National Cybersecurity Capacity Building Framework for counties in a Transitional Phase

***(Using Spring Land as a case study)***

**Mohamed Altaher Ben Naseir**

A thesis submitted in partial fulfilment of the requirements of Bournemouth University for the degree of Doctor of Philosophy

*Supervisors:*

*Dr. Huseyin Dogan*

*Dr. Edward Apeh*

*Professor Raian Ali*

# COPYRIGHT

## Declaration

I certify all the work contained in this thesis is my own. The thesis does not contain material which has been submitted previously unless it is cited according to the ethics procedures and guidelines. The content of this thesis is the result of work which has been carried out since the official commencement date of the approved research program. The results of this research have been, fully or partially, presented twice at two conferences as declared in publications arising from this thesis section.

# Thesis Abstract

Building cybersecurity capacity has become increasingly a subject of global concern in both stable countries and those countries in a transitional phase. National and international Research & Technology Organisations (RTOs) have developed a plethora of guidelines and frameworks to help with the development of a national cybersecurity framework. Current state-of-art literature provides guidelines for developing national cybersecurity frameworks but, relatively little research has focused on the context of cybersecurity capacity building especially for countries in the transitional stage. Countries in a transition phase are typically characterised by civil war; political and economic upheaval; the absence of law. This has resulted in a critical knowledge gap that must be addressed through empirical research to guide these countries to develop and implement cybersecurity capacity platform.

This thesis proposes a National Cybersecurity Capacity Building Framework (NCCBF) that relies on a variety of existing standards, guidelines, and practices to enable countries in a transitional phase to transform their current cybersecurity posture by applying activities that reflect desired outcomes. The NCCBF provides stability against unquantifiable threats and enhances security by embedding leading and lagging performance security measures at a national level.

The NCCBF is inspired by a Design Science Research methodology (DSR) and guided by utilising modelling approach IDEF0. Developing this framework resulted in two qualitative studies, Interactive Management (IM) and Focus groups as the main data elicitation approach. These studies involving government officials, private sector, managers and general employees participating in security development from areas such as defence, e-services, the private sector, banking, the Digital Crime Unit, the Immigration and Foreigners Affairs Authority, the oil and gas sector and intelligence agencies. A set of objectives was derived from these studies to identify the key initiatives for the development of national cybersecurity capacity in the country. This research also used secondary data sources such as government reports, global indices, to validate the results of the research study.

The findings suggest that countries in a transitional phase are vulnerable to cybersecurity risks, such as cybercrime and cyber terrorism, and that they lack of cybersecurity capacity

areas such as; an adequate knowledge and awareness of cybersecurity, cybersecurity strategies and policies, technical controls, and incident response capabilities.

Based on the research findings and analysis, a National Cybersecurity Capacity Building Framework (NCCBF) was constructed and evaluated, highlighting the key areas necessary for improving cybersecurity capacity of countries that are in a transitional phase.

Furthermore, the NCCBF was evaluated by a structured set of criteria conducted within focus groups with experts from different countries including those from countries that were in a transitional phase. The evaluation demonstrated the valuable contribution of the NCCBF's in representing the challenges in National Cybersecurity Capacity Building and the complexities associated in the build.

Table of Contents

Thesis Abstract....2

List of Figures....14

List of Tables....17

List of Abbreviations....20

Acknowledgment....22

Publications arising from this thesis....23

1. CHAPTER 1....24

1.1 Introduction....24

1.2 The Rationale of the Study....24

1.4 Research Questions....28

1.5 Aims and Objectives....29

1.6 Mapping the thesis....31

1.7 Chapter Summary....33

2. CHAPTER 2: LITERATURE REVIEW....34

2.1 Introduction....34

2.2 Cybersecurity Definition....34

2.3 Cyber Threats Landscape on National Security....35

2.4 Cybersecurity in Context (Spring Land)....43

2.4.1 Cyber Threat Impacts on Spring Land.....44

2.5 Global and Organisational Cybersecurity Frameworks.....45

2.5.1 The International Telecommunication Union (ITU) guide.....45

This guide focuses on the strategic pillars that typically assist nations to create coherent national and globally companionable programs for protecting critical infrastructure against cyber threats (Segura-Serrano 2015; ITU 2018b). .....46

2.5.2 The North Atlantic Treaty Organization (NATO) framework .....46

2.5.3 The European Union (EU) Guide .....47

2.5.4 The Organisation for Economic Co-operation and Development (OECD) Guide .48

2.7.5 National Institute of Standards and Technology (NIST) Cybersecurity Framework .....49

2.5.6 Microsoft Approach for Developing a National Cybersecurity Strategy .....50

2.5.7 The International Organization for Standardization (ISO 27032:2012) Guidance.50

2.5.9 Primarily Attributes of Global Selected Frameworks.....51

2.6 Cybersecurity Capability Maturity Models (CCMMs).....52

2.6.1 Cybersecurity Capability Maturity Model (C2M2) .....52

2.6.3 Cyber Resilience Review (CRR) Assessment Model.....53

2.6.4 Cybersecurity Capacity Maturity Model for Nations .....53

2.7 National Cybersecurity Strategies (NCSs) Case Studies.....54

2.7.1 The United Kingdom (UK) Cybersecurity Strategy .....55

2.7.2 Egypt Cybersecurity Strategy .....55

2.7.3 Turkey **Cybersecurity Strategy** .....56

2**.7.4 Primarily Attributes of Reviewed NCSs Case Studies** .....56

2.8 Cybersecurity Capacity Building (CCB) Dimensions from World Perspective.....57

2.8.1 Global Indices Models of Cybersecurity Capacity Building .....58

2.8.2 Dimensions of Cybersecurity Capacity Building (CCB).....65

2.9 Chapter Summary .....98

3. CHAPTER 3: RESEARCH METHODOLOGY .....101

3.1 Introduction.....101

3.2 Research Philosophy.....102

3.3 Research Approach .....104

3.4 Research Methodological Approaches .....106

3.5 Research Strategy and Design .....108

3.5.1 Research Strategy.....108

3.5.2 Research Design.....109

3.5.3 Data Collection Techniques.....115

3.6 Modelling Function IDEF0.....120

3.6.1 IDEF0 Diagrams .....123

3.7 Observe, Orient, Decide and Act (OODA) Model .....124

3.8 Constructing (Authoring) an IDEF0 template analysis .....126

3.8.1 Input statement template ..... 126

3.8.2 Dimensions and Functions statement template ..... 127

3.8.3 Mechanisms and Controls Template analysis ..... 128

3.8.4 Output template statements ..... 128

3.9 Research ethics ..... 131

3.10 Chapter summary: ..... 133

4. CHAPTER 4: CONTEXTUALISING THE PROBLEM SPACE IN SPRING LAND ..... 134

4.1 Introduction ..... 134

4.2 Research Goal ..... 134

4.3 Research Method ..... 135

4.3.1 Process and Participants ..... 136

4.3.2 Idea Writing technique ..... 138

4.3.3 Nominal Group Techniques (NGT) ..... 144

4.3.4 Interpretive Structural Modelling (ISM) ..... 149

4.5 Chapter Summary ..... 156

5. CHAPTER 5: ASSESSMENT OF NATIONAL CYBERSECURITY CAPACITY MATURITY LEVELS IN SPRING LAND ..... 158

5.1Introduction ..... 158

5.2 Research Goal ..... 158

5.3 Research Method ..... 159

5.3.1 Focus group ..... 159

5.3.2 Participants' profile ..... 159

5.4 Cybersecurity Capacity Maturity levels of Spring Land ..... 161

5.4.1 Cybersecurity Policy and Strategy Indicators ..... 161

5.4.2 Cyber Culture and Society Indicators ..... 164

5.4.3 Cybersecurity Education, Training and Skills Indicators ..... 167

5.4.4 Legal and Regulatory Frameworks Indicators ..... 168

5.4.5 Standards, Organisations, and Technologies Indicators ..... 169

5.5 Critical Reflection of Nation State Posture ..... 170

5.6 Chapter Summary ..... 177

6. CHAPTER 6: DEVELOPMENT OF THE NATIONAL CYBERSECURITY CAPACITY BUILDING FRAMEWORK (NCCBF) FOR COUNTRIES IN A TRANSITIONAL PHASE ..... 178

6.1 Introduction ..... 178

6.2 Designing and Developing the Framework (The Artefact) ..... 180

6.3 Developing OODA Activities into NCCBF Artefacts ..... 185

6.3.1 Observation phase (to the NCCBF Artefact) ..... 186

6.3.2 Orientation phase (to the NCCBF Artefact) ..... 188

6.3.3 Decision phase (to the NCCBF Artefact) ..... 190

6.3.4 Action phase (to the NCCBF Artefact).....191

6.4 Further development of the National Cybersecurity Capacity Building Dimensions based on OODA'S Loop utilising the Spring Land Case Study.....192

6.4.1 Dimension (D1): Build strategic capacity.....192

6.4.1.4 Action phase for dimension one (D1).....204

6.5 Development of the Other Dimensions of the National Cybersecurity Capacity Building (NCCBF).....205

6.5.1 Dimension (D2): Build Cyber culture and society capacity.....205

6.5.2 Dimension (D3): Build Cybersecurity Education, Training and skills.....207

6.5.3 Dimension (D4): Build legal and regulations capacity.....209

6.5.4 Dimension (D5): Build technical capacity.....211

6.6 Chapter Summary.....214

7. CHAPTER 7: EVALUATION OF THE FRAMEWORK.....216

7.1 Introduction.....217

7.2. Research Strategy.....217

7.2.1 Participants' profile.....218

7.3 Purpose and Objectives of the Evaluation.....222

7.4 Sessions' Plan.....222

7.5 Key findings from the Evaluation.....225

7.6 Modification to the framework.....228

7.7 Threats to Validity ..... 230

7.8 Chapter Summary ..... 230

8. CHAPTER 8: CONCLUSION AND FUTURE WORK ..... 231

8.1 Key findings and outcomes ..... 231

8.2 Research Contributions ..... 233

8.3 Strengths and Limitations of the Research ..... 234

8.4 Future work ..... 236

8.5 Conclusions ..... 237

8.6 Recommendations ..... 237

9. References ..... 242

10. Appendices ..... 263

# List of Figures

FIGURE 2.1 GLOBAL RISK MAP 2018 (WEFORUM 2018) ..... 38

FIGURE 2.2 CYBER-ATTACK MOTIVATIONS (PASSERI 2017). ..... 39

FIGURE 2.3 THE FIVE MANDATES AND THE SIX ELEMENTS OF THE CYBERSECURITY INCIDENT CYCLE (KLIMBURG 2012) ..... 47

FIGURE 2.4 COORDINATION BETWEEN EU AND NATIONAL AGENCIES (SABILLON ET AL. 2016) ..... 48

FIGURE 2.5 (NIST) CYBERSECURITY FRAMEWORK (NIST 2014A) ..... 50

FIGURE 2.6 NICE CYBERSECURITY COMPETENCY MODEL (NICE 2016) ..... 69

FIGURE 2.7 RISK INPUTS TO SENIOR DECISION-MAKERS ADAPTED FROM (ENISA 2013) ..... 75

FIGURE 2.8 NATIONAL-LEVEL RISK ASSESSMENT ADAPTED FROM (ENISA 2013) ..... 75

FIGURE 2.9 BASIC FRAMEWORK FOR A CYBER DOCTRINE (ORMROD AND TURNBULL 2016) ..... 80

FIGURE 2.10 NIST INCIDENT RESPONSE LIFE CYCLE (CICHONSKI ET AL. 2012) ..... 84

FIGURE 2.11 JOHNSON AND SCHOLES' CULTURAL WEB (JOHNSON AND WHITTINGTON 2009) ..... 87

FIGURE 2.12 AN EXAMPLE OF CYBERSEEK CAREER PATHS (CYBERSEEK 2016) ..... 91

FIGURE 2.13 THE KNOWLEDGE AREAS THAT ARE THE FOUNDATION OF THE DISCIPLINE OF CYBERSECURITY IN THE CYBOK FRAMEWORK (DCMS 2018). ..... 92

FIGURE 3.1 THE RESEARCH ONION (SAUNDERS ET AL. 2009) ..... 101

FIGURE 3.2 DESIGN SCIENCE RESEARCH CYCLES (HEVNER ET AL. 2004) ..... 110

FIGURE 3.3 DSR PROCESS INCLUDING INPUTS, ACTIVITIES, AND OUTPUTS ADAPTED FORM (JOHANNESSON AND PERJONS 2014) ..... 112

FIGURE 3.4 A GENERIC IDEF0 DIAGRAM (IDEF0 1993) ..... 123

FIGURE 3.5 DECOMPOSITION STRUCTURE OF IDEF0 ..... 124

FIGURE 3.6 THE OODA LOOP (GRAY ET AL. 2015) ..... 125

FIGURE 4.1: ILLUSTRATION DIMENSION FRAMEWORK (GCSCC 2017) ..... 135

FIGURE 4.2 INTERPRETIVE STRUCTURAL MODEL ..... 150

FIGURE 5.1 RESULTS OF ALL CCMM DIMENSIONS ..... 177

FIGURE 6.1 THE FIVE DIMENSIONS OF NCCBF ..... 179

FIGURE 6.2 GENERIC NCCBF IMPLEMENTATION USING OODA LOOP ..... 181

FIGURE 6.3 DETAILED NCCBF IMPLEMENTATION USING OODA LOOP ..... 184

FIGURE 6.4 DEMONSTRATION OF THE NCCBF TOP-LEVEL WITHIN THE OODA LOOP ..... 185

FIGURE 6.5 ADAPTIVE OBSERVE PHASE OF THE NCCBF MODEL DEVELOPMENT ..... 187

FIGURE 6.6 ADAPTIVE ORIENTATION PHASE OF THE NCCBF MODEL DEVELOPMENT ..... 189

FIGURE 6.7 ADAPTIVE DECISION PHASE OF THE NCCBF MODEL DEVELOPMENT ..... 190

FIGURE 6.8 THE ADAPTIVE ACTION PHASE OF THE NCCBF MODEL DEVELOPMENT ..... 192

FIGURE 6.9 TOP-LEVEL ACTIVITY FOR D1 ..... 193

FIGURE 6.10: AN IDEF0 REPRESENTATION FOR DIMENSION 1 ..... 204

FIGURE 6.11: TOP-LEVEL OF D2 ..... 206

FIGURE 6.12 : AN IDEF0 REPRESENTATION FOR DIMENSION 2 ..... 207

FIGURE 6.13 : THE TOP LEVEL ACTIVITY (D3) ..... 208

FIGURE 6.14 : AN IDEF0 REPRESENTATION FOR DIMENSION 3 ..... 209

FIGURE 6.15 : THE TOP LEVEL ACTIVITY (D4) ..... 210

FIGURE 6.16 : AN IDEF0 REPRESENTATION FOR DIMENSION 4 ..... 211

FIGURE 6.17 : THE TOP LEVEL FOR DIMENSION 5 ..... 212

FIGURE 6.18: AN IDEF0 REPRESENTATION FOR DIMENSION 5 ..... 213

FIGURE 6.19 : THE NCCBF ACTIVITIES ..... 214

FIGURE 7.1 : PROTOCOL FOR EVALUATION SESSIONS ..... 223

FIGURE 8.1: THE SCOPE OF THE RESEARCH ..... 235

# List of Tables

TABLE 1.1 MAPPING THE OBJECTIVES WITH RESEARCH QUESTIONS AND THESIS CHAPTERS 31

TABLE 2.1 GLOBAL CCB MODELS (ITU 2017B) 62

TABLE 2.2 MAPPING CCMM DIMENSION WITH GCI PILLARS. 65

TABLE 2.3 EXAMPLE: CRITICALITY SCALE FOR NATIONAL INFRASTRUCTURE (CABINETOFFICE 2010) 73

TABLE 2.4 EXAMPLES OF RISK ASSESSMENT AND MANAGEMENT METHODS (NCSC 2016) 78

TABLE 3.1 RESEARCH PHILOSOPHIES AND DATA COLLECTION METHODS (DUDOVSKIY 2016) 104

TABLE 3.2 DIFFERENCES BETWEEN DEDUCTIVE AND INDUCTIVE APPROACHES (SAUNDERS ET AL. 2009, P.126) 106

TABLE 3.3 A SNAPSHOT TOWARDS THE TYPE OF DATA COLLECTION TECHNIQUE ADOPTED FOR EACH OBJECTIVE 119

TABLE 3.4 INPUT TEMPLATE STATEMENT 127

TABLE 3.5 FUNCTIONS STATEMENT TEMPLATE 128

TABLE 3.6 MECHANISMS AND CONTROLS TEMPLATE ANALYSIS 128

TABLE 3.7 OUTPUT TEMPLATE STATEMENTS 130

TABLE 4.1 IM PARTICIPANTS DETAILS 138

TABLE 4.2 INTERACTIVE MANAGEMENT QUESTION SET 140

TABLE 4.3 LIST OF CCB CHALLENGES IN SPRING LAND 142

TABLE 4.4 CATEGORISATION OF IDEA 143

TABLE 4.5 LIST OF OBJECTIVES 146

TABLE 4.6 PARTICIPANT'S RANKING OF OBJECTIVES 148

TABLE 4.7 RESULTS OF THE IMPORTANT OBJECTIVES 149

TABLE 4.8 ADJACENT MATRIX 152

TABLE 4.9 LIST OF TOP THREE FUNCTIONS 155

TABLE 5.1 FOCUS GROUP PARTICIPANTS'DETAILS 160

TABLE 5.2 EXAMPLE OF MULTI-DIMENSIONAL NATIONAL CYBERSECURITY QUESTION SET FOR THE REVIEW OF THE SPRING LAND SECURITY POSTURE 161

TABLE 5.3 GCI INDEX 2017, 2018 SPRING LAND RESULTS 171

TABLE 5.4 MAPPING FOCUS GROUP RESULTS WITH GCI REPORTS RESULT 173

TABLE 5.5 MATURITY LEVELS OF ALL DIMENSIONS OF SPRING LAND CYBERSECURITY CAPACITY 176

TABLE 6.1 CHALLENGES OF CYBERSECURITY CAPACITY OF D1 194

TABLE 6.2 MATURITY LEVELS INDICATORS FOR D1 195

TABLE 6.3: LIST OF FUNCTIONS USED IN D1 197

TABLE 6.4:LIST OF MECHANISMS AND CONTROLS FOR D1 203

TABLE 6.5 : FUNCTIONS LIST OF DIMENSION TWO (D2) 206

TABLE 6.6 : FUNCTIONS LIST OF DIMENSION THREE (D3) 208

TABLE 6.7 : FUNCTIONS LIST OF DIMENSION FOUR (D4) 210

TABLE 6.8 : FUNCTIONS LIST OF DIMENSION FIVE (D5) 212

TABLE 7.1: PARTICIPANTS DETAILS IN THE EVALUATION STUDY 221

TABLE 7.2 : THE EVALUATION QUESTIONS 224

TABLE 7.3 : KEY FINDINGS FROM THE EVALUATION 227

## List of Abbreviations

| | |
|---|---|
| 4Ps | Pursue, Prevent, Protect and Prepare |
| APTs | Advanced Persistent Threats |
| C2M2 | Cybersecurity Capability Maturity Model |
| CERT | Computer Emergency and Response Team |
| CCMM | Cybersecurity Capacity Maturity Model |
| CERT- RMM | CERT -Resilience Management Model |
| CRR | Cyber Resilience Review Assessment Model |
| CCMMs | Cybersecurity Capability Maturity models |
| COP | Common Operational Picture |
| CSDP | Common Security and Defence Policy |
| CIIs | Critical Information Infrastructure |
| DHS | Department of National security |
| DSR | Design Science Research |
| DIME | Diplomatic, Information, Military and Economic |
| DDoS | Distributed Denial of Service |
| EU | European Union |
| ENISA | European Union Agency for Network and Information Security |
| GCHQ's | Government Communications Headquarters |
| GCI | Global Cybersecurity Index |
| GCA | Global Cybersecurity Agenda |
| GCSCC | Global Cybersecurity Capacity Centre in University of Oxford |
| GPTC | General Post and Telecom Company |
| HCI | Human–Computer Interaction |
| IA | Information Assurance |
| ICTs | Information and communication technologies |

IDEF0 Icam DEFinition for Function Modelling

IM Interactive Management

ISM Interpretive Structural Model

ISO the International Organization for Standardization

IT Information Technology

ITU International Telecommunication Union

IW Idea Writing

LPTIC Spring Land Post, Telecommunication and Information Technology Company

LTT Spring Land Telecommunication and Technology

MCIT the Ministry of Communications and Information Technology of Egypt

MENA The Middle East and North Africa region

NATO the North Atlantic Treaty Organization

NCA National Crime Agency

NCSC National Cybersecurity Centre

NGT Nominal Group Techniques

NCSA National Information Security and Safety Authority

NIST National Institute of Standards and Technology

OECD The Organisation for Economic Co-operation and Development

OODA

NCCBF National Cybersecurity Capacity Building Framework

SMART Specific, Measurable, Attainable, Realistic, Timely

SoS System of Systems

UN United Nation

## Acknowledgment

I would like to sincerely thank almighty Allah (God), for His richest grace and mercy for the accomplishment of this thesis.

This thesis is dedicated to the beloved soul of my father Altaher and my lovely son Shahein who died before completing my research with my sincere thankfulness to them, for their great role in my life and their numerous sacrifices for me.

I would like to thank my supervisors' team, Dr. Huseyin Dogan, Dr. Edward Apeh, and Professor Raian Ali for their guidance and encouragements during this research. In addition, I would love to thank my ex-supervisor Dr. Christopher Richardson for expert guidance, insightful discussions, and valuable feedback during my research.

A special thank you enclosed with love to my beloved wife Eman and my lovely son Shehab Edien for their patience and support and for being a source of inspiration during my PhD study. Eman has been a constant source of love, strength, and encouragement. Without you, this end will not be easily accomplished. I am grateful also to my mother for her spiritual prayers and wishes to succeed in my study.

Last but not least, I would like to express my deepest gratitude to my brothers, my sisters, my mother and father- in- law, and my friends for their role in encouraging me to finish this piece of work.

Mohamed Ben Naseir

25/07/2020

# Publications arising from this thesis

1. Ben Naseir M.A., Dogan H., Apeh E., Richardson C., Ali R. (2019) Contextualising the National Cyber Security Capacity in an Unstable Environment: A Spring Land Case Study. In: Rocha Á., Adeli H., Reis L., Costanzo S. (eds) New Knowledge in Information Systems and Technologies. WorldCIST'19 2019. Advances in Intelligent Systems and Computing, vol 930. Springer, Cham.
2. Ben Naseir, M.; Dogan, H.; Apeh, E. and Ali, R. (2020). National Cybersecurity Capacity Building Framework for Countries in a Transitional Phase. In Proceedings of the 22nd International Conference on Enterprise Information Systems - Volume 2: ICEIS, ISBN 978-989-758-423-7, pages 841-849. DOI: 10.5220/0009576708410849

# 1. CHAPTER 1 i

## 1.1 Introduction

This chapter presents the motivation for undertaking research on developing a National Cybersecurity Capacity Building Framework (NCCBF) for *countries in transitional phase,* in particular, by using Spring Land as a case study. This chapter outlines and explains the details of the research, its objectives, and the research questions whilst further providing details on the scope, rational of this research study and an overview of its innovation and impact of this research.

## 1.2 The Rationale of the Study

Over decades, the global cybersecurity environment has been characterised by several security insufficiencies, which have been defined as government's inability to meet their national security obligations. Consequentially, security failures can lead to state instability. Unstable and countries in a transition phase often demonstrate dramatic clear examples of unsuccessful governance and public supervision failure (DeRouen Jr et al. 2012). Generally, an unstable country or those in a transition state are characterised by civil war; political and economic upheaval; the absence of law and the lack of a reliable body representing the state beyond its borders at the inter-national level.

Transition phase refers to the intermediate phase that begins with the dissolution of an old regime and ends with the establishment of a new one (Guo and Stradiotto 2014). There are a number of factors affecting the success or failure of transition stage. These factors include, the type of regime prior to the transition stage, the characteristics of the new leader of the transitional government and the influence of information and communication technologies (ICT) (Strachan and Anna 2017). For example, we have witnessed the "Arab Spring" states and their reoccurring transitions. These transitioning states have tentatively gained independence but lack stability towards national solidarity and good governance. It is possible for a group of people with tacit experience to organise these states and lead them to stability (Kaplan, 2012). According to Mohamed and Abdulmajid H (2017) *"these states are historically less developed and lack even basic infrastructure despite the huge*

*wealth generated out of it. This problem is witnessed by the current drastic disruption of oil production and its logistics along the areas involved in the conflict. In other words, we regard the lack of socio-economic development as the root cause of the continuing violent, political conflict"*.

Many countries with poor infrastructure and poor governance are rapidly starting to establish their presence in the cyberspace, the 5th Domain of modern warfare (Richardson 2012). The impact of expanding non-secure ICT infrastructure in these nations also threatens the global community and many economically stronger nations (Garlock 2018). As globally, connected networks facilitate rapid globalisation they also enable cybercriminals to freely operate across borders. Many of developing or those in a transition state attract global attention as the major source of cyber-attacks, with the insecure ICT infrastructure being used as an instrument for committing international cybercrime (Kshetri 2019). Recent study from Business Software Alliance, two countries with the world's highest software piracy rates in 2017 were from developing nations: Libya now referred as Spring Land in this Thesis and Zimbabwe. The proportions of unlicensed software in the two countries were 90% and 89% respectively. Since pirated software products cannot take advantage of updates from manufacturers, they accelerate the spread of malware (Kshetri 2019). Spring Land considered as one of countries in a transition stage due to political and armed conflict after the socio-political storm named Arab Spring.

The increased prevalence cyber-attacks and cybercrime in these countries can be credited to defenceless systems and their lack of cybersecurity practices (Kshetri, 2019). One more problem is linked to the lack of skills among Internet users to protect themselves from rapidly escalating cyber-threats and with most people inexperienced and not technically savvy. A majority of users in these countries also lack English language, a key component of coding and technical standards (Kshetri 2019).

The situation in developing and countries in transitional phase is more complicated and needs bigger attention due to the absence of local expertise and limited resources. As many these nations increase reliance on ICT to enable economic growth, they fail to commit an equivalent level of investment into cybersecurity. There is little clarification given regarding what the appropriate required level is based upon risk and resources (Pawlak 2014). The use of Cyberspace and Information Communication Technologies in developing countries and

those countries in a transitional phase has grown significantly over recent years. This growth has been accompanied by particularly increased susceptibility to cyber-attacks (Brechbühl et al. 2010).

Building cybersecurity capacity has become increasingly a subject of global concern in both stable countries and those countries in a transitional phase. National and international Research & Technology Organisations (RTOs) have developed a plethora of guidelines and frameworks to help with the development of a national cybersecurity framework (Hameed et al. 2018). Although extensive research has been carried out on CCB, to our knowledge no other single study exists which focuses on countries in a transitional phase. In addition, there are presently no other published research linking existing frameworks and initiatives with benchmarking models, and thus this effort from the CCMM is presented (Hameed et al. 2018).

Therefore, this research hypothesis that, there is a demonstrable gap (an extensive and vibrant chasm!) between the assurance of a stable, self-assured State that adheres to ISO Standards, Policies, Procedures and Good Practice, underpinned by security technologies, training and skills as opposed by States in a transitional phase that exhibit little Governance, Risk Management and Compliance of their 5$^{th}$ Domain -Cyberspace.

Can a collaborative research study bridge this gap?

Will building cybersecurity capacity to States in a transitional phase, be grounded in conducting, evaluating, and building a reliable National Cybersecurity Capacity Building Framework (NCCBF)?

Recently, researches have shown that comprehensive frameworks to cybersecurity are highly problematic around the world (Oltramari et al. 2014; Donaldson et al. 2015). Although there are many efforts undertaken at national and international level, building capacities of individual countries in cybersecurity remains a challenge and facing various problems such as lack of strategy, duplication of initiatives and cyber capacity gap between favored and neglected countries includes countries in a transitional phase (Pawlak et al. 2017; Hameed et al. 2018). Pawlak et al. (2017), identified that when development communities decides to get involved with Cybersecurity Capacity Building (CCB), they often lack security expertise

,methodological toolkits and know-how to tackle cyber related crime. There is also the 'dual-use challenge' of cybersecurity according to Hohmann et al. (2017) where they articulated highlighted that, cybersecurity capabilities and technologies can hypothetically be used harmfully to increase surveillance and social control and to empower repressive governments as well as cyberwarfare, espionage and cybercrime.

This double-edged phenomenon is supported by Muller (2015) who argued that, methods to date have not managed to cover Cybersecurity Capacity Building (CCB) as a whole on a global scale or else they argue for CCB, but without indicating how to go about implementing it. Some approaches set out a scope that is either too broad or too narrow, while others focus on different ways of highlighting the problems that come with increased access to cyberspace, but without indicating solutions (Muller 2015).

The hypothetical gap presents an opportunity for exploring current global trends in CCB efforts and identifying the principles for successful CCB framework. This research study aims to bridge this gap by collecting and analysing a variety of existing standards, guidelines, and practices and link it with well-known benchmarking model the Cybersecurity Capacity Maturity Model (CCMM). The output of the study proposes a National Cybersecurity Capacity Building Framework (NCCBF) for countries in a transitional phase using Spring Land as a case study. Spring Land is a fictional name given to a country to provide a case study. The NCCBF progress is guided and managed by utilising modelling approaches.

The choice of Spring Land for this research was justified by several facts and it was decided to use Spring Land as a metaphor to a country in a transitional state rather than the real state of Libya. Firstly, Spring Land is in the transitional phase with an unstable environment, which set Spring Land critical infrastructure under Advanced Persistent Threats (APTs) and the associated threats of Cyber space. Secondly, Spring Land is in early stages of adopting the use of the online services platform. Thirdly, Spring Land does not have a cogent National Cybersecurity framework (ITU 2015). Fourthly, existing literature concentrates on the challenges and factors of adopting e-services in Spring Land only, e.g., e-government (Sweisi 2010; Seema et al. 2012; Ahmed et al. 2013; Abuzawayda 2016; Darbok 2016), e-banking (Farag and Hilles; Elgahwash et al. 2014; MTMC 2016; Ward et al. 2017), e-commerce (Moftah et al. 2012; NISSA 2013; GCSCC 2017) and e-learning (Kitzinger 1995a; Warfield

et al. 2002; Gill et al. 2008; Goldman 2010; Herrington and Aldrich 2013; DOE 2014; Hult and Sivanesan 2014).

Hence, no scholarly research has currently been completed on Spring Land's posture to implementing appropriate Cybersecurity Capacity Building frameworks. In addition, there are no studies addressing the factors that influence the development of a National Cybersecurity Capacity Building Framework NCCBF in a chaos ecosystem. Finally, access to the information and collected data is more straightforward, as the researcher is a Libyan citizen and sponsored by the Libyan government. Thus, this research seeks to create a framework for countries in a transition stage against stable threats that will contribute to the protection of the metaphorical Spring Land critical infrastructure. This Research Study will further comprise of a social technical analysis (e.g. using Interactive Management Technique) and Focus Group discussion to contextualize and assess the Spring Land problem space. This contextualisation analyses the Cybersecurity capacity of the state by applying a modified version of the Cybersecurity Capacity Maturity Model for Nations Model (CCMM) - V1.2. The original model had been designed by Global Cybersecurity Capacity Centre, University of Oxford (GCSCC 2017).

## 1.4 Research Questions

This PhD research will question, how protected data within situations in countries in a transitional phase is under Advanced Persistent Threats (APTs), and the associated challenges of Cybersecurity. The impact of E-government, e-banking and e-commerce are currently being analysed in depth, but there is yet to be a coherent proposal for a resolution to effectively protect the metaphorical Spring Land information infrastructure, and for all intents and purposes, the Spring Land government itself.

The research proposition is to develop a National Cybersecurity Capacity Building Framework (NCCBF) as an outcome for countries in a transitional phase, the assurance and exploitation of its capabilities within the 5$^{th}$ Domain - Cyberspace. This research study will comprise of a Social-Technical Analysis (e.g. using soft systems) that builds conceptual models to determine and contextualise the hypothetical problem space. To achieve this research aim and provide an outcome to the study's hypothesis a number of objectives have evolved from the following research questions:

The main question is*: How can we develop a National Cybersecurity Capacity Building Framework that supports the National Security for countries in a transitional phase?*

In order to validate and resolve the challenge of the main research question, further analytical questions developed the notions posed in the main question.

Q1- What are the known challenges in delivering effective Cybersecurity Capacity Building Platform?

Q2- What are the key elements of a successful Cybersecurity Capacity Building Framework and consequentially what are the possible modelling approaches for better and effective guiding Cybersecurity Capacity Building Framework?

Q3- What are the current issues of cybersecurity capacity within a metaphorical Spring Land and what would be done to address cybersecurity across Spring Land?

Q4- How do we measure the current maturity levels of cybersecurity capacity in a metaphorical Spring Land?

Q5- How to translate the finding of Q2, Q3 and Q4 into a transformative design method which could help to develop a National Cybersecurity Capacity Building Framework (NCCBF) for countries in a transitional phase?

## 1.5 Aims and Objectives

The aim of this research is to develop a National Cybersecurity Capacity Building Framework (NCCBF) for countries in a transitional phase using Spring Land as a case study to ensure and exploit its capabilities. This will comprise of two qualitative studies such as Interactive Management (IM) and Focus groups to assess and contextualise the Spring Land problem space. To achieve this research aim, fives objectives are formulated using the acronymic SMART (Specific, Measurable, Attainable, Realistic, Timely) criteria:

**Objective 1** – (S) To investigate a state of the art cybersecurity frameworks and cybersecurity capacity building frameworks, with a view to challenges, key elements of a successful Cybersecurity Capacity Building Framework and possible modelling approaches for better and effective guiding Cybersecurity Capacity Building Framework. (M) The

performance of this investigation will be measured by the quality of the research and use of its literature review and supporting references. (A) This objective will be attained by a comprehensive literature review. (R) The realistic outcome of State of Art will reinforce the suspension that the Cybersecurity Capacity Building Frameworks is wholly inadequate to resist APTs. (T) the literature review should be finished within 4 years.

**Objective 2** – (S) To contextualise the problem space that is centred on the current Spring Land National security state. (M) The contextualisation will analyse the security operations of the state by the use of qualitative approach called Interactive Management. The outputs are to be aligned with the Cybersecurity capability and risk of current defences. (A) The contextualisation will be enhanced through a risk impact analysis and based on the CCMM for nations. (R) This will feed into requirement analysis for NCCBF and the possibility to organise and test the Spring Land Cyber Defence. (T) This objective is will be completed by 2018.

**Objective 3** – (S) To assess the current maturity levels of cybersecurity capacity in Spring Land. (M) The evaluations will analyse the maturity levels of the Spring Land cybersecurity capacity of the state by the use of focus group discussion. The outputs are determining areas of capability that are required by the Spring Land Government in order to improve cybersecurity capacity of the state. (A) The assessment will be enhanced based on the CCMM for nations. (R) This will feed into requirement analysis for NCCBF and the possibility to organise and test the Spring Land Cyber Defence. (T) This objective is will be completed by 2018.

**Objective 4** – (S) To develop the NCCBF framework. (M) The NCCBF will be managed and guided by modelling functions techniques. (A) The framework will be attained through acceptance of NCCBF in the Spring Land National Defence. (R) Realistically NCCBF will be developed for National Security. (T) This will be ready by 2019.

**Objective 5** - (S) To evaluate the NCCBF for countries in a transitional stage. (M) The NCCBF will be evaluated against a set of criteria (Completeness, Correctness, Acceptability and the Overall Evaluation of the framework. (A) The NCCBF will be evaluated by conducting a focus group with experts from different countries including experts from countries that in transitional phase. (R) Realistically an enhanced NCCBF for countries in

transitional stage will be developed. (T) The evaluation will be completed by 2020.These objectives are mapping with the research questions and thesis chapters and presented in Table 1.1.

| Research Objectives | Research Question | Chapters |
|---|---|---|
| Objective 1 | Q1- What are the known challenges in delivering effective Cybersecurity Capacity Building Platform?<br>Q2- What are the key elements of a successful Cybersecurity Capacity Building Framework and consequentially what are the possible modelling approaches for better and effective guiding Cybersecurity Capacity Building Framework? | Chapter 2 |
| Objective 2 | Q3- What are the current issues of cybersecurity capacity within a metaphorical Spring Land and what would be done to address cybersecurity across Spring Land? | Chapter 4 |
| Objective 3 | Q4- How do we measure the current maturity levels of cybersecurity capacity in a metaphorical Spring Land? | Chapter 5 |
| Objective 4<br>Objective 5 | Q5- How to translate the finding of Q2, Q3 and Q4 into a transformative design method which could help to develop a National Cybersecurity Capacity Building Framework (NCCBF) for countries in a transitional phase? | Chapter 6 and Chapter 7 |

Table 1.1 Mapping the objectives with research questions and thesis chapters

## 1.6 Mapping the thesis

This thesis consists of eight chapters. The first chapter has outlined the scale of the study, explains the details of the research objectives and the research questions. Furthermore, provides details on the scope, rational of the study.

***Chapter 2*** addresses the background of this multi-disciplinary research from literature. The chapter articulates definitions, facts and theories associated with the related disciplines. A special attention was given to Global Cybersecurity Capacity Frameworks and Global and Organisational Cybersecurity frameworks. Additionally, deliberate the Cybersecurity Maturity Models that are used to identify the Cybersecurity capacity maturity levels. In

additional, IDEF0 function model and Observe, Orient, Decide, Act model are discussed in this chapter.

***Chapter 3*** details the methodology and research design along with the instruments of data collection methods used in the study. It explains all research methods used within this research, which include two qualitative methods (focus group and interactive management). Additionally, provides brief details about the development of the framework using a Design Science Research methodology (DSR) and modelling functions technique (IDEF0). Data analysis, Ethical considerations and evaluation of the proposed framework are also presented.

***Chapter 4*** explores qualitative findings and delivers a contextualisation of Spring Lands' current situation based on the CCMM. This chapter also presents the set of objectives derived from the IM approach that employed to support the management of a national cybersecurity capacity.

***Chapter 5*** explores qualitative findings of focus group and delivers an assessment of Spring Lands' current NCB maturity levels based on the CCMM.

***Chapter 6*** describes the development of the proposed NCCBF framework. The framework consists of five main dimensions which represent the outcome of literature review and based on CCMM. These dimensions are: build strategic capacity; build cyber cultural and society capacity; build cybersecurity Education, Training and skills capacity; build legal and regulations capacity and build technical capacities. These dimensions are decomposed to three activities used to improve the capacity of each dimension. These activities are representing using IDEF0 modelling function.

***Chapter 7*** highlights a critical phase of this research where the framework and its associated activities are evaluated and validated by conducting a focus group with experts from different countries including experts from countries that in transitional phase. The evaluation has been done against set of requirements and questions about the completeness, the correctness, and the acceptability of the framework.

***Chapter 8*** draws the research to conclusion by recapitulating and discussing the research outcomes with research questions, reflecting on the strengths and weakness of the research, and the directions of the future research.

## 1.7 Chapter Summary

Building cybersecurity capacity has become increasingly a subject of global concern in both stable countries and those countries in a transitional phase. This chapter presented an introduction to topics related to the area focus of this thesis and its hypothesis. The research aims to develop a National Cybersecurity Capacity Building Framework for countries in transitional phase. A set of five SMART objectives were defined to be achieved by this research as well as five questions to be answered through Investigation. The outcome of a designed, developed and validated framework is proposed as the main contribution to knowledge amongst the critical thoughts and models expressed in this thesis..

# 2. CHAPTER 2: LITERATURE REVIEW

## **2.1** Introduction

This chapter provides a review of literature in key areas related to the present study. These include national security perspectives to the 5th Domain - Cyberspace; Cyber threats impact on National Security; Cybersecurity in the context of (Spring Land); Cybersecurity Threats impact on Spring Land National Security; Models of Cybersecurity Capacity Building; Global and Organisational Cybersecurity frameworks; overview of national Cybersecurity strategies in a further three selected countries.

## **2.2** Cybersecurity Definition

Security is usually the state of free from, or degree of defence against, risks, harm, failure or attacks. Security is "a type of protection where a distinction is established between the assets and the hazard" (Herzog 2010). In other words, security is about safeguard of assets from numerous threats posed by certain inherent vulnerabilities (ISO27002 2005; Von Solms and Van Niekerk 2013). Ullman in the 1980s has defined security as " An action or sequence of events that (1) threatens drastically and over a relative brief span of time to degrade the quality of life for the inhabitants of a state, or (2) threatens significantly to narrow the range of policy choices available to the government of a state, or to private, nongovernmental entities (persons, groups, corporations) within the state" (Ullman 1983).

Over the last decades, the global security (Physical, Personnel and Information) threats are continuing to evolve and spread across our hyperconnected world, irrespective of any international borders, in both their elaboration and scale of impact (Richardson 2012). Modern cyberspace is an intertwined domain of public, government, and private companies, all of which utilise its affordances to operate and communicate in daily life. The growing dependency on extant information and communication infrastructures makes them particularly attractive to cyber-attackers (Choo 2011).

The persistent challenge to national security in the 5th Domain (Shashi 2016) is exacerbated by an ever-escalating threat landscape and the growing attack surfaces that represent State

Critical Infrastructures. According to Klimburg (2012) in the past two decades, around 50 countries have become concerned with cyberspace, cybercrime and cybersecurity.

