    schedule.run_pending()
    time.sleep(1)
```

Figure J.4: Python code suggested by AI about how to run a Python script at a specific time

In the above code, we import the *schedule* and *time* modules. We define a function *job()* that represents the code you want to run at a specific time. The *schedule.every().day.at("10:30").do(job)* line schedules the *job* function to run at 10:30 AM every day. You can modify the time to match your desired schedule.

The *while True* loop ensures that the scheduler keeps running continuously. The *schedule.run_pending()* function checks if there are any pending jobs and executes them accordingly. The *time.sleep(1)* statement is used to avoid excessive CPU usage by pausing for 1 second between iterations.

3. Save the file and run it:



```bash
$ python scheduled_code.py
```

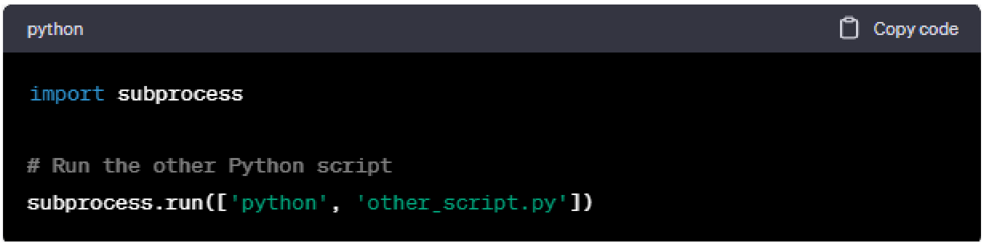
Figure J.5: Python code suggested by AI about how to run a Python script

Now, the code inside the *job()* function will be executed at the specified time each day.

You can customize the scheduling as per your requirements using the various methods provided by the *schedule* library. For example, you can schedule code to run on specific days of the week, at specific intervals, or fixed intervals using the available functions and syntax.

Question asked: How to tell a Python code to run another python .py file?

ChatGPT answer: To run another Python *.py* file from your main Python code, you can use the *subprocess* module. The *subprocess* module allows you to spawn new processes, including executing other Python scripts. Here's an example:



```python
import subprocess

# Run the other Python script
subprocess.run(['python', 'other_script.py'])
```

Figure J.6: Python script suggested by AI for telling a Python script to run another Python script

In the above code, *subprocess.run()* is used to run the *other_script.py* file. The script is executed by calling the *python* command followed by the name of the script file as a list of arguments.

You can customize the execution further by providing additional arguments to *subprocess.run()*. For example, you can capture the output or handle any errors that occur during the execution. Refer to the *subprocess* module documentation for more information on the available options and functions.

Make sure that the *other_script.py* file is in the same directory as the main Python script or provide the full path to the script if it is located in a different directory.

When you run the main Python script, it will execute the specified *other_script.py* file as a separate process.

Question asked: To run a Scheduled code should the terminal remain open?

ChatGPT answer: Yes, to run a scheduled code using a package like *schedule*, the terminal or command prompt typically needs to remain open. The scheduled code runs within an infinite loop that continuously checks for pending jobs and executes them.

If you close the terminal or command prompt, the Python process, and the scheduled code will terminate, and the scheduled jobs will no longer be executed.

To keep the scheduled code running continuously, you need to leave the terminal or command prompt open. You can minimize the terminal window or run the code in the background if your operating system allows it. Alternatively, you can run the code on a server or in the background as a daemon process.

If you want to run the scheduled code without keeping the terminal open, you can explore options like running the code as a service or using task scheduling tools provided by your operating system. These methods allow you to run the code in the background without the need for an open terminal. The specific steps for setting up background execution may vary depending on your operating system and requirements.

Note: We tested the Python scripts suggested by ChatGPT AI, and all worked well.

NTNU

Norwegian University of
Science and Technology