The concept of cybersecurity ranges from national to international organisations to scholars, based on their needs, viewpoints, goals and the environment. For instance, the International Telecommunication Union (ITU) defined cybersecurity as: the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisations and user's assets. Organisations and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Meanwhile, ENISA declared "there is no universally accepted not straightforward definition of cybersecurity (ENISA 2016). This view is supported Dunn (2005) by who writes that "there is no generally accepted definition of cybersecurity, and several different terms are in use that have related meanings, such as information assurance, information or data security, critical information infrastructure protection".

## 2.3 Cyber Threats Landscape on National Security

The threat from the 5$^{th}$ Domain cyberspace to national security is viewed as a potential interruption to a common way of life, one built on information technology and vital infrastructure services, with very little direct human interest (Cavelty 2014). For most of the countries, the potential risks and threats posed to the cyberspace revolve around organised cybercrimes, state- sponsored attacks, cyber terrorism, unauthorised access to and interception of digital information, electronic forgery, vandalism and extortion etc (Shafqat and Masood 2016). Cyber threats are regarded as a form of hybrid threat that has only relatively recently emerged and has subsequently received considerable attention from various parties. Cyber threats are sometimes referred to as cyber warfare and they present challenges in the fifth domain of warfare when they entail prolonged and concerted attempts to attack the digital systems of a foreign territory. This can result in widespread disruption to the network of that country, possibly involving the use of malware and spam.

What distinguishes these cyber warfare attacks from conventional cybercrime is the extent and veracity of their operations. In cyber warfare, 'success' entails not only denying the

operation of IT infrastructure and the associated disturbance but also defacement and deception for political purposes rather than monetary gain (e.g. fraud) (Bachmann and Dov 2012).

This is a relatively new form of conflict that occurs in the fifth domain, posing hybrid threats requiring innovative, holistic countermeasures spanning counter intelligence, counter cybersecurity and law enforcement to ensure a dynamic response when required (Bachmann and Gunneriusson 2014). Hoffman (2010) states that hybrid threats are those posed by an adversary that entail the simultaneous deployment of conventional weapons, terrorism, haphazard tactics and criminal behaviour in an attempt to realise political objectives. The Arab Spring uprisings that gripped several countries across the Maghreb and the Middle East during 2010 and 2011 provide an excellent example of how cyberspace can present threats capable of shifting the political landscape. A range of hybrid threats resulted during this period including widespread civil unrest, the proliferation of advanced weaponry, failed states, regional extremism and weapons of mass destruction (Bachmann and Dov 2012).

Previously, the World Wide Web was merely an e-commerce outlet, whereas nowadays it is entrenched in the dissemination of critical information infrastructure (Singer and Friedman 2014). Fred (2015) states that the broader scope of Internet usage has added a new field of warfare after mainland, sea, air, and space domain. More recent global attention has focused on the provision of safeguarding strategies for enhancing critical infrastructures. Razzaq et al. (2014) warn that with the growing use of World Wide Web, users started storing and sharing a lot of data and information, however the web applications used for data storing are very vulnerable to cyber-attacks and therefore unsafe.

In the USA, President Obama said, "*Our Nation's critical infrastructure is central to our security and essential to our economy. Technology, energy, and information systems play a pivotal role in our lives today, and people continue to rely on the physical structures that surround us*" (Obama 2015). Obama stressed that, we must remain vigilant and ensure resilience of our complex critical infrastructure systems whether physical or cyber by mitigating the threats and stresses that can weaken them (Obama 2015).

From the European perspective, the EU has taken into account the significance of Critical Information Infrastructure (CIIs). Roman et al. (2007) pointed out in their study, CIIs include

energy, banking, transportation and these constitute the prosperity of many spheres such as economy, security and standards of living. Said organisation has sought to solidify the CII cyber situation awareness and neutralise terrorist cells, as well as serious and organised crime syndicates (Argomaniz 2015). Nowadays, one of the core methods, which aid terrorist's prosperity, is based on the aggressive application of information and communication technologies (ICTs) in a virtual space (Sahyoun 2015).

World Economic Forum (WEF) issues annually Global Risks reports which identifies the most serious and vital risks that the world faces. The analysis of Global Risks reports helps place the global risk landscape into context and point out which areas should be ready either for some action or protection. According to the Global Risks report from 2007 shows that highest risk in that year was the breakdown of critical information infrastructure. Such breakdown may have a detrimental effect on large part of the population. In 2012 and 2014 cyber-attacks were considered fairly serious and posed danger to the society. However, according to the Global Risks in Terms of Likelihood issued for year 2018, cyber attacks and data fraud or theft appeared on 3rd and 4th place. This shows the increasing risk of misusing the cyber space and also higher cyber crime. Furthermore, The Global Risks report from 2015 addressed the risks of increasing cyber attacks and the need for better privacy protection and prevention against cyber crime. The 2018 Global Risks Interconnections Map in Figure (2.1) shows that Data fraud and theft is directly linked to cyberattacks, which are a linkage to Terrorist Attacks and Failure of critical infrastructure (Weforum 2018). When considering the view of Figure (2.1), it is vital that interconnecting systems work within a coherent protocol so they are not subject to breach from dangerous sources. This will maintain essential interoperability and minimise potential inefficiency and ambiguity as information sharing is processed (Richardson 2012).

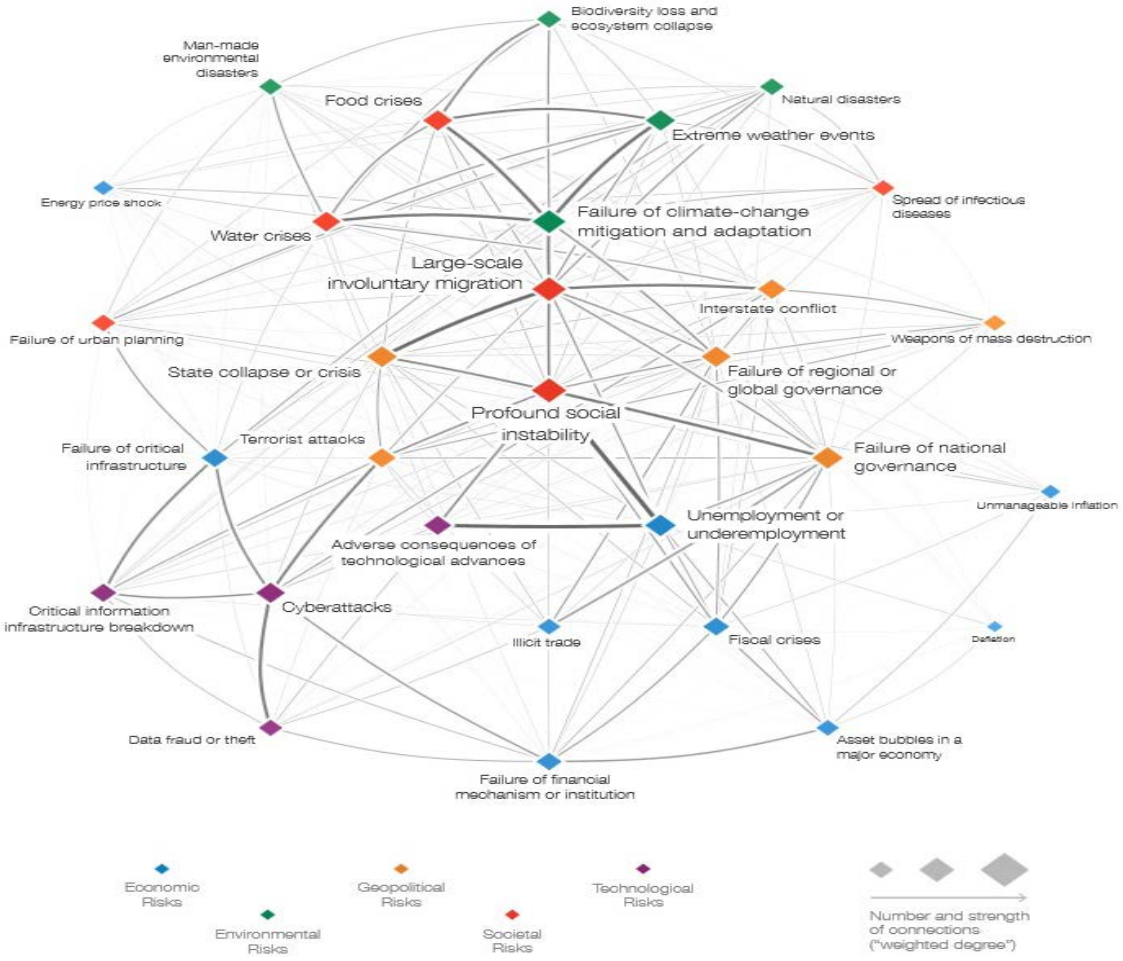



Figure 2.1 Global Risk Map 2018 (Weforum 2018)

Today, cyberspace has become an intertwined domain which public, government and private companies utilise to operate and communicate in daily life. The growing dependence on the national information and communication infrastructures (ICT) make these infrastructures particularly susceptible to cyber-attacks (Choo 2011). Furthermore, this growth has been accompanied by an increase in the number of malicious attackers who pursue to conduct all types of nefarious deeds in cyberspace (Jasper and Wirtz 2017). For instance, the majority of cybersecurity issues today comprise of e-mail spam, malware, phishing, and denial of service attack. Razzaq et al. (2014) differentiate three main types of cybercrimes: Cybercrimes against persons, cybercrimes against all forms of property, cybercrimes against Government. The threats in cyberspace can be criminals, hackers, terrorists, and nation-states. Cyberattacks cause great damage to national security and hit major harm on the world economy (Hipp 2017). As illustrated in Figure (2.2), the motivation behind most attacks in 2017 were cybercrime, hacktivism, cyber espionage, and cyber warfare (Passeri 2017).

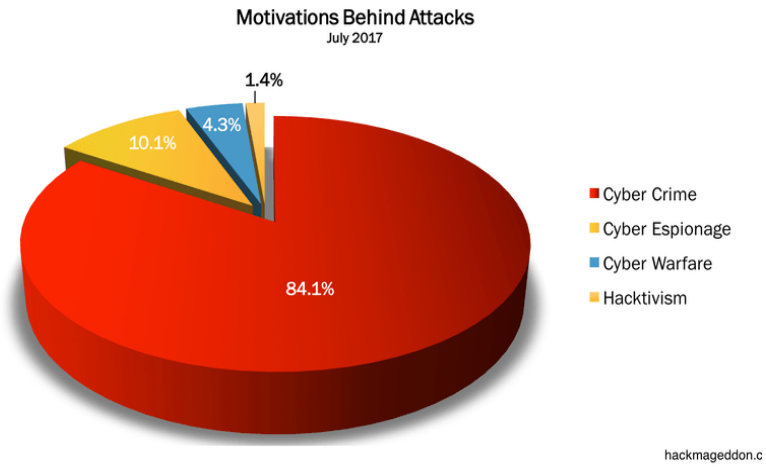



Figure 2.2 Cyber-attack motivations (Passeri 2017).

According to Gordon and Ford (2006) despite the fact that cybercrime is a widely used term, it is rather challenging to find a fitting definition. For instance, The Council of Europe's Cybercrime Treaty describes this phenomenon as offences that vary from ‘criminal activity against data to content and copyright infringement (Krone 2005). Nevertheless, some academics and researchers agree that Krone’s definition is too broad and for instance The United Nations (UN) extended the definition by adding ‘fraud, forgery, and unauthorised access’ as part of cybercrime (1995).

***Cybercrime*** has also been defined as a group of illegal hackers focussing on economic gains through illegal penetration of computer networks, replacing traditional forms of crime, and affecting the global economy (Kim et al. 2009). Cybercrime is a global issue; no country is invulnerable. According to Graham (2017), cybercrime cost the global economy over **$450 billion** in 2016, with over 2 billion personal records stolen in the U.S. alone, and over 100 million Americans having had their medical records stolen. In the UK during the same year, the influence of cybercrime on UK businesses was enormous, with **2.9 million** British companies being hit by some sort of cybercrime at a total cost of **£29.1 billion** (Samarati 2017)**.** Over the years, the risk of malicious attack affecting the financial sector has increased. If we should focus on unstable countries, recently, a Bangladesh Bank official's computer was hacked and **$81 million** was stolen by an organised group from North Korean (Hipp 2017). Metaphorically Spring Landis, increasingly open to exploitation by cyber-criminal groups due to the growing level of Internet connectivity. With the launch 4G-LTE network in many cities to enhance the coverage and performance and to get more customers by

providing a high-speed internet connection which also leads to all sort of problems related to cybercrime (BenIbrahim 2017).

***Cyber Warfare*** is another threat of cyber space in the national security realm that is going to be discussed in this study and which the US Department of Defense (DoD) has termed as the 5th Domain (DoD 2008). There is an increasing body of evidence suggesting that Cyber warfare has been conducted as an act of war. Nation-states directly employ Cyber weapons to disrupt the nation-state's critical infrastructure and computer systems. The most-known Cyber malware was used by Russia in 2007. Russia launched an enormous Distributed Denial of Service (DDoS) on Estonia's internet infrastructure that shut down service to major websites and communication across the country (Bryson 2018). Yet again, in 2008 the physical war between Georgia and Russia that turned into cyber war and DDoS attacks applied to shut down communication systems in Georgia.

Another example is the attack on Iran's nuclear program via the Stuxnet worm in 2010 (Shafqat and Masood 2016). In the Middle East and North Africa (MENA) region, Cybercrime and cyber warfare has so far been politically or ideologically motivated (Pahl and Richter 2007). Conflict between Saudi Arabia and Iran in recent years turned to using cyber warfare. Johnson et al. (2008) states that a self-proclaimed hacker from Saudi Arabia calling himself "Da3s" apparently attacked the websites of Iran's Statistical Centre and Registration Office. A day after Da3s's attacks, a group calling itself the "Iran Security Team" retaliated by targeting Saudi Arabia's General Authority for Statistics and King Abdulaziz University. Recently, a large cyber-attack was launched using the WannaCry virus. This virus has infected more than 230,000 computers in 150 countries that use Microsoft Windows systems in a few days (Ehrenfeld 2017). Similar to the WannaCry virus, a new ransomware called Petya has infected many countries around the world (Symantec 2017).

Spring Land is at risk from cyber warfare for a range of reasons; the U.S debated whether to expose the mission with a new kind of warfare: a cyber offensive to disrupt and even disable the Spring Land air-defense system in 2011 (Libicki 2011). Additionally, disruptive aggrieved political parties whose agenda will not form a cohesive government which affect political sensibilities of another nation. As an example, a vote page of Egypt's Ministry of Information (moinfo.gov.eg) has been attacked by a group called the Spring Land Cyber

Army (The GreaT TeAm) and hackers posted a picture of the Spring Land flag, the message “Hacked by The GreaT TeAm,” and a link to their Facebook page (Segura Serrano 2015).

Likewise, ***Cyber*** *Espionage* has become an ever-more significant factor in the art of war due to cyber technology development, turning traditional intelligence into cyber espionage. Obama (2013), argues that the US intelligence agencies have a long-held view that the Chinese government has a national policy of economic cyber-espionage. According to Grierson (2017), the GCHQ’s Cybersecurity chief has said that Britain is being hit by dozens of cyber-attacks a month, including attempts by Russian state-sponsored hackers to steal defence and foreign policy secrets. Ciaran Martin, Head of GCHQ’s National Cybersecurity Centre (NCSC), warned there had been a “step change” in Russia’s online aggression against the West, as well as more attacks on “soft targets” such as local councils and charities to steal personal data, and universities to steal research secrets (Kerbaj 2017).

In October 2011, CrySyS Lab in Budapest, Hungary discovered Duqu, a malware with striking similarities to Stuxnet, but seemingly with a different motive. Certainly, Duqu does not intend to cause physical destruction, but it is an information-gathering malware used for cyber espionage (Obama 2013). Flame is another method for collecting information using a malware tool. Flame has received worldwide attention in security expertise due to its advanced spreading techniques based on masquerading as a proxy for Windows Update (Obama 2013).

In the case of Spring Land, the malware named the "Book of Eli", has been targeting mainly Spring Land entities. It was first discovered in 2012, and is known for scattering via social networks such as Twitter and Facebook (Patton 1990). Patton (1990) clarifies that the "Book of Eli" malware is a classic information-stealing Trojan that attempts to collect various information. It can be deployed in various configurations. The full-featured version of the malware can log keystrokes, collect profile files of Mozilla Firefox and Google Chrome browsers, record sound from the microphone, grab desktop screenshots, capture photo from the webcam, and collect information about the version of the operation system and installed anti-virus software.

***Hacktivism*** is also considered as one of the main motivations behind the exposed attacks. According to Ho (2014), the term “hacktivism” has been denoting a range of political

practices that make creative use of information technologies or, conversely, technical inventions and software hacks that have explicitly political goals. A good example of hacktivism is a group that identifies itself as LulzSec, who hacked into SonyPictures.com and compromised the personal information of more than 1 million users (Myers 1997a).

With the increase of cyber attacks, another threat has occurred. It can be referred to as ***'cyber terrorism'***. However, as it is quite complicated to define the term 'terrorism', there has been no consensus on what the definition of cyber terrorism should be (Wilson 2005).

According to Caruso (2002), cyber terrorism has been defined in the United States as *"Cyberterrorism meaning the use of cyber tools to shut down critical national infra-structures (such as energy, transportation, or government operations) for the purpose of coercing or intimidating a government or civilian population is clearly an emerging threat."* Denning (2001) defines cyberterrorism accordingly 'politically motivated hacking operations intended to cause grave harm such as loss of life or severe economic damage.' Wilson (2005) combines several definitions and suggests the following definition 'the use of computers as weapons, or as targets, by politically motivated international, or sub-national groups, or clandestine agents who threaten or cause violence and fear in order to influence an audience, or cause a government to change its policies. '

Nevertheless, as Prichard and MacDonald (2004) noted, cyber terrorism is computer-based terrorism, yet it still demonstrate the four elements that are shared by all acts of terrorism:

1. They are planned and premeditated and therefore not just acts of rage.
2. There is political motivation behind the act whose aim is to corrupt or completely destroy the system; in this instance computer system as pointed out by (Galley 1996).
3. They are targeted at civilians and they result in violence against people, which generates fear
4. They are conducted by ad hoc groups, not by national armies.

The last point distinguishes cyber terrorism form cyber warfare in the sense that cyber warfare, which according to Prichard and MacDonald (2004) are attack conducted by agents of a nation-state.

## 2.4 Cybersecurity in Context (Spring Land)

In recent years, there has been an increasing interest in using the online communication platform in states such as Spring Land. Spring Land metaphorical is a fictitious name given to the country of Libya, where the present case study was conducted. According to the Internet World Stats (2017), Spring Land's population is approximately 6 million and the number of Internet users is around 2.8 million, which forms 44% of the population (InternetWorldStats 2017). The telecom sector consists of an operator, owned by the state, which provides postal services and telecommunications (Spring Land Post, Telecommunication and Information Technology Company "LPTIC", General Post and Telecom Company "GPTC"). Spring Land Telecommunication and Technology (LTT) Corporation provide Internet service, and two mobile phone networks in Spring Land. Meanwhile, the online security in Spring Land has not been reinforced and enhanced in the same way that it has evidently been in other countries like the UK and the US. Moreover, it was in 2013 when the Spring Land government officially established the National Cybersecurity Authority (NCSA). NCSA's primary mission is to encourage and sustain secure use of ICTs as well as to prevent, detect, and respond effectively to the associated cyber risks (NISSA 2013). In the same year, with the support of (ITU), Spring Land-CERT has been established with national-level responsibilities and is charged with prevention, detection, and mitigation of cyber threats (Matsubara 2014).

Due to the current political conflict and the austerity measures, NCSA faces lack of funding which hindered most of the attempts of advancing cybersecurity in the context (Matsubara 2014). Thus, Spring Land's ability to address cybersecurity concerns is currently not at a level that inspires sufficient public confidence; hence, a cogent methodology to optimise its IT resources is most necessary. The onus is on the Spring Land national security to prevent any possible terrorist threats and protect the country's critical infrastructure, which can only be achieved by coherent strategising between all relevant departments. This would provide assurances of streamlined, secure and resilient intelligence sharing, both internally and

internationally in order to safeguard the essential national infrastructures. It has to be noted that Spring Land's cyber offensive and defensive capabilities clearly demonstrate a relative lack of security with respect to most of the Spring Land communications network and infrastructure (CSFI 2011).

According to the Cyberwellness Profiles report, many countries like Spring Land do not have a cogent National Cybersecurity and information assurance framework. Therefore, its suitability to conduct effective and efficient information sharing is severely compromised (ITU 2015). Its main weakness is a lack of national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, practices and guidelines need to be applied in either the private or the public sector. The Global Cybersecurity Index (GCI) project ranks such countries like Spring Land's preparedness for cyber threats at 105 out of 134 worldwide countries (ITU 2017a). According to El-Guindy (2013) the lack of security measures, coupled with poor security awareness and other ICT vulnerabilities in the Middle East, may lead to potentially harmful attacks from the underground market.

### 2.4.1 Cyber Threat Impacts on Spring Land

Spring Land like any country in the world is under constant, persistent, sometimes overwhelming online attacks. Attacker employ wide range of attackers vectors to hack government agencies, private organisations, as well as influential and political figures. Spring Land is well-known for its unstable political system, civil war and militant groups fighting for land and oil control, however, the global community knows very little about the country's malicious cyber activities, cyber espionage or hacking groups (Cyberkov 2016). Nevertheless, Cyberkov observed that a high-profile Spring Land influential and political figure was attacked by malware, which spreads extremely fast using the Telegram messenger application in smartphones. Microsoft Security Intelligence Report discloses that our metaphorical Spring Land has the highest percentage of unprotected computers and also the highest infection rate (Microsoft 2016).

Furthermore, the report from Kaspersky Lab Solutions gathering information about malicious attacks from online resources located in 190 countries all over the world, shows that Spring Land rounded off the top 3 for the highest proportion of users attacked by banking Trojans in the world (Kaspersky 2017). Moreover, according to Matsubara (2014) Spring Land

classified as one of the top ten Source of Phishing Hosts and Command and Control servers (C&C servers) in Africa during 2016. Abuzawayda (2016), reported that, a hacker belonging to a group calling itself the Spring Land Worms provided statistics which showed that the worms group was able, in a short period, to control over 99% of the Spring Land government websites. In addition, the hacker declared that they got access to the systems of the Central Bank of Spring Land, civil registration and national figures. Another cyber-attack targeted the website of the Civil Registry Authority, the attack affected the authority's daily services to the people(libyaobserver 2016). Many of these activities, because of their motive, origin, or objective, threaten Spring Land National Security and public safety.

## 2.5 Global and Organisational Cybersecurity Frameworks

In the new global economy, Cyberspace challenges impact every facet of society including economic, social, cultural and political developments. Developing national securities is one of the greatest challenges that we are facing. However, national and international organisations as well as researchers have developed a multiplicity of guidelines and frameworks to help in the development of a Cybersecurity framework. In this section presents some of the common Cybersecurity frameworks.

### 2.5.1 The International Telecommunication Union (ITU) guide

The International Telecommunication Union (ITU) has published guide to developing a national cybersecurity strategy. The guide aimed to enhance security and assurance in cyber space. In addition, to build confidence and trust that critical information infrastructure would work dependably and continue to sustain national welfares even when under attack (ITU 2018b). According to ITU (2018b) the guide is built on five strategic pillars, the first three, i.e. legal framework, technical measures, and organizational structures need to be undertaken at national and regional levels but also harmonized at the international level. The last two pillars, e.g. capacity building and international cooperation, crosscut in all areas. In addition to this and based on the GCA, the ITU developed a National Cybersecurity Strategy Guide which provides a holistic view of the Cybersecurity.

This guide focuses on the strategic pillars that typically assist nations to create coherent national and globally companionable programs for protecting critical infrastructure against cyber threats (Segura-Serrano 2015; ITU 2018b).

### 2.5.2 The North Atlantic Treaty Organization (NATO) framework

The North Atlantic Treaty Organization (NATO) proposes a National Cybersecurity Framework Manual in 2012 to address national Cybersecurity in NATO Member States or NATO partner countries. This framework, according to Klimburg (2012), will serve as a guide to develop, improve or confirm national policies, laws and regulations, decision-making processes and other aspects relevant to national cybersecurity. Furthermore, the manual has three pillars (Dimensions, Mandates and Dilemmas), that should be considered in developing a National Cybersecurity Strategy (NCS). Three Dimensions of NCS; a Whole of Government approach (Governmental), a Whole of System approach for improving international and national coordination (International), and a Whole of Nation approach for cooperating with non-state actors (National).

Five mandates that should be considered also in the $5^{th}$ Domain cyberspace are: Military Cyber, Counter Cyber-Crime, Intelligence and Counter-Intelligence, Critical Infrastructure Protection and National Crisis Management, and Cyber Diplomacy and Internet Governance (Klimburg 2012). Moreover, the Five Dilemmas that try to control costs and benefits that will have consequences on inhabitant freedoms, economic development (Sabillon et al. 2016). Klimburg (2012) states that, the framework provides the elements of the six Cybersecurity incident management model for each mandate as shown in Figure 2.3.


Figure 2.3 the Five Mandates and the Six Elements of the Cybersecurity Incident Cycle (Klimburg 2012)

### 2.5.3 The European Union (EU) Guide

The European Union Agency for Network and Information Security (ENISA) had created a practical guide on national Cybersecurity strategies (NCSS) and updated it in 2016, to support Europe Member States in developing robust national cyber resilience capability. Additionally, ENISA had created an Evaluation Framework in 2014 to provide guidance and practical tools to the Member States for evaluating their NCSS (ENISA 2016). According to ENISA (2016), the aim of the present good practice guide is to provide a comprehensive overview of different steps and objectives in order to develop and implement NCSS. Klimburg (2012) says that this guide indicates that Cybersecurity actions should extend across three key pillars, e.g. Network and Information Security (NIS), law enforcement, information and defence. The NIS directive has been adapted by the European Parliament, to ensure a high-level of network and information security across the Union, by pushing

member states to have a proper CSIRT, as well as a capable national network and information systems authority (Matania et al. 2017). In addition, the EU organised the level of coordination among different EU and National agencies to respond and prevent cyber threats based on Cybersecurity, law enforcement and defence divisions as shown in Figure 2.4.

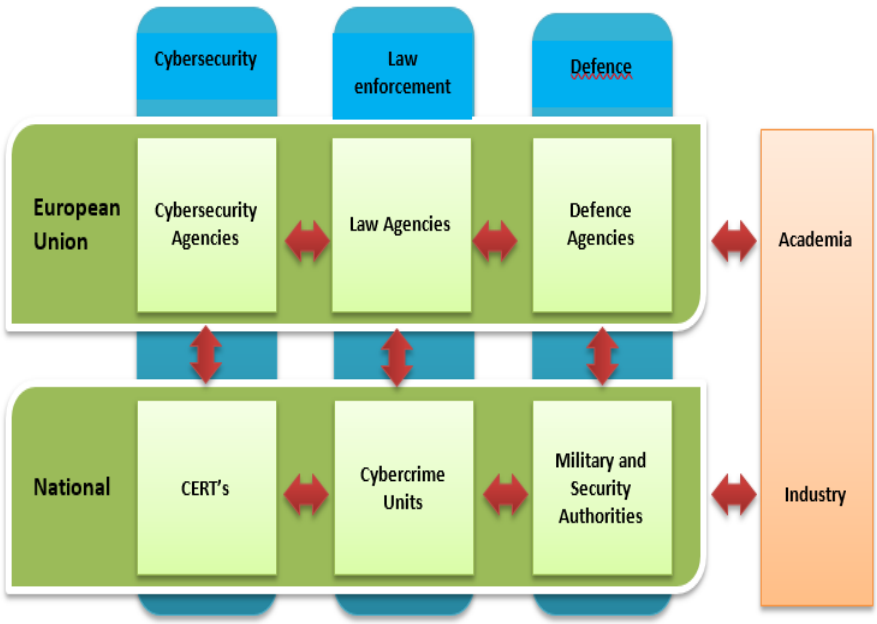



Figure 2.4 Coordination between EU and National Agencies (Sabillon et al. 2016)

### 2.5.4 The Organisation for Economic Co-operation and Development (OECD) Guide

This guide was released in 2015 by (OECD) to provide guidance for creating a national strategy to manage digital security risk and enhance the economic and social benefits anticipated from digital realm (OECD 2015). According to OECD (2015), this guide recommends that cyber risks should not be treated as technical problems, but should be approached as economic and social activities. In addition, this guide has put forward general and operational principles. The general principle focused on: Awareness, skills and empowerment, Stakeholders responsibility, Human Rights and fundamental values, Public and Private Partnership. The operational principle includes Risk assessment and treatment cycle, Security measure, Innovation, and Preparedness and continuity. Additionally, this guide encourages governments to include crucial elements in implementing the national Cybersecurity strategy. These measures include the previous principles and create a national

Computer Security Incident Emergency Response Team (CSIRT), implementing a comprehensive framework to tackle cybercrime, and Strengthen international co-operation and mutual assistance (OECD 2015).

### 2.7.5 National Institute of Standards and Technology (NIST) Cybersecurity Framework

In February 2013, US president Obama issued an executive order which required the National Institute of Standards and Technology (NIST), a non-regulatory agency of the Department of Commerce, to develop a "Cybersecurity framework" to identify and mitigate cyber risks that could possibly affect national and economic security (Obama 2013). According to Segura Serrano (2015) the order takes a holistic approach that is meant to address the three main areas of concern: information sharing, a risk-based framework of core practices based on existing standards, and privacy protections.

In February 2014, the NIST put out its Cyberseurity framework, titled "Framework for Improving Critical Infrastructure Cybersecurity" as the result of a collaborative process between the government and the private sector (Shackelford et al. 2015). According to NIST (2014a) the Framework consists of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers as shown in Figure 2.5. The Framework Core is a set of communal cybersecurity performances and anticipated results, and involves five simultaneous and continuous tasks, e.g. identify, protect, detect, respond, and recover. After assessment, these functions provide a sophisticated, strategic vision of business requirements, risk tolerance, and resources. The framework implementation tiers evaluate the extent of which an entity's Cybersecurity risk management practices display the features defined in the framework, e.g., risk and threat aware, repeatable, and adaptive (Shackelford et al. 2015).


Figure 2.5 (NIST) Cybersecurity framework (NIST 2014a)

### 2.5.6 Microsoft Approach for Developing a National Cybersecurity Strategy

Microsoft has published a set of recommendations that support governments on developing a national Cybersecurity and handling cyber threats on national critical infrastructures (Goodwin and Nicholas 2013). Microsoft recommends six foundational principles as the basis for a national Cybersecurity strategy. It must be: Risk-based, Outcome-focused, Prioritised, Practicable, Respectful of privacy and civil liberties, and globally relevant. Goodwin and Nicholas (2013) said that, Microsoft approach recommends thinking holistically and realistically about dangers and threats to a nation and set up strong practices to prevent, detect, contain, and recover from an incident. The approach also suggests creating a clear role for national CERT, as well as raising public awareness and public-private partnership.

### 2.5.7 The International Organization for Standardization (ISO 27032:2012) Guidance

The International Organization for Standardization (ISO) provides technical guidance for tackle well-known Cybersecurity risks, including: social engineering attacks, hacking, malware proliferation, spyware and unwanted software Furthermore, the guide includes controls for addressing these risks like preparing for attacks, detecting and monitoring, and responding to cyber-attacks. The Standard also provides an explanation of stakeholders' definitions and their roles in Cybersecurity. Moreover, this International Standard also delivers a framework for information sharing, coordination and incident handling (ISO 2012).

### 2.5.9 Primarily Attributes of Global Selected Frameworks

The previously discussed Global Selected frameworks are each generally concerned with developing a Cybersecurity framework, nevertheless individual approaches, strategies and focuses chosen for the development of such frameworks vary. This section is going to highlight the main differences. The ITU Global Security framework attempts to strengthen Cybersecurity through engaging its five pillars that operate on three levels: international, national and regional. This framework not only does improve security but also build confidence and trust in order to sustain national welfares even when under attack. The main focus is global domain and the global cyberspace protection. On the other hand, National Cybersecurity Framework Manual works as a guide for NATO member states in order to strengthen and improve the national policies, law and regulations that are related to national Cybersecurity. It was introduced in 2012 and operates on international and national level with the main emphasis on the national coordination and policies. Another framework is the European Union Guide which was created in 2014 and revised in 2016 and whose aim is to provide assistance and a guide to help EU member states to assess their national Cybersecurity space security and finds solutions for improvements of individual tools in individual states. Additionally, OECD guide was published 2015 and its main target is to establish national strategy in order to eliminate digital security risk. The guide suggests that cyber risks should be managed through economic and social activities, and not treated as technical problems. NIST Cybersecurity Framework was developed in 2013 in the United States and is primarily concerned with managing and mitigating cyber risks that could affect national and economic security and how individual cyber risks should be identifies, approached and dealt with. In 2013, Microsoft published guidelines that instruct governments how to develop and strengthen national Cybersecurity. Microsoft suggests that Cybersecurity should be approached holistically and nations should be prepared to prevent, detect, contain and recover from an accident. With the main focus on the national level, Microsoft believes that public should be aware and prepared to stand up to cyber risks. Lastly, ISO created a framework focussing on the international level and raises the awareness and encourages nations to be prepared to fights various types of cybercrime. Despite the various perspectives and contexts for the frameworks there are similarities shared across the frameworks (Azmi et al. 2018). Some of these include criteria such as, involving as many stakeholders as possible and centralising competence (Inclusive), promoting Fundamental of Human Rights by

recognising current International Standards, Protocols and Interoperability (Coherent). The framework should include Domestic and International Tools such as Budapest Convention to enhance international cooperation in tackling cybercrime. Moreover, these frameworks encourage states and organisations to develop cyber culture programmes and adopt risk based approaches in their national cybersecurity capabilities (Klimburg 2012; ENISA 2016; ITU 2018b). These shared criteria and others are used to evaluate the proposed framework in this study.

## 2.6 Cybersecurity Capability Maturity Models (CCMMs)

Increased attention to the potential risks and threats of cyber space to the national critical infrastructure, has created a high demand to assess and report on the readiness of the organisations and countries using the Cybersecurity Capability Maturity Models (CCMMs) (Miron and Muita 2014). The CCMMs deliver the stages for an evolutionary pathway to developing strategies and policies for the security and reporting of cybersecurity readiness of critical infrastructure. This section explores main attributes of the common existing CCMMs which has been designed and used in different organisations and nations. These CCMMs models such as, the International Organization for Standardization's Systems Security Engineering Capability Maturity Model (SSE- CCMM), the National Institute of Standards and Technology (NIST) Cybersecurity framework the U.S. Department of Energy's Cybersecurity Capability Maturity Model (C2M2).

### 2.6.1 Cybersecurity Capability Maturity Model (C2M2)

The C2M2 has been designed by the Department of Energy's in the U.S. to analyse and improve organisation Cybersecurity programs (DOE 2014). This model according to the U.S. Department of Energy, enables the organisations to; define its current state, determine its future, more mature state and identify the capabilities it must attain to reach that future state. The said model has 10 domains consist of a structured set of Cybersecurity practices. These domains include: Risk Management, Asset Change and Configuration Management, Identify and Access Management, Threat and Vulnerability Management, Situational Awareness, Information Sharing, Event and Incident Response, Supply Chain and Eternal Dependencies Management, Workforce Management, and Cybersecurity Program Management. In addition,

the model has four maturity indicator levels (MILs), MIL0 through MIL3 that applied individually to each domain.

### 2.6.3 Cyber Resilience Review (CRR) Assessment Model

The CRR is an assessment technique that was moulded by the Department of National Security (DHS) for the purpose of evaluating the cybersecurity and resilience of critical infrastructure owners and operators (US-CERT 2016). This model is based on the Cyber Resilience Evaluation Method and the CERT -Resilience Management Model (CERT-RMM), both has been developed at Carnegie Mellon University's Software Engineering Institute. The CRR contains ten domains of practices that represent vital capabilities that contribute to the cyber resilience of the institution. These domains are: Asset Management, Controls Management, Configuration and Change Management, Vulnerability Management, Incident Management, Service Continuity Management, Risk Management, External Dependencies Management, Training and Awareness and Situational Awareness. For each domain a set of goals and linked practice questions, and a standard set of maturity indicator level questions look at the institutionalisation of practices contained by an organisation. These domains are scored on a six levels (Incomplete, Performed, Planned, Managed, Measured, Defined) (US-CERT 2016). This model helps organisations to recognise their Cybersecurity posture and measure their development in improving cyber resilience.

### 2.6.4 Cybersecurity Capacity Maturity Model for Nations

The Cybersecurity Capacity Maturity Model for Nations (CCMM) has been developed by Global Cybersecurity Capacity Centre in the University of Oxford through collaboration with international stakeholders. These include the Organization of American States (OAS), World Bank, Commonwealth Telecommunications Organisation (CTO) and the International Telecommunication Union (ITU)(GCSCC 2017). According to GCSCC (2017), this model is an academic politically neutral expertise offering a comprehensive analysis of cybersecurity capacity through five different dimensions:

- Cybersecurity Policy and Strategy
- Cyber Culture and Society.

- Cybersecurity Education, Training and Skills.
- Legal and Regulatory Frameworks.
- Standards, Organisations, and Technologies.

Each dimension has a multiple factors and attributes, with significant aspect for capacity building within each dimension. In each factor, there are five stages of maturity, where the lowest indicator would imply a non-existent or inadequate level of capacity, and the highest level both a strategic approach and an ability dynamically to enhance against environmental considerations (operational, threat, socio-technical and political) (GCSCC 2017). According to CCMM the five levels of maturity are:

1- Start-up: this level shows that either nothing exists, or it is very embryonic in nature.

2- Formative: in this level indicate that some features are formulated but poorly defined.

3- Established: at this level the element of sub-factors are in place, and defined.

4- Strategic: in this level the selections of which parts of indictors are vital or less important, have been made for particular institution / nation based on certain conditions.

5- Dynamic: At the Dynamic level, there are clear mechanisms in place to modify strategy subject to the prevailing circumstance

This model has been deployed to review cybersecurity capacity in over 40 countries including UK, Kosovo, Bhutan, Uganda, Senegal and Indonesia (GCSCC 2017).

## 2.7 National Cybersecurity Strategies (NCSs) Case Studies

In this section, a review of selected national Cybersecurity strategies and policies of the UK, Egypt, and Turkey was performed. These countries were chosen as they have different views of creating Cybersecurity strategies and frameworks. Furthermore, all selected countries are members of The International Telecommunications Union (ITU). The ITU has developed the National Cybersecurity Guide that addresses security challenges facing the digital world and

is accepted by the majority of countries. In addition, some selected Islamic countries (Egypt and Turkey) sharing the same cultural and religious values as Spring Land. On the other hand, the UK has been chosen as it has ranked fifth in a global survey ranking of Cybersecurity development (Mack 2010). Moreover, according to Archick et al. (2006) Spring Land governments made a few agreements with Great Britain since 2012 for developing the communications infrastructure in Spring Land. The two governments agreed that Spring Land should accept the model of E-government of Great Britain, which contains three main points: Information and Communication Technology (ICT), ICT applications, particularly E-government, E-commerce and E-learning, and Regulatory framework.

### 2.7.1 The United Kingdom (UK) Cybersecurity Strategy

The UK Cybersecurity Strategy 2016-2021 focuses on keeping the nation safe and delivering a competent government. It has the vision that by 2021 the UK will be secure and resilient to cyber threats, prosperous and confident in the digital world. Three main objectives were indicated in the strategy (Defend, Deter, and Develop). **Defend** the UK against cyber threats and respond effectively to any cyber incidents, to ensure the UK infrastructure networks and information systems are fully protected and resistant to any cyber-attacks. **Deter** aims to make the UK government a hard target for attacks. It also seeks to detect, understand, investigate and disrupt any hostile actions in cyberspace against the UK. Furthermore, the government will reinforce the national cyber offensive capabilities in virtual space. The **Develop** objective aims to build essential knowledge and skills in a growing UK Cybersecurity industry. It correspondingly supports IT training and education on Cybersecurity in schools and other learning institutions. All previous objectives are reinforced by international action and investing in partnerships that shape the global evolution of cyberspace in a manner that advances economic and security interests (Heath Kelly 2013).

### 2.7.2 Egypt Cybersecurity Strategy

The Ministry of Communications and Information Technology (MCIT) of Egypt has released the Egyptian National ICT Strategy for 2012-2017 (MCIT 2013). According to MCIT, the strategy focused on develop an appropriate legislative and regulation framework for cybersecurity with the participation of the private and public sectors; enhance confidence in

online services; build human capacity program; raising awareness and promote cooperation with other countries and international organisations.

### 2.7.3 Turkey Cybersecurity Strategy

Turkey in its 2016-2019 National Cybersecurity action plan has focused on two key objectives (MTMC 2016). First, secure cyber space is a part of national security. Second, getting the capability that will allow taking organisational and technological protection measures for sustaining the absolute security of all critical infrastructures in national cyber space. In addition, it provides the action plan to achieve these objectives such as; ensuring the security, confidentiality and privacy of all e-services, enhance national incident response, domestically developing critical technologies and products for assuring Cybersecurity. Yet, the action plan targeted to cover all technical dimensions, an integrated approach including legal, organisational, economic, political and social dimensions.

### 2.7.4 Primarily Attributes of Reviewed NCSs Case Studies

The output of this analysis presents that the content of the national cyber strategy differs broadly. Despite of common cyber threats affects these nations, each of them has a different approach to minimise and prevent cyber threats. For instance, the UK cybersecurity strategy considered cyber-attacks as a Tier one threat to the national security and Turkey identified cybersecurity as a part of national security. Meanwhile, Egypt considered cybersecurity strategy as a part of the National ICT Strategy for 2012 – 2017. Each country has a paradigm of the strategy based on specific needs linked to protection of national infrastructure. These strategies comprehensively address national issues related to cybersecurity such as the public and private partnership, develop cybersecurity defence capability, capacity building; legal and regulation frameworks, cyber resilience, stockholders involves, cyber awareness program, international cooperation and cyber intelligence gathering. As such, safeguarding cyberspace is a main concern today for every country. Thus, Spring Land, which is gradually providing e- services, needs a National Cybersecurity Capacity Building Framework to address the challenges of cyber threats.

## 2.8 Cybersecurity Capacity Building (CCB) Dimensions from World Perspective

Cyberspace has become an essential part of the development of any country. A robust cybersecurity capacity is vital for states to progress and develop in economic, political and social spheres (Muller 2015; Pawlak 2016). Capacity according to Goodman et al. (1998) is "the ability to carry out stated objectives". Capacity is supposed to develop in "stages of readiness" which indicate improvements or decline (Goodman et al. 1998; Mackay and Horton 2002; LaFond and Brown 2003)

Capacity building is commonly viewed as a mechanism to bridge the gap between the problems of poor governance and what is considered to be an adequate level of state capacity to deliver its main functions (Beesley and Shebby 2010; Pawlak 2016). Generally, capacity building is a process or activity that improves the ability of a person or organisations to "carry out stated objectives" (Goodman et al. 1998; LaFond and Brown 2003). Capacity building is influenced directly and indirectly by contextual factors or elements of the external environment. Contextual influences include cultural, social, economic, political, legal, and environmental variables. The impact of these factors may be critical to the success of capacity building, nevertheless they are often difficult to control or measure (Mackay and Horton 2002; LaFond and Brown 2003).

Cybersecurity Capacity Building (CCB) viewed as a way to achieve developmental goals by reducing cybersecurity risks (Hohmann et al. 2017). CCB is also considered as a transformation process and 'dynamic field' since it is connected to technological, political and social developments, which are constantly growing (Bellasio et al. 2018). Transformation is considered the main component of capacity building (United-Nations 2018). Through transformations, countries can invent, develop, and maintain institutions and organizations that are capable of contributing to the development of capacity building. Capacity building is not a matter of "one-time effort to improve short-term effectiveness", but rather a continuous improvement strategy (Hohmann et al. 2017).

Governments, international organisations, and non-state actors all recognise that CCB is crucial to mitigating the negative cross-border externalities of increasing connectivity and maximizing the benefits of cyberspace (Hohmann et al. 2017). However, national and

international organisations as well as academics have developed a multiplicity of guidelines and frameworks of CCB to reduce and handle the risks of cyber threats. States such as the UK, Netherlands, or the US, international and regional organisations including the OAS, ITU, and the EU and other actors like Oxford University or Microsoft are slowly lending support and resources to building capacity. For some, CCB has even become a tool for foreign policy as a means to advocate for a particular model of internet governance, create market access for domestic companies, or promote specific technical standards. This section provides an offer view of existing global frameworks that used to measure CCB efforts and initiatives for countries. The organisational models are out of scope in this section as it focuses on institutional levels not on national level.

### 2.8.1 Global Indices Models of Cybersecurity Capacity Building

Cybersecurity Capacity Building (CCB) models purposed to provide states with theoretical and practical support that help to categorise the cybersecurity requirements, as well as the opportunities for action in each country (Hohmann et al. 2017). These models provide a benchmark for states to enable them to identify where they are along that path. Numerous frameworks and models have been developed worldwide. Yet, it is worth to take into account, that there is not a perfect and unique model that has been developed or that has been recognized as a 'one-size-fits-all' solution that is able to afford an all-in solution to cybersecurity issues (Pawlak 2014). According to Pawlak (2014), each model considers each state's specific requirements and resources although taking into consideration the different cultural, political and social environments. These models look at, among others, policy and regulatory aspects, organisational measures, national strategies, and cooperative efforts. Some frameworks simply compare and contrast measures amongst countries, while others provide an index scoring based on indicators. Others provide rankings based on the scoring. All offer valuable information on cybersecurity practices and gaps at the nation state level (ITU 2017b). Cybersecurity Capacity Building (CCB) is complex and challenging (Trimintzios 2017).

Table (2.1) presents different metrics, areas of focus, research method, number of countries and contents of global CCB models. The formation of such models is beneficial for countries to assess and scale the maturity of their cybersecurity capacity, empowering decision makers to identify future priorities (Pawlak 2014; Hohmann et al. 2017). According to Muller (2015),

existing models and assessments of CCB are successful in evaluating national levels of CCB in individual countries, however the ability to aid countries in how to improve their cyber capacities is still lacking. Developing Countries especially countries in transitional stage will need to deal with challenges in all types of activities connected to CCB from human resource development, institutional reform, organizational adaptions, to the support provided to increase their access to, and ability to benefit fully from, the Internet and other elements of cyberspace (Muller 2015).

These frameworks and approaches indicate that there are five main pillars that build cybersecurity capabilities and capacity: human, organisational, infrastructure, technology, law and regulation (Azmi et al. 2018). CCB aims to help states to escalate their access and ability to benefit from cyberspace and advanced technology. CCB includes progress in technical, political and legal frameworks. For instance, technical improvement can be achieved by building national incident response capabilities. Political progress is achieved through cybersecurity policies and strategies. Legal progress is achieved through effective legislation that addresses “the issues that affect the order and good governance” (Hohmann et al. 2017). These models to date have not managed to cover CCB as a whole on a global scale or else they argue for CCB, but without indicating how to go about implementing it (Muller 2015). Some approaches set out a scope that is either too broad or too narrow, while others focus on different ways of highlighting the problems that come with increased access to cyberspace, but without indicating solutions (Muller 2015)

| Models and developer | Research method and no. of indictors | Content and area of focus | No. of countries and region | Metrics |
|---|---|---|---|---|
| Cyber Maturity in the Asian Pacific Region (https://www.aspi.org.au/report/cyber-maturity-asia-pacific-region-2017) | Secondary data based on data provided by the (ITU). A set of 11 indicators has been produced and each state's level of cyber maturity has been measured against the benchmark provided with each indicator. | The index is focused on Cyber Maturity of countries in five topics governance; financial cybercrime enforcement; military application; digital economy and business; and social engagement. | 25 countries in the Asia and the Pacific | Scores |
| National Cybersecurity Index (NCSI), developed by Estonian e-Governance Academy & Estonian Foreign Ministry. (https://ncsi.ega.ee/ncsi-index) | Data is collected using both primary & secondary sources. The NCSI has organised into 3 categories, 12 capacities and 46 indicators. | The index measures the preparedness of countries to prevent cyber threats and manage cyber incidents. The NCSI focuses on measurable aspects of cybersecurity implemented by the central government: Legislation in force, Established units such as existing organisations, Cooperation, and Outcomes such as policies, exercises, technologies. | 152 (Global) | Rank & Score |
| Global Cybersecurity Index developed by the International Telecommunication Union (ITU)<br><br>(https://www.itu.int/en/action/c | A total of 194 countries have been analysed, 135 of which have been subjected to both primary and secondary research and only 59 a subject of secondary research. The index has 25 main indicators | The index aims to provide insight into the cybersecurity engagement of sovereign nation states. Rooted in the ITU's Global Cybersecurity Agenda (GCA), the GCI looks at the level of commitment in five strategic pillars: Legal, Technical, Organizational, | 194<br><br>(Global) | Rank and score |

| | | | | |
|---|---|---|---|---|
| ybersecurity/Pages/gca.aspx) | | Capacity building and Cooperation measures | | |
| Cyber Readiness Index (CRI 2). The CRI 2.0 is developed by the Potomac Institute for Policy Studies.<br><br>(https://potomacinstitute.org/images/CRIndex2.0.pdf) | Data is collected using both primary & secondary sources. The CRI 2.0 blueprint identifies over seventy unique data indicators across seven essential features | The CR 2.0 aims to evaluate nation state's cyber maturity as well as their overall commitment to cyber issues. The index is mainly focused on national strategy, incident response, e-crime and law enforcement, information sharing, investment in R&D, diplomacy and trade, and defense and crisis response. | 125 country | Score |
| Asia-Pacific Cybersecurity Dashboard. The Dashboard is a publication developed by BSA \| The Software Alliance.<br><br>(http://cybersecurity.bsa.org/2015/apac/assets/PDFs/study_apac_cybersecurity_en.pdf) | This study is based on an assessment of 31 criteria across six themes. Each criteria is given a "Yes," "No," "Partial," or "Not Applicable" status. The data is collected using a desk-technique based on publicly available information, and did not involve direct interviews with national agencies. | Dashboard examines the cybersecurity policy environment with a focus on five key areas: Legal foundations for cybersecurity; Operational capabilities; Public-private partnerships; Sector-specific cybersecurity plans and Education. The aim of this cybersecurity dashboard is to provide a reference base, which allows the evolution of countries' cybersecurity policies by comparing them with the other Asia and the Pacific countries. | 10 countries | There are no overall rankings or scores in this study. |
| Cyber Power Index and is developed jointly by the Economist's Intelligence Unit and sponsored by Booz Allen Hamilton. | The data is collected using secondary sources. in the index are: the Economist Intelligence Unit; the UN Educational, Scientific and Cultural Organization (UNESCO); the International Telecommunications | The goal of the index is to benchmark the ability of the G20 countries to withstand cyber-attacks and to deploy the digital infrastructure needed for a productive and secure economy. The index consists of four categories and 39 sub-indicators. These | 19 countries of the Group of 20 (G20) | Rank and Score |

| | | | | |
|---|---|---|---|---|
| (https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/EIU%20-%20Cyber%20Power%20Index%20Findings%20and%20Methodology.pdf) | Union (ITU); and the World Bank. | categories are Legal and Regulatory Framework; Economic and Social Context; Technology Infrastructure; and Industry Application | | |
| CyberGreen Index Version 2.0. The index is developed by Cyber Green Initiative supported by JPCertCC, CSA Singapore and Foreign Commonwealth Office.<br><br>(https://www.cybergreen.net/statistics/) | The index is based on open source intelligence (secondary data) collection then put into the Collective intelligence Framework (CIF) and stored in an elastic search database. | The CyberGreen project seeks to collect and present comprehensive data on infections or vulnerable systems on the Internet, measure it based on six metrics, visualise it, and re-distribute it to countries, CERTs, or ISPs. The index focused on helping to improve the health of the global Cyber Ecosystem. The v2.0 CyberGreen Index equates risk to others to the size of unmet mitigation tasks required to zero the country's, the AS's, or the alternate entity's risk to others. | 145 countries | Rank and Score |

Table 2.1 Global CCB models (ITU 2017b)

The Global Cyber Security Capacity Centre (GCSCC) at Oxford University has taken a step towards closing the gaps between the works of these organisations, with the foundation of the Cyber Security Capacity Maturity Model (CCMM) (Muller 2015; GCSCC 2017). This model has been developed through collaboration with international stakeholders, this academic model is politically neutral, offering a comprehensive analysis of CCB through five different dimensions: (i) Cybersecurity Policy and Strategy; (ii) Cyber Culture and Society; (iii) Cybersecurity Education, Training, and Skills; (iv) Legal and Regulatory Frameworks; and (v) Standards, Organisations, and Technologies. Each dimension includes multiple factors and attributes, each making a significant contribution to CCB.

Alongside with these concepts Pawlak (2014) proposing some principles, which bring an overview of how CCB should be understood (Hameed et al. 2018). These principles include:

- Increase education and awareness across all government sectors by establishing Cyber knowledge agency.
- Principles-based CCB models, principle-based approach solutions, and best practices.
- Closing the 'cyber capacity gap' developed vs developing countries.
- Identify substantial overlaps or gaps by conducting continuous mapping of CCB activities.
- Enhance Computer Security Incident Response Teams (CSIRTs), forensics capabilities, law enforcement capacity and strategies.
- Consider human rights
- Seek advice from regional and global champions who are mature and willing to engage.

These principles are important to perceive how the countries in a transitional stage are understanding, approaching CCB and how these principles are manipulating CCB

models as will be studied later in this study. Since this study is aiming to assess and contextualise the problem space of cybersecurity capacity in counties that are in a transitional phase based on five areas: Organisational, Technical, Legal, Cultural, and Education. Based on the given criteria, the applicable models for measurements were the GCI index and the CCMM (GCSCC 2017; ITU 2018a).

The GCI index examines levels of commitment on five distinct pillars (ITU 2017a, 2018a): 1. Legal. 2. Technical. 3. Organisational. 4. Capacity building, and 5. Cooperation. The index applying different mechanisms for assesses cyber maturity to derive rankings and scores that empower comparisons between states and regions. In this study, direct one-to-one mapping between the CCMM Dimensions and the GCI Areas, such as in the areas of strategy, legal and technical, there are GCI pillars such as Capacity Building and Cooperation that cut across all CCMM Dimensions. This mapping is adapted from analysing trends and success factors of international cybersecurity capacity building initiatives study by Hameed et al. (2018). The study shows that, the results of mapping CCB to the CCMM AND GCI. The gathered CCB initiatives, it noticeably reveals that about half of the initiatives 47% are geared towards the first dimension of the CCMM model, Cybersecurity Policy and Strategy; followed by the fourth dimension: Legal and Regulatory Frameworks 33%. The third dimension: Cybersecurity Education, Training and Skills concerns 14% of the initiatives, followed by the fifth dimension: Standards, Organisations, and Technologies with 7%, and lastly the lowest number of initiatives are focused on the second dimension Cyber Culture and Society 7% (Hameed et al. 2018). Table (2.2) the results of mapping CCMM dimension with GCI pillars.

The reason for mapping the CCMM dimensions with ITU GCI Pillars is to validate and verify the results of focus group discussion in **Chapter 5**. The GCI reports 2017and 2018 (ITU 2017a, 2018a) along with other official government or ministry websites will provide further information used to define the particular stages of maturity for each factor of the CCMM. In next section, the dimensions of CCB are presented in more details.

| CCMM Dimensions | ITU GCI Pillars | |
|---|---|---|
| Cybersecurity Policy and Strategy | Organisational | Cooperation |
| Cyber Culture and Society | - | |
| Cybersecurity Education, Training and Skills | Capacity building | |
| Legal and Regulatory Frameworks | Legal | |
| Standards, Organizations, and Technologies | Technical | |

Table 2.2 mapping CCMM dimension with GCI pillars.

### 2.8.2 Dimensions of Cybersecurity Capacity Building (CCB)

This section presents an overview on dimensions of cybersecurity capacity building. These dimensions are chosen based on main pillars of ITU GCI and the CCMM that build cybersecurity capabilities: human capacity, strategies and organisational, infrastructure protection, technology, law and regulation.

#### 2.8.2.1 Cybersecurity Strategies

Over the past decade, national regimes have been developing national cybersecurity strategies (NCS) to address emerging threats associated with the rapidly expanding use of ICT. These cybersecurity issues have evolved into significant national-level problems that require government consideration, including the protection of assets, systems, and networks vital to the operation and stability of a nation, and the livelihood of its people. Threats against these critical resources target corporations and citizens and include cybercrime such as identity theft and fraud, politically motivated -hacktivism, and sophisticated economic and military espionage (Goodwin and Nicholas 2013; Asadli 2018).

In many countries, NCS has become a priority supported by stronger leadership and establishment of a National Council for Cybersecurity with a clear mandate, appropriate statutory powers, and an organisational structure is required (Goodwin and Nicholas

2013; GCSCC 2017). The rationale for creating the council is to perform a crucial function in coordinating across different organisations in the public and private sectors. Also, forming a strong leadership role at the highest level contributes to recognition of the NCS. Many countries around the world have established, or are looking to establish, agencies or other administrative bodies to manage their cybersecurity strategy . For instance, the organisational structure in France is highly centralised and is consistent with France's wider political structure. Meanwhile, in Finland the organisational structure reflects the existing separation of duties between the authorities . From orgnistational prespective, Microsoft has accumulated a set of good practices for structuring and organising an authority. Based on Microsoft an ideal national cybersecurity agency would be composed of five component parts includes: Policy and planning unit; Regulatory unit; Outreach and partnership unit; Communications unit; Operations unit / Computer emergency response team (Paul Nicholas and Kaja Ciglic 2017).

To some extent, the national cybersecurity council will be expected to steer a complex environment that spans other government sectors, national legislatures, established regulatory authorities, civil society groups, public and private sector organisations, and international partners. It is therefore important that all stakeholders have a clear expectation of what the mandate of the national cybersecurity agency is, so they know what to expect and who to talk to. It is also critical that the responsibilities of the national cybersecurity agency are distinct from those of other governmental groups involved in cybersecurity (Paul Nicholas and Kaja Ciglic 2017; ITU 2018b).

The roles and responsibilities can be defined using an assignment chart such as the RACI matrix that maps out every task, and assigns roles are responsible for each action item, the personnel who are Accountable, and, who needs to be Consulted or Informed (CTO 2015). This matrix can be used with the Enterprise governance of IT, as defined through COBIT 5. Another asspect related to develop NCS is human capital. The rational for develop a human capital is to close the cybersecurity skills gap and strengthening cybersecurity skills and competences in the state. According to Evans and Reeder (2010), a critical element of a robust cybersecurity framework is having the right people at every level to identify, build and staff the defenses and responses. The

shortage of cybersecurity professionals to address this risk, and a lack of education programs to train these professionals, has led to a human capital crisis in cybersecurity (Evans and Reeder 2010, p.1).

Many states around the world have instituted initiatives for determining the combined necessary knowledge, skills, and abilities (KSA) of cybersecurity such as cybersecurity competency program. Competency is defined by Draganidis and Mentzas (2006, p.52) as: “a specific, identifiable, definable, and measurable knowledge, skill, ability and/or other deployment-related characteristic (e.g. attitude, behaviour, physical ability) which a human resource may possess and which is necessary for, or material to, the performance of an activity within a specific business context”. The term KSAs covers all possible knowledge, skills, and abilities required to perform a specific job function. KSAs are also directly linked to specific actions that are required to complete job tasks (Baranowski and Anderson 2005; Baker 2013).

In the extent of cybersecurity, the most relevant effort in this direction was put in practice by the US government that through the National Initiative for Cybersecurity Education (NICE) and the Department of Labor (DOL) developed standardized professional requirements for cybersecurity (Newhouse et al. 2017). The NICE suggested a National Cybersecurity Workforce Framework, that defines seven groups of typical job duties, covering cybersecurity work in 31 speciality areas across industries, organizations, and job types as shown in Figure 2.6. For each of such areas, the Framework clearly identifies knowledge, skills, and abilities that professionals must demonstrate to perform their job tasks effectively. The seven categories, that correspond to typical cybersecurity professional positions, are the following:

- Securely provision : responsible for conceptualizing, designing, and building secure IT systems.

- Operate and maintain : responsible for providing support, administration and maintenance necessary to make IT systems secure without affecting effectiveness and efficiency.

- Protect and defend: responsible for identification, analysis, and mitigation of threats internal to IT systems or networks.

- Investigate: responsible for investigation of IT systems and networks aimed at identifying suspect events, potential crimes and digital evidences.

- Collect and operate : responsible of specialized denial and deception operations and collection of cyber security information that may turn useful to develop intelligence.

- Analyse : responsible for highly specialized review and evaluation of incoming cyber security information to determine its usefulness for intelligence.

- Oversee and Govern: responsible of providing leadership, management, direction, and development needed to allow individuals and organisations to effectively conduct cybersecurity work.

For instance, to build skills required in this dimension, the Oversee and Govern category is used (NICE 2016). This category provides details about the knowledge, skills and abilities that needed to manage cybersecurity. These knowledges such as; Knowledge of cyber threats and vulnerabilities; Knowledge of cybersecurity and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data; Knowledge of resource management principles and techniques.

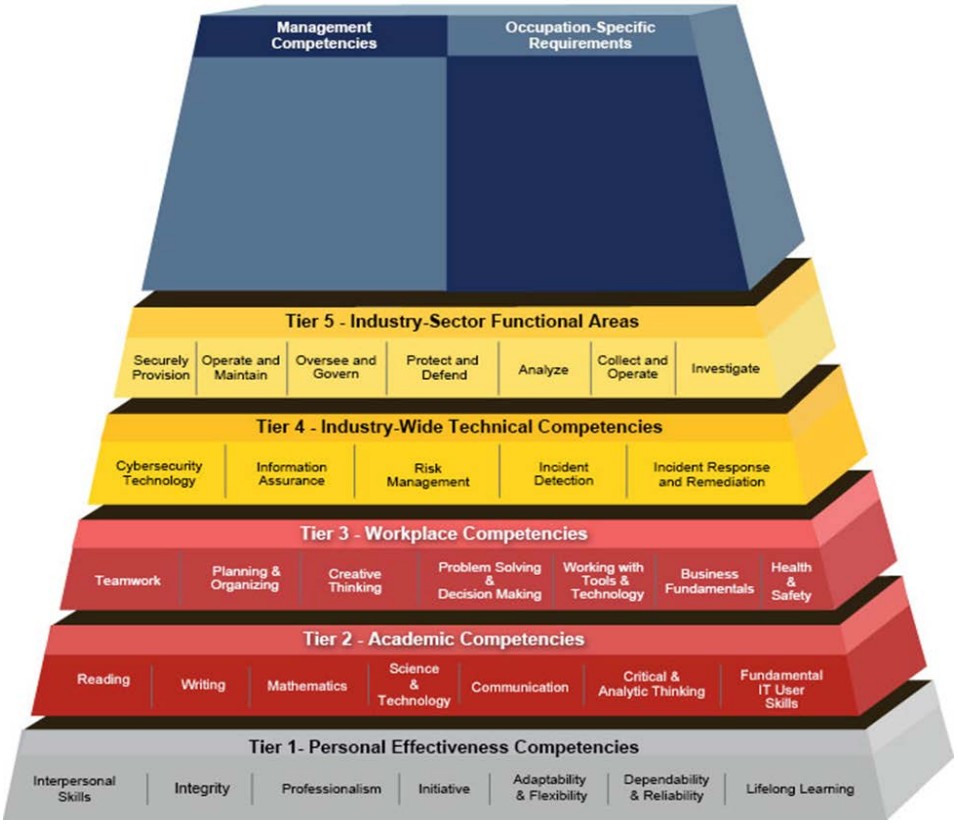



Figure 2.6 NICE Cybersecurity Competency Model (NICE 2016)

The skills required such as; creating policies that reflect system security objectives; Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes. The abilities for example; ability to identify critical infrastructure systems with information communication technology that were designed without system security considerations; ability to integrate information security requirements into the acquisition process; using applicable baseline security controls as one of the sources for security requirements; ensuring a robust software quality control process; and establishing multiple sources (e.g., delivery routes, for critical system elements).

To develop NCS, guiding principles are used to guide the preparation and enforcement of cybersecurity policies. Many existing frameworks such as ITU, ENISA, Microsoft and Commonwealth approach (Goodwin and Nicholas 2013; CTO 2015; ENISA 2016;

ITU 2018b) provides principles, which taken together in the development of NCS. These guiding principles are;

- Risk-based. Assess risk by identifying threats, vulnerabilities, and consequences, then manage it through mitigations, controls, costs, and similar measures;
- Outcome-focused. Focus on the desired end state, rather than prescribing the means to achieve it, and measure progress towards that end state;
- Prioritised. Adopt a graduated approach to criticality, recognizing that disruption or failure are not equal among critical assets or across critical sectors;
- Practicable. Optimise for adoption by the largest possible group of critical assets and implementation across the broadest range of critical sectors;
- Respectful of privacy and civil liberties. Include protections for privacy and civil liberties based upon the established privacy and civil liberties policies, practices, and frameworks;
- Globally relevant. Integrate international standards to the maximum extent possible, keeping the goal of harmonization in mind wherever possible.
- Appropriate set of policy instruments. The Strategy should utilise the most appropriate policy instruments available to realise each of its objectives, considering the country's specific circumstances.

2.8.2.2 Risk Management and Critical Infrastructure Protection

Building a risk management approach is another important factor in this dimension. Risk defined as "future situations or circumstances that exist outside of the control of the project team that will have an adverse impact on the project if they occur (Dey et al. 2007). It is defined also as the influence of uncertainty on the attainment of goals (ISO31000 2009; Purdy 2010). Barata et al. (2015) provided what a definition for risk includes (i) when the expected outcome of an event differs from the real outcome and

(ii) the impact that is connected with the outcome. Furthermore, the risk is gained more attention in information system researches for example, in business process management (BPM) and enterprise modelling (Barata et al. 2015).

The literature has discussed different stages of the risk management process. In (Guiling and Xiaojuan 2011; Avdoshin and Pesotskaya 2016) they mentioned that most of the methods of risk management divided into risk identification, risk analysis, risk planning or mitigation, risk monitoring and control. Boehm (1991), categorised the risk management process into risk identification, analysis, prioritisation and control.

According to NIST (2014b), the risk management framework delivers a process that integrates security and risk management activities into the system development life cycle. The risk-based approach to security control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, Executive Orders, policies, standards, or regulations. On the national level there are several high-level guidance documents concerning the process of establishing a National-level Risk Assessment. These range from generic guidance, which applies to Risk Analysis at the national level, to specific guidance looking at Critical Information Infrastructures (CII) (ENISA 2013).

Identify the Critical Infrastructures (CI) assets and critical National Information infrastructure (CNI), are crucial to develop measures and procedures for the protection of CNI and reduce the risk of cyberattacks. The Critical Infrastructures (CI) is a term used to describe assets that are essential to the functioning and security of a society and economy in any given nation; and Critical Information Infrastructures (CII) are IT and ICT systems that operate key functions of the critical infrastructure of a nation (ITU 2018b). States addressing the topic of Critical Infrastructure Protection (CIP) are sometimes hampered because of their confusion and lack of clarity about the key concepts, related definitions and terminology. In the CIIP area, such confusion is sometimes caused by the fact that a relatively small group of experts tries to convey the CIIP concept to government policy-makers in unnecessarily complex terminology (Luiijf et al. 2016).

According to Luiijf and Klaver (2019), most of the CI-related efforts stem from the national homeland security, antiterrorism and all hazard disaster approaches. In addition, the economic pillar responsible ministry in nations often covers the digital domain and cyber security policies. Societies critically depend on the proper functioning of the CI such as energy supply, telecommunications, financial systems, drinking water, and governmental services. In turn, these CI often critically depend on the proper functioning of CII. CII is a complex concept and includes information and communication technologies (ICT), and operational technologies (OT). OT is also known as industrial control systems and SCADA systems that monitor and control critical cyber-physical processes. The CII comprises (1) critical ICT infrastructures (e.g. mobile telephony and internet services), (2) critical ICT and OT systems that are part of each CI, and (3) new CII services beyond these established domains (Luiijf et al. 2016).

CIIP is a critical component of cybersecurity systems and is most frequently stated or written about in relation to cybersecurity, in particular as regards National Cybersecurity Strategies (NCS) and National Cybersecurity Centres (NCSC) (Luiijf and van Schie 2017). Based on literature, four methodological methods offer a systematic approach to the identification process. These steps were inspired by the European Critical Infrastructure Directive which starts bottom-up from within a sector that potentially may be critical (Klaver et al. 2011; Luiijf and van Schie 2017) :

- Apply sector-specific criteria, a first selection of CI and CI services within a sector can be made based on sector-specific criteria. Such criteria may be the market share, the transport capacity, cross-border connectivity, and supply of critical services to government, industry or population. This step also narrows down the number of potential CI operators in the case where the sector has multiple operators. Be aware that sector-specific criteria may be treated as classified information by some nations as they could reveal dependencies, vulnerabilities and sensitivities. This leads to a short-list of CI from which further deliberations are to be made. This method clearly favours objective, quantifiable criteria rather than subjective, qualitative criteria (Luiijf and van Schie 2017). Table (2.3) provides an example on how Criticality Scale for national infrastructure in the UK.

| Criticality Scale | Description |
|---|---|
| **Cat. 5** | This is infrastructure the loss of which would have a catastrophic impact on the UK. These assets will be of unique national importance whose loss would have national long-term effects and may impact across a number of sectors. Relatively few are expected to meet the Cat 5 criteria. |
| **Cat. 4** | Infrastructure of the highest importance to the sectors should fall within this category. The impact of loss of these assets on essential services would be severe and may impact provision of essential services across the UK or to millions of citizens. |
| **Cat. 3** | Infrastructure of substantial importance to the sectors and the delivery of essential services, the loss of which could affect a large geographic region or many hundreds of thousands of people. |
| **Cat. 2** | Infrastructure whose loss would have a significant impact on the delivery of essential services leading to loss, or disruption, of service to tens of thousands of people or affecting whole counties or equivalents. |
| **Cat. 1** | Infrastructure whose loss could cause moderate disruption to service delivery, most likely on a localised basis and affecting thousands of citizens. |
| **Cat. 0** | Infrastructure the impact of the loss of which would be minor (on national scale). |

Table 2.3 Example: Criticality Scale for national infrastructure (CabinetOffice 2010)

- Assess criticality; this step is to assess criticality of the short-list from the previous step based on the nation's CI definition.

- Assess dependencies; this step is used to identify CI dependencies. CI sectors and their critical services have dependencies with other CI sectors and their critical services.

Assess crosscutting criteria; crosscutting criteria may support the criticality of certain infrastructure services to a nation, both under normal circumstances and during emergencies. Conducting risk assessment is part of risk management. The rational of conducting risk assessment is to identify the threats to national security on cyberspace. According to Dorfman (2007), a distinction is often made between risk analysis (or risk assessment) and risk management (i.e. the implementation of measures to address the risk identified, which might be to avoid, reduce, share or retain the risks). Definitions used in a particular risk assessment will need to take into account that, from an operational perspective, it may be possible to significantly reduce a risk (rendering the chances of it occurring infinitesimally small), but that statistically it may not be possible to eliminate it entirely (ENISA 2013). Risk assessments can be implemented for many reasons and have many purposes. The purpose of risk assessment according to (ISO31000 2009) is to "provide evidence-based information and analysis to make informed decisions on how to treat particular risks and how to select between options".

The use of a consistent risk assessment process allows an organisation to understand risk levels, compare those risks, and address those with the greatest risk first. Literature shows that there are some useful guidance on the practice of risk assessment in the context of national and international risks, but much of the of them concerns risk analysis in the context of organisational ICT risks, rather than national-level risk assessment (ENISA 2013). These guidance and standards such as; ISO 27005: 2008, ISO 15408: 2009 and ISO 31010:2009 (reference). In addition, some guidance was identified on conducting cybersecurity and CII-related Risk Assessments at the organisational level. As an example NIST risk assessment technique from the US National Institute of Standards and Technology (NIST) and the UK HMG Technical Risk Assessment IA Standard No. 1. In addition, ENISA has an extensive inventory of the most common Risk Analysis methods (HMG 2009; ENISA 2011; NIST 2012). According to ENISA (2013), in some of the countries, cyber National-level risk assessments sometimes sit alongside risk assessments done in other sectors. Figure (2.7) demonstrates the national-level structures when this is the case.

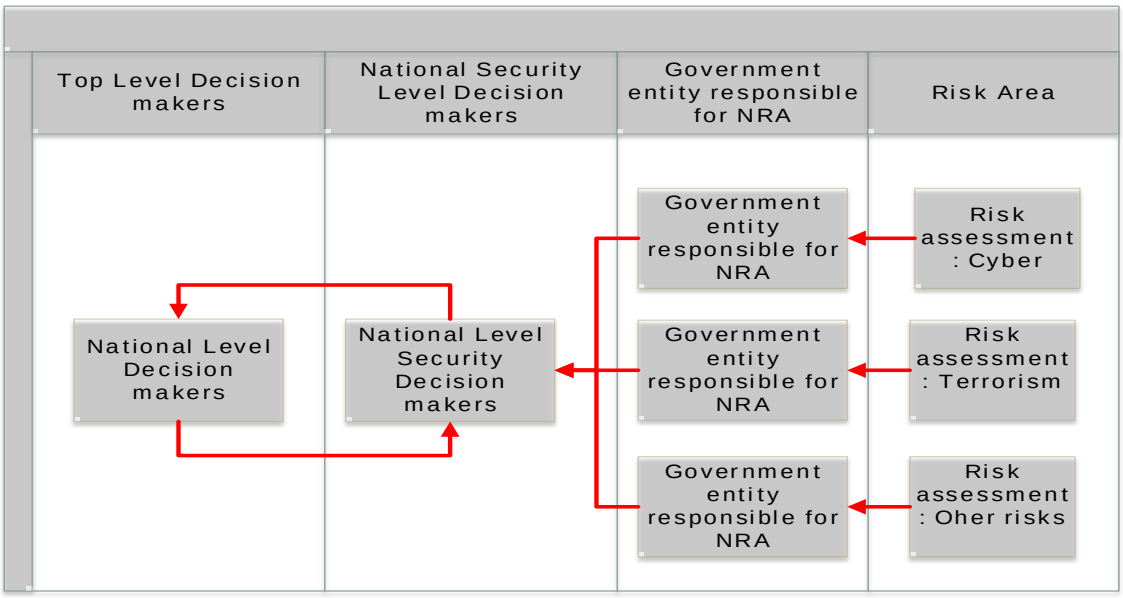



Figure 2.7 Risk inputs to senior decision-makers adapted from (ENISA 2013)

Moreover, ENISA (2013) study has presented findings oh research conducted to identify how countries have implemented their National-level Risk Assessment, key challenges and lessons learned in domain of cybersecurity. Based on these findings ENISA have provided the possible inputs to the National-level Risk Assessment as shown in Figure 2.8.

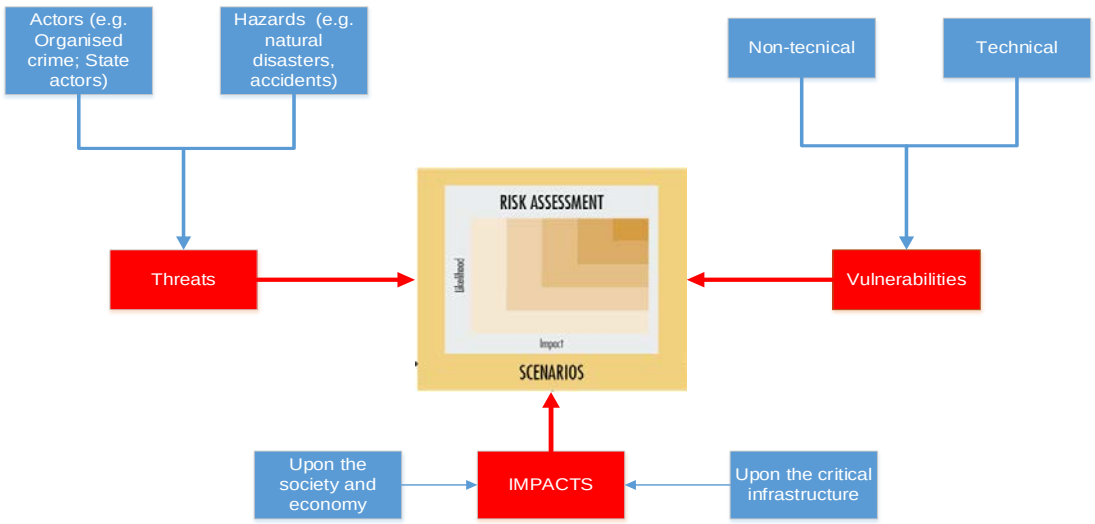



Figure 2.8 National-level Risk Assessment adapted from (ENISA 2013)

A list of commonly used component-driven cyber risk management and assessment frameworks can be found at (NCSC 2016). The list also includes a brief description, an overview of how they work, who should use it, and an indication of cost and prerequisites. Examples of these frameworks are represented in Table (2.4).

| Method / Framework | What is it? | How does it work? | Who is it for? | Cost and prerequisites |
|---|---|---|---|---|
| ISO/IEC 27005:2011 | An international standard providing guidelines for information risk management. Although it does outline a generic risk assessment process, it leaves the choice of that risk assessment technique to the business.<br><br>ISO 27005 is part of the ISO 27000 family of standards. | The standard is not prescriptive about which risk management technique should be used. As such, this could encompass system-driven as well as component-driven techniques. However, ISO 27005 requires that a risk assessment takes into account threats, vulnerabilities, and impacts, which emphasises a component-driven approach. | The principles of ISO 27005 can be applied to a variety of types and sizes of organisation. | Given the broad nature of the guidance, specialist skilled resources are needed to tailor the implementation to the requirements of the business. The cost of these resources should be considered along with the cost of purchasing the standards. |
| Information Security Forum (ISF) IRAM 2 | The ISF's risk management methodology is intended to help organisations better understand and manage information risks. | This approach uses a number of phases to identify, evaluate and treat risks through the analysis and assessment of risk components (threat, vulnerability and impact). | IRAM 2 is aimed at organisations. | IRAM 2 is only provided to members of the ISF and organisations will need to have in place information risk management expertise to use it |

| | | | | |
|---|---|---|---|---|
| | | | | effectively. This should be factored into the cost. |
| ISACA COBIT 5 for Risk | COBIT 5 for Risk is provided by ISACA and provides guidance covering the governance of and understanding of enterprise IT risk. | COBIT 5 for Risk provides risk management and governance framework in the form of principles and guidance. | COBIT 5 for Risk is likely to suit organisations seeking to improve their approach to security risk management and governance | The COBIT 5 for Risk book is available for purchase on the ISACA website. An organisation looking use COBIT 5 for Risk will also need to take into account any specialist resources necessary to implement its guidance and principles. |

Table 2.4 Examples of Risk Assessment and Management Methods (NCSC 2016)

2.8.2.3 Cyber Defence and Military Capabilities

Develop cyber defence capabilities is another important factor in the international indexes. With the development of the cyber as a new tool for politics, espionage and military activities, cybersecurity has become central topic for national and international security. The states addressed in this primary assessment were selected by looking at their levels of military spending and the degree of internet connectivity, assuming that those states with low military spending and little internet connectivity would be less likely to have cyber capabilities (Lewis and Timlin 2011). Many states has recognised that cyberspace has emerged as a war-fighting domain in its own right and will enhance deterrence in air, space, and cyberspace by improving the state's ability to attribute and defeat attacks on systems or supporting infrastructure (Pernik et al. 2016).

Lewis and Timlin (2011) in their study, “Preliminary Assessment of National Doctrine and Organisation” identified that 33 states have included cyberwarfare in their military planning and organisation. These range from states with very advanced statements of doctrine and military organisations engaging hundreds or thousands of individuals to more basic preparations that incorporate cyberattack and cyberwarfare into existing capabilities for electronic warfare. Common elements in military doctrine include the use of cyber capabilities for reconnaissance, information operations, the disruption of critical networks and services, for “cyberattacks”, and as a complement to electronic warfare and information operations. Some countries include specific plans for informational and political operations(Lewis and Timlin 2011).

Others tie cyberwarfare capabilities with existing electronic warfare planning. The linkages between electronic warfare and cyberwarfare are likely to be an area of expanded attention as computer networks (or their access points) become increasingly mobile and wireless. In addition, NATO has recognised cyberspace as a domain of military operations, with the Cyberspace Operations Centre as the focal point for coordinating and directing effects in cyberspace in the context of Alliance operations and missions (Bigelow 2019). A NATO Cooperative Cyber Defence Centre of Excellence was established in Tallinn in Estonia. Nearby, at the NATO Cyber Range in Tartu, cyber experts can develop their capabilities through realistic exercises. In United States, the Department of Defence (DoD) defines cyberspace as an operational sub-domain within the information environment, formed of technology infrastructures and data. The allocation of ‘domain’ status to cyberspace

(alongside maritime, land, air, and space) serves a bureaucratic purpose to ensure that CO receives sufficient financial and material support. The US has established on 1 October 2010 and was intended to be the Army's single point of contact for external organizations regarding information operations and cyberspace (Bellasio et al. 2018).

From academic literature perspective, a framework for a cyber defence doctrine has been developed and identifies five questions, presented in Figure 2.9 below, that should be considered when developing a cyber defence doctrine. Each concept builds upon the other. The intent is to define a single solid and comprehensive baseline framework upon which more complex concepts can be developed in the future. A consistent international military language would also assist in communication between multinational partners and the creation of integrated doctrine across services and nations (Ormrod and Turnbull 2016).

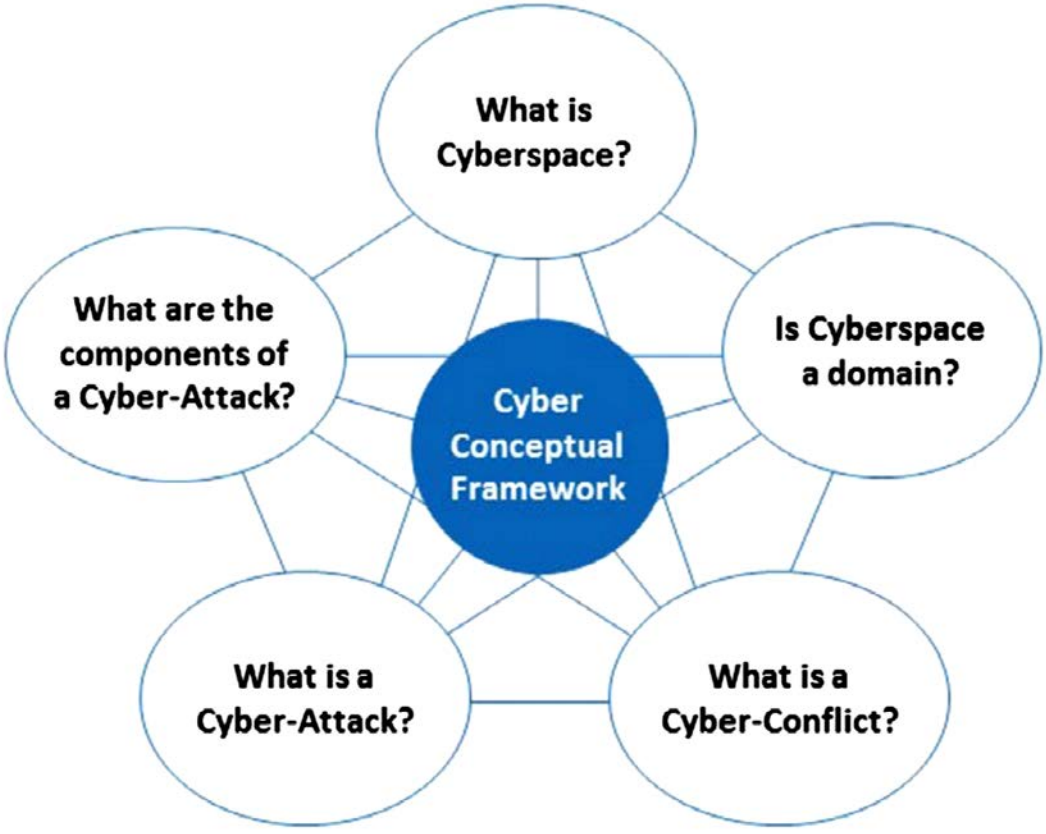



Figure 2.9 Basic framework for a cyber doctrine (Ormrod and Turnbull 2016)

2.8.2.3 National Incident Response Capabilities

Building a National Incident Response Capabilities also considered as crucial part in developing CCB. Launching a national cybersecurity incident management capability can be

an important step in managing cyber threats (Haller et al. 2010; Bellasio et al. 2018). Often, this capability takes the form of one or more National Computer Security Incident Response Teams (National CSIRTs) or Computer Emergency Response Teams (CERTs hereinafter referred to collectively as CSIRTs responsible for managing incident response in the event of natural or man-made cyber-related disasters that affect critical services and information infrastructures (Demchak et al. 2015). Establish a national-level CSIRT not only from a technical viewpoint but also through the development of appropriate organisational and communication measures (Bellasio et al. 2018). According to Bellasio et al. (2018) several guides exist that outline activities required to establish a CSIRT such as:

- Defining a mission (what does the CSIRT intend to do?);
- Identifying relevant stakeholders;
- Defining the CSIRT's position in the wider institutional framework;
- Defining a constituency (for whom does the CSIRT act?);
- Establishing a CSIRT through legal frameworks;
- Defining capabilities and services offered by the CSIRT (consistent with the mission);
- Establishing an organisational structure, both internally and in relation to other organisations.

The National CSIRTs and organisations like them ideally act as critical components of the national cybersecurity strategy (Haller et al. 2010; CTO 2015). The implementation of CSIRTs is considered one of the best starting points for countries in transitional stage in the effort to secure cyberspace. Since they collect and analyse information about computer security incidents on a daily basis, National CSIRTs are an excellent source of lessons learned and other information that can help stakeholders mitigate risk. National CSIRTs can also help catalyse a significant national discussion about cybersecurity and awareness by interacting with private and governmental sectors (Haller et al. 2010). Establishing an organisational structure, both internally and in relation to other organisations is vital because it provides clear delegation of roles and responsibilities in a CSIRT (Haller et al. 2010;

Bellasio et al. 2018). The following elements are recommended as a minimum initial structure (ENISA 2015; Bellasio et al. 2018):

- Management: This includes strategy, budget, operational organisation, liaison and communication with external stakeholders, and media relations.
- Operations: This includes incident management and monitoring of threats.
- IT: This includes maintenance of the IT infrastructure, and support to operations and research and development (R&D).
- R&D: This includes research into developing technology, statistical analysis of threat and incident trends, development of systems and tools, training, and support to operations.
- Support services: This includes marketing, legal support, media relations, administration and finance.

The most crucial point in establishing national CSIRT is identifying relevant stakeholders who may both support and benefit from its existence. Most literature (Haller et al. 2010; Bada et al. 2014; Bellasio et al. 2018) indicates that In the case of a national CSIRT, the community of stakeholders engaging with it typically includes:

- Government and government agencies
- Law enforcement agencies
- Defence establishment
- Academic sector
- Internet service providers (ISPs)
- Financial and other critical sectors
- National and international organisations working groups.

In addition to the identifying relevant stakeholders, the capabilities and role of a national CSIRT should also be defined (Haller et al. 2010; Bellasio et al. 2018). According to (ENISA 2015), these capabilities can be broken down into four categories as follows :

- Formal capability refers to the official mandate of the CSIRT
- Operational-technical capability refers to the technical services that the CSIRT provides to both external and internal organisations.
- Operational-technical capability refers to the technical services that the CSIRT provides to both external and internal organisations.
- Operational-technical capability refers to the technical services that the CSIRT provides to both external and internal organisations.

Maintain trust and cooperation relationships is important factor after identify relevant stakeholders. On a national level, national / governmental CSIRTs cooperate with numerous organisations, first and foremost with their constituencies. And, depending on the country, a national / governmental CSIRT will also have cooperative relationships with stakeholders such as law enforcement agencies, the military and intelligence community, policymakers, other CSIRTs (ENISA 2010). According to Haller et al. (2010), by forming relationships and partnerships with owners and operators of national critical infrastructure and other key constituents, the National CSIRT gains access to information crucial to its operations. These relationships and partnerships are directly with the National CSIRT and among constituents. The National CSIRT may act as a trusted communications channel between key constituents. If organisations and end users do not specifically trust the CSIRT, they will not be able to exchange the data with the CSIRT and will not be able to access all the facilities on offer. Trust is important for partner organisations and the organisations themselves would want assurance that the CSIRT will treat confidential information safely (Bada et al. 2014).

Define, document and operate incident response processes are main responsibility of national CSIRT. An incident-handling response process is a set of defined steps that a CSIRT will follow to successfully counter a cybersecurity incident. It is a method that is defined and developed independent of a specific incident, with the aim of developing a framework that enables a structured, coordinated, methodical and consistent approach to incident response. (Bellasio et al. 2018). Cyber incident response (IR) according to (NCSC 2019) is complicated

by two factors. Firstly, no two incidents are ever the same. Secondly, all responses require people, process and technical elements to work together in order to be successful. Incident-handling response processes are regularly established at a high level, and then refined into more specific procedures for particular types of attack (Bellasio et al. 2018). A good example of an incident response process is from the National Institute of Standards and Technology (NIST). NIST framework structures incident handling response process into four key stages as shown in Figure (2.10) (Cichonski et al. 2012). These processes are:

- Preparation refers to the period before an incident occurs;
- Detection and analysis aims to identify and understand a cyber-attack once it has occurred;
- Containment, eradication and recovery refers to the period after the initial identification and analysis of a cyber-attack.; and
- Post-incident activity that involves collecting and storing information and evidence from the incident, and identifying lessons learned from the response in order to improve future incident-handling processes.

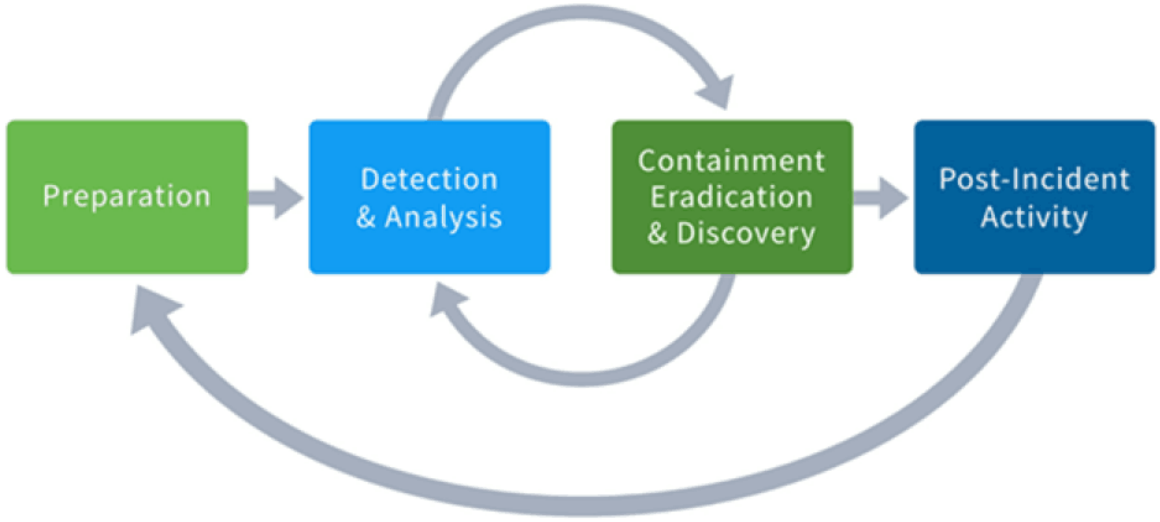



Figure 2.10 NIST Incident Response Life Cycle (Cichonski et al. 2012)

The National CSIRT / CERT will provide the most up- tools and guidance and the guidance they offer must be sound that demands high standards of professional competence in order to retain this benefit. This may lead to the CSIRT having only a small number of good quality

capabilities in the beginning, rather than lots of poor quality capacities (Haller et al. 2010; Bada et al. 2014; Bellasio et al. 2018). A variety of tasks can be needed by the CSIRT team to ensure that incidents are handled and organised effectively. It is crucial to insure that the CSIRT is equipped with an adequate number of personnel with the appropriate qualifications to execute its incident response functions (Haller et al. 2010; Bellasio et al. 2018).

The set of basic skills of CSIRT staff are separated into two broad groups: personal skills and technical skills. The staff of the CSIRT, who are technologically skilled and have outstanding leadership skills, will improve the reputation of the team and increase the confidence of the team (both the public and those with whom the team interacts) (Bada et al. 2014; SE-Institute 2017). The personal skills required such as, Communication skill, Ability to Follow Policies and Procedures, Team Skills, and Problem Solving. Meanwhile, the specific technical skills required by CSIRT members have been split into two categories: technical base skills and incident management skills (Bada et al. 2014; SE-Institute 2017). Technological foundation skills include a clear knowledge of the fundamental technology utilised by the CSIRT and the electoral district, as well as an awareness of the problems surrounding the department or part.

Incident management capabilities require an understanding of the procedures, decision points and support mechanisms (software or applications) needed for the day-to-day operation of CSIRT operations (SE-Institute 2017). There are several frameworks developed by international organisations such as Cybersecurity Workforce Framework from the National Institute of Standards and Technology of the United States (US) Department of Commerce, through the National Initiative for Cybersecurity Education (NICE) (Newhouse et al. 2017). This framework can be used to map the knowledge, skills and competences required for different types of cybersecurity professional roles, including those pertaining to CSIRTs and incident response more broadly (Bellasio et al. 2018).

#### 2.8.2.4 Cyber Culture and Awareness

Cybersecurity culture is referred to the beliefs, expectations, behaviours, values, opinions and awareness that people have about information security and how they communicate with technology (ENISA 2017). According to Gcaza et al. (2015), technology alone cannot be a shield against cyber-attacks, but humans can take centre stage across the culture of cybersecurity. Security of valuable information, infrastructure and individuals from cyber-attacks has become crucial, because most countries, particularly countries in transformation

phases, are transforming into information societies. For these reasons, bulling cybersecurity culture capacity is needed among society at the individual and governmental level. A solid cybersecurity culture is transforming people's mind-sets and technology habits, which should serve as a human shield against threats without coercion (ENISA 2017).

To improve national cybersecurity culture and awareness capacity many factors and aspect needs to be considered. These aspects such as, cybersecurity mind-set and behavior change among the public sector, the private sector, individual users and other actors present in the cyber ecosystem. Improve e-services, in order to promote the required level of trust including using government e-services and e-commerce platforms. Develop an evaluation criterion and reporting mechanisms to promote information sharing and Effectively communicate the benefits of paying attention to threats and vulnerabilities (Bellasio et al. 2018).

Develop a national awareness program is to influence the implementation of secure behaviour online. However, effective influencing requires more than simply notifying people about what they should and should not do: they need, first of all, to accept that the information is relevant, secondly, understand how they ought to respond, and thirdly, be willing to do this in the face of many other demands (Bada et al. 2019a). Awareness is not training. Security awareness activities are designed to change behavior or reinforce good security practices (Wilson and Hash 2003). The purpose of awareness program is simply to focus attention on security and allow individuals to recognize IT security concerns and respond accordingly (Bada et al. 2019a).

To develop the awareness program, the agency's awareness and training needs to be identified, and wide awareness and training plan is developed, organisational buy-in is required and secured, and priorities are established. According to Bada et al. (2019a), following factors can be extremely helpful at enhancing the effectiveness of current and future campaigns: (1) security awareness has to be professionally prepared and organised in order to work. (2) Invoking fear in people is not an effective tactic, since it could scare people who can least afford to take risks. (3) Security education has to be more than providing information to users it needs to be targeted, actionable, doable and provide feedback. (4) Once people are willing to change, training and continuous feedback is needed to sustain them through the change period. (5) Emphasis is necessary on different cultural contexts and characteristics when creating cybersecurity awareness campaigns.

An awareness campaign should use simple consistent rules of behaviour that people can follow. This way, people's perception of control will lead to better acceptance of the suggested behaviour (Bandura et al. 1999; Ajzen 2002). There is a numerous behaviour change techniques are useful and can be used in awareness program. These techniques such as, Behaviour change wheel by (Michie et al. 2011) and Johnson and Scholes' Cultural Web Model (Johnson and Whittington 2009) as shown in Figure (2.11).

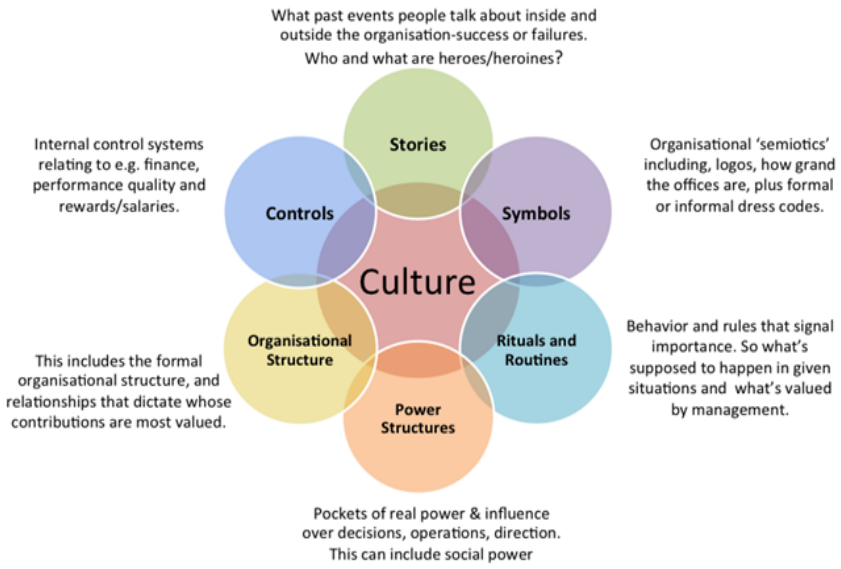



Figure 2.11 Johnson and Scholes' Cultural Web (Johnson and Whittington 2009)

An awareness campaign also needs to be monitored and evaluated. Based on literature a set of criteria has been suggested to evaluate the effectiveness of the awareness campaign. These criteria such as; benchmarks must be declared; success indicators must be defined; and periodic status reports must be generated (Kortjan and Von Solms 2014; Bellasio et al. 2018; Bada et al. 2019a). Focusing on the design and implementation of awareness raising programs, literature suggests that successful awareness programs need to be a "learning continuum" (Kritzinger et al. 2017; Bada et al. 2019b).

Improve e-services, in order to promote the required level of trust including using government e-services and e-commerce platforms are another vital factor in this dimension. According to Fakhoury and Aubert (2015), Trust has become a key area in e-government literature since it is a factor for the adoption of e-government. Citizens are reluctant to use e-government services mainly for security, privacy and transparency issues. Trust in government is "based on the individual's prior experience when dealing with government"

,while trust in the Internet is associated with user perceptions of the institutional environment, including whether the associated structure, regulation, and legislation make an environment feel safe (Hussein et al. 2010; Fakhoury and Aubert 2015).

This factor considers the trust and confidence of the society in their ability to use the Internet in a secure and private way. It concentrates on trust and confidence in government e-services and private and public sector e-commerce, but it also includes broader use of the Internet outside of these two categories (Juell-Skielse and Perjons 2009; GCSCC 2017). In order to increase the trust and confidence on the cyber space different steps are required. These steps includes, creating an e-government strategy, governance structure, a strategic plan for e-government that includes government eservices, launch and continuously develop government e-services and define benchmarks, success indictors for initiatives and publish periodic. In addition, the setting up of a legal framework is considered essential for its sustainable growth (GCSCC 2017; Bellasio et al. 2018).

Privacy compliance framework is important factor to secure the personal data they process on cyber space. Privacy is a fundamental human right recognized in the United Nation (UN) Declaration of Human Rights, the International Convenant on Civil and Political Rights and in many other international and regional treaties (Finn et al. 2013; Rotenberg and Jacobs 2013). Many countries such as European countries have recognised privacy as fundamental right for many years (Rotenberg and Jacobs 2013). European countries have created toughest privacy and security law in the world the General Data Protection Regulation (GDPR) (European 2018). This framework defines an array of legal terms such as; Personal data, Data processing and Data controls.

Reporting mechanisms are another fundamental factor in this dimension. Reporting mechanisms let individual citizens and businesses to report cybercrime and cyber-attacks directly to relevant public authorities. Reporting mechanisms are important for users to report cyber-enabled crimes, including online fraud, cyber-bullying, child abuse, identity theft, privacy and security breaches, and other incidents (Kortjan and Von Solms 2014; Bellasio et al. 2018). Many countries and international organisation have created useful frameworks for reporting mechanisms. For instance, Action Fraud in the UK , Internet Signalement, France and Consumer Sentinel Network (CSN), USA (GLACY 2014; Gercke 2016).

In case of developing countries, practically those countries in a transitional phase do not have proper cyber culture awareness programs in place. These countries include many Arab spring countries that considered in a transitional stage (Kortjan and von Solms 2012). Recent Arab spring has also brought into highlight another dimension of cyberspace exploitation i.e. destabilising the governments (Zareen et al. 2013). Unlike in developed countries, cybersecurity awareness is not included in the schools and academic curriculum. The lack of awareness in these countries is noticeable in the literature such as in the ITU Cybersecurity Work Program for Developing Countries (Tagert 2010; ITU 2014; Newmeyer 2015).

Existing literature highlighted that many these countries are facing many challenge in adopting e-services in, e.g e-government (Ahmed et al. 2013; Karaim and Inal 2019), e-banking (Farag and Hilles; Elgahwash et al. 2014; MTMC 2016; Ward et al. 2017), e-commerce (Moftah et al. 2012; NISSA 2013; GCSCC 2017) and e-learning (Kitzinger 1995a; Warfield et al. 2002; Gill et al. 2008; Goldman 2010; Herrington and Aldrich 2013; DOE 2014; Hult and Sivanesan 2014). In addition, Many of these countries suffer from the digital, and they are not able to deploy the appropriate ICT infrastructure for e-government deployment (Alshehri and Drew 2010; Forti et al. 2014). Government departments in some of these countries such as Spring Land are using different ICT tools, which make it difficult to centralise the services from various departments and avail to citizens through e-Government platform (Forti et al. 2014).

#### 2.8.2.5 Cybersecurity Education, Training and Skills

Cybersecurity education aspects have been considered as part of national capacity building strategies, workforce development, and education-specific studies (Bellasio et al. 2018; Švábenský et al. 2020). Based on literature review, to develop national cybersecurity education program there are many steps required. These steps include select the task owner and the audience of the cybersecurity education programme, map the existing cybersecurity education landscape and identify gaps in provision, foster research and development in cybersecurity and combine the education with practical training and Preparing future cyber security workforce (McGettrick 2013; Newhouse et al. 2017; Bellasio et al. 2018). According to Bellasio et al. (2018), cybersecurity education is relevant to many different areas of society, from industry and government to academia, primary and secondary education. A designated task owner should be able to engage with each of these sectors, both internally

through collaboration with other government departments that operate in these areas, and externally through engagement with private stakeholders.

Once the task owner is nominated and the audience has been classified mapping and identifying gaps in provision are needed. It is also important to understand present and future requirements in the professional atmosphere, and map these to educational requirements, primarily at secondary and tertiary levels of education (Newhouse et al. 2017; Bellasio et al. 2018). Cybersecurity program cybersecurity should also decide how this programme would actually be delivered (Bellasio et al. 2018). However, develop national cybersecurity education and cybersecurity curriculum guidelines are needed for schools and universities.

There is need for a range of academic degree programs in cybersecurity from the technical aspects to courses based on psychology, psychiatry, criminal justice, business (i.e. policy and economics) and more (McGettrick et al. 2014). Many countries have combined education of cybersecurity and skills at all levels of education. For instance, in the UK cyber strategy has incorporated a schools program to create a step change in specialist cybersecurity education and training for talented 14-18 year olds. These steps involving, classroom-based activities, after-school sessions with expert mentors, challenging projects, and summer schools (HMGovernment 2016). Current strategy include, supporting schools (e.g., "Girls get coding"), providing resources (e.g., The Open University), apprenticeships, support for undergraduate and postgraduate research, cybersecurity career opportunities, and internships (Švábenský et al. 2020). In addition, many international organisation such as; Association for Computing Machinery (ACM); IEEE Computer Society (IEEE CS); Association for Information Systems Special Interest Group on Security (AIS SIGSEC) and International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8), have developed comprehensive curricular guidance in cybersecurity education that will support future program development and associated educational efforts (AMC 2017).

Developing and implementing a professional cybersecurity training platform at a national level is considered an important aspect to possess leadership skills to manage security policies, as well as managerial and communications skills (Yang and Wen 2017). Developed countries such as the United States, structures a holistic framework called the National Initiative for Cybersecurity Education (NICE), under the National Institute of Standards and Technology (NIST) (Newhouse et al. 2017). Said framework would foster a corporation

between government, academia, and the private sector, as it focuses on cybersecurity education, training, and workforce development. Moreover, a cybersecurity career path framework (CyberSeek) by NIST for professionals in this field has been created to cover technical cybersecurity areas (including computer science skills development), non-technical elements (including management and policy) and communication (including skills for communicating technical issues to non-technical audiences) (CyberSeek 2016). An example on how to use this framework is presented in Figure 2.12.

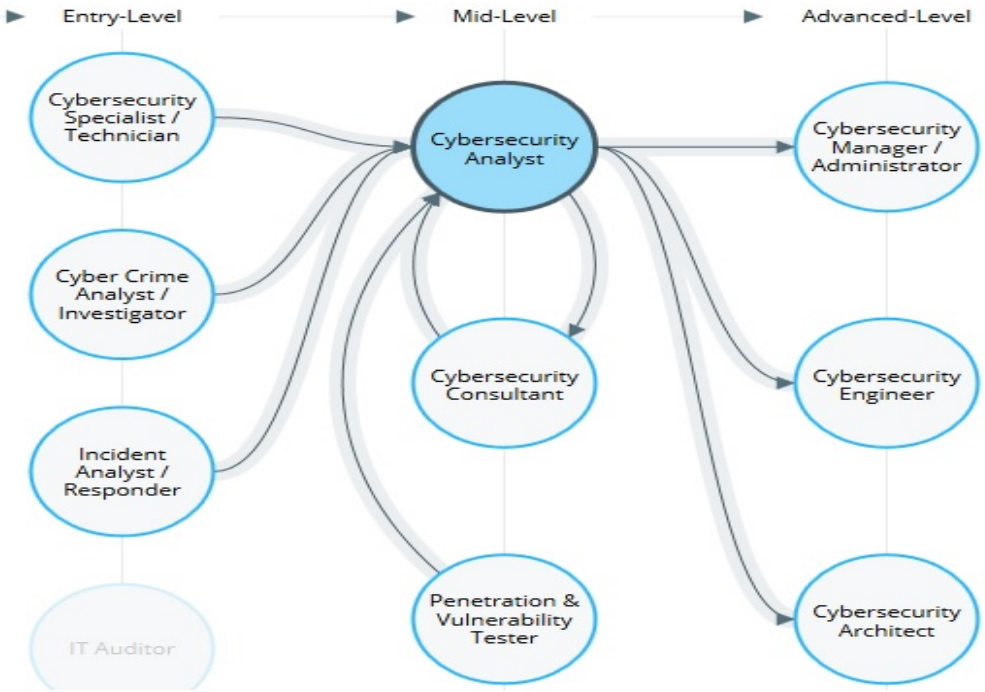



Figure 2.12 an example of CyberSeek career paths (CyberSeek 2016)

In the UK, the National Cyber Security Strategy (NCSS) 2016-2021 has defined one of the main key initiatives to deliver as: "*developing the cyber security profession, including through achieving Royal Chartered status by 2020, reinforcing the recognised body of cyber security excellence within the industry and providing a focal point which can advise, shape and inform national policy*" (HMGovernment 2016). A career framework for security professionals in the UK government (CyBOK) has been created to build the capacity and capabilities of security specialists across government, covering Physical, Personnel, Cyber, Technical Security and Corporate Enablers based on their national strategy (GSF 2020 ). Figure (2.13), shows the knowledge areas that are the foundation of the discipline of cybersecurity in the CyBOK framework (DCMS 2018). In addition, the European agency for cybersecurity ENISA has established roadmap and introduces steps that can be implemented

in order to be in line with best practice in the area of Network and Information Security (NIS) (Berendt et al. 2014).

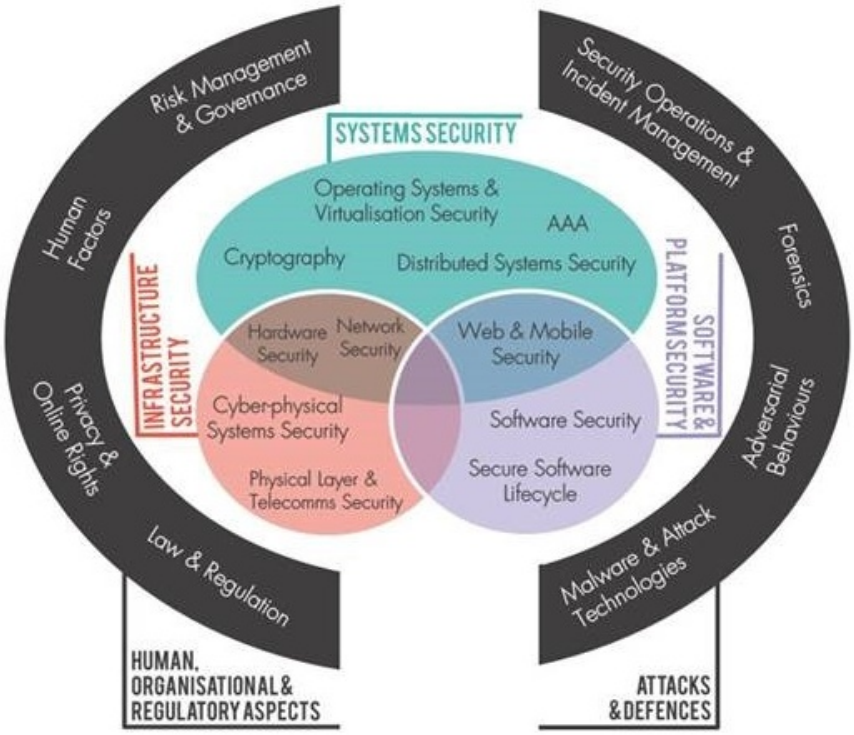



Figure 2.13 the knowledge areas that are the foundation of the discipline of cybersecurity in the CyBOK framework (DCMS 2018).

Among countries in a transitional phase , the literature addresses some aspect of cybersecurity capacity building challenges , including cyber education for children, specific areas of teaching, and regional cybersecurity practices. For instance, some Arab Spring countries are facing many issues due to current political unrest and the austerity measures that affect local government. These issues such as, lack of funding has hindered most of the attempts of advancing cybersecurity including education (Symantec 2016). Muller (2015), stated that cybersecurity capacity is challenge in these countries due to many reasons including institutional stability, and building knowledge. Cyber education in these countries is concisely mentioned as a part of the discussion and as an crucial part of securing cyberspace (Muller 2015). In addition, these countries are facing other challenges such as, lack of awareness and fear of the consequences of technology in educational bases, lack of training courses for academic staff and increased emigration of academics due to political situation (Othman et al. 2013). However, building education capacity and foster research and

development in cybersecurity are needed. This can be done by adopted international formworks as base line to develop their cybersecurity capacity.

2.8.2.6 Legal and Regulations

A legal and regulations framework is a set of guidelines that governs the rights and obligations of government, companies and citizens. It encompasses national legislation, policy, regulations, agreements and where applicable a country's constitution (Bellasio et al. 2018). Cyberspace, as the fifth common domain after land, sea, air and outer space, is in great need for coordination, cooperation and legal measures among all nations (Schjolberg and Ghernaouti-Helie 2011). Lacking a clear legal basis, it can be difficult or impossible to carry out these functions, which in turn places significant limitations on a country's ability to successfully secure cyberspace (Bellasio et al. 2018). Building legal capacity to tackle cyber threats requires from nation states to address many challenges. These challenges according to the WorldBank (2017), limited understanding and experience with cyber laws among different stakeholders, a scarcity of both human and financial resources, developing legislation takes time and enforcing and prosecuting cybercrime is particularly difficult.

Cyber-attacks particularly cybercrime have become increasingly affect national security and stability (Appazov 2014). According to Tikk (2011), attacks with national security implications test the limits of the existing legal framework for data protection, electronic communications and access to public information around the world. The same author suggests ten principles for creating national laws and regulation on cyber space. These rules are including;

- the territoriality principle empowers nations to impose their sovereignty on information infrastructure located within their territory or otherwise subject to their jurisdiction;
- the responsibility principle if the cyber-attacks launched in state's territorial sovereignty;
- the cooperation with other states rule;
- the self-defence rule which means every country has the right to self-defence;

- the Data Protection Rule;
- the Duty of Care Rule, every state has the responsibility to implement a reasonable level of security in their information infrastructure;
- the Early Warning Rule;
- the Access to Information Rule, the public has a right to be informed about threats to their life, security and well-being;
- The Criminality Rule, every nation has the responsibility to include the most common cyber offences in its substantive criminal law;
- the Mandate Rule, an organisation's capacity to act (and regulate) derives from its mandate;

These ten principles outline fundamental concepts and areas that must be included or addressed in a comprehensive legal approach to cybersecurity and raise awareness about existing legal difficulties involving cybersecurity (Tikk 2011). Literature indicated that many international organisations have recommended different steps to develop legal framework. These steps are including development and adoption of relevant legislation supporting the strategy that would enhance cybersecurity. This requires substantive criminal law, procedural law, digital evidence, international cooperation and the responsibility of Internet service providers. The first the necessary substantive criminal-law provisions to criminalize acts such as computer fraud, illegal access, data interference, copyright violations and child pornography (ITU 2009; African-Union 2014).

Substantive law outlines the rights and responsibilities of legal subjects, which include persons, organisations, and states. Sources of substantive law include statutes and ordinances enacted by city, state, and federal legislatures (statutory law), federal and state constitutions, and court decisions (UNODC 2019). Legal framework is varying from state to state. According to UNODC (2019)each state has its own legal system, which affects the creation of substantive criminal law on cybercrime. These systems include Common law, Civil law, Customary law, Religious law and Legal pluralism

Procedural law draws the processes and procedures to be followed to apply and to enable the enforcement of substantive law. A significant part of procedural law is criminal procedure,

which includes general rules and guidelines on the manner in which suspected, accused, and convicted persons are to be handled and processed by the criminal justice system and its agents (Boas et al. 2011; Capers 2018; UNODC 2019).

Another crucial aspect of developing a national legal framework is developing criminal justice power includes Law enforcement and digital forensic power capacity building. These include assign a task owner and develop a cybercrime strategy, developing training modules, provide forensic tools, cooperation platform and regulations. Assigning a national-level cybercrime agency is a vital step in building cybercrime capacity within criminal justice system. Digital forensics competences should also be developed so that law enforcement agencies are able to process, interpret and analyse digital evidence once it has been recovered from a crime scene (Bellasio et al. 2018). Furthermore, cybersecurity policies and techniques for vulnerability disclosure and national and international cooperation mechanisms are required. Vulnerability disclosure technique according to the International Organization for Standardization (ISO) is used to describe the overall activities associated with receiving vulnerability reports and providing remediation information. Additional activities such as investigating and prioritizing reports, developing, testing, and deploying remediation's, and improving secure development are called "vulnerability handling" and are described in ISO/IEC 30111 (ISO/IEC29147 2018).

Establishing cooperation platforms are also considered an important aspect to combat cybercrime. International cooperation has become increasingly necessary for governments, international organisations and private sector actors affected by this type of crime (Boes and Leukfeldt 2017; Bellasio et al. 2018). States need to cooperate since cyber criminals are not limited by national boundaries, and digital evidence relating to a single crime can be dispersed across multiple regions (Cerezo et al. 2007).There are numerous international conventions on cybercrime. For instance, 2001, the Budapest Convention its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation (Weber 2003). In addition, The African Union (AU) has created Convention on Cybersecurity and Personal Data Protection to address cybercrime issues.

In addition to international cooperation among states and law enforcement agencies, partnership mechanisms among public and private sector actors are required. The public and private partnership has repeatedly been referred to as the 'cornerstone' or 'hub' of cyber-

security strategy in different countries and international organisations such as the World Economic Forum, the United States and United Kingdom (Carr 2016). For instance, in the UK, Cybersecurity Information Sharing Partnership (CiSP) has been created to exchange cyber threat information in real time in a secure, confidential and dynamic environment (UK-CERT 2015). The World Economic Forum has provided guidance on Public- Private Information Sharing against cybercrime. The guidance provided key considerations for types of information that should be shared between public and private sectors. These considerations include share all information not limited by legal constraints, information sharing should be a two-way street, no sharing personal information without checking applicable legal framework and better to share processed data than raw data. In addition, said guidance presents main considerations on how information should be shared such as, real-time and 24/7 sharing, secure channels, know you counterpart and share processed data (WEF 2017).

Countries in a transitional phase venture into using cyberspace services without proper legal and regulations frameworks. The Global Cybersecurity Index (GCI) from the International Telecommunication Union (ITU) indicates that most of these countries are lacking of legal and regulations to tackle cybercrime (ITU 2017a, 2018a). According to this report, the main challenge for national criminal legal systems in these countries is the delay between the recognition of potential cyber technology and necessary amendments to the national criminal law.

2.8.2.7 Standards and Technologies

Standards and technologies are important aspects that help countries to develop a secure cyber ecosystem. A large body of literature is frequently growing on the topics of technical information controls, Internet protocols, cryptographic standards, and cybersecurity compliance, auditing and certification processes. Standards help countries and organisation to establish common security requirements and the capabilities and skills needed for secure solutions (Scarfone et al. 2008). Scarfone et al. (2008), indicates that Standards may be compared with certain types of documents, usually called guidelines. Both standards and guidelines provide guidance to enhance cybersecurity, but guidelines usually lack the level of consensus and formality associated with standards.

Cybersecurity standards improve security and contribute to risk management in several significant ways. According to Bellasio et al. (2018), all governments and stakeholders have

a role to play in adopting voluntary and common ICT security, technology, cybersecurity, and risk-management standards and protocols, such as those published by ISO and the International Electrotechnical Commission (IEC). This is because the scope of cybersecurity includes the protection of complex environments, resulting from the interaction of persons, software and services on the cyberspace by means of technology devices and networks connected to it (ENISA 2019). Adhere to standardisations in cybersecurity providing many benefits to countries and organisation. These benefits such as: interoperability, reusability, knowledge development and cybersecurity awareness, harmonisation of terminology, consistency between different manufacturers, vendors and users, repeatability, performance checking, security evaluation, supply chain integrity and security .

Identify baseline ICT security, cybersecurity and risk-management standards and promote their adoption across the public and private sectors is a crucial aspect in building state capacity. Security baselines are useful in improving cybersecurity because they can cover a range of risks that are applicable across a variety of environments (Craig 2018). According to Craig (2018), countries that are evolving security baselines can promote and foster such a holistic cybersecurity risk management approach by focusing on: utilizing an open, collaborative, and iterative development process; bridging risk management understanding both within and between organisations; advancing security through a risk-based and outcomes-focused approach; and leveraging existing best practices to the greatest extent practicable.

In order to benefit from best practice and the economic advantages of global coordination standards and guidelines should be continually adopted (Bellasio et al. 2018). To build capacity in these areas, it is desirable to refer to the latest version of official vendor documentation and the state-of-the-art standards due to the rapid pace of technological development (Bellasio et al. 2018). States can adhere to a numerous of general resources for building capacity in ICT security standards, cryptographic controls, cybersecurity standards, risk-management standards and audited assessment. These include standards from International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC), International Telecommunication Union – Telecommunication Standardization Sector (ITU-T), Internet Engineering Task Force, Institute of Electrical and Electronics Engineers (IEEE) and the World Wide Web Consortium, and National Institute of Standards and Technology (NIST) (Bellasio et al. 2018).

Another vital aspect in building capacity in this dimension is resilience of national Internet services and national critical infrastructure, business continuity plan, technical security controls and enhances physical security of national critical infrastructure. In order to build a national resilience capacity plan, a number of policy areas needed to be addressed. These in particular: good practice guides should be implemented to strengthen the capacity, resilience and survivability of networks; and critical national infrastructure plans for the IT sector should be commissioned. Physical security of national critical infrastructure encompasses all the physical parts of the infrastructure, such as cable links, radio equipment, power systems, connection points, satellite links and building (Bellasio et al. 2018). The threat of cyberterrorism including unauthorized access to a system, disruption or denial-of-service, unauthorized use of a system, or unauthorized changes to system hardware or software — can be as destructive as physical acts of terrorism. Quickly recovering from any type of business interruption is critical to a state's to provide good services on cyber space. This can be achieved by building business continuity plan capacity (Cerullo and Cerullo 2004; Bellasio et al. 2018).

Technical security controls implementations are a responsibility for all actors in the state includes private and public sectors. Several good practices and technical security controls can be implemented, including multi-factor authentication, digital certificates or public key infrastructure and application whitelisting (Scarfone et al. 2008; Bellasio et al. 2018; ENISA 2019).

## 2.9 Chapter Summary

To summarise, this chapter discusses cybersecurity definition, its impact on states, the military concepts of the 5$^{th}$ Domain and the various policies, procedures and good practices from State Institutions, Standards Bodies and Corporations; each providing a different perspective to the domain. The Literature Review narrows down the topics of cyber threat landscape on national security such as, Cyber Crime, Cyber Attacks, Cyber Terrorism and Warfare. It highlighted that, Cybersecurity has become a central issue for many countries; and thus it is becoming extremely difficult to ignore the existence of cyber threats and risks to national security. These serious attacks highlight a significant need to protect critical national resources and have become a tier-1 focus of national concern. The literature shows that, countries in a transitional phase are more likely to face cybersecurity issues as dependency of

governments, private sectors and society on the ICT tools and cyberspace surge over the years.

In addition, this Literature Review discusses the global and organisational cybersecurity frameworks. It has been identified that, the selected frameworks discuss global threats and cybersecurity measures on the global level, they have been mainly focussing on stable and mature nations and environments. Tagert (2010), pointed out that, these approaches to be insufficient for developing countries includes countries in a transitional phase due to the limited technical capacity, ICT maturity levels and socioeconomic conditions and lack of human capital. He found the problems required more multifaceted and tailored approaches aimed at improving the technical capability and policy implementation skills of both government and the private sector in the countries he studied. Yet, despite growing attention from state governments and international organizations, the defense against attacks on national critical systems has appeared to be generally fragmented and varying widely in effectiveness (Atoum et al., 2014).

The chapter also reviewed and discussed the Cybersecurity Capacity Building (CCB) definition, models and dimensions. The literature on CCB model has highlighted that, these models to date have not managed to cover CCB as a whole on a global scale or else they argue for CCB, but without indicating how to go about implementing it (Muller 2015). Some approaches set out a scope that is either too broad or too narrow, while others focus on different ways of highlighting the problems that come with increased access to cyberspace, but without indicating solutions (Muller 2015).

In addition, the reviewed literature emphasised that both stable counties and countries in a transitional phase are facing cybersecurity challenges from managing cyber risks to building cybersecurity capacity. These challenges are likely to be acute in those countries in a transitional phase due to lack of security experts, lack cybersecurity leadership, financial resources, legal capacity to fight against cybercrimes and due to lack of investment in cybersecurity technologies and adhere to cybersecurity standards.

Although extensive research has been carried out on CCB, to our knowledge no single study exists which focuses on countries in a transitional phase. In addition, there are no efforts so far in linking existing frameworks and initiatives with benchmarking models, and thus this effort from the CCMM is presented (Hameed et al. 2018). In addition, there are no studies

addressing the factors that influence the development of a National Cybersecurity Capacity Building Framework NCCBF in a chaos ecosystem.

Thus, this thesis investigates the development of cybersecurity capacity building framework for countries in a transitional using Spring Land as case study. The framework relies on a variety of existing standards, guidelines, and practices to enable countries in a transitional phase to transform their current cybersecurity posture by applying activities that reflect desired outcomes. The following chapter presents the research methodology used to find answers to the research questions earlier defined in **Chapter 1**.

# 3. CHAPTER 3: RESEARCH METHODOLOGY

## 3.1 Introduction

This chapter begins by presenting research paradigms germane to research methodologies, and describes the research design and the process that advances throughout the research. The methodology applied in this study was adopted from the research onion diagram developed by Saunders et al. (2009) to create a cohesive alignment between research objectives and the research methodology. Saunders research onion as shown in Figure (3.1) provides a number of key steps in the positioning of research methodology; the research philosophy, research approach, research strategy and design, and data collection techniques. Moreover, the use of the Saunders' model allows for the discussion of primary and secondary data sources, data collection, and further analysis applied with use of certain techniques.

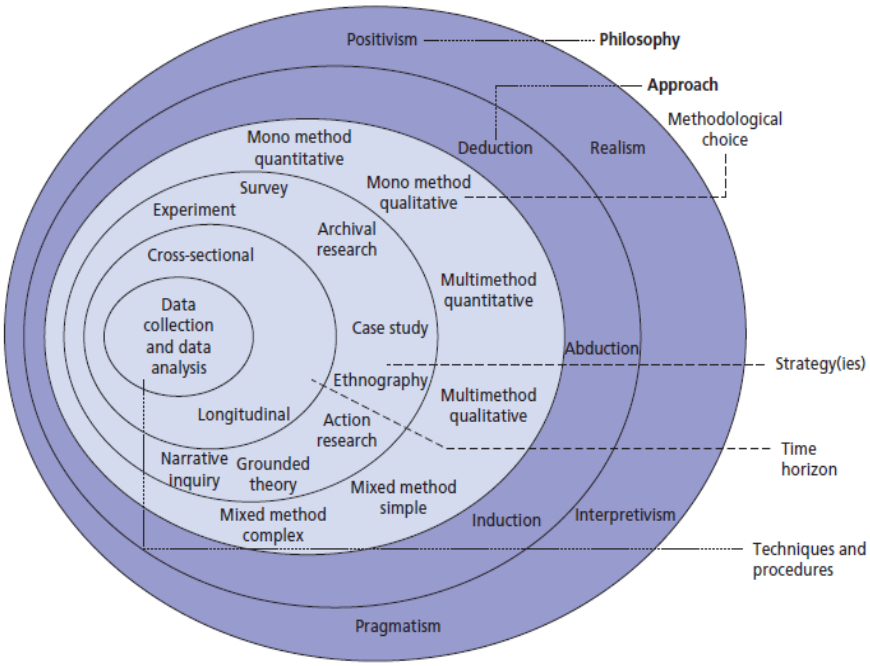



Figure 3.1 The research onion (Saunders et al. 2009)

## 3.2 Research Philosophy

The term “research philosophy” relates to the development of knowledge and the nature of that knowledge (Myers 1997b; Saunders et al. 2009, p.107). The adoptions of research philosophy hold the important hypothesis of how we see the world, and these hypotheses will subsequently support and underpin our research strategy and the methods we choose as part of that strategy (Saunders et al. 2009, p.108). Remenyi and Williams (1998) suggests that a number of major questions related to the research occur. However, the crucial one is ‘Why research?’ as researchers must understand the deeper purpose and necessities of their research.

There are several approaches and ways in research philosophy which determine the way a researcher is building a relationship between the knowledge of the subject and process that develops the knowledge. As Burrell and Morgan (1979) claim, researchers make several assumptions that have an impact on the development of the knowledge. This section is going to examine and describe two common paradigms of social sciences appearing in the research onion in Figure 14; positivism and interpretivism. Ozanne and Hudson (1989), advocate that these two approaches are very different from one another as they are based on different goals and assumptions. Nonetheless, they both have proven to contribute to research and are therefore one of the most popular methods.

Firstly, positivism approach will be explained and supported by particular literature showing examples and main points of this approach. According to Dudovskiy (2016), positivism adheres to the view that only “factual” knowledge gained through observation (the senses), including measurement, is trustworthy. This view is supported by Mack (2010) who demonstrates that, in the positivism paradigm all genuine knowledge is based on sense experience, and can be advanced only by means of observation and experiment. Furthermore, Clarke (2009) emphasises that positivism builds upon experience, observation and testing, which helps expands the knowledge.Aliyu et al. (2014) argue that, positivism can be considered as a research approach which is based the ontological principle and the fact that facts and reality are independent of the viewer and observer. Furthermore, Ozanne and Hudson (1989), state that positivists are convinced that ‘unchanging reality exists’ and can be dismantled into smaller pieces an those individual pieces can be observed separately in a controlled environment.

In positivism studies, the role of the researcher is limited to data collection and results via recognised test regime; hence, research findings are usually quantifiable by observations. Olesen (1994), provides the list of methodologies that are used by positivist researchers: confirmatory analysis, nomothetic experiments, quantitative analysis, laboratory experiment and deduction.

Interpretivism, on the other hand, integrates human interest into the research. The interpretivist paradigm considers the social reality as something that is subjectively constructed by people's thoughts and actions (Denscombe 2014, p.19). Ozanne and Hudson (1989), suggest that from the interpretivists' perspective, it is believed that each individual or group perceive reality differently and therefore many different realities exist. Interpretivists emphasise the importance of context and the determinant of events or behaviour. Therefore, realities always differ with respect to context and therefore the events have to be observed in its natural setting rather than being studied separately. This claim is supported by Lincoln and Guba (1985) who assert that reality should be perceived holistically. Additionally,Walsham (1995) believes that our knowledge of reality is created by 'human actors'. Therefore, researcher may change the perceptions of the observed subjects and the perceptions of both parties might be eventually different.

Each of these paradigms has its best means of obtaining the required information that forms the basis for the research design and data collection methods. The selection of appropriate paradigms is 'a matter of horses for courses' (Denscombe 2014, p.163). There are several considerations before choosing the appropriate paradigms. These include the suitability towards research strategy, the review of each paradigm towards the problem under investigation, and the potential opportunity of mixing two methods (Denscombe 2014, p.164). Wahyuni (2012) also points out the importance of choosing the right research approach and diagram in order to conduct the research with respect to the social phenomena and framing. Saunders et al. (2009), also add that research purpose is important to be established in order to develop an appropriate research design. These popular set of data collection methods associated with each research philosophy are demonstrated in Table (3.1). A positivist approach allows the researcher to adopt objective measurements; the surveys pursuing huge samples are usually the most proper methods of data collection (Denscombe 2014). As Bryman (1984) exemplifies, the techniques associated with positivism are participant observation or social survey. While with interpretivist research, in-depth studies

of phenomena through interviewing small samples can be a useful approach (Denscombe 2014).

To sum the two paradigms, the interpretivist paradigm is associated with qualitative research, whereas the positivist paradigm is associated with quantitative research. As this research will question how protected data within countries in a transitional phase information infrastructure is under Advanced Persistent Threats (APTs) and the associated challenges of cybersecurity capacity. An interpretivist approach is conducted in this research. The interpretivist approach will thus help the researcher towards understanding Spring Land Cybersecurity socio-technical issues in-depth, rather than quantifying them. Furthermore, it offers the researcher an opportunity to observe peoples' views and perceptions towards how research problems should be resolved or where challenges occur.

| Positivism | Interpretivism |
|---|---|
| • Highly structured<br>• Large samples<br>• Measurement<br>• Quantitative but can use Qualitative | • Small samples<br>• In-depth investigations<br>• Qualitative |

Table 3.1 Research philosophies and data collection methods (Dudovskiy 2016)

## 3.3 Research Approach

There are different research approaches that can be used to address a research study. As Saunder's research onion shows, they can be divided into three approaches: induction, deduction and abduction approach (Saunders et al. 2009). The choice of research approach is linked to the research philosophy and in the following section provides examples on how particular approaches linked to individual research philosophies. However, the abductive approach is going to be omitted in the description as it of very little relevance to the present study and furthermore, there is very scare data on abductive approach, which according to Svennevig (2001) complements deductive and inductive approach.

The inductive approach which focuses on observations, and theories are proposed towards the end of the research process as a result of observations(Andreewsky and Bourcier 2000). In this approach, researchers move from factual findings to theory (Danermark et al. 2001;

Kovács and Spens 2005). No theories or hypotheses would apply in inductive studies at the beginning of the research, and the researcher is free in terms of altering the direction of the study after the research process had commenced. Stentoft Arlbjørn and Halldorsson (2002), noted inductive research helps develop new theories and therefore contributes to the theoretical field of research. Research using an inductive approach is mainly concerned with the context in which such events were taking place (Ozanne and Hudson 1989). For instance, using a study with a small sample of subjects might be more appropriate than a large number as with the deductive approach (Saunders et al. 2009, p.126).

Contrary to the inductive approach, deduction approach which according to Minnameier (2010) is associated with logical thinking and correct reasoning. Saunders et al. (2009, p.124) assert, deduction is used mainly in the positivism paradigm. Moreover, Andreewsky and Bourcier (2000) state that researchers using deductive approach follow the route from a general law to a specific case. According to Dudovskiy (2016), a deductive approach can be explained by the means of hypotheses, which can be derived from the propositions of the theory. In other words, a deductive approach is concerned with deducting conclusions from premises or propositions (Danermark et al. 2001). According to Stentoft Arlbjørn and Halldorsson (2002), deduction is one of the most prevailing approaches among researchers as it test already existing theories and does not establish or form any new sciences.

The inductive approach is highly associated with qualitative research, whilst the deductive approach is more commonly linked with quantitative research (Gabriel 2013). In this research, the inductive approach has been chosen in order to develop a national framework with a focus on cybersecurity capacity building as a contemporary national security issue unstable environments and countries in a transitional phase. In addition, the initial motivation of this study is the shared interest between the author, decision makers, government officials, managers and general employees regarding security development in Spring Land. The aim is to devise a secure framework that can be generalised over the various organisations covering many of the Spring Land enterprise systems. This shifts the focus into the Spring Land homeland problem space, to be observed with the objective of conceptualising the various issues to be solved by developing the National Cybersecurity Capacity Building Framework (NCCBF).

Table (3.2) shows the major differences between deductive and inductive approaches to research adopted from (Saunders et al. 2009). This results in the construction of a conceptual

model that can be generalised as a basis for formulation and consideration about requirements of NCCBF from different stakeholder perspectives. Therefore, the methodology of this research comes in accordance with the interpretivist approach. Furthermore, the complexity of the Cybersecurity problem is also of high attention and thus it requires a detailed view using various perspectives and understanding of different issues, such as social, technical, legal, etc. This makes an inductive approach more suitable than a deductive approach which depends on particular quantitative factors.

| Deduction | Induction |
|---|---|
| • Moving from theory to data<br>• The need to explain causal relationships between variables<br>• The collection of quantitative data<br>• The application of controls to ensure validity of data<br>• The operationalisation of concepts to ensure clarity of definition<br>• A highly structured approach<br>• researcher independence of what is being researched<br>• The necessity to select samples of<br>• sufficient size in order to generalise conclusions | • Gaining an understanding of the meanings humans attach to events<br>• A close understanding of the research context<br>• The collection of qualitative data<br>• A more flexible structure to permit changes of research emphasis as the research progresses<br>• A realisation that the researcher is part of the research process<br>• Less concern with the need to generalise |

Table 3.2 differences between deductive and inductive approaches (Saunders et al. 2009, p.126)

## 3.4 Research Methodological Approaches

Various methodological approaches are differentiated in order to address a research study and utilise the obtained data to maximum. This section focuses on the following methods: quantitative and qualitative, and a mix of the two, referred to as mixed method. According to Kothari (2004), quantitative research is based on the measurement of quantity or amount. It is applicable to phenomena that can be expressed in terms of quantity. Moreover, (Carey 1993)

implies that sample sizes used in quantitative research are considerably bigger to ensure that statistical approach can be used and more data is available.

Qualitative research, on the other hand, is concerned with qualitative phenomenon, i.e., phenomena relating to or involving quality or kind(Kumar et al. 2008). Myers (1997b) states that, qualitative research methods were developed in the social sciences to enable researchers to study social and cultural phenomena. Denzin and Lincoln (2000), assert that, qualitative researchers study things in their natural settings, attempting to make sense of, or to interpret, phenomena in terms of the meanings people bring to them. Berger and Luckmann (1966) concluded that because there are many contexts and therefore many realities, consequently, there are many different points of views and truths based on how individual reality is constructed.

In terms of comparing the alternative research methods, quantitative research sets out to measure variables and test hypotheses on the basis of numerical data that can be acquired and analysed (Creswell 2013). In contrast, qualitative research provides an opportunity to interpret text, such as the opinions of various stakeholders regarding possible security strategies (McCusker and Gunaydin 2015). For the purposes of the current study, a qualitative approach has been deemed most suitable because the stated aim is to examine the various cybersecurity issues facing Spring Land. By avoiding the use of statistical data, a qualitative approach arguably affords a more realistic interpretation of events in the world. A further advantage associated with qualitative methods is that they offer greater flexibility in terms of how the data are collected and analysed (Boodhoo and Purmessur 2009). Examples of qualitative research methods include interactive management and focus groups which can be used to garner opinions about a specific subject. For instance, these methods can be used to explore opinions about cybersecurity or gain insight from key personnel with specialist knowledge or who are able to offer an institutional perspective, thereby giving a better appreciation about a certain event, condition or experience at a personal level. In addition, qualitative research could entail analysis of text or other documents such as company reports or government papers to provide insight into private or distributed knowledge stored in various formats (Hammarberg et al. 2016).

## 3.5 Research Strategy and Design

### 3.5.1 Research Strategy

A strategy is a plan of act, considered to achieve a specific goal (Denscombe 2014, p.18). Denscombe pointed out that, researchers who implement the strategy are able to use the whole range of methods within the strategy to achieve the aim of the study. There are different kinds of research strategies, which is valuable for different kinds of research purpose. For instance, a survey research, case study, ethnography, action research, experimental research, and grounded theory (Denscombe 2014, p.21). Survey research aims to gather large amounts of data and therefore provides quantitate descriptions and detailed information about the study population (Glock and Bennett 1967). Pinsonneault and Kraemer (1993) emphasise that as opposed to standard survey, survey research is conducted to obtain advanced scientific knowledge. On the other hand, ethnography is a qualitative research strategy that has very specific features such as the thorough investigation of patterns of social interaction(Gumperz 1981), a holistic view and analysis of societies(Lutz 1981). Walker (1981) perceives ethnography as a story-telling and Yates (1987) points out that ethnography can give us the necessary context that may lead to changes in our ways of thinking and understanding of races and cultures.

This research strategy is conducted for a long period of time and therefore can provide very consistent data (Hammersley and Atkinson 1983). With regards to action research, as noted by Avison et al. (1999), Baskerville and Wood-Harper (1996) is a strategy that combines both theory and practice. According to Greenwood and Levin (1998), action research is carried out by professional practitioners who seek to improve the situation or issues experienced by participants. MacColl et al. (2005), state that action research has two steps - collaborative analysis that is carried out by participants and collaborative change that takes place with respect to the formulated theory based on the collaborative analysis.

Experimental research according to Druckman et al. (2006) allows for casual interference through the randomness of group control and observations. This type of research uses quantitative and qualitative methods. Another example of very rigorous qualitative research is grounded theory. Charmaz and Belgrave (2007) defines this research strategy as collected set of data and analytic procedures that have been gathered together in order to formulate a theory. This theory helps shape qualitative materials and creates patterns and relationships

that are generated through the data analysis. This claim is supported by Strauss (1987) who also created a set of written guidelines that should be followed when building a grounded theory. Strauss and Corbin (1998), also point out that a theory is generated based on the gathered and analysed data.

Case study strategy is the most mutual qualitative method used in information systems. Case study strategy empowers an analyst to nearly look at the information inside a particular setting. Case study strategy is the most mutual qualitative method used in information systems according to Schell (1992) thanks to its flexibility regarding the design and therefore it allows for an investigation of the holistic characteristics of events. According to (Yin 2004), the case study research is not limited to a signal source of data, and good case studies benefit from having various data sources. Benbasat et al. (1987) describe three major reasons to use case study in information research:

- Researchers can collect data and find evidence from the context then create theories in practice.
- The case study method allows researchers to answer 'how' and 'why' questions.
- The case study method is an appropriate method to conduct research in an area in which few previous studies have been conducted. Case studies use multiple methods to gather data and information from one or more person or organisation enclosed in the scope of a problem.

A case study strategy was chosen to apply in this study in order to investigate and explore the factors that may affect the cybersecurity capacity in Spring Land, and how NCCBF will improve the situation. Furthermore, this gives the researcher an opportunity to gather people’s views, attitudes and experiences in relation to Spring Land cybersecurity capacity issues, which allows new issues to arise.

### 3.5.2 Research Design

Research design is the overall plan for collecting data and the methods. As De Vaus (2001) explains that research design is critical for researchers to create a plan before they start a data collection and that obtained data will provide us with a clear and straightforward answer and explanation of the proposed research question or hypotheses. Therefore, research design will

be used to collect and analyse data to help answer the research question. As this research aims to develop a secure framework with a focus on cybersecurity, the design science (DSR) methodology in information systems research is used. The fundamental principle of DSR is that knowledge and understanding of a design problem and its solution are acquired in the building and application of an artefact (Hevner et al. 2004).

Figure (3.1) illustrates the interaction and cycle in DSR framework. This framework has been adjusted to the scope of the research topic. According to the environment defines the problem space; its people, organisation and technology. Participants involved in this research include Information Security experts and other strategy related employees of targeted stakeholders within a cybersecurity domain. The framework takes strategic views in mind across the organisation, structure, process and culture. In addition, all technical factors are taken in account during the development of the framework.

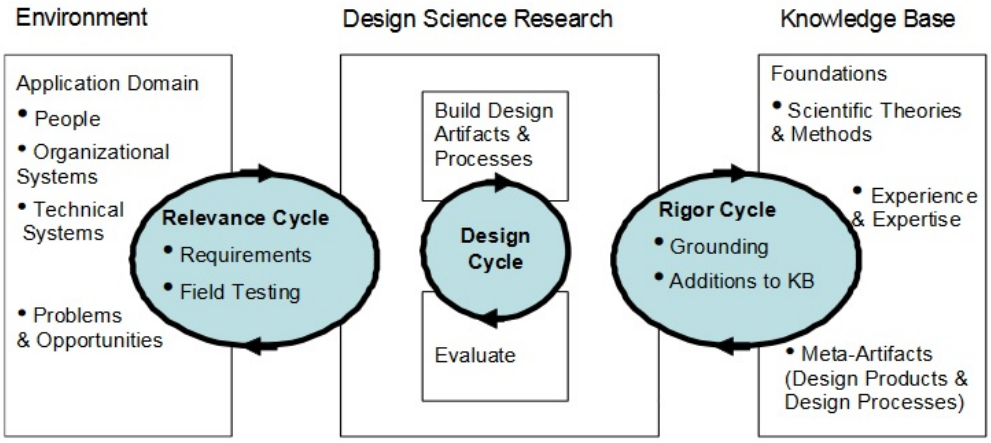



Figure 3.2 Design Science Research Cycles (Hevner et al. 2004)

The major principle of DSR is that knowledge and understanding of a design problem and its solution are acquired in the building and application of an artefact (Hevner et al. 2004). The DSR is the research method used for design and evaluation of artefacts for information models (abstractions, architects, frameworks, conceptual systems intended to solve an identified fuzzy organisational problem (Farrell and Hooker 2013)

Many researchers have utilised DSR method to develop and evaluate cybersecurity frameworks, cybersecurity strategies (Dennis et al. 2014; Muegge and Craigen 2015), protecting critical infrastructure and cyber defence approach (Peursum 2015; Smith 2019).

The DSR research process carried out in this study included five research activities as defined by the DSR framework of Johannesson and Perjons (2014). This process involves of activities such as problem identification and motivation, objectives for a solution, design and development, evaluation, and communication and Knowledgeable by these activities. This framework is represented using the OODA as a modelling baseline and guided by IDEF0 method where channels conveying data or objects are related to each activity, and represent different types of knowledge depending on the direction of the arrows. In Figure (3.3), Johannesson and Perjons (2014) define the channels as follows:

- Input describes what knowledge or object is the input to an activity (arrows from left);
- Output defines what knowledge or object is the output from an activity (arrows to right);
- Controls refer to what knowledge is used to manage an activity, including research strategies, research methods, and creative methods (arrows from above);
- Resources outline what knowledge is used as the basis of an activity, i.e. the knowledge base including models and theories (arrows from below).

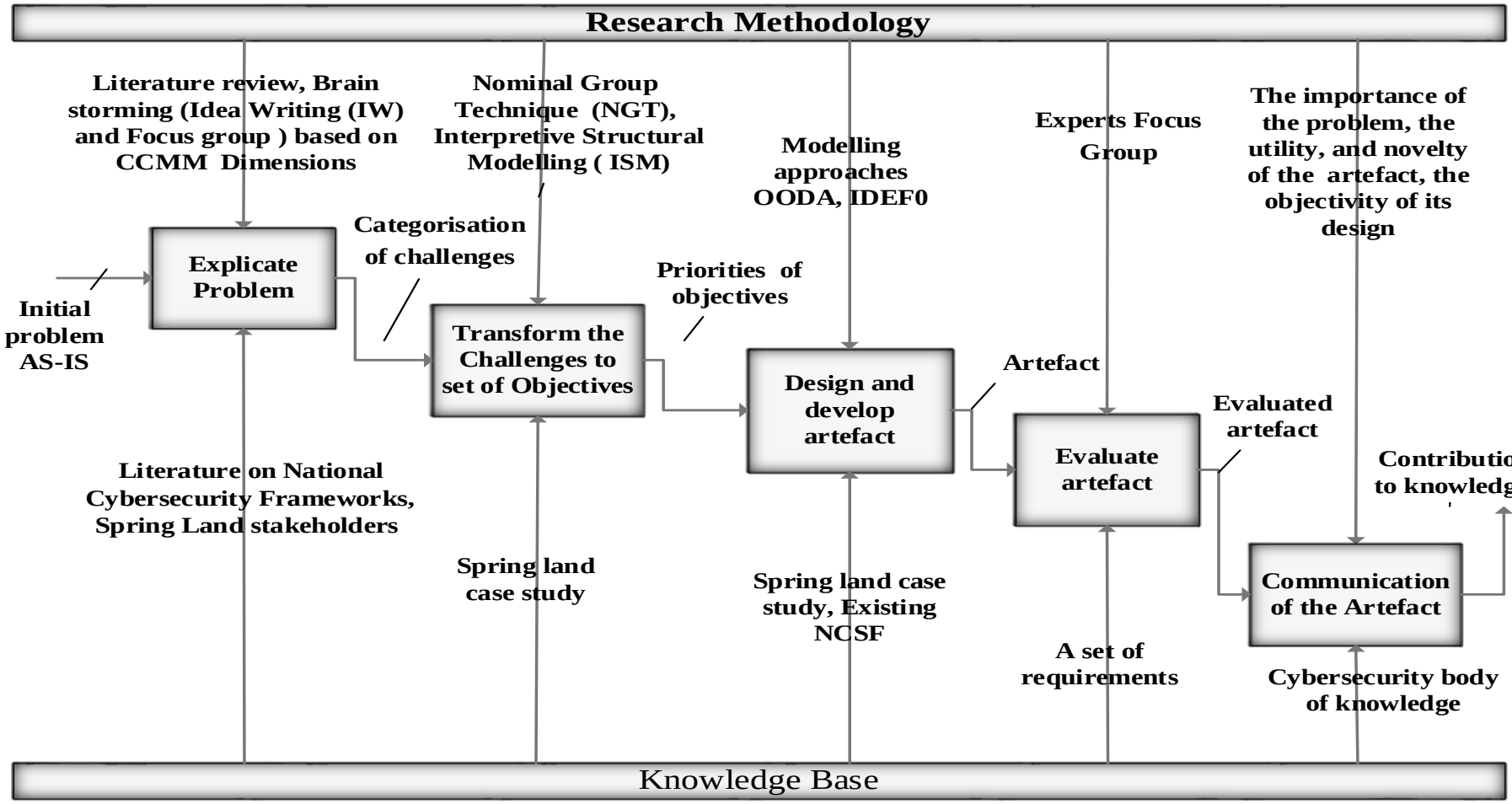



Figure 3.3 DSR Process including Inputs, Activities, and Outputs adapted form (Johannesson and Perjons 2014)

These activities and their application are presented below:

#### 3.5.2.1 Problem Identification and Motivation

The first step in DSR is to identify the initial problem and motivation of why the artefacts, in this study the national cybersecurity capacity building framework for countries in transitional phase, need to be developed and evaluated. Hence, no scholarly research has currently been done on countries in a transitional phase posture to implementing appropriate cybersecurity capacity building framework. In addition, there are no studies addressing the factors that influence the development of a National Cybersecurity Capacity Building Framework (NCCBF) in a chaos ecosystem. According to Hevner et al. (2004), convenient design research is based on the novelty, generality, and significance of the designed artefact. Furthermore, artefact may empower the solution of an unsettled problem by either extending the knowledge base or applying existing knowledge in new innovative ways.

#### 3.5.2.2 Define Objectives for a Solution

The second activity in the design science process is to define the objectives for a solution. The development of NCCBF through the reliance of multiple established sources, by using literature, conducting focus group interviews, Interactive Management (IM) and studying existing cybersecurity frameworks. In this study, utilises the Cybersecurity Capacity Maturity Model (CCMM) for Nations, originally proposed by the Cybersecurity Capacity Centre at the University of Oxford, as a baseline. The ultimate aim of the section is to provide benchmark for measuring and planning cybersecurity for countries in transitional phase. A focus group study was performed using this model with the members of the Spring Land National Cybersecurity Authority (NCSA). NCSA leads the Cybersecurity program in Spring Land in terms of technical, operational and strategical level. In addition, an Interactive Management technique was used. A one-day Workshop hosted by NCSA was conducted for a total of 26 participants from different stakeholders. The set of problem statements and objectives derived from the IM approach has been employed to support the management of a national cybersecurity capacity for countries in a transitional phase, similar to the case study exemplar presented herein.

#### 3.5.2.3 Design and Develop the Artefact

The third steps in DSR method is design and develop the artefact which address the identified problem and define objectives for a solution. In this study, the OODA was used as a modelling baseline, selected for its simplicity and adaptability. To develop a framework that enhances the national cybersecurity capacity, OODA steps were used to construct and guiding the requirements of IDEF0. These steps were instantiated with the CCMM and finding from the conducted empirical studies and literature.

#### 3.5.2.4 Demonstrate and Evaluate the Artefact

The fourth and fifth design science steps are to demonstrate and evaluate how well the artefact solves the real-world problem taking in account the previously identified objectives. The focus group was conducted with group of experts from different countries. The participants were selected due to their contributions in their decision-making roles, and included government officials, managers, and general employees participating in security development areas. These areas such as Defence, e-services, Private Sector, Banking and Finance, Regulations of ICT sectors, National cybersecurity agencies and authorities , Technical Advisor and capacity Buildings , High Education, IT security division , planning and projects Unit, Integrated Digital applications and ICT sectors.

#### 3.5.2.5 Communication of the Artefact

The last step in DSR n design science is the communications of the artefact. Communications include the significant of the problem space, the usefulness, and novelty of the artefact, the objectivity of its design, and the effectiveness of researchers and public (Hevner et al. 2004; Petter et al. 2010). The vital point of communicating this research was to contribute to the cybersecurity body of knowledge. The results of Chapter 4 has been published in 2019 as part of the Advances in Intelligent Systems and Computing book series (AISC, volume 930) (Ben Naseir et al. 2019). Two scientific papers also have cited these results. In addition, the development of a proposed NCCBF framework has been published in 22nd International Conference on Enterprise Information Systems (ICEIS 2020) (Ben Naseir et al. 2020). The researcher will continue to seek opportunities to publish the work at academic conferences and journals.

### 3.5.3 Data Collection Techniques

This section looks at data collection tools and analysis. The data sources in the qualitative approach include participant observation (e.g. fieldworks), literature review , interviews, focus group discussion, questionnaires, documents and texts, and the researcher's impressions and reactions (Myers 1997b). Literature review is the analysis and summary of documents that gives an overview of a particular topic without data collection (Seuring and Müller 2008). Furthermore, based on a literature review researchers can develop a theory.

In this study, interviews and focus groups with domain experts will be the main method of collecting a data set for this study. The research will involve decision makers, government officials, managers and general employees regarding security development in Spring Land. According to Kvale (1994), interviews have gained their popularity over the years and become the most frequently used data collection techniques with respect to qualitative research. Interviews can be divided into several types, such structured, semi-structured and unstructured interviews. Campion et al. (1994) highlight the fact that structured interview questions has an impact on the validity and utility of the study as the questions affect the sections of participants. DiCicco-Bloom and Crabtree (2006) mentions that, structured interviews commonly produce quantitative data due to its high validity and reliability. On the other hand, semi-structured and unstructured interviews are the most commonly used interviewing plan for qualitative research because of their flexibility in garnering detailed information (DiCicco-Bloom and Crabtree 2006). Wong (2008), describes this technique as a research methodology that uses a small group of participants who analyse through discussion a particular topic. That was data is generated for the research purposes. Wong also points out that the main feature of this method is the interaction between the moderator and the group members. Kitzinger (1995a) supports the previous definition of this method and adds that focus groups belong to qualitative research and the interaction between the moderator and the group member encourages discussing among all the participants of this research method. The group discussion also helps generate and clarify ideas that would not be accessible during one-to-one interviews.

In addition, methodologies from the Socio-Technical-Systems (STS) disciplines will be used. According to Baxter and Sommerville (2011), an STS approach towards design considers human, social and structural factors, as well as technical factors in the design of organisational systems. This is supported by Appelbaum (1997) and Trist (1981) by claiming

that STS design functions on the presumption that an organisation is a combination of social and technical parts open to its environments. Moreover, Appelbaum (1997) emphasises that this design is different from the traditional methods that combines physical products and social/psychological outcomes. This model leads to a better understanding of the problem situation and helps capture the stakeholders' needs and requirements. Manz and Stewart (1997) emphasise that, STS recognises the significance of social forces and technical components, which according to Trist (1981) leads to improved group work, which is supported by Lawler (1986) who claim that thanks to STS, companies adopted self-managing work teams and collaborative relationships are encouraged.

An as example of such cooperation and interaction is Interactive Management (IM) which provides contextualisation of the problem space that comprise an intricate connection between people, machines and the natural parts of the work system in the current era (Christakis 1985).

#### 3.5.3.1 Interactive Management (IM)

The IM technique is one of the STS approaches used within this research. The IM is based on the recognition that when dealing with complex situations, there is a need for a group of people, knowledgeable of the situation, to tackle together the main aspects of issue, to develop a deep understanding of the situation under analysis, and to detail the basis for effective action (Warfield and Cárdenas 2002). It was Warfield and Christakis who developed the concept of IM in 1980 (Banathy 1996) and the concept creates a situation when all the participants comes a mutual agreement, not a consensus that is held by the majority. The same authors pointed out that, IM offers the framework for a real and deep understanding of the circumstances that is under consideration. The people involved in an IM activity are exposed to a real sharing of ideas and information, and thus are passively learning about the problem at hand. The main benefits of this method are; the efficient use of participant's time; provision for iteration and documentation; and effective communication between participation (Dogan 2013). IM has a three phases as described below:

**The Planning phase:** at this phase the situation is defined and the scope of the issue becomes clear. This is completed with the scope and context statement writing, proof of actor identity, and State of Definition Assessment. In addition, at this stage participants will find out who is involved and what is required to gather a comprehensive view of the problem. Once the state

of definition has been finished, the type of questions that need to be answered during the next phase (The Workshop phase) will be revealed, which might considerably yield in respect of an efficient solution (Warfield et al. 2002)

**The Workshop phase:** the Workshop Phase involves bringing jointly a group of participants who understand the issue or situation (Warfield et al. 2002). According to Ward et al. (2017), the IM workshop will be made of three procedures: Idea Writing, Nominal Group Technique, and Interpretive Structural Modelling. In idea writing, a trigger question is offered to participants to noiselessly write down ideas about. The written ideas are then swapped over with others where additional ideas are added. Everything is then collated and divided into categories, then presented to the group. Following is the Nominal Group Technique, where participants generate further ideas after a more holistic view of the problem is gained from idea writing. This also allows for clarification and editing of problem statements. Participants then rank each idea based on importance. The final part of the workshop is to transform idea statements into objectives and then build an Interpretive Structural Model (ISM) to identify relationships amongst various items surrounding the problem. In this study, a one-day Workshop hosted by NCSA was conducted for a total of 26 participants from different stakeholders. NCSA had issued an invitation letter to all stakeholders to help the researcher in contextualising the problem space that is centred on the current Spring Land National security state. The following group of stakeholders were involved in the workshop:

1. Telecommunication and Internet service providers.
2. Intelligence agency.
3. Ministry of defence.
4. Digital crime unit in Ministry of defence.
5. Private companies.
6. National ID project and Spring Land Passport, Immigration and Foreigners Affairs Authority.
7. Oil and energy sector.
8. Finical sector.

9. Training and Education department of Spring Land Army.
10. Spring Land Army Signal corps.
11. National Cybersecurity Authority (NCSA).
12. Spring Land E-government.

**The Follow-up Phase:** in this phase, the outcome and objectives derived from the previous phase is set into action, starting the implementation plan of the solution. In this research study, IM method was utilised in **Chapter 4.** The IM was conducted to contextualise the challenges of CCB in Spring Land.

3.5.3.2 Focus Groups

Focus group discussions aim to explore a range of ideas and feelings that individuals have about certain issues, as well as illuminating the differences in perspective between groups of individuals (Tong et al. 2007). When using a focus group technique, the data are collected through precise group collaboration on a chosen topic (Doody et al. 2013). Gill et al. (2008) declares that, the interaction is the key of a successful focus group. Using the focus group method as a qualitative approach, enables participants to elaborate and engage in conversation with one another (Hu et al. 2014). The important consideration in this technique is the group size. Stewart et al. (1990) recommend that the ideal size for a focus group is six to eight, but it can work effectively with as limited as three, and as more as fourteen participants.

In this study, the focus group method was utilised in **Chapters 5** and **Chapter 7**. The focus group conducted in **Chapter 5** was to assess the Spring Land cybersecurity capacity maturity levels by utilising the CCMM model. Five experts from NCSA were interviewed in sessions hosted in Spring Land capital city. The chosen experts then reflected on their role in NCSA and the limitations of the study. This sample was selected based on a purposive sample technique. The purposive sample technique relies upon the judgment of the researcher when it comes to choosing the case that is to be investigated (Tongco 2007; Marshall et al. 2013). What is more, Cronin (2014) and Onwuegbuzie and Byers (2014) described that despite the fact a minimum of four to 15 participants is anticipated, the primary focus is on gathering thick, rich data and not on the number of participants. As the CCMM model was used to

assess the Spring Land Cybersecurity capacity, participants of the focus group discussion were those working in NCSA with a role of managing cybersecurity program in Spring Land. In **Chapter 7**, the focus group has been conducted to evaluate the proposed framework (NCCBF). The framework has been evaluated by 13 experts in the field the cybersecurity from different countries including experts from countries that in transitional phase, during a workshop session by using the focus group technique.

Table (3.3) below, provides a snapshot towards the type of data collection technique adopted for each objective in this study. The final evaluation of the approach will be done through more than one case study in real-world settings, incorporating expertise-based feedback.

| Research Objectives | Purpose | Data Collection Technique and methods |
|---|---|---|
| **1-** To **investigate** a state of the art cybersecurity and cybersecurity capacity building frameworks. | State of Art will reinforce the suspension that the Spring Land National security is wholly inadequate to resist APTs. | This objective will be attained by a comprehensive literature review. |
| **2-** To **contextualise** the problem space that is centred on the current Spring Land cybersecurity capacity state. | This will feed into requirement analysis for NCCBF and the possibility to organise and test the Spring Land Cyber Defence. | The contextualisation will analyse the security operations of the state by the use IM and focus group interview |
| **3-** To **assess** the current maturity levels of cybersecurity capacity in Spring Land. | Determining areas of capability that are required by the Spring Land Government in order to improve cybersecurity capacity of the state | The assessment will analyse the maturity levels of the Spring Land cybersecurity capacity of the state by the use of focus group discussion. |
| **4-** To **develop** the NCCBF for countries in transitional stage | The NCCBF will supports the National security for countries transitional stage | The NCCBF will be managed and guided using modelling functions techniques. |
| **5-** To **evaluate** the proposed framework (NCCBF) | Enhancing the NCCBF for countries in a transitional phase. | The NCCBF will be evaluated by using focus group and experts' feedback. |

Table 3.3 a snapshot towards the type of data collection technique adopted for each objective

#### 3.5.3.3 Data Analysis

This section presents the data analysis method that used to analyse and evaluate the collected data. As the data collected in this research using qualitative approaches, the content analysis technique was used to analyse the data generated by IM and focus group. Qualitative data analysis in general consists of three stages (Strauss and Corbin 1997). These stages are includes the information about a topic such as a specific context, components and their prosperities and dimensions and knowledge is gained by studying these components. Qualitative data analysis is, in summary, “the process of making sense out of the data" (Ruona 2005, p.236). The common approaches used in qualitative data analysis are thematic analysis and content analysis. Their main characteristic is the systematic process of coding, examining of meaning and provision of a description of the social reality through the construction of theme (Vaismoradi et al. 2016).

Thematic analysis according to Braun and Clarke (2006) is “a method for identifying, analysing and reporting patterns (themes) within data”. Content analysis according to Vaismoradi et al. (2013) is “a systematic coding and categorising approach used for exploring large amounts of textual information unobtrusively to determine trends and patterns of words used their frequency, their relationships, and the structures and discourses of communication”. The main difference between them lies in the possibility of quantification of data in content analysis, conversely, thematic analysis provides a purely qualitative, detailed, and nuanced account of data (Vaismoradi et al., 2013). For this reason, content analysis is employed in this study. Since the data were captured the themes are identified based on the indicators of the CCMM. The input template analysis that constructed in next section is used in Chapter 4 and Chapter 5 to analyse the data.

## 3.6 Modelling Function IDEF0

There are many techniques and methods available, such as UML (Eracar and Kokar 2014), BPMN (Gerber et al. 2014), Colour Petri Net, BPEL (Herrera et al. 2012), Integration Definition for Function Modelling (IDEF0) (IDEF0 1993), modelling language, etc.

The IDEF and Unified Modelling Language (UML) modelling methodologies have become widely used in industrial and academic circles. IDEF comprises a suite of graphical modelling techniques aimed to formally specify and communicate important aspects of

enterprise engineering projects, whereas UML is a modelling language that can be used to generate computer executable models that encode key aspects of software engineering projects (Kim, Weston et al. 2003).

The IDEF (originally an acronym for ICAM DEFinition) family of languages has its origins in the 1970's US Air Force Integrated Computer Aided Manufacturing (ICAM) program, which designed to create computer-implementable modelling methods for analysis and design (Noran 2003). The IDEF suite of enterprise modelling approaches, which comprises IDEF0, IDEF1, IDEF1x, IDEF3 and other graphically based modelling notations have been applied extensively in support of large industrial engineering projects.

The Unified Modelling Language (UML) has fast become a de facto software engineering standard. It provides a set of modelling notations designed to support various domain specialisms and life phases involved in the engineering of object-oriented software systems. It follows that UML provides suitable and widely-used modelling constructs for developing structured, configurable, reusable and readily-distributed multi-perspective models of IT systems (IDEF0 1993).

The IDEF0 modelling method has proven effective in detailing the system activities for function modelling, which was the original structured analysis communication goal for IDEF0 (Fortier and Dokas 2008).

Currently, the IDEF0 technique is widely used in the government, industrial and commercial sectors, supporting modelling efforts for a wide range of enterprises and application domains (Commerce. 1993). As a function modelling language, IDEF0 has the following characteristics:

1. It is comprehensive and expressive, capable of graphically representing a wide variety of business, manufacturing and other types of enterprise operations to any level of detail.

2. It is a coherent and simple language, providing for rigorous and precise expression, and promoting consistency of usage and interpretation.

3. It enhances communication between systems analysts, developers and users through ease of learning and its emphasis on hierarchical exposition of detail.

4. It can be generated by a variety of computer graphics tools; numerous commercial Product products specifically support development and analysis of IDEF0 diagrams and models.

5. It is well tested and proven, through many years of use in Air Force and other government development projects, and by private industry.

IDEF0 is an engineering technique for performing and managing needs analysis, benefits analysis, requirements definition, functional analysis, systems design, maintenance, and baselines for continuous improvement.

IDEF0 models provide a "blueprint" of functions and their interfaces that must be captured and understood in order to make systems engineering decisions that are logical, affordable, integratable and achievable.

The IDEF0 method is used to specify function models ('what to do'). It is loosely based upon the Structured Analysis and Design Technique (SADT) method developed by Douglas Ross from SofTech in the 1970s (IDEF0 1993). Figure (3.4), shows a generic view of IDEF0 model. IDEF0 allows the user to illustrate a view of the process including the inputs, outputs, controls and mechanisms (which are referred to generally as ICOMs):

- Function is a transformation of inputs to outputs, by means of some mechanisms, and subject to certain controls, that is identified by a verb or verb phrase that describes what must be accomplished and modeled by a box.

- Inputs are resources transformed (refined) by the process.

- Outputs are the things created through the transformation of the inputs by the process to achieve desired outcomes.

- Controls are the things guiding the process: policies, guidelines, laws, standards, and best practice.

- Mechanisms are the agents that accomplish the actions (activities) contained by the process.

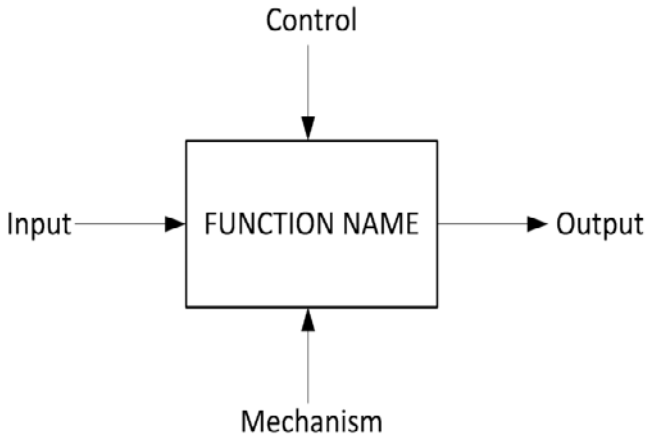



Figure 3.4 A generic IDEF0 diagram (IDEF0 1993)

### 3.6.1 IDEF0 Diagrams

The IDEF0 models consist of three types of information: graphic diagrams, text and glossary. These diagram forms are cross-referenced. The graphic diagram is the main component of the IDEF0 model, containing boxes, arrows, box / arrow links and associated links. Boxes are each primary feature of the subject. These tasks are broken down or broken down into more detailed diagrams before the subject is represented to the level required to meet the goals of a specific project. The top-level diagram in the model gives the most general or abstract description of the subject represented by the model (IDEF0 1993). These diagrams are discussed below.

1. Top-Level Context Diagram

The top-level diagram in the model provides the most common or abstract description of the subject represented by the model. This diagram is followed by a chain of child diagrams providing more detail about the subject. Each model shall have a top-level context diagram, on which the subject of the model is represented by a single box with its bounding arrows. This is called the A-0 diagram (pronounced A minus zero) (IDEF0 1993) .

2. Child Diagram

The single function represented on the top-level context diagram may be decomposed into its major sub-functions by creating its child diagram. In turn, each of these sub-functions may be decomposed, each creating another, lower-level child diagram. On a given diagram, some of the functions, none of the functions or all of the functions may be decomposed. Each child

diagram contains the child boxes and arrows that provide additional detail about the parent box (IDEF0 1993).

3. Parent Diagram

A parent diagram is one that contains one or more parent boxes. Every ordinary (non-context) diagram is also a child diagram, since by definition it details a parent box. Thus, a diagram may be both a parent diagram (containing parent boxes) and a child diagram (detailing its own parent box). Likewise, a box may be both a parent box (detailed by a child diagram) and a child box (appearing on a child diagram). The primary hierarchical relationship is between a parent box and the child diagram that details it. The decomposition structure of IDEF0 is illustrated in Figure (3.5).

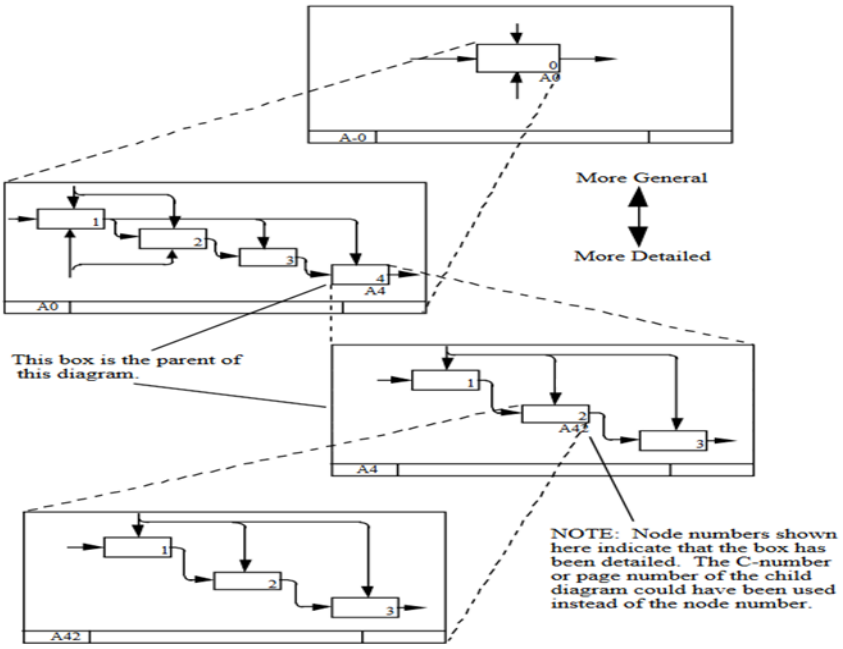



Figure 3.5 Decomposition Structure of IDEF0

## 3.7 Observe, Orient, Decide and Act (OODA) Model

The OODA Loop is a model for conceptualising how individuals and organisations make decisions (Gray et al. 2015). The OODA loop has been developed by Colonel John Boyd in 1986, as outcomes of his years of research and analysis in his effort to describe the nature of adversarial engagements (Boyd 1996; Zager 2017). Boyd's concept created the ability to formulate and implement strategies in constantly changing environments. The OODA loop is a subject of significant discussion in the cybersecurity community (Gray et al. 2015; Zager

2017) . For instance, Cisco summarises the significance of the OODA loop to cybersecurity "The OODA Loop assumes that continuous improvement is an integrated part of the process, allowing you to learn from your previous experiences, feeding lessons learned into the loop activities to achieve better performance every time you complete the four steps" (Muniz et al. 2015). An OODA loop consists of following steps as shown in Figure (3.6).

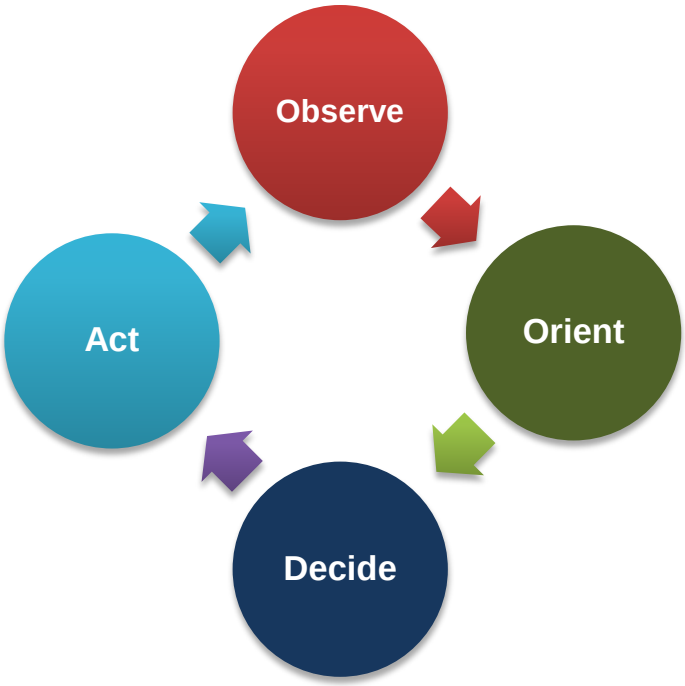



Figure 3.6 The OODA loop **(**Gray et al. 2015)

These steps are observe, orient, decide and act. In context of cybersecurity capacity, the four steps as follows:

- Observation phase: this phase is the earliest stage of OODA loop process. The observation phase continuously analyse the social, internal, and external challenges.

- Orientation phase: this phase is the most critical part of the OODA loop. The raw of information obtained from the observation phase is analysed and synthesised into usable information that can be used to support decision phase. According to Coram (2002) the orientation phase is a "nonlinear feedback system" that spontaneously generates a new cognitive image of the unfolding circumstances.

- Decision phase: the information gained from the observation and orientation phases including, social internal and external challenges, implicit and explicit guidance within the state, and the context of the circumstances under consideration, leads to the point at which a decision is made.

- Action phase: As outlined in Boyd's diagram, one can consider this process of acting upon opportunities discovered in the decision phase. Once the action is executed, the OODA loop closes (Coram 2002).

The OODA Loop provides an abstract yet easily understood framework that can be applied to national cybersecurity and integrated into a broader capacity building process within a country. Its ability to adapt to a continuously changing environment allows the OODA Loop to formulate strategies and building cybersecurity capacity germane to the problems in the Digital Age (Sims 2011).

## 3.8 Constructing (Authoring) an IDEF0 template analysis

This section describes the statement templates that used to construct fundamentals of IDEF0 requirements to develop the proposed framework. These templates are, Input statement template, Dimensions and Functions statement template, Mechanisms and Controls Template analysis and Output statement template.

### 3.8.1 Input statement template

This template has been built based on CCMM to model to review the key issues and assess the maturity levels of the Spring Land cybersecurity capacity. Moreover, it describes the state's cybersecurity ecosystem; legal and regulation aspects, cultural and social aspects, educational aspects and mitigating risks over standards, organisations and technologies resilience. In addition, this template is used for analyse the data captured in **Chapter 4** and **Chapter 5**. These findings provide the basis for the requirements of the NCCBF for countries in a transitional stage.

Each dimension includes multiple factors and attributes (GCSCC, 2017), each making a significant contribution to capacity building. Each factor, involves five stages of maturity (Start-Up (S-UP), Formative (F), Established (E), Strategic (S) and Dynamic (D). The lowest indicator implies a non-existent, or inadequate, level of capacity, and the highest indicates

both a strategic approach, and ability to dynamically enhance environmental considerations, including operational, socio-technical, and political threats. Table (3.4) presents the template statement that was used to capture the key challenges and assess the maturity levels of CCB.

| Dimensions | Factors | Indicators | | | | | Challenges and issues |
|---|---|---|---|---|---|---|---|
| | | S-UP | F | E | S | D | |
| | | | | | | | |
| | | | | | | | |

Table 3.4 Input template statement

3.8.2 Dimensions and Functions statement template

Function is a transformation activity or process required for transform inputs to outputs, by means of some mechanisms, and subject to certain controls, that is identified by a function name and modelled by a box. As described in **Section 3.6.1**, in IDEF0 models the whole top-level function is segmented into sub-function parts. In this study, the Dimension ID is used to describe the top level activity name for each dimension of the NCCBF based on the five dimensions of the CCMM. Table (3.5), presents the template statement that was used to create the functions for each dimension and the interaction of each activity with other activities in the same dimension of other dimensions. Function ID is used to describe the activities or the processes required for NCCB in each dimension. The function statements were created based on the stakeholders' view from within the case study country and the existing national cybersecurity frameworks (Ben Naseir et al. 2019). More details on how to use this template will be described in **Chapter 6.**

| Dimension ID | Function ID and description (Activities) | Interactions |
|---|---|---|
| Used to identify the name of the dimension. | Used to identify the name of the function and describe its purpose. | Used to indicate the interactions of a given activity with other activities. |

Table 3.5 Functions statement template

3.8.3 Mechanisms and Controls Template analysis

This template is used to capture related mechanisms and controls for each dimension. The mechanisms are the different types of resources such as the cross-functional teams, systems and technology that are used to support functions (activities) to achieve change.

| Mechanism ID and description | Rational of the mechanism | Control ID and description | Reference and Access |
|---|---|---|---|
| Identifies and indicates the function that the mechanism is related to. | Describes the motivation to use the mechanism | Identifies the mechanism that the selected control is related to. | Identifies the milieu of the selected supporting material and whether it is considered to be open source or proprietary. |

Table 3.6 Mechanisms and Controls Template analysis

The controls are tools or checklists that ensure adherence to best practices such as the budget, knowledge and regulations. Table (3.6), above presents the template statement that was used to create the mechanisms and controls for each dimension. More details on how to use this template will be described in **Chapter 6**.

3.8.4 Output template statements

The output template statements perform two major activities: 1) Find the gaps in the implementation process in each dimension, and 2) Measuring maturity levels improvement in each dimension. Countries or organisations may have the capacity to change, but lack certain key capabilities. States need to mature cybersecurity capacity and capabilities at national level in order to facilitate the requirements expressed through national authoritative or

stakeholders. These national cybersecurity capabilities typically consist of people, processes and technology (Jacobs et al. 2017). However, a comprehensive way to define work deliverables and work standards, and provides a way to measure the work deliverables is needed. One of the weaknesses that burdens IDEF0, is the dearth of modelling notations in any form of mistakes. This happens because the existence of IDEF0 based totally to the outline of the manner path and not to the identification or prediction of errors. Moreover, is not apparent to any form of quit user the effects that an blunders may have (Tsironis et al. 2008).

In this study OODA model is used to observe and react to the changing environment more quickly through the decision cycle. Based on the Mechanisms and Controls template analysis, the mechanisms are the different types of resources such as the cross-functional teams, systems and technology that are used to support functions (activities) to achieve change. The controls are tools or checklists that ensure adherence to best practices such as the budget, knowledge and regulations. These mechanisms and controls must be cross-examined to the fullest for a cost-effective and find the gaps in the implementation process in each dimension. The gap report suggests corrective actions to observation, orientation and decision phases by adding/updating functions, mechanisms and controls. After finds and measure capacity building gaps and react to it in each dimension, the maturity levels are measured to check the targeted maturity levels are achieved. In this study, the output template has been created based on the CCMM, existing maturity models and cybersecurity indexes that discussed in **Chapter 2**. Table (3.7) shows the template that used for measuring maturity levels improvement in each dimension.

| Function | Mechanisms and Controls | Maturity Indicators | | | | |
|---|---|---|---|---|---|---|
| | | Start-Up | Formative | Established | Strategic | Dynamic |
| Function ID | Mechanisms | Government is aware of the mechanism principles, but have not yet created. | Government has created the mechanism, but are yet to approved and reviewed | Government has created and approved the mechanism. | Government has review the mechanism and renewal process are confirmed | Government has created and approved the mechanism and is constantly involved in a review process to keep the mechanism in line with country needs |
| | Controls | Government is aware of the control principles, but have not yet created. | Government has created the control, but are yet to approved and reviewed | Government has created and approved the control. | Government has reviewed the control and renewal processes are confirmed. | Government has created and approved the control and is constantly involved in a review process to keep the mechanism in line with country needs |

Table 3.7 Output template statements

## 3.9 Research ethics

Research ethics are the moral principles that govern how researchers should carry out their work. According to Bhattacherjee (2012, p.137), research ethics is significant because, science has often been manipulated in unethical ways by people and organisations to advance their private agenda and engaging in activities that are contrary to the norms of scientific conduct. In social science there are ethical principles as indicated by (Bhattacherjee 2012; Bryman 2016): the first principle is 'Voluntary participation and harmlessness', the researcher must be aware not only physical harm but also psychological harm should be avoided to the participants. In addition, participation in the study is voluntary, that participants have the freedom to withdraw from the study at any time without any unfavourable consequences.

In this research, no vulnerable groups such as children or people with disabilities. In order to avoid any harm, numerous measures were taken such as;

- All participants were voluntary.
- Considering the organisations that participants were employed, consent for their participation was gained from the host organisation.
- All participants were clearly informed that they could withdraw at any time.

The second principle was 'informed consent'. All the participants were informed on the goal, purposes, and the nature of the study. According to Bhattacherjee (2012, p.138), researchers must retain these informed consent forms for a period of time (often three years) after the completion of the data collection process in order comply with the norms of scientific conduct in their discipline or workplace. In this study, comprehensive information was offered to the participants so that they could make an informed decision on the participation of the research. These included the following :

- All participants were notified to potential risks in invitation information.
- All participants were reminded of the risks before the start of survey and interview.

- All participants were informed that data would be published but would be untraceable and anonymous.
- Signed consent was acquired.
- All participants were provided with the University supervisory details for making a complaint.

The third was ‘Anonymity and Confidentiality’. Anonymity indicates that the researcher or readers of the final research report or paper cannot identify a given response with a specific respondent. Bhattacherjee (2012, p.138), mention that in some research designs such as face-to-face interviews, anonymity is not possible. In other designs, such as a longitudinal field survey, anonymity is not desirable because it prevents the researcher from matching responses from the same subject at different points in time for longitudinal analysis. Under such circumstances, subjects should be guaranteed confidentiality, in which the researcher can identify a person’s responses, but promises not to disclose that person’s identify in any report, paper, or public forum.

This research did not use any covert methods and no particular privacy issues were expected. It has been guaranteed that both interviewees were protected under anonymity and confidentiality by applying following steps:

- Participants were coded anonymously
- All data not in the public domain was anonymous
- Data in the public domain, traceable to an anonymous participant, was anonymised or discarded
- Raw data was not shared with anyone else including colleagues in the University

The fourth and last principle was ‘no deception’. Experimental or empirical research often uses deception to inspire natural responses of participants (Bryman, 2016). This research did not involve any experimental settings but sought verbal and written answers based on their pre-existing perceptions and knowledge of their organisations.

## 3.10 Chapter summary:

This chapter outlined the methodology adopted for this study, which were chosen in order to achieve the research objectives. The methodology applied in this study was adopted from the research onion diagram developed by Saunders et al. (2009) to create a cohesive alignment between research objectives and the research methodology. Saunders research onion provides a number of key steps in the positioning of research methodology; the research philosophy, research approach, research strategy and design, and data collection techniques.

The overarching research approach used in this research is Design Science Research methodology (DSR). The major principle of the DSR is that knowledge and understanding of a design problem and its solution are acquired in the building and application of an artefact (Hevner et al. 2004). The DSR research process carried out in this study included five research activities as defined by the design science method framework of (Johannesson and Perjons 2014). In this study, data has been collected through Interactive Management (IM) and Focus Group discussion approaches, by utilising the CCMM for Nations as a baseline. Data collection techniques are used for in qualitative researches, they encourage interaction between all the participants, and therefore data that are more complex are obtained. The findings of collected data was analysed using a content analysis technique.

This chapter also describes the statement templates that used to construct fundamentals of IDEF0 requirements to develop the proposed framework. In addition, research ethics have been discussed in this chapter. The following two chapters present the findings and analyses of empirical data.

# 4. CHAPTER 4: CONTEXTUALISING THE PROBLEM SPACE IN SPRING LAND

## 4.1 Introduction

This chapter discusses the results of the Interactive Management (IM) through using the Cybersecurity Capacity Maturity Model (CCMM) for Nation. As explained in *Chapter 3*, two qualitative approaches Interactive Management (IM) and Focus Group discussion have been conducted to analyse and review of the current state of Spring Land's cybersecurity capacity. The participants in this stage are from different government agencies and national experts (lead practitioners) from the Spring Land National Cybersecurity Authority (NCSA). The participants were chosen for the purposes of this study where they reflected upon their roles within (NCSA), the responsibilities for Cybersecurity and the boundaries of the study. The results have provided a good opportunity to highlight the fact that countries in transitional stage are not operating in isolation and their failure in certain critical areas such as cyberspace are likely to have a ripple effect in destabilising stable states.

The structure of this Chapter is as follows: in Section 4.2 the research goal is presented. In Section 4.3, the research method and process are discussed. The Process and Participants in this stage are provided in Section 4.3.1 and the Idea Writing (IW) are deliberated in Section 4.3.2. The Nominal Group Techniques (NGT) and Interpretive Structural Modelling (ISM) outcomes are delivered in Section 4.3.4. Section 4.5 provides a summary of this chapter.

## 4.2 Research Goal

The primary purpose of this chapter is to contextualise the challenges that Spring Land face in relation to cybersecurity capacity. As explained in **Chapter 1**, the questions of this thesis served as reference points to guide the contextualisation questions. The questions in this stage were built based on the CCMM dimensions. Global Cybersecurity Capacity Centre in University of Oxford has developed the Cybersecurity Capacity Maturity Model for Nations (CCMM) through collaboration with international stakeholders. These include the Organization of American States (OAS), World Bank, Commonwealth Telecommunications

Organisation (CTO) and the International Telecommunication Union (ITU) (GCSCC 2017). According to GCSCC (2017), *"The CCMM allows the review of current national cybersecurity capacity maturity. In each case, understanding the requirements to achieve higher levels of capacity should directly indicate areas requiring further investment, and the data required to evidence such capacity levels."*

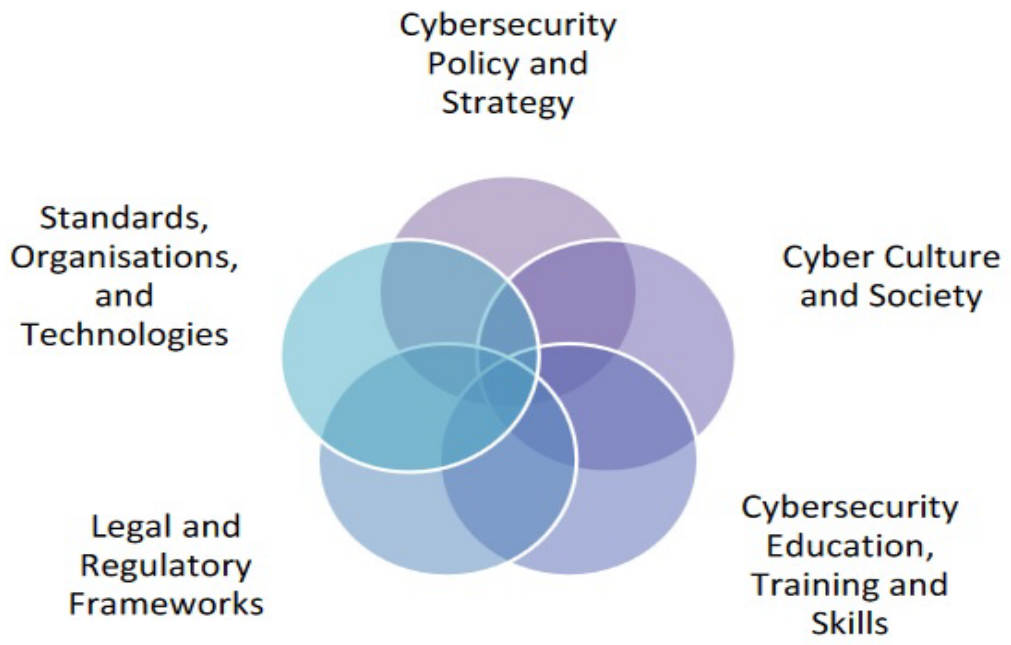



Figure 4.1: Illustration Dimension Framework (GCSCC 2017)

Figure (4.1) illustrate the main five dimensions that considered for enhancing cybersecurity capacity on national or organisational level. These dimensions are helps Nation states to develop the Common Operational Picture (COP) of the State-of-Art of the Cyber defence and its threat landscape (GCSCC 2017).

## 4.3 Research Method

This chapter adopted an Interactive Management (IM) as research method and data collection. IM is a technique aimed to manage the complex conditions through structured group discussions between groups of participants familiar to the particular issue. Concentrating on the problem in detail and building a deeper understanding of it prevents premature solutions not fit for purpose (Warfield and Cárdenas 2002). According to Ward et al. (2017), IM supports a consensus of decision-making where group members reach an

agreement on a solution together, rather than voting and leaving some members unhappy with the outcome. It promotes effective communication, participation, and is an efficient use of participants' time.

### 4.3.1 Process and Participants

In this study, a one-day Workshop hosted by NCSA was conducted for a total of 26 participants from different stakeholders. NCSA had issued an invitation letter to all stakeholders to help the researcher in contextualising the problem space that is centred on the current Spring Land National security state. The information details of participants involved in the workshop are listed below in Table (4.1).

| Code | The Organisation | Job Role | Years of Experience |
|---|---|---|---|
| P1 | National ID project | General Director of National ID project | 2 |
| P2 | Aman Private IT Security company | Representor of the company and Sales Manger | 2 |
| P3 | Spring Land Army | IT Engineer in Army Signal Corps | Since 2009 |
| P4 | Private IT Security company | Private IT Security company | +5 |
| P5 | Spring Land Passport, Immigration and Foreigners Affairs Authority | IT Engineer in Spring Land Passport , Immigration and Foreigners Affairs Authority | 3 |
| P6 | Central Bank of Spring Land | Head of Information Security department | 10 |
| P7 | Ministry of Interior | Digital Crime unit | 12 |
| P8 | Ministry of Interior | Digital Crime unit | 10 |
| P9 | Ministry of Defence | MOD – General Manager of Human Resources Development Department | +10 |

| | | | |
|---|---|---|---|
| P10 | Ministry of Information and Telecommunication | Head of Information Security department –Technology company | 5 |
| P11 | Ministry of Information and Telecommunication | Deputy Director of Safety and Security - Mobile Phone and internet public company | +4 |
| P12 | Ministry of Information and Telecommunication, Internet service providers | Deputy Head of Information Security department - Spring Land Telecom and Technology (LTT) (Main ISP in Spring Land) | +8 |
| P13 | Intelligence agency | IT Engineer | +3 |
| P14 | Ministry of Information and Telecommunication | General Manager of e-services in Spring Land | 5 |
| P15 | Ministry of Telecommunication | Information Technology centre | 12 |
| P16 | National Oil Corporation | General Manager of IT Department | 5 |
| P17 | National Oil Corporation | IT Security Engineer - IT Department | +2 |
| P18 | National Oil Corporation | IT Security Engineer - IT Department | +2 |
| P19 | Spring Land Army | Training department – Spring Land Army | - |
| P20 | Spring Land Army | Training department – Spring Land Army | - |
| P21 | Ministry of Information and Telecommunication | Head of Information Security department –mobile phone and internet services company | Not specify |
| P23 | Spring Land Army | IT Security Engineer in Army Signal | +4 |

| | | | |
|---|---|---|---|
| | | Corps | |
| P24 | Ministry of Information and Telecommunication | Deputy Director of National Information Security and Safety Authority (NCSA) | Almost 15 years |
| P25 | Spring Land Army | General Manager of Spring Land Signal Corps | +25 |
| P26 | Ministry of Information and Telecommunication | Director of National Information Security and Safety Authority (NCSA) | +4 |
| P27 | Ministry of Defence | Head of Human Resources Development Department | Since 2015 |

Table 4.1 IM Participants Details

In this workshop, the researcher presented a brief explanation about the aim of this study, and how it will contribute to secure Spring Land cyber space. The participants were asked to read and complete a Participant Agreement Form before starting the session. Moreover, the researcher prepared a form used to gather information about the characteristics of participants, such as their roles in the organisation and years of experience. Related information is demonstrated in Appendix (1). The researcher then introduced IM techniques. This included Idea Writing (IW), Nominal Group Techniques (NGT) and Interpretive Structural Modelling (ISM). The (IW) technique has been used in order to gain participant's ideas about Spring Land Cybersecurity issues and how we can tackle them.

### 4.3.2 Idea Writing technique

As explained in the section 3.4.3.1 of the research methodology chapter, IW needs a trigger question so participants can brainstorm ideas and exchange ideas. Participants were divided to three groups where *ideas* were collected. After a short break, results of the data were presented to them using a projector. The trigger question was:

*"What are the current issues of Cybersecurity in Spring Land?"*

In addition, the researcher has created a table with a set of interactive questions based on the CCMM model represented in the Table (4.2). These questions are designed to help participants understand the content of the CCMM model in order to identify the problems and weaknesses of state institutions, and how to solve them.

| Dimensions | Interactive questions | Key Question |
|---|---|---|
| D1- Cybersecurity policy and strategy | 1. What are the key objectives of the Cybersecurity policy and strategy?<br>2. What is their comprehension of the strategic goals?<br>3. What are current issues driving cybersecurity in the Spring Land context? | When will the state be in a position to publish its national Cybersecurity strategy? |
| D2- Cyber culture and society | 1. What would be the top priority to address cybersecurity across Spring Land?<br>2. What is the cultural attitude of various agencies and co-operation to Cybersecurity defence?<br>3. What are society challenges to imbedded Cybersecurity in the home/mobile? | How do we address our societal challenges in the Digital Economy? |
| D3- Cybersecurity education, training and skills | 1. What are the key objectives of the Cybersecurity education strategy?<br>2. When will the Spring Land Government introduce Cybersecurity education in the schools?<br>3. How will the Government tackle the skills gap in Cybersecurity training? | Who has the national consciences to prioritise national Cybersecurity education and address the growing skills gap? |
| D4- Legal and regulatory frameworks | 1. How do we manage and regulate data protection loss (DPL)?<br>2. Is our intellectual property rights (IP) fit for purpose?<br>3. How will we align to the EU General Data Protection regulation (GDPR)? | When do we start legislating for the Digital Economy? |

| | | |
|---|---|---|
| D5- Standards, organisations, and technologies | 1. What do we need to facilitate a risk management culture?<br>2. How can we engage Small Medium Enterprise (SME) and individuals to design and create next –generation security products? | How do we intensify individuals or organisations to improve our national security posture? |

Table 4.2 Interactive Management Question Set

During the session, participants were divided randomly into three groups to discuss the trigger question and provide their views about the issues related to the Cybersecurity in Spring Land. After IW, the information was numbered and organised, then placed into categories in which each ideas related to each of the CCMM dimensions. The lists of ideas generated from the groups question are represented using the input template analysis that created in **Section 3.5.1** as shown in Table (4.3) below.

| Dimensions | Challenges and issues |
|---|---|
| D1 - Cybersecurity Policy and Strategy | D1-1. Lack of national Cybersecurity strategy.<br>D1-2. Lack of national risk management plan and threat of cyber space has not identified on the national or sectors level.<br>D1-3. There is no national roadmap for Cyber Defence strategy.<br>D1-4. Difficulties in implementing the Cybersecurity strategy due to political issues and scarcity of resources for preparation of national Cybersecurity blueprint (government funding and human resources).<br>D1-5. Lack of public and private partnership. In addition, there are no government forums to share information.<br>D1-6. There is no national crisis management protocol and Incident response plan for national critical infrastructure assets have not been prioritised.<br>D1-7. There is no national Cybersecurity framework to monitor the adoption of international cybersecurity standards in the government sectors. |

| | |
|---|---|
| D2 - Cyber Culture and Society | D2-1. Lack of Cybersecurity culture and absence of understanding of cyber-risk and consequences by citizens, employee of public and private sectors and decision makers.<br>D2-2. Lack of awareness programs on the governmental level except some initiative from NCSA.<br>D2-3. Citizens' confidence in the use of e-government services is weak due to the lack of interest of some sectors in providing distinctive and secure services. |
| D3 - Cybersecurity Education, Training and Skills | D3-1. Dearth of experienced people for train and teach Cybersecurity programs and migration of experiences due to the security situation in the country.<br>D3-2. There is no national plan or curriculums in educational system that meets the needs of Cybersecurity environment.<br>D3-3. Education outputs in cybersecurity domain are weak and focused only on technical issues.<br>D3-4. Lack of training collaboration between public and private sector.<br>D3-5. There is no strategic view for Cybersecurity capacity building. |
| D4 - Legal and Regulatory Frameworks | D4-1. There is no cybersecurity legislation or regulations to protect personal, commercial and governmental data from unauthorized access, modification, destruction or misuse. In addition, the initiatives to issue laws related to cybersecurity and e-transactions issues are facing difficulties as a result of the political situation.<br>D4-2. There is no legislation or regulations to report breaches and abuses on cyber space.<br>D4.3. Absence of legislative system due to unrest political situation.<br>D4-4. Poor cooperation between the authorities in the Ministries of Justice and Interior, especially in the field of digital criminal investigation<br>D4-5. Absence of human rights law on cyber space.<br>D4-6. There is no official national policy or framework for |

| | |
|---|---|
| | reporting of or sharing technical vulnerabilities**.**<br>D4-7. There is no specific legislation concerning to cybercrime, and there are no courts to handle cybercrime cases.<br>D4-8. Lack of resources, expertise and laboratories for digital criminal investigation. |
| D5 - Standards, Organisations, and Technologies | D5-1. Lack of use of information security management system (ISMS) is a set of policies and procedures in all governmental sectors except some telecommunications provider (Almadar Mobile Operator).<br>D5-2. Most government sectors use technologies and applications from third parties and international companies without paying attention to reviewing the security vulnerability in the systems.<br>D5-3. There is no national agency for digital certification and there is no national Public Key Infrastructure (PKI).<br>D5-4. There is no national benchmarking, auditing and risk assessment policy.D5-5. There is no national infrastructure resilience plan due to lack of coordination between the governmental agencies with respect to governing resilience efforts. In addition, military and political conflicts have extremely affected the resilience of infrastructure and exposed the sectors of telecommunications, electricity and water to destroy or stolen.<br>D5-6. Most government sectors use technologies and applications from third parties and international companies without paying attention to reviewing the security vulnerability in the systems. |

Table 4.3 List of CCB Challenges in Spring Land

After IW was categorised participants were asked to rank them between one and five, based on the importance of each category as represented in Table (4.4) were one is the most important and five is less important.

| Category | Ideas | Rank |
|---|---|---|
| Policy and strategy | D1.1,D1.2,D1.3,D1.4,D1.5,D1.6,D1.7 | 1 |
| Culture and Society | D2.1,D2.2,D2.3 | 2 |
| Education, training and skills | D3.1,D3.2,D3.3,D3.4,D3.5 | 3 |
| Legal and regulatory frameworks | D4.1,D4.2,D4.3,D4.4,D4.5,D4.6,D4.7,D4.8 | 2 |
| Standards, organisations, and technologies | D5.1,D5.2,D5.3,D5.4,D5.5,D5.6 | 4 |

Table 4.4 Categorisation of Idea

In view of the aforementioned issues in Spring Land, these are revealing participants concerns. The lack of National Cybersecurity policy and strategy, legal framework, and cyber culture and awareness were ranked the most important issues. These issues need greater attention from the government because they are impacting the Spring Land Cybersecurity ecosystem. These issues were raised due to political issues and scarcity of resources for preparation of national Cybersecurity blueprint (government funding and human resources). Furthermore, participants also perceived that the absence of these frameworks creates more potential issues. For instance, there is lack of national risk management plan, and the threat of cyber space on national security has not identified. Likewise, there is no government forum to share information or report incidents, even between the government organisations or between public and private sectors. Moreover, there is no national roadmap for a Cyber Defence strategy.

Participants also noted that there is a lack of Cybersecurity culture, and absence of understanding of cyber-risk and consequences by citizens, employees and decision makers. However, this issue identified that inside attacks provide the most challenges for governmental agencies. Furthermore, participants also observed that, there is no national plan or curriculums in educational system that meets the needs of Cybersecurity environment; this contributed to the shortages of skilled people. In addition, a lack control over mixed technologies and lack of Disaster Recovery and Business Continuity plan in all governmental sectors were identified by the participant group.

### 4.3.3 Nominal Group Techniques (NGT)

After the ideas writing was organised and numbered, the participants were asked to transformer these ideas into a set of objectives. These objectives were used to create an interpretive structural model and summarise the interactions between them. Table (4.5) shows the list of objectives generated by participants.

| Dimensions | Objectives (Functions) |
|---|---|
| D1 - Cybersecurity Policy and Strategy | D1.1- Adopt a national Cybersecurity framework and create collaborative model for include all stakeholders to write the national Cybersecurity strategy.<br>D1.2- Develop information sharing mechanism between the public and the private sectors.<br>D1.3- Establishment of a central committee for cybersecurity.<br>D1.4-Increase the development of the Spring Land CERT and provide clear processes that define roles and responsibilities<br>D1.5-Specify a national level for reporting of incidents and boost reporting.<br>D1.6-Create a national list of Critical National Infrastructure (CNI) assets and identify the risk priorities<br>D1.7-Allocate funding for implement Cybersecurity framework<br>D1.8-Start the development of a national cyber defense strategy and identify the threats to national security on cyber space. |
| D2 - Cyber Culture and Society | D2.1-Foster the efforts of the awareness at all decision makers level of government to raise understanding of risks and threats<br>D2.2-Develop national awareness program compatible with the current situation targeting all society<br>D2.3- Encourage all stakeholders to run regular awareness campaigns and provide training needs.<br>D2.4-Improve e-services to promote required trust and improve the application of security measures. |
| D3 - Cybersecurity Education, Training and Skills | D3.1-Develop national Cybersecurity education Cybersecurity modules.<br>D3.2-Provide a sufficient budget for capacity building in understanding Cybersecurity issues, cryptographic techniques.<br>D3.3-Combine the education with practical training.<br>D3.4-Classify the training needs and develop cyber exercises and drills<br>D3.5-Prepare specialised programs to attract distinguished people in this field including hackers and guide them to the right path. |

| | |
|---|---|
| | D3.6- Establish national Cybersecurity researches centre and develop collaborative training platforms between public and private sector. |
| D4 - Legal and Regulatory Frameworks | D4.1-Draft a national laws and regulations related to digital crime<br>D4.2-Create a strong national legal framework for sharing of information incidents, vulnerability disclosure and report.<br>D4.3- Build and strengthen national capacities in law enforcement , cyber related crimes investigation and prosecutors and judges<br>D4.4-Establishing a specialised centre for digital forensic studies<br>D4.5-Enhance national and international cooperation and mutual legal assistance in combating digital crime.<br>D4.6-Develop privacy and data protection standards |
| D5 - Standards, Organisations, and Technologies | D5.1-Adapt and adopt of international standards such as ISO27000 in all stakeholders.<br>D5.2-Create a national risk assessment, crisis management and auditing framework.<br>D5.3-Establish a national agency to issue digital signature certificate and create public key infrastructure.<br>D5.4-Increase reliability of e-government and develop national resilience plan.<br>D5.5-Enhance physical security.<br>D5.6- Embed security-by-design, in buying technology or install software from overseas. |

Table 4.5 List of Objectives

In the last part of the workshop, we used NGT where participants were asked to choose their top three objectives from the list of each dimension. Each objective was rated between the numbers one and three, with one being the less important and three the most important. Table (4.6) shows the results of rating the objectives.

During this stage a total of 19 participants voted on the objectives, and 7 participants failed to vote have because they were committed to other scheduled meetings, as department managers at their organisations.

| objectives | | P1 | P2 | P3 | P4 | P5 | P7 | P8 | P10 | P11 | P12 | P13 | P14 | P15 | P16 | P17 | P18 | P21 | P22 | P23 | Total |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| D1 | D1-O1 | 2 | 2 | 3 | 1 | 3 | 3 | 1 | | 3 | 3 | 3 | | 3 | 2 | 3 | 3 | 2 | 2 | 2 | 41 |
| | D1-O2 | | | | | | | | | | 1 | | | | | | | | | | 1 |
| | D1-O3 | 1 | 3 | 2 | 3 | | 2 | 3 | 2 | 2 | | 2 | 1 | 2 | 3 | 2 | 2 | 3 | 3 | 1 | 37 |
| | D1-O4 | | | | | | | | | | | | | | | | | | | 3 | 3 |
| | D1-O5 | | 1 | | | | 1 | | 3 | | | 1 | | | 1 | 1 | | | | | 8 |
| | D1-O6 | 3 | | 1 | 2 | 2 | | 2 | | | 2 | | 3 | | | | | 1 | 1 | | 17 |
| | D1-O7 | | | | | | | | 1 | | | | 2 | 1 | | | 1 | | | | 5 |
| | D1-O8 | | | | | 1 | | | | 1 | | | | | | | | | | | 2 |
| D2 | D2-O1 | | 1 | 1 | 1 | 1 | | 3 | 1 | | 1 | | 1 | 1 | | 2 | 1 | | 1 | 1 | 16 |
| | D2-O2 | 3 | | 3 | 2 | 3 | 3 | | 3 | 2 | 2 | 3 | 2 | 2 | 3 | | 2 | 2 | 3 | 2 | 40 |
| | D2-O3 | 2 | 3 | | 3 | 2 | 2 | 2 | 2 | 3 | 3 | 2 | 3 | 3 | 2 | 1 | 3 | 1 | 2 | | 39 |
| | D2-O4 | 1 | 2 | 3 | | | 1 | 1 | | 1 | | 1 | | | 1 | 3 | | 3 | | 3 | 20 |
| D3 | D3-O1 | 2 | 2 | 3 | | 3 | 3 | 3 | 2 | 3 | 2 | 3 | 2 | 2 | 3 | 1 | 3 | | 3 | | 40 |
| | D3-O2 | 3 | 3 | 2 | 3 | 1 | 2 | 2 | 3 | 1 | 3 | 2 | 3 | 3 | 2 | | 2 | 1 | | 3 | 39 |
| | D3-O3 | | | | 2 | 2 | | | | | | | | | 1 | 2 | | | 2 | | 9 |
| | D3-O4 | | 1 | 1 | 1 | | | 1 | | | 1 | | | | | 3 | | 2 | | 2 | 12 |
| | D3-O5 | | | | | | | | 1 | | | | 1 | 1 | | | | 3 | 1 | 1 | 8 |
| | D3-O6 | 1 | | | | | 1 | | | 2 | | 1 | | | | | 1 | | | | 6 |
| D4 | D4-O1 | 3 | 3 | 3 | 3 | 2 | 3 | 3 | 3 | 3 | | | | 3 | 3 | | 3 | 1 | 2 | 2 | 40 |
| | D4-O2 | 2 | 2 | | 2 | | | | 1 | 2 | 3 | 3 | 3 | | 2 | 3 | 1 | 3 | 3 | 1 | 31 |
| | D4-O3 | | 1 | 2 | | 3 | 2 | 2 | | | 2 | 1 | 2 | 2 | | 2 | 2 | 2 | 1 | 3 | 27 |
| | D4-O4 | 1 | | 1 | | 1 | 1 | | | 1 | 1 | | | | 1 | | | | | | 7 |
| | D4-O5 | | | | | | | 1 | 2 | | | | | | | | | | | | 3 |
| | D4-O6 | | | | 1 | | | | | | | 2 | 1 | 1 | | 1 | | | | | 6 |
| D5 | D5-O1 | | 3 | | 3 | 2 | 3 | 3 | 2 | 3 | 2 | 1 | 3 | 1 | 2 | 1 | 1 | 3 | 3 | 3 | 39 |
| | D5-O2 | 3 | | | | 3 | 2 | 2 | 3 | 2 | 1 | 3 | 1 | 2 | 3 | 2 | 3 | 1 | | | 31 |
| | D5-O3 | | 2 | | 2 | | | | | | | | | | | | | | 2 | 2 | 8 |
| | D5-O4 | 1 | 1 | 2 | | | | | | | | | | | | | | | | | 4 |
| | D5-O5 | 2 | | 3 | 1 | 1 | | 1 | 1 | 1 | 3 | | | 3 | | 3 | 2 | 3 | 1 | 1 | 26 |
| | D5-O6 | | | 1 | | | | | | | | 2 | 3 | | 1 | | | | | | 7 |

Table 4.6 Participant’s ranking of objectives

### 4.3.4 Interpretive Structural Modelling (ISM)

The ISM technique helped the participants to examine the inter-relationships between the elements gained through the NGT process, and provided a structure for tackling its complexity (Dogan et al. 2011). The ISM is an acknowledged methodology for classifying relationships among a set of interconnected criteria, which define a problem or an issue (Shahabadkar 2012). The ISM was first proposed by Warfield in 1973, to analyse complex systems issues (Warfield 1974). In order to create a clear ISM, firstly the objectives generated in **Section 4.3.3** were grouped by similarity, to facilitate the identification of the three most important objectives from each dimension, which are presented in Table (4.7).

| objectives | | P1 | P2 | P3 | P4 | P5 | P7 | P8 | P10 | P11 | P12 | P13 | P14 | P15 | P16 | P17 | P18 | P21 | P22 | P23 | Total |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| D1 | D1-O1 | 2 | 2 | 3 | 1 | 3 | 3 | 1 | | 3 | 3 | 3 | | 3 | 2 | 3 | 3 | 2 | 2 | 2 | 41 |
| | D1-O3 | 1 | 3 | 2 | 3 | | 2 | 3 | 2 | 2 | | 2 | 1 | 2 | 3 | 2 | 2 | 3 | 3 | 1 | 37 |
| | D1-O6 | 3 | | 1 | 2 | 2 | | 2 | | | 2 | | 3 | | | | | 1 | 1 | | 17 |
| D2 | D2-O2 | 3 | | 3 | 2 | 3 | 3 | | 3 | 2 | 2 | 3 | 2 | 2 | 3 | | 2 | 2 | 3 | 2 | 40 |
| | D2-O3 | 2 | 3 | | 3 | 2 | 2 | 2 | 2 | 3 | 3 | 2 | 3 | 3 | 2 | 1 | 3 | 1 | 2 | | 39 |
| | D2-O4 | 1 | 2 | 3 | | | 1 | 1 | | 1 | | 1 | | | 1 | 3 | | 3 | | 3 | 20 |
| D3 | D3-O1 | 2 | 2 | 3 | | 3 | 3 | 3 | 2 | 3 | 2 | 3 | 2 | 2 | 3 | 1 | 3 | | 3 | | 40 |
| | D3-O2 | 3 | 3 | 2 | 3 | 1 | 2 | 2 | 3 | 1 | 3 | 2 | 3 | 3 | 2 | | 2 | 1 | | 3 | 39 |
| | D3-O4 | | 1 | 1 | 1 | | | 1 | | | 1 | | | | | 3 | | 2 | | 2 | 12 |
| D4 | D4-O1 | 3 | 3 | 3 | 3 | 2 | 3 | 3 | 3 | 3 | | | | 3 | 3 | | 3 | 1 | 2 | 2 | 40 |
| | D4-O2 | 2 | 2 | | 2 | | | | 1 | 2 | 3 | 3 | 3 | | 2 | 3 | 1 | 3 | 3 | 1 | 31 |
| | D4-O3 | | 1 | 2 | | 3 | 2 | 2 | | | 2 | 1 | 2 | 2 | | 2 | 2 | 2 | 1 | 3 | 27 |
| D5 | D5-O1 | | 3 | | 3 | 2 | 3 | 3 | 2 | 3 | 2 | 1 | 3 | 1 | 2 | 1 | 1 | 3 | 3 | 3 | 39 |
| | D5-O2 | 3 | | | | 3 | 2 | 2 | 3 | 2 | 1 | 3 | 1 | 2 | 3 | 2 | 3 | 1 | | | 31 |
| | D5-O5 | 2 | | 3 | 1 | 1 | | 1 | 1 | 1 | 3 | | | 3 | | 3 | 2 | 3 | 1 | 1 | 26 |

Table 4.7 Results of the important Objectives

The interpretive structural model (ISM) derived from Table 19 and their interaction based on the dimensions of the CCMM is represented in Figure (4.2). The participants stressed that the national strategy is most important objective for enhancing Spring Land Cybersecurity Capacity. Although the priorities of the current government are, counterterrorism, political stability and solidity of the security, these efforts are all facilitated by security of Spring Land cyber space. The national blueprint is also important because of state interactions in cyberspace are characterised by uncertainty, rather than predictability of this era. This is manifested by the lack of national cyber frameworks, as well as the continued development of terrorist groups' cyber capabilities in the region. Given this dilemma, an official cyber strategy is vital in both national and international contexts.

The group of participants were concerned with how to balance the need to implement a national framework and the availability of government funding and human resources within a political situation of unrest. Moreover, the participant group believed that, creation of national

a strategy drives to create an effective national legal framework. The legal framework would assist to improve the sharing of information, incidents vulnerability disclosure and report between governmental sectors.

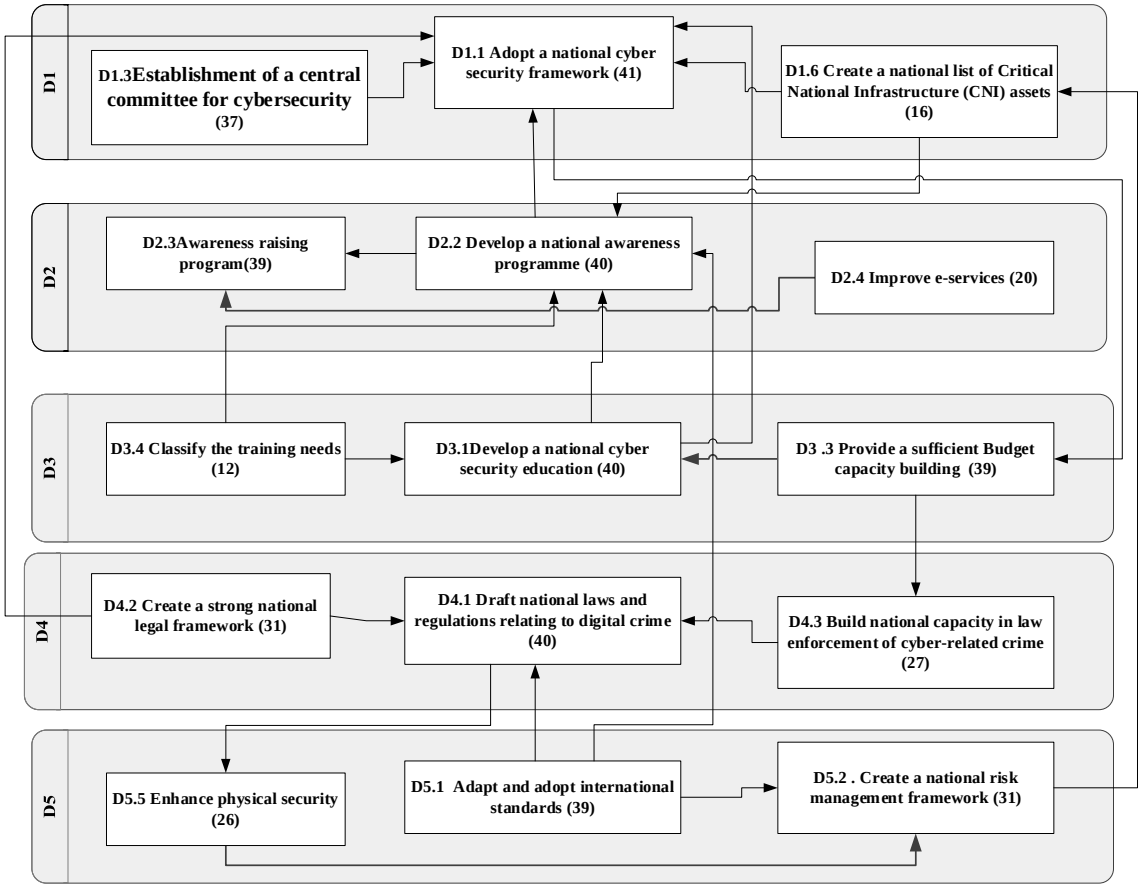



Figure 4.2 Interpretive Structural Model

In addition, providing a robust national awareness program on consequences of cyber threats program compatible with the current situation, and targeting all society, is considered as a significant factor to improve the national Cybersecurity. This program would reinforce training needs on Cybersecurity issues to change the Cybersecurity culture. Furthermore, from the diminished shortages of skilled people, a sufficient budget is required to establish a national Cybersecurity research centre, and to develop collaborative training platforms between public and private sectors. The group advocated the adaptation of international standards such as ISO27000 in all governmental agencies helps in strengthening of the technical controls process. Nevertheless, development of the national resilience plan whilst

enhancing the physical security would help to increase national and organisational capabilities to resist and react to internal and external threats.

The relationships among objectives were obtained from the judgment of the researcher and based on existing literature review. These relationships are then analysing using the adjacency matrix. The adjacency matrix is a binary matrix describing the graph with vertices and their order with respect to whether they are adjacent or not (Broome and Keever 1986). This matrix demonstrates the dependencies among objectives and it is constructed by setting (**1)** whenever there is a relationship in ISM graph between objectives and setting (**0)** when there is no relationship as shown in Table (4.8). The term Function (F) is used instead of objectives in this Table (20) based on the IDEF0 requirements. As described in **Section 2.9**, the function is a transformation activity that describes what must be accomplished, which herein are the objectives. For instance, F1.1 means objective D1.1, F1.2 means objective D1.1 and it is same for other objectives. In addition, the top three objectives in each dimension are represented sequentially. For example, F1.3 is used in dimension one equivalent to objective D1.6 and F5.1 is equivalent to objective D5.5, and same procedure is used in all dimensions.

| Dimensions/ Functions | | D1 | | | D2 | | | D3 | | | D4 | | | D5 | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | F1.1 | F1.2 | F1.3 | F2.1 | F2.2 | F2.3 | F3.1 | F3.2 | F3.3 | F4.1 | F4.2 | F4.3 | F5.1 | F5.2 | F5.3 |
| D1 | F1.1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| | F1.2 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | F1.3 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| D2 | F2.1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | F2.2 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | F2.3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| D3 | F3.1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | F3.2 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | F3.3 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| D4 | F4.1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 |
| | F4.2 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | F4.3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| D5 | F5.1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 |
| | F5.2 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | F5.3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| Dependencies | | 5 | 0 | 1 | 5 | 0 | 1 | 2 | 1 | 1 | 1 | 2 | 0 | 0 | 2 | 1 |

Table 4.8 Adjacent Matrix

Based on the results from Table (4.8), the function template analysis created in **Section 3.5.2** has been used to capture all required functions for each dimension and the interaction of each activity with other activities in the same dimension of other dimensions as shown in Table (4.9). These functions are used as main activities in the proposed framework in **Chapter 6**.

| Dimension ID | Functions ID and description (Activities ) | Interaction |
|---|---|---|
| D1 | F1.1.Adopt a national Cybersecurity framework and create collaborative model for include all stakeholders to write the national Cybersecurity strategy. | • Depends on F1.2,F1.3,F2.2,F3.1, and F4.2<br>• Supports F3.2 |
| | F1.2. Establishment of a central committee for cybersecurity. | • Supports F1.1 |
| | F1.3.Create a national list of Critical National Infrastructure (CNI) assets and identify the risk priorities | • Depends on F5.2<br>• Supports F1.1 and F2.2 |
| D2 | F2.1. Develop national awareness program compatible with the current situation targeting all society | • Depends on F1.3,F2.2,F3.1,F3.3, and F5.1<br>• Supports F1.1 and F2.2 |
| | F2.2. Encourage all stakeholders to run regular awareness campaigns and provide training needs. | • Depends on F2.3<br>• Supports F2.1 |
| | F2.3. Improve e-services to promote required trust and improve the application of security measures. | • Supports F2.2 |
| D3 | F3.1. Develop national Cybersecurity education Cybersecurity modules. | • Depends on F3.2, and F3.3<br>• Supports F2.1 |
| | F3.2.Provide a sufficient budget for capacity building in understanding Cybersecurity issues, cryptographic techniques. | • Depends on F1.1<br>• Supports F3.1and F4.3 |

| | | |
|---|---|---|
| | D3.4. Classify the training needs and develop cyber exercises and drills | • Supports F2.1and F3.1 |
| D4 | F4.1. Draft a national laws and regulations related to digital crime | • Depends on F4.2,F5.1 and F4.3<br>• Supports F1.1,F5.3 |
| | F4.2. Create a strong national legal framework | • Supports F1.1 and F4.1 |
| | F4.3. Build and strengthen national capacities in law enforcement | • Depends on F3.2, and F3.3<br>• Supports F2.1 |
| D5 | F5.1.Adapt and adopt of international standards such as ISO27000 in all stakeholders. | • Supports F2.2,F4.1 and F5.2 |
| | F5.2.Create a national risk assessment, crisis management and auditing framework | • Depends on F5.1, and F5.2<br>• Supports F1.3 |
| | F5.3.Enhance physical security. | • Depends on F4.1<br>• Supports F5.2 |

Table 4.9 List of top three functions

## 4.5 Chapter Summary

In conclusion, the IM workshop provided a rational grounding on what the current Cybersecurity challenges in Spring Land, and how we can address them. All participants agreed that the current challenges should be tackled urgently, with a need towards developing a national cybersecurity framework. These challenges are summarised below:

1. There are no Spring Land official documents describing the cyber threats to Spring Land, which means no national strategy related to the Cybersecurity field is exist. This lack is due to political instability and scarcity of resources for preparing the national Cybersecurity blueprint (government funding and human resources).

2. There are a Lack of Cybersecurity culture and absence of understanding consequences of cyber-risk by citizens, employee of public and private sectors and decision makers. The reasons for this are no large-scale of training and an awareness campaign on Cybersecurity with all governmental sectors is provided. Thus, Citizens' confidence in the use of e-government services is weak

3. Dearth of experienced people for train and teach Cybersecurity programs and migration of experiences due to an unstable situation in the state. This is as a result of lack of strategic view for Cybersecurity Capacity building that meets the needs of Cybersecurity environment in the Spring Land. Furthermore, there is no sufficient budget for training needs such as cyber exercises and drills. As well as, there is no interdisciplinary research centres that are developed collaborative training platforms between public and private sector and involved in a wide-ranging study related to the Cybersecurity issues.

4. There is no cybersecurity legislation or regulations to protect personal, commercial and governmental data from unauthorized access, modification, destruction or misuse. In addition, there is no national mechanism to report breaches and vulnerabilities on cyber space. This is due to absence of legislative system due to unrest political situation.

5. There is no national infrastructure resilience plan due to lack of coordination between the governmental agencies with respect to governing resilience efforts. In

addition, military and political conflicts have extremely affected the resilience of infrastructure and exposed the sectors of telecommunications, electricity and water to destroy or stolen. In addition, most government sectors in Spring Land are vulnerable as it immensely relies on overseas software and technology products, without exploring the potential the security vulnerability and holes.

# 5. CHAPTER 5: ASSESSMENT OF NATIONAL CYBERSECURITY CAPACITY MATURITY LEVELS IN SPRING LAND

## 5.1 Introduction

This chapter discusses the results of applying the CCMM model to review the key issues related to the Libyan cyber security policy and strategy. Moreover, it describes the state's cybersecurity ecosystem; legal and regulation aspects, cultural and social aspects, educational aspects and mitigating risks over standards, organisations and technologies resilience. The results show that Spring Land has many issues such as lack of cybersecurity culture and collaborative road-map across government sectors which results in instability within the country. The assessments feed into the requirement analysis of the National Cybersecurity Capacity Building Framework that can be utilised to organise and test the cybersecurity for nations. The assessment results of the CCMM have been verified and validated by mapping them with ITU GCI Pillars reports 2017 and 2018. More information is available in **Section 5.4**.

The structure of this Chapter is as follows: Section 5.2 provides the research goal. The research method, data collection technique, and profiles of participants are discussed in Section 5.3. Section 5.4 discusses the levels of Spring Land cybersecurity capacity maturity for each dimension in the CCMM. Critical Reflection of Nation State Posture is delivered in Section 5.5. The summary of this chapter is discussed in Section 5.6.

## 5.2 Research Goal

The main goal of this Chapter is to assess the current maturity levels of Cybersecurity capacity in Spring Land by using the CCMM, and to determine areas of capability that are required by the Spring Land Government in order to improve Cybersecurity Capacity of the state. In order to gather the data, the Focus Group Discussion method has been chosen and applied. This method ensures to obtain a high quantity of data through interaction with and between participants.

## 5.3 Research Method

### 5.3.1 Focus group

Focus group discussions aim to explore a range of ideas and feelings that individuals have about certain issues, as well as illuminating differences in the perspectives of groups of individuals (Tong et al. 2007). When using a focus group technique, the data are collected by means of precise group collaboration on a chosen topic (Doody et al. 2013). Similar to the interview technique, focus groups are an interactive approach with the benefit that during the process of collecting data and information, diverse perspectives and conceptions can emerge. The authors had selected focus group method since it offers a richer set of data compared to other qualitative approaches (Kitzinger 1995b)

### 5.3.2 Participants' profile

Five national experts (lead practitioners) from (NCSA) participated in sessions hosted in Tripoli where they reflected upon their roles within NCSA, the responsibilities for National security and the boundaries of the study. National Cybersecurity Authority (NCSA) was established by a decree No # (28) on January 22, 2013 by the Ministerial Council of the State of Spring Land (NISSA 2013). NCSA leads the national Cybersecurity program in Spring Land in terms of technical, operational and strategic levels for the State to achieve resilience.

Table (5.1) represents participant details, their roles in NCSA, and work experience in the field of Information Security. For confidentiality purposes, the names of participants were not disclosed. The researcher set-up a table and a set of questions based on CCMM, then distributed them to the participants in the discussion. Table (5.2) represents the example of these dimensions and the questions. Additional information can be found in Appendix (3).

The discussion was recorded using a smartphone application, then later transcribed into a word document in Arabic language, which the researcher then translated into the English language. For more information, refer to Appendix (4).

| Code | Job Description | Role in NCSA | Years of Experience |
|---|---|---|---|
| N1 | Deputy Director of National Cybersecurity Authority (NCSA). | Assisting the general director of NCSA and Chairman of the committee of preparing the Cybersecurity Strategy in Spring Land. | Almost 15 years |
| N2 | Head of Spring Land-CERT | Managing and monitoring the Cybersecurity incidents response team and Communicate with international and local organisations. | 8 years |
| N3 | Head of Awareness and General Relations | Develop Cybersecurity awareness and training programs. Communicate with public and private sectors regarding the preparation of awareness programs. | 2 years |
| N4 | Head of Internal Auditor office | Review the NCSA business process. | 2 years |
| N5 | Director of National Cybersecurity Authority (NCSA). | Chairman of the committee of preparing the Cybersecurity Strategy in Spring Land | 2 years |

Table 5.1 Focus group participants'details

In all focus group meetings, the researcher served as the facilitator and moderator. The role of the facilitator (Patton 1990) was to encourage participants to take an active part in high-quality discussions centred on the topic of State Resilience. Moreover, the researcher provided a brief explanation of the idea of the project, domains of CCMM model, and the interview questions. NCSA participants were asked to complete a Participant Agreement Form before commencement of these discussions, more information can be found in Appendix (1). Furthermore, the researcher also prepared a form to profile the characteristics of each participant, such as their roles in NCSA and their years of experience. Further information can be found in Appendix (2).

| Dimensions | Factors | Indicators | | | | | Challenges and issues<br>Rational for Indicator Selection |
|---|---|---|---|---|---|---|---|
| | | S-UP | F | E | S | D | |
| D2 | D2-1 | | | | | | Are we conducting Cybersecurity awareness activities for the critical services? How?<br>What are the cybersecurity issues currently been addressed and what is the degree of importance of each issue?<br>Are there any standard, policies and security measures to promote trust in e-services<br>Is there legislation or regulations detailing privacy? |
| | D2-2 | | | | | | |
| | D2-3 | | | | | | |
| | D2-4 | | | | | | |

Table 5.2 Example of Multi-Dimensional National Cybersecurity Question Set for the Review of the Spring Land Security Posture

## 5.4 Cybersecurity Capacity Maturity levels of Spring Land

The outcomes of the Spring Land Cybersecurity capacity discussion using CCMM are summarised as follows:

### 5.4.1 Cybersecurity Policy and Strategy Indicators

This dimension according to the GCSCC (2017), explores the capacity of the government to design, create, organise and implement the cybersecurity strategy. Through the discussion, this dimension was classified from start-up to strategic stages. In Spring Land, no national Cybersecurity strategy exists; however, NCSA has been assigned to be in charge of the Cybersecurity program.

"*NCSA leads the security of information and cybersecurity in Spring Land and there is no body or group related to cybersecurity in Spring Land. In general, we can say that we are in a strategic level with lack of financial support because of the political situation''- N1*

NCSA has a plan to provide a national Cybersecurity strategy and framework by 2019. The plan will aim to engage multiple stakeholders' directly and indirectly, and target all public and private sectors. In addition, NCSA had created a national Computer Emergency Response Team (SPRING LAND-CERT), which is working at the level of NCSA departments only. This is due to lack of co-operation on the state level for many reasons such as ; lack of a national strategy, administrative complications, and furthermore there is no trust between all sectors, political orientations and poor awareness.

*''In general, we have national accreditation to represent Spring Land in the world, but there is no national plan, and also, the communication channels between the sectors is very weak due to the fear of dealing with each other for several reasons; including obstruction of administrative procedures suffering from a lack of information sharing between all sectors, political orientations and poor awareness'' - Director of Spring Land-CERT.*

According to the Director of Spring Land-CERT,

*''there is a good cooperation on the international level as Spring Land is a member in different international organisations such as; the Organisation of The Islamic Cooperation – Computer Emergency Response Teams (OIC-CERT); AfricaCERT; and for the future has a plan to get a membership in the global Forum of Incident Response and Security Teams (FIRST) by 2019''.*

Furthermore, NCSA has a good co-operation with Oman-CERT and Tunisia-CERT. The participants agreed that Spring Land is in a strategic level due to national and international recognition as an organisation, but there are no a co-ordination mechanisms for incident response at the national level.

*''generally we can say that the international cooperation is high, due to the existence of international concerns of cyber risks, but at the national level, it is weak and the cooperation is based on the personal relations between the authority and some other government sectors''* - Director of Spring Land-CERT

The NCSA team had mentioned that they were thinking about the creation of a National Security Operation Centre, containing Spring Land-CERT and cyber threat intelligence within one centre.

On the subject of Critical National Infrastructure (CNI) Protection, the Spring Land government has not issued a list of (CNI). Yet, the physical security is very impressive and most of the Spring Land critical systems have been destroyed. For instance, the SCADA system in the Man-Made River that provides water to all cities in Spring Land was destroyed as result of fighting between Militias.

*''In the aspect of Critical National Infrastructure (CNI) Protection, Spring Land is at an extremely low-scale and the government has not issued a list of (CNI). In general, the physical security has a negative impact on CNI and there are no clear processes to reveal who is in charge of protecting all sectors, except the telecommunication sector''* - Director of Internal Auditor Department.

Moreover, the Deputy Director of NCSA declared that the NCSA awareness team have planned to conduct a workshop about SCADA security to the Man-Made River authority, but their response was:

"The *SCADA system is out of service for a year or more, because all links and cables were stolen, because militias were thinking that the cables were made from a copper wire to sell them''*.

Additionally, there is no national response plan to handle Cybersecurity incidents, and there is no co-ordination mechanism established. According to the Director of Spring Land-CERT,

*''National strategy for risk assessment is currently unavailable and is not specified or rated, but there is a considerable interest within the telecommunications sector in the field of physical security to protect Spring Land's telecommunications infrastructure. Nevertheless, at the level of the state, we are in a start-up level''*.

In relation to crisis management, there are no government strategies or protocols dealing with cyber or physical crisis.

*‘‘There is no national framework for analysing and identifying risks and threats. There are currently efforts to establish a centre, and we are working on it. The proposal is submitted to the Prime Minister’s Council to build a homeland crisis centre (National Crisis Management Centre). We could say that we are still in the start-up-level’’* - Deputy Director of NCSA.

Additionally, all participants have mentioned that Spring Land does not have a cyber defence policy as a result of political instability.

In relation to Digital Redundancy, there is no official business continuity plan or recovery on the national level, and there is a lack of co-ordination between public and private sectors. In addition, most of the organisation does not have a disaster recovery plan or log and event management.

*‘‘For example, there is a Spring Land institution that I cannot mention its name due to the confidentiality that has lost millions of Dinars, and when we investigated that, we found that there is no log management or disaster recovery plans in this organisation’’* - Director of Spring Land-CERT.

On the other hand, the NCSA team has mentioned that some sectors in Spring Land, like the Spring Land central Bank and Telecommunications sector have a business continuity recovery plan, but at the state level, there is not. These sectors are acting freely with NCSA, and NCSA as an authority is considered as an umbrella for applying future plans to co-ordination on local level.

*‘‘NCSA is acting freely in the telecommunications sector, acting in a way of simple freedom in the banking sector, and acting more freely in the oil and gas sector. Thus, in every sector, we gain trust for a while, but the authority is considered as an umbrella for applying future plans, and we can say that we are in Formative level’’* -Head of Awareness & General Relations Division.

### 5.4.2 Cyber Culture and Society Indicators

According to the GCSCC (2017) model, this dimension looks at reviewing vital elements of a responsible cyber-culture and society at the individual and governmental level, as observed by a variety of stakeholders. During the discussion, we came to understand that the Spring

Land capacity of this dimension is considered as a Start-up level. The Head of Awareness & General Relations Division in NCSA pointed-out that "*NCSA has conducted awareness activities for the governmental sectors. As a result of these activities, NCSA reported a lack of awareness program in all governmental sectors and society''*. It was also mentioned that NCSA had run a volunteer campaign (Karin) that targeted some universities in Tripoli. This campaign addressed different Cybersecurity issues to raise Cybersecurity culture between students.

*''One of the things that we have been focused on is the increase in the use of internet by citizens of all age groups, for example, social networking sites in Spring Land specifically. We have prepared a range of lectures to raise awareness from 8 to 10 different topics, such as social networking, cloud computing, information security, Internet stuff, personal computer security, spam, ransom viruses, how the terrorists hide their online activities, and privacy protection in the digital community''* - Head of Awareness & General Relations Division.

Another part of national awareness activity from NCSA is the Child Online Protection program. This program is targeting children and their families within a timeframe from 5 to 10 years. Additionally, NCSA has a plan to adopt and apply international standards from ITU about cyber awareness programs.

*''The authority is trying to apply international standards from ITU, and we have a written implementation plan to launch the program. We can say that we are in the start-up level with lack of government support''* - Head of Awareness & General Relations Division.

Furthermore, NCSA had prepared a leaflet written in Arabic language and sent it to all public sectors in Spring Land to improve and change the Cybersecurity mind-set. This leaflet has covered different topics such as: Spam, Scam, Phishing, Information Security, Wireless Network security and Cloud Computing Security. Likewise, NCSA has prepared a national awareness program on cybersecurity in general. This program focused heavily on spamming, phishing, and dangers of smart phone mobile application, specifically Android applications. For example, it was discussed that most mobile users in Spring Land had been targeted by malware attacks, which is considered as a big dilemma due to lack of user awareness.

*"We have noted that most of mobile users in Spring Land is a target to malware attacks, and this a big problem we are currently facing*" - Head of Awareness & General Relations Division.

Furthermore, NCSA has reported that some members of an organised crime group in Tripoli have been arrested. This group was supported by external parties for unknown reasons, which were likely to be political and the group are targeting certain individuals in Spring Land.

*''There was an investigation by a security organisation in co-operation with the NCSA, and the result was discovered that a group of organised crime supported by external parties and for unknown reason, which is likely to be political, especially in Tripoli. This group is targeting certain individuals, and some of these group members have been arrested''* - Deputy Director of NCSA.

Another essential point that has been mentioned by the NCSA team is where there is a lack of skilled people and Cybersecurity awareness raising campaigns to deal with Cybersecurity incidents in most government sectors. Consequently, the cybersecurity threats and vulnerabilities have been dramatically increased.

With regards to confidence and trust on the Internet, some e-government services in Spring Land have been developed and implemented, but there is a lack of trust because there are no efforts to improve online security from most of the governmental sectors. Some examples of lack of trust in online services were given by NCSA members. In certain online services provided by most organisations using social media, such as Facebook, there is a lack of security procedures. As a result of this, a majority of the organisations were subjected to cyber-attacks and material losses. For example, one of the commercial banks had been hacked from outside of Spring Land with co-operation from employees working inside the bank by using fake Facebook pages. These pages were used to activate the VISA credit card and increase the limit of withdrawal of foreign currency (USA Dollar). The reason behind that is no national public key infrastructure or digital signature certificates were in place.

*''Spring Land has been considered as a target of e-hunting; these are hackers from inside and outside Spring Land. These hackers are creating fake pages for banks to register your data in foreign exchange services, or activation of Visa card services, or increasing the*

*withdrawal limit. Most of these people are unfortunately from within the banking institutions acting in co-operation with people outside of Spring Land, and there are no public key structure and digital certificates to protect it''* - Director of Internal Auditor Department.

Furthermore, there is no legislation on privacy online that has been issued, and the maturity of this factor is considered in a Start-up stage. Spring Land has not taken steps to raise the maturity of this factor, except some initiative to issue law for electronic transactions. These initiatives are not accredited officially due to political issues and absence of the legislative body.

5.4.3 Cybersecurity Education, Training and Skills Indicators

This dimension reviews the availability and superiority of national Cybersecurity education, training, and skills development (GCSCC 2017). Through the discussion, it has been noted that Cybersecurity education, training and skills capacity in Spring Land is appearing in Start-up level. There are no plans at the national level to raise the efficiency of education in the field of cybersecurity.

*''There are no plans at the state level in defining the required educational curricula in cybersecurity''* - Head of Awareness & General Relations Division.

Additionally, there are no financial allocations for it at the state level. There is no co-ordination between universities and private companies related to Cybersecurity training, and there are no plans to continue with training government employees in Cybersecurity.

*''There are no plans at the level of the state in the field of raising the efficiency of employees in public and private sectors''* - Deputy Director of NCSA.

Through the discussion, participants mentioned that NCSA have their own plan to train the authority staff, and tried to make it as a guide to all sectors, but most of them were not interested. The NCSA team had joined some international workshops, cyber drill and conferences related to Cybersecurity.

*''The authority participated in some workshops and international cyber drill, several international conferences in Tunis, Qatar. Also, the cyberspace evaluation's conference in Amman, and attended the annual meetings of the Organisation of the Islamic Cooperation*

*(OIC), accompanied by training courses to improve the efficiency of our employees''* - NCSA team.

Moreover, the NCSA team noticed that within some enterprise boards, their executives within private and state-owned companies understand the seriousness of the subject, but there is no real training plan for the staff. The executive director depends on IT departments to deal with Cybersecurity issues in the organisations.

*''The awareness exists, but there are no real initiatives, and there is no plan in the field of raising the efficiency of employees in public and private sectors''* - NCSA team.

5.4.4 Legal and Regulatory Frameworks Indicators

This dimension looks intently at the government's capacity to design and develop national legislation and accompanying by-laws, directly and indirectly relating to cybersecurity. This particularly focuses on the topics of ICT security, privacy and data protection issues, cybercrime, and on the law enforcement, prosecution services, and courts (GCSCC 2017).

In Spring Land, the level of maturity for this dimension is considered at Start-up phase. There is no cyber and ICT security related legislation or regulation, except some initiative by the e-Commerce Chamber of the Ministry of Economy in co-operation with some specialised companies from Korea. This is to prepare a proposal generally aimed towards the issues of the Electronic Transaction law and Electronic Crime law. These initiatives are facing many problems, but the crucial problem is jurisdictional fragmentation due to political instability.

*''The e-Commerce Chamber of the Ministry of Economy in co-operation with some specialised companies from Korea prepares a proposal and that generally aims to draft an electronic crimes law to conduct electronic government transactions and services in cooperation with the authority, and the participation of the former committee. But these initiatives are not issued yet due to jurisdictional fragmentation from political instability''* - Director of Internal Auditor Department.

Moreover, there is a Digital crime unit in the Ministry of the Interior that deals with this type of crime by applying other laws relating to ordinary crime. For example, where a theft may occur that would be dealt with under traditional laws, rather than cyber-specific laws.

Regarding Privacy, data protection and human rights, Spring Land does not have any related regulations or laws.

‘‘*There are no laws related to protect systems and data’’* - NCSA team.

In addition, law enforcement, along with the investigation and prosecution of cybercrime services in Spring Land are facing a shortage of skills to handle cybercrime cases. Moreover, there is no national mechanism to report or disclosure cyber related crime and vulnerability. Also, there are no specific courts dealing with digital crime, and no training provided to build capacity in this particular dimension.

5.4.5 Standards, Organisations, and Technologies Indicators

According to CCMM model, this dimension explores the significance of employing Cybersecurity standards, and at least minimal adequate practices (GCSCC 2017). Through the discussion, all participants agreed with the statement that Spring Land is at Start-up stage. There are no Cybersecurity standards adapted to procurement and Software Development in all governmental sectors. As explained by the NCSA team, there is an attempt to start the project of implementing international standards, but there is a shortage of skilled people and financial resources.

‘‘*There is an attempt to start the project of implementing international standards, but we have a lack of resources and expertise in the public and private sectors’’* - NCSA team.

There is no national agency or framework to monitor the implementation of standards, and minimal acceptable practices in all governmental sectors. In addition, there is a lack of research centres in this field and poor co-operation between the public and private sector in training and skill development.

‘‘*There is no national framework or organisation to monitor the adaption of international standards. But, there is some future plans from the authority. In addition, there are no existing national research centres in this field’’* - NCSA team.

As motioned by participants in the discussion of Dimension 1, not all sectors have a Disaster Recovery plan or Business Continuity plan. All participants pointed-out that the government does not have a plan to manage, monitor, and evaluate national infrastructure resilience.

## 5.5 Critical Reflection of Nation State Posture

A discussion of the focus group was recorded using a smartphone application, then later transcribed into a word document in Arabic language, which the researcher then translated into the English language. For more information, please refer to in Appendix (4).

The analysis method used in this stage was content analysis as a qualitative approach. Since the data were captured the themes are identified based on the indicators of the CCMM. The input template analysis that constructed in **Section 3.5.1** was used to analyse the data. Table (5.5), presents the maturity levels of all dimensions of Spring Land cybersecurity capacity based on the CCMM. These results were mapped with ITU GCI Pillars to validate and verify the results. The GCI report 2017 and 2018 (ITU 2017a) along with other official government or ministry websites will provide further information used to define the particular stages of maturity for each factor of the CCMM.

The 2017, 2018 GCI reports are finer grained having 25 indicators with 157 binary, (0) for none compliance or (1) full compliance questions distributed among the indictors. These indictors have been selected based on the five pillars (Organisational, Legal, Technical, Capacity Building and Cooperation). Each of the indictor is associated with a specific colour. The report summarise the countries' level of commitment to every pillar and sub-pillars (green for high, yellow for medium, and red for low) (ITU 2017a). The ranking is calculated based on the following notations:

$$\text{GCI2017, 2018: } CIc = \frac{Iqc}{157}$$

*Where: Iqc* is a Normalized value of individual indicator q for country c.

*CIc* is a Value of the composite indicator for country c.

The 2017 report indicates that, Spring Land scored *CIc* = 35.12 out of 157 which is 0.226 GCI out of 1 as shown in Table (24). In the 2018 report Spring Land scored *CIc* = 32.34 out of 157 which is 0.206 GCI out of 1 as shown in Table (5.3). The difference between scores from 2017 and 2018 demonstrate dramatic changes in the GCI scores with Spring Land being the highest negative change of (-2.78). The GCI reports show that Spring Land's

preparedness for cyber threats has descended from 104 out of 136 in 2017 to 117 out of 155 worldwide countries.

| Index score | | Regional Rank | | Global Rank | |
|---|---|---|---|---|---|
| 2017 | 2018 | 2017 out of 17 Member States | 2018 out of 22 Member States | 2017 out of 136 Member States | 2018 out of 155 Member States |
| 0.224 | 0.206 | - | 16 | 104 | 117 |

Table 5.3 GCI index 2017, 2018 Spring Land results

The both reports show that, Spring Land government officially established the National Cybersecurity Authority (NCSA). NCSA's primary mission is to encourage and sustain secure use of ICTs as well as to prevent, detect, and respond effectively to the associated cyber risks (NCSA 2013). Additionally, NSCA is responsible as standardisation body to set the cybersecurity good practices and provide professional training courses for government sectors. In the same year, with the support of (ITU), Spring Land-CERT has been established with national-level responsibilities and is charged with prevention, detection, and mitigation of cyber threats. Due to the current political conflict and the austerity measures, NCSA faces lack of funding which hindered most of the attempts of advancing Cybersecurity in the context (Matsubara 2014).

In stark contrast, despite these lacks, Spring Land has been demonstrating strength in the cooperation pillar specifically in International participation. Spring Land is a member in different international such as the Organisation of The Islamic Cooperation (OIC), Africa-CERT and the Forum of Incident Response and Security Teams (FIRST) (NCSA 2013). The overall results of GCI index from ITU are mapped to the results of the focus group and presented in Table (5.4). The results show that, Spring Land's ability to address cybersecurity concerns is currently not at a level that inspires sufficient public confidence; hence, a cogent methodology to optimise its IT resources is most necessary.

| The GCI reports 2017 and 2018 results (ITU 2017a, 2018a) | Focus group results |
|---|---|
| Spring Land has Responsible Agency has been established. | "NCSA leads the security of information and cybersecurity in Spring Land and there is no body or group related to cybersecurity in Spring Land. In general, we can say that we are in a strategic level with lack of financial support because of the political situation''- N1. |
| The Responsible agency is presents Spring Land in international community and responsible for international cooperation. | ''In general, we have national accreditation to represent Spring Land in the world'' N2 |
| Spring Land does not have an officially recognised national cybersecurity strategy. However, NCSA is currently developing a national cybersecurity strategy. | ''In general, we have national accreditation to represent Spring Land in the world, but there is no national cybersecurity plan or strategy" N2,N5 |
| Spring Land-CERT is up and running since February 2013 providing some basic services under the umbrella of the National Cybersecurity Authority (NCSA). | "NCSA had created a national Computer Emergency Response Team (SPRING LAND-CERT), which is working at the level of NCSA departments only" N2,N5. |
| Spring Land has officially recognised partnerships with the following organizations: as the Organisation of The Islamic Cooperation (OIC), Africa-CERT and the Forum of Incident Response and Security Teams (FIRST) | ''there is a good cooperation on the international level as Spring Land is a member in different international organisations such as; the Organisation of The Islamic Cooperation – Computer Emergency Response Teams (OIC-CERT); AfricaCERT; and for the future has a plan to get a membership in the global Forum of Incident Response and Security Teams (FIRST) by 2019'' N1,N2,N5 |
| NSCA is running a national program in raising the awareness | "NCSA has conducted awareness activities for the governmental sectors. As a result |

| | |
|---|---|
| and promoting cybersecurity specific educational program among the public and private sectors. | of these activities, NCSA reported a lack of awareness program in all governmental sectors and society'' N1,N3,N4 |
| Spring Land does not have any officially recognised national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector. | ''There are no plans at the state level in defining the required educational curricula in cybersecurity'' N3.<br>''There are no plans at the level of the state in the field of raising the efficiency of employees in public and private sectors''N1 |
| Spring Land does not have specific legislation pertaining to cybercrime. | ''There are no laws related to protect systems and data online'' - NCSA team. |
| Spring Land does not have any certified government and public sector agencies certified under internationally recognised standards in cybersecurity. | ''There is no national framework or organisation to monitor the adaption of international standards. However, there are some future plans from the authority. In addition, there are no existing national authority'' - NCSA team. |

Table 5.4 Mapping Focus group results with GCI reports result

After mapping the results with the GCI pillars, the input template analysis was used to analyse the data collected from focus group discussion to identify the maturity level of each dimension. Based on the CCMM, each dimension has multiple factors and attributes (GCSCC, 2017), each making a significant contribution to capacity building. Each factor, involves five stages of maturity (Start-Up (S-UP), Formative (F), Established (E), Strategic (S) and Dynamic (D). The lowest indicator implies a non-existent, or inadequate, level of capacity, and the highest indicates both a strategic approach, and ability to dynamically enhance environmental considerations, including operational, socio-technical, and political threats. The rating scale from 1 to 5 is based on the CCMM model, where 1 means there is no Cybersecurity maturity or it is primitive in nature, and 5 is in a dynamic level of maturity.

To concluded, the results of the discussion indicate that the level of maturity of Spring Land's Cybersecurity capacity, which has been evaluated using the five dimensions of the CCMM, is in Start-up level. In some dimensions, such as the policy and strategy dimension, despite the fact that there is no national Cybersecurity strategy, certain factors are considered to be in a formative or strategic level. For instance, the organisation leading Cybersecurity program (NCSA) and national CERT in Spring Land has been identified. This means that raising the level of maturity of these factors helps to fill some gaps in the Spring Land Cybersecurity ecosystem.

Furthermore, one of the most significant findings to emerge from this assessment is that Spring Land does not have a blueprint of a cyber defence strategy in place; this is the result of the political fragmentations. Consequently, without any existing cyber defence strategy, Spring Land faces a big challenge in dealing with cyber threats from other states, and therefore the threat posed by terrorism, extremism and instability increases.

Dimension 2, concentrated mainly on Cyber Culture and Society Indicators. Despite the fact that the NCSA has conducted some awareness activities that are needed to change the mind-set of governmental sectors, there is still poor awareness across public and private sectors. Additionally, there is a lack of information sharing and vulnerability disclosure mechanisms which places all sectors at risk of potential cyber threats.

In other dimensions, such as the national education capacity building initiative, and the legal and regulatory frameworks, there was no existing capacity regarding these factors. There is

no national plan for enhancing the efficiency of education in the field of cybersecurity. As a result of this, there is a shortage of skilled people. Moreover, there are no comprehensive national legal and regulatory frameworks that address cyber related crime, or adequate capacity to enforce the existing laws. The implication of this is the possibility that Spring Land will continue to face challenges in tackling and responding to a cybercrime.

Finally, the last dimension in the CCMM revealed a lack of international standards adoption across all organisations. Similarly, there is a lack control over mixed technologies which increases the vulnerabilities in all systems in which the government rely on. More importantly, there is deficiency of disaster recovery and business continuity plan in all governmental sectors. And thus, the Spring Land government does not have a plan to manage, monitor or evaluate of national infrastructure resilience.

The most obvious finding obtained from the analysis is that, the unstable situation in Spring Land has a big influence on physical security and hinders the development of Spring Land Cybersecurity in all aspects. As a result of the instability and transitional stage within the state, there is an absence of a legislative system, a lack of cyber defence strategy, and insufficient funding from the government to support the national Cybersecurity program. Table 5.5 provides the results of maturity levels of all dimensions of Spring Land cybersecurity capacity.

| Dimensions | Factors | S-Up | F | E | S | D |
|---|---|---|---|---|---|---|
| D1 | D1-1 National cybersecurity strategy | | | | * | |
| | D1-2 Incident Response | | * | | | |
| | D1-3: Critical National Infrastructure (CNI) Protection | * | | | | |
| | D1-4: Crisis Management | * | | | | |
| | D1-5: Cyber Defence Consideration | * | | | | |
| | D1-6: Digital Redundancy | * | | | | |
| D2 | D2-1: Cyber Security Mind-set | * | | | | |
| | D2-2: Cyber security Awareness | * | | | | |
| | D2-3: Confidence and trust on the Internet | * | | | | |
| | D2-4: Privacy online | * | | | | |
| D3 | D3-1: National availability of cyber education and training | * | | | | |
| | D3-2: National Development of cyber security education | * | | | | |
| | D3-3 Corporate training & educational initiatives within companies | * | | | | |
| | D3-4: Corporate Governance, Knowledge and Standards | * | | | | |
| D4 | D4-1: Cybersecurity legal frameworks | * | | | | |
| | D4-2: Legal Investigation | * | | | | |
| | D4-3: Responsible Disclosure | * | | | | |
| D5 | D5-1: Adherence to standards | * | | | | |
| | D5-2: National Infrastructure Resilience | * | | | | |
| | D5-3: Cybersecurity marketplace | * | | | | |

Table 5.5 maturity levels of all dimensions of Spring Land cybersecurity capacity

These findings contribute in several ways to our understanding of the Spring Land Cybersecurity capacity, and provide a basis for the requirements of the NCCBF. The maturity levels are presented in Figure (5.1) using the radar chart. The next chapter discusses the development of a proposed NCCBF framework to improve national cybersecurity capacity for countries in transitional phase.

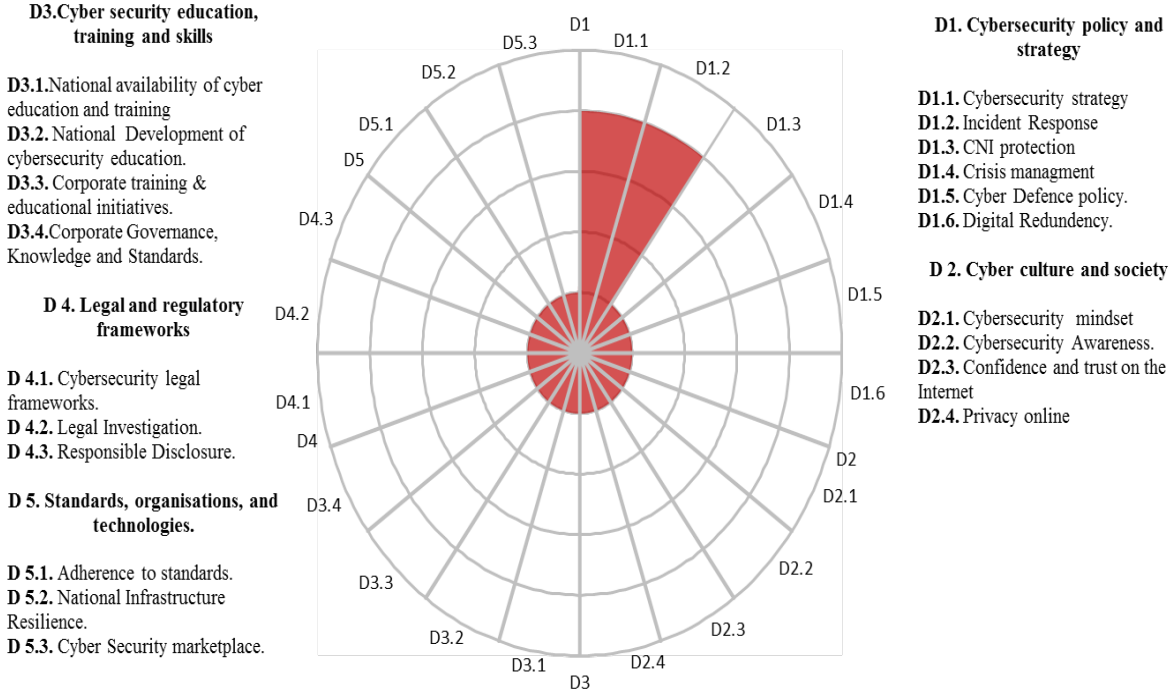



Figure 5.1 Results of all CCMM dimensions

## 5.6 Chapter Summary

This chapter has presented the results of the assessment of the level of maturity of Spring Land's Cybersecurity capacity, which has been assessed using the five dimensions of the CCMM. From the findings of the research undertaken this has assisted in areas of focus and supported the introduction of the CCMM. When aligning the output of the focus groups with the literature review findings and results of Chapter 4, this enabled a clear picture towards identifying research gaps that need to be addressed.

The next chapter will describe and discusses the development of a proposed NCCBF framework to improve national cybersecurity capacity for countries in transitional phase.

# 6. CHAPTER 6: DEVELOPMENT OF THE NATIONAL CYBERSECURITY CAPACITY BUILDING FRAMEWORK (NCCBF) FOR COUNTRIES IN A TRANSITIONAL PHASE

## 6.1 Introduction

This chapter discusses the development of a proposed NCCBF framework to improve national cybersecurity capacity for countries in transitional phase. The NCCBF incorporates the 5-dimensions of national cybersecurity capacity derived from the Oxford University's Cybersecurity Capacity Maturity Model (CCMM) for Nation States. The University's Global Cybersecurity Capacity Centre developed this maturity model through collaboration with international stakeholders. These include the Organization of American States (OAS), World Bank, Commonwealth Telecommunications Organisation (CTO) and the International Telecommunication Union (ITU). In addition, these dimensions represent an accumulation of syntheses and issues derived from the experience and perspectives of a range of cybersecurity professionals in Spring Land and other existing international frameworks for cybersecurity. These dimensions are presented in Figure (6.1) and summarised below:

- Dimension one: build strategic capacity (D1). This dimension looks at the steps required to implement and review a national cybersecurity strategy and the capacity in terms of incident response, crisis management, critical infrastructure protection, communications, redundancy, crisis management and cyber defence.

- Dimension two: build cyber cultural and society capacity (D2). This dimension covers vital features of a cyber-culture across stakeholders at the individual, public, private, and societal levels that contribute towards enhancement the maturity levels of the cyber ecosystem.

- Dimension three: build cybersecurity Education, Training and skills capacity (D3). This dimension is used to deliver essential steps for cybersecurity education, training, and skills development.

- Dimension four: Build legal and regulations capacity (D4). This aspect offers a different step required to form and update the national legislation and laws relating to cybersecurity.

- Dimension five: build technical capacities (D5). This dimension discusses the CCB steps that a country or organisation can implement to employ cybersecurity standards, and at least minimal adequate practices.

These 5-dimensions are then decomposed to three activities used to improve the capacity of each dimension. The activities have been chosen based on the most important objectives that were created by various stockholders during the contextualising and assessment of the NCCB in Spring Land.

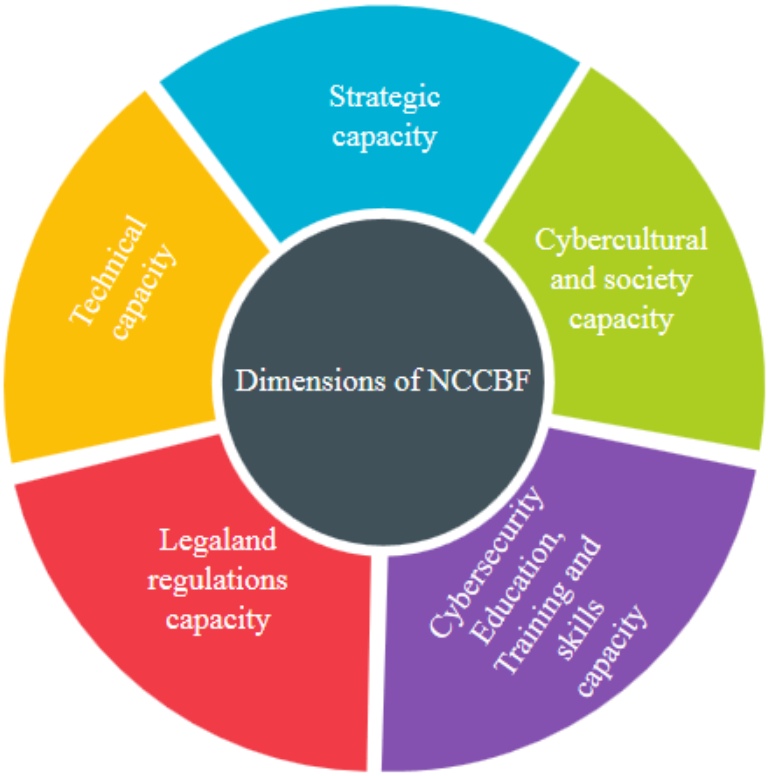



Figure 6.1 The Five dimensions of NCCBF

## 6.2 Designing and Developing the Framework (The Artefact)

The framework was developed based on the outcome from **Chapter 2** the literature review as well as contextualisation and assessments of the problem space in Spring Land in **Chapter 4** and **Chapter 5**. The OODA loop steps were used to construct and guiding the requirements of IDEF0. These steps were instantiated with the CCMM and finding from the conducted empirical studies and literature. The framework is illustrated by a modelling function technique IDEF0, which outline various issues identified by the research. These steps address the following question: *What can be developed to provide a National Cybersecurity Capacity Building Framework (NCCBF) for transitional state countries?*

As argued in Chapter 1, to validate and resolve the NCCBF challenge we required further analytical questions to develop notions posed by this challenge, in that:

Q1- What are the known challenges in delivering effective Cybersecurity Capacity Building Platform?

Q2- What are the key elements of a successful Cybersecurity Capacity Building Framework and consequentially what are the possible modelling approaches for better and effective guiding Cybersecurity Capacity Building Framework?

Q3- What are the current issues of cybersecurity capacity within a metaphorical Spring Land and what would be done to address cybersecurity across Spring Land?

Q4- How do we measure the current maturity levels of cybersecurity capacity in a metaphorical Spring Land?

Q5- How to translate the finding of Q2, Q3 and Q4 into a transformative design method which could help to develop a National Cybersecurity Capacity Building Framework (NCCBF) for countries in a transitional phase?

These steps are shown in Figure (6.2) and described below:

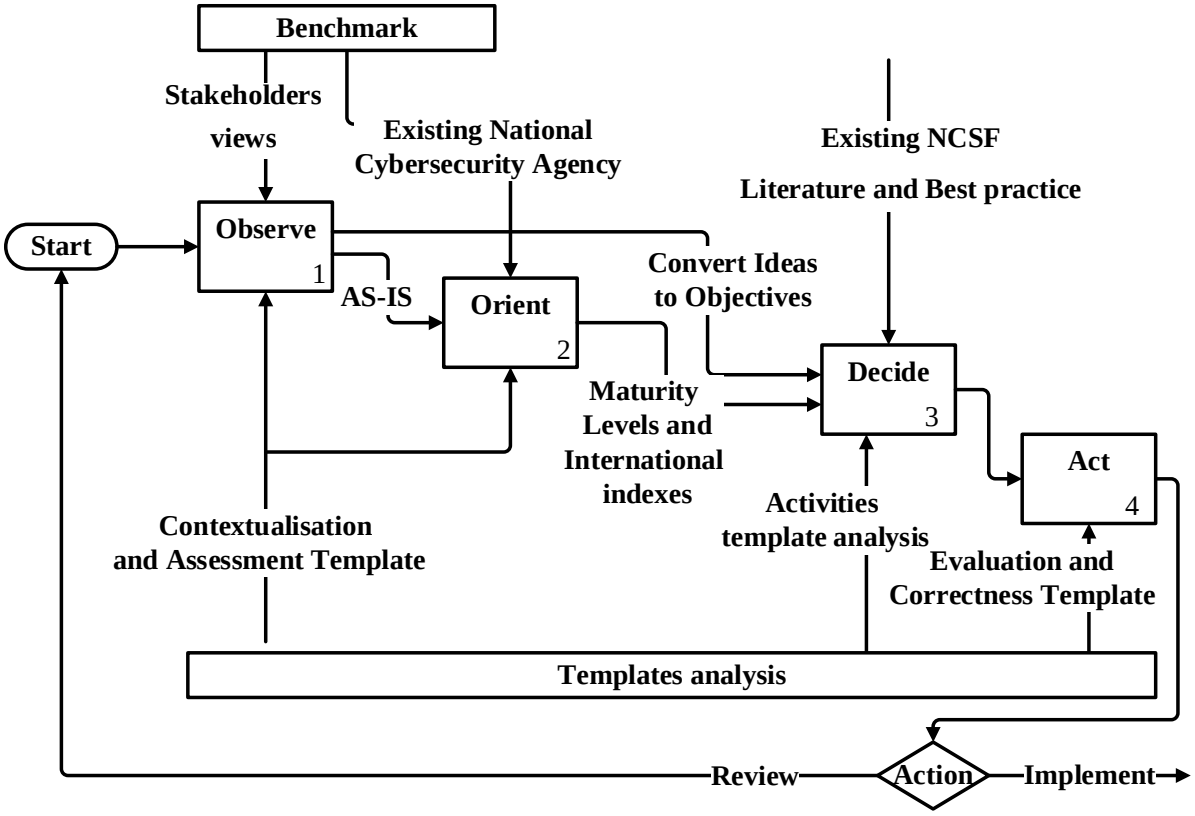



Figure 6.2 Generic NCCBF Implementation using OODA Loop

- **OODA- Observation phase**: this phase is the earliest stage of OODA loop process where the observation phase continuously analyse the social, internal, and external challenges. Within the 5th Domain – Cyberspace, this phase can be applied to contextualise the cybersecurity capacity challenges based benchmarking models. The NCCBF contextualisation step will analyse the security operations of the state within the transitional phase, with stakeholders, by performing a risk analysis, SWOT and PESTEL models. In pursuit of this research an input template analysis was created and IM techniques (Idea Writing (IW), Nominal Group Techniques (NGT) and Interpretive Structural Modelling (ISM)), were used to capture the challenges of NCB in Spring Land as described in **Chapter 4**. In addition, a set of objectives was derived to support identified the key initiatives for the development of national cybersecurity capacity in the country. These objective were employed to support the management (OODA-Decision phase) of a national cybersecurity capacity for countries in transitional phase.

- **OODA - Orientation phase**: this phase is the most critical part of the OODA loop. The raw of information obtained from the observation phase will be analysed and synthesised into usable information that can be used to support Decision phase. According to Coram (2002) the Orientation phase is a "nonlinear feedback system" that spontaneously generates a new cognitive image of the unfolding circumstances as seen in 5th Domain Lens. This phase can be adopted to assess the cybersecurity capacity maturity levels of the state by using the maturity model such as the CCMM and determine areas of capability that are required by the State in order to improve Cybersecurity capacity.

  In this research the focus group discussion were employed to assess the national cybersecurity capacity in Spring Land based on the CCMM dimensions as described in **Chapter 5.** The focus group method and input template analysis were used to determine areas of capability that are required by are required by any Government in order to improve the cybersecurity capacity of the State. As determined throughout the Observation Phase, the Orientation challenges that were captured in the previous step were validated in this stage by NCSA. The step-phase outcomes were employed with the objectives from previous stage to support the next step the OODA-Decision phase. It should also be noted that both the Observe and Orient steps were also used to identify requirements of AS-IS stage in IDEF0.

  - **OODA - Decision phase:** the information gained from the observation and orientation phases including, social internal and external challenges, implicit and explicit guidance within the State, and the context of the circumstances under consideration, leads to the point at which a decision is made. Building cybersecurity capacity within the NCCBF requires a detailed evaluation of cybersecurity capacity dimensions. This phase will be used to establish policies and legislation, build awareness program and create education framework that that are relevance and succinct to the current cyber environment and the Governance, Risk Management and Compliance (GRC) of the 5th Domain-Cyberspace. The threshold for the OODA-Decision phase will be based upon the existing cybersecurity frameworks and best practice as discovered in **Chapter 2**. In this Research Study, the outcomes of observe and

orient steps are used to develop the functions, mechanisms and controls for each dimension by using the template analysis that created in **Chapter 3**.

- **OODA - Action phase:** As outlined in Boyd's diagram, one can consider this process of acting upon opportunities discovered in the decision phase. Once the action is executed, the OODA loop closes (Coram 2002). For building cybersecurity capacity, this phase can be used to define work deliverables and work standards, and provides a way to measure the work deliverables. States need to mature cybersecurity capacity and capabilities at national level in order to facilitate the requirements expressed through national authoritative or stakeholders. These national cybersecurity capabilities typically consist of people, processes and technology (Jacobs et al. 2017). The output template analysis is used in this stage. This template has been created based on CCMM and other maturity models to check the improvement level for each dimension. Figure (6.3), show the steps and methodology approaches that were taken to develop the NCCBF for the Spring Land case study based on the CCMM .

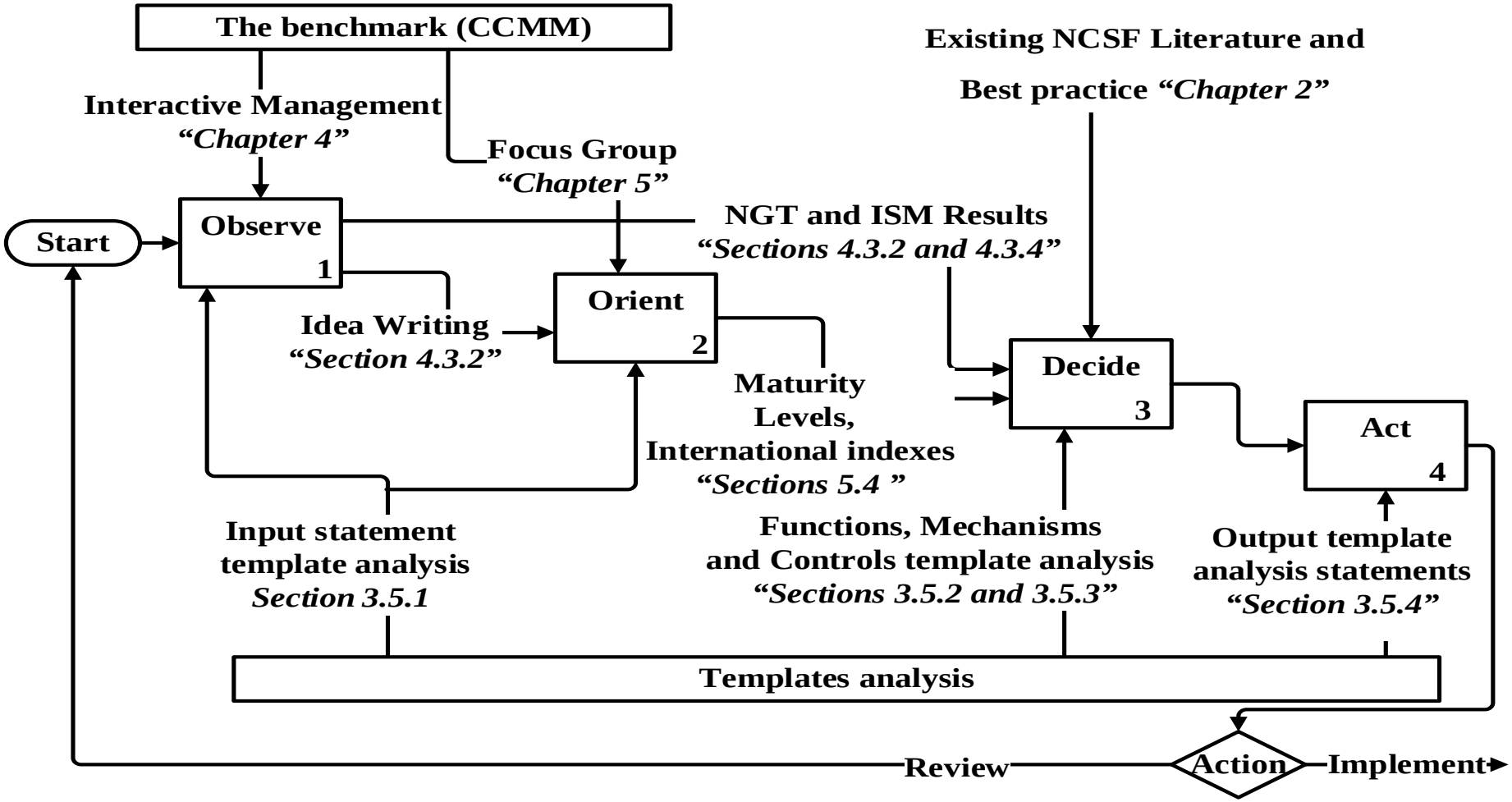



Figure 6.3 Detailed NCCBF implementation using OODA Loop

The elements of the OODA Process within the Framework were first described in Chapter 2's **Section 2.9.1** where the IDEF0 model presents a progression of the steps that support the development of the NCCBF. The top-level function of the NCCBF is numbered A0 based on IDEF0. Subsequently, A0 activity is segmented into five activities (dimensions) based on the CCMM model (GCSCC, 2017). The top-level function of the NCCBF is numbered A0 based on IDEF0. Subsequently, A0 activity is segmented into five activities (dimensions) based on the CCMM model (GCSCC, 2017). Figure (6.4) shows how the top level of the NCCBF is based within the OODA loop.

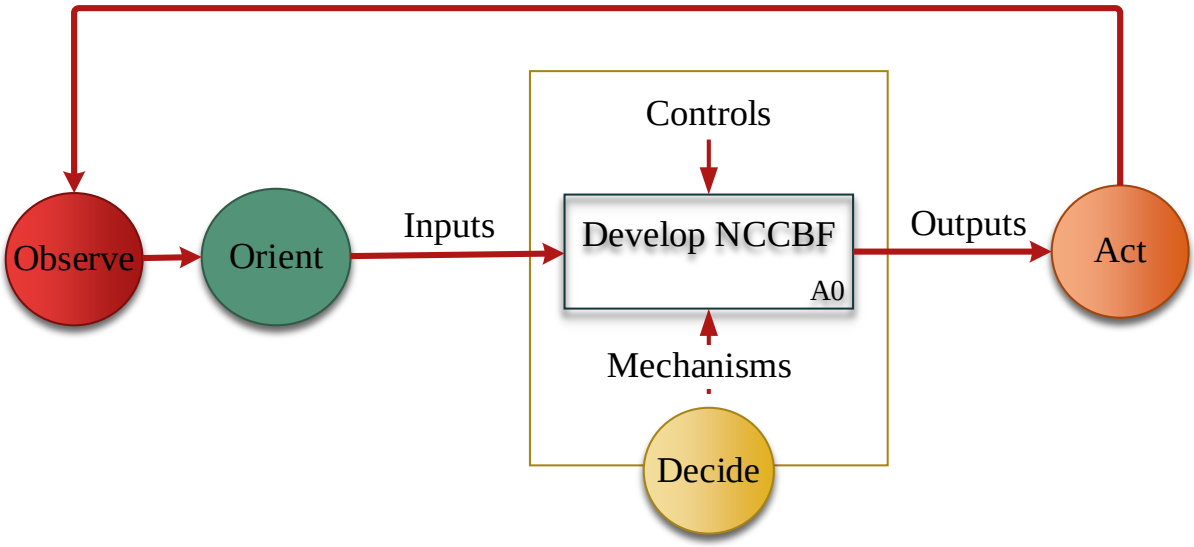



Figure 6.4 Demonstration of the NCCBF Top-level within the OODA loop.

## 6.3 Developing OODA Activities into NCCBF Artefacts

As described in the above Figure 6.4, the OODA process of four phases: observation, orientation, decision and action phase allow for an iterative loop of many cycles and hence provides a progressive methodology for constant validation and hence a valuable defensive asset to APTs, and a key design feature and NCCBF artefact. In this section, every phase is described in depth, which also shows how this phase or step is used to develop the NCCBF.

### 6.3.1 Observation phase (to the NCCBF Artefact)

The first step is to observe the AS-IS situation. This step, aimed to contextualise the problem space based on dimensions of CCMM. The contextualisation will analyse the security operations of the state based on the CCMM's five dimensions. In this research an input template analysis and IM techniques (Idea Writing (IW), Nominal Group Techniques (NGT) and Interpretive Structural Modelling (ISM)), were used to capture the challenges of NCB in Spring Land. In addition, a set of objectives was derived to support identified the key initiatives for the development of national cybersecurity capacity in the country.

The Challenges generate a number of complex situations within the 5$^{th}$ Domain-Cyberspace and utilising IM techniques which requires groups of people, who are knowledgeable in terms of the situation, to collaborate in tackling the main aspects of an issue, to develop a deep understanding of the situation under analysis as it provide effective details and safeguards for assured action. During this stage a trigger question, *"What are the current issues of cybersecurity in Spring Land*?" is presented to the participants with a forum to brainstorm and exchange ideas based on five dimension of CCMM. A template analysis is used to capture the challenges of NCB in Spring Land and has been discussed in second phase of the loop (Orientation). Following the organising and numbering of the challenges and ideas, the ideas were transformed into a set of objectives, which were used to create an interpretive structural model (ISM), and to summaries the interactions between them.

The final part of this stage, the NGT technique were employed to select the top three objectives from the list for each dimension, with one being the least important, and three the most important. These top objectives were used after summaries the interactions between them to develop the functions for each dimension in the NCCBF. This step is applied for all dimensions of the NCCBF and more details how to use it each dimension will be discussed in **Section (6.4)**. Figure (6.5) shows how this adaptive step was developed and progressed.

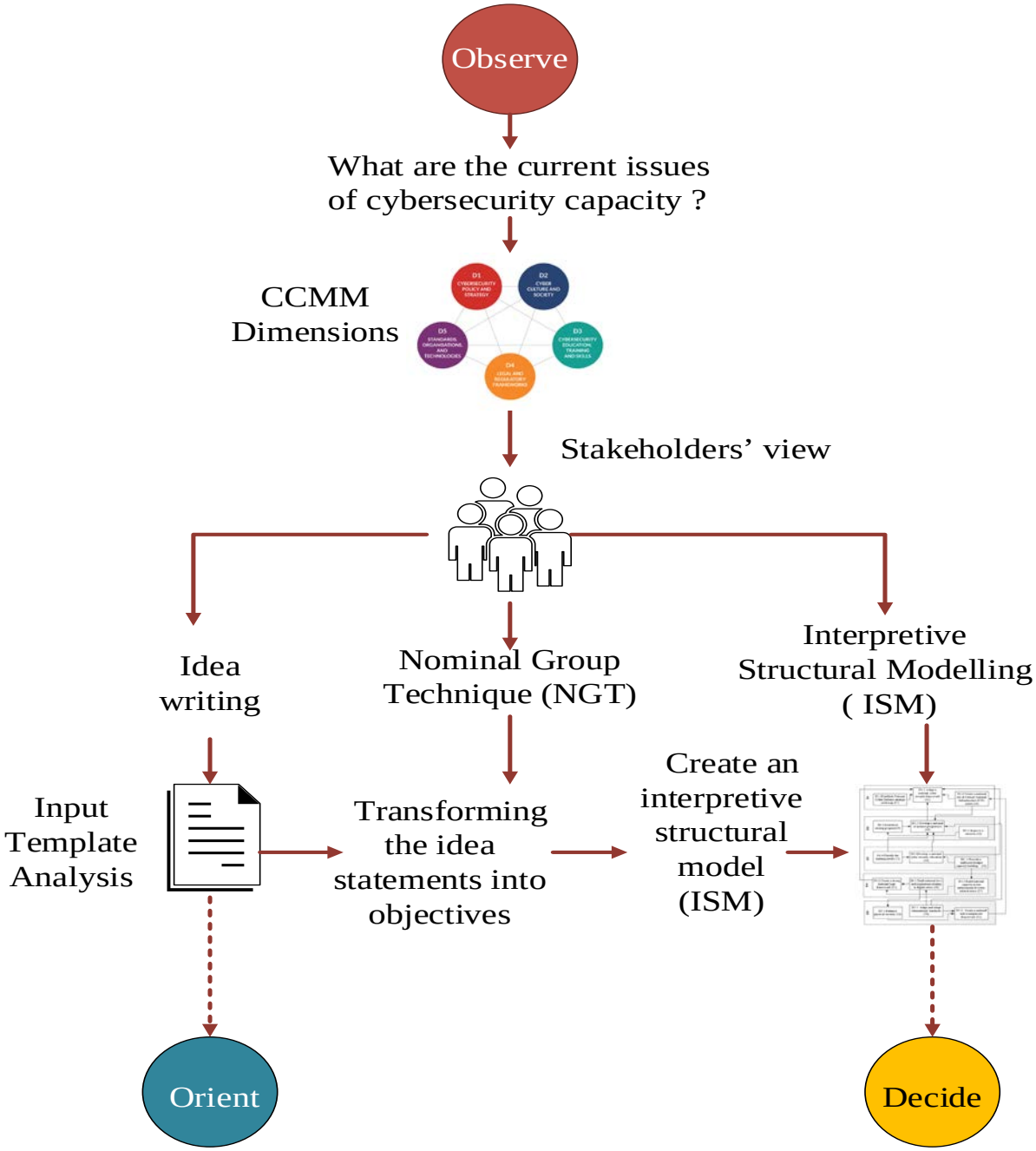



Figure 6.5 Adaptive Observe phase of the NCCBF model development

### 6.3.2 Orientation phase (to the NCCBF Artefact)

Earlier research argued to assess the current maturity levels of a State can be done by applying the CCMM and determine areas of capability that are required by the State in order to improve its cybersecurity capacity. Assessment is one of steps corresponding to OODA's Orient. In this research, focus group method and input template analysis were used to determine areas of capability that are required by the State's government in order to improve cybersecurity capacity of that State. The challenges that captured in previous step OODA-Observe step were validated at this stage by NCSA, but other recognised institutions, such as the UN's ITU or the WEF could have been employed. The rationale was for that, stakeholders might not be always aware of recent developments in their country, for instance whether the country has signed a convention on child protection or not.

During this stage a generic question, "*What are the maturity levels of cybersecurity capacity*?" was presented to the participants with a set of questions, based on five dimension of CCMM. These questions were used to guide the discussion around the indicators to provide evidence on how many indicators have been implemented by a country and to determine the maturity level of every aspect of the CCMM. Additional information about the questions can be found in Appendix (3). The authors uses a focus group method since it offers a richer set of data compared to other qualitative approaches (Williams 2003). The method is valuable for exploring people's knowledge and experiences and can be used to examine not only what people think but how they think and why they think that way. It is this interaction and tension that offers benefit over other methods, making it possible for a level of consensus to be reached amongst participants and for a better understanding of cybersecurity practices and capacities to be obtained (Kitzinger 1995b; GCSCC 2019) .

In addition, an input template analysis was used to capture the maturity level indicators and challenges for each dimensions of CCMM. These indicators of maturity levels have been validated using international cyber security indexes such as Global Cybersecurity Index developed by the International Telecommunication Union (ITU). The motivations of using the international indexes are to categorise the cybersecurity capacity requirements, as well as the opportunities for action in the country (Hohmann et al. 2017). In addition, it used in order to validate and verify the results. The outcomes of this step are employed with the objectives

from previous stage to support the next step (Decide). Observe and orient steps are used to identify requirements of AS-IS stage in IDEF0. Figure (6.6) shows how this step is established.

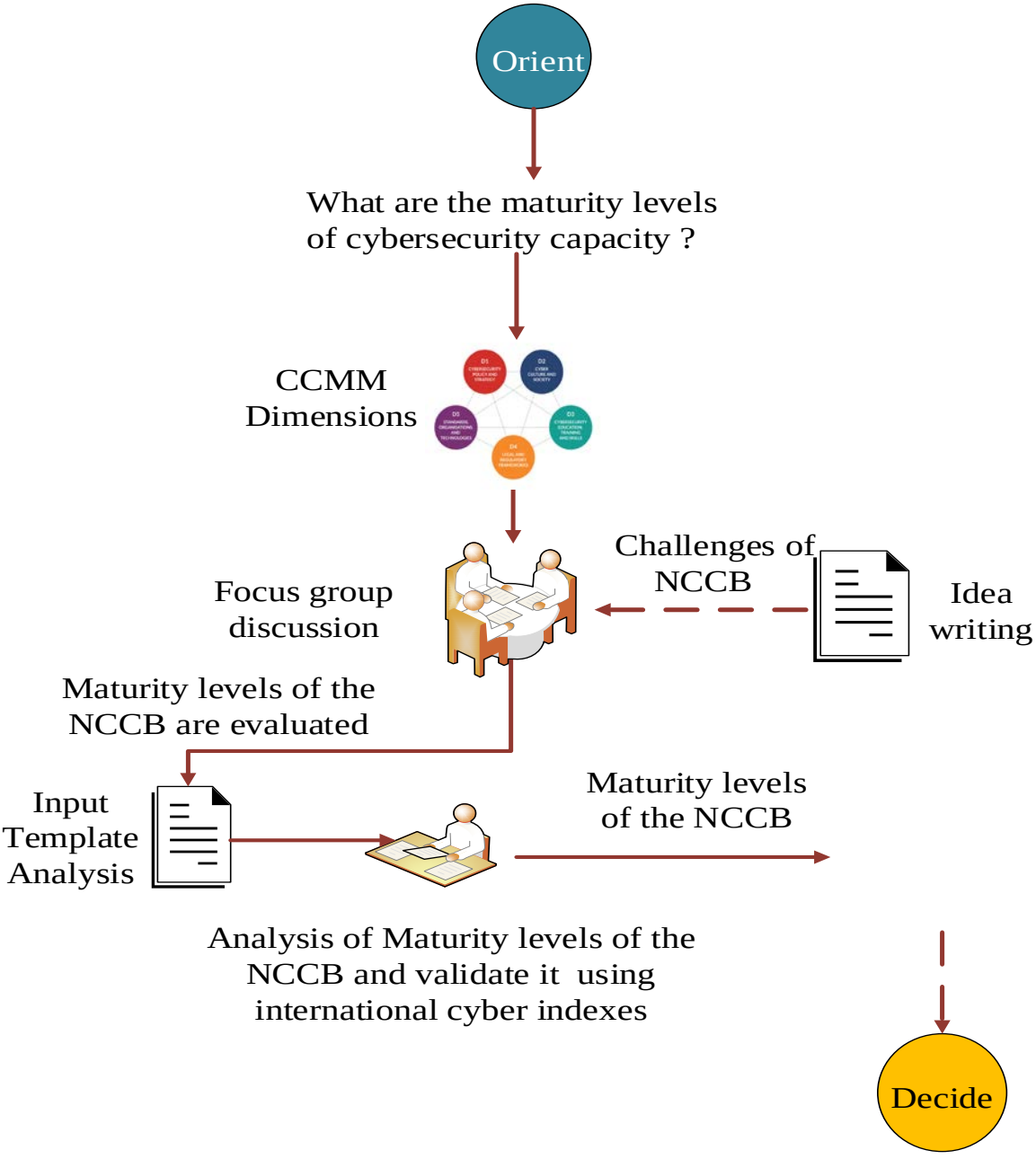



Figure 6.6 Adaptive Orientation phase of the NCCBF model development

### 6.3.3 Decision phase (to the NCCBF Artefact)

In this phase, the OODA Decision phase to building the NCCBF artefact, the functions, mechanisms and controls for the proposed framework were created for each dimension using template statements analysis. Figure (6.7) shows how this step is designed and conducted. This step address the following question, *"What can be developed to provide a National Cybersecurity Capacity Building Framework (NCCBF) for transitional state countries?"*

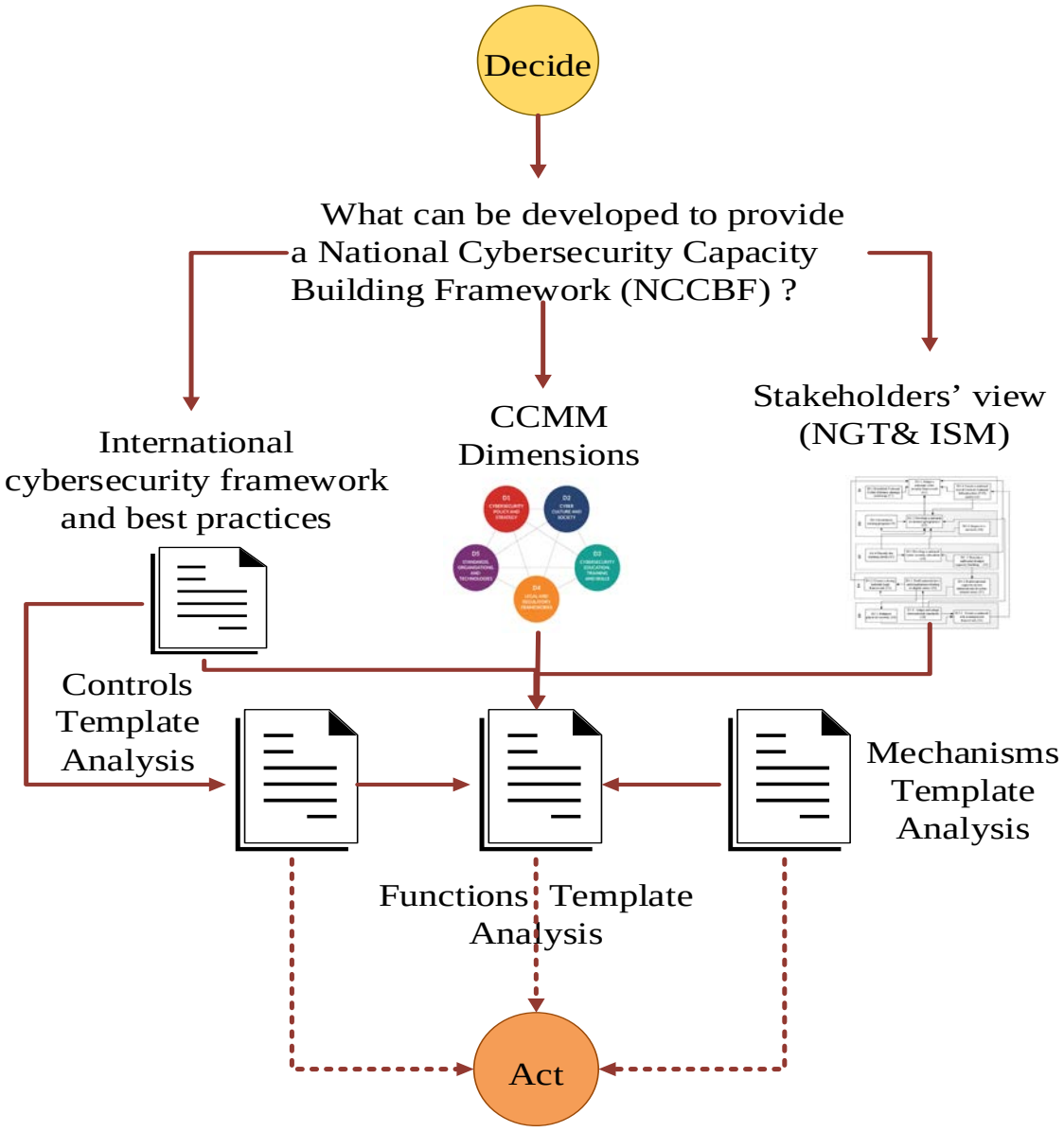



Figure 6.7 Adaptive Decision phase of the NCCBF model development

The function statements were created based on the stakeholders' view from within the case study country based on CCMM and the existing national cybersecurity frameworks. The mechanisms are the different types of resources; such as the cross-functional team, systems, and technology that used to support functions (activities) to achieve change. The controls are tools or checklists that ensure adherence to best practices such as the budget, knowledge, and regulations.

### 6.3.4 Action phase (to the NCCBF Artefact)

In this final phase of the OODA loop, the output template statements that created in **Section 3.5.4** were used to perform two major activities:

1) Find the gaps in the implementation process in each dimension, and
2) Measuring maturity levels improvement in each dimension.

This template has been created based on CCMM and other maturity models to check the improvement level for each dimension. Figure (6.8) shows how this step is conducted.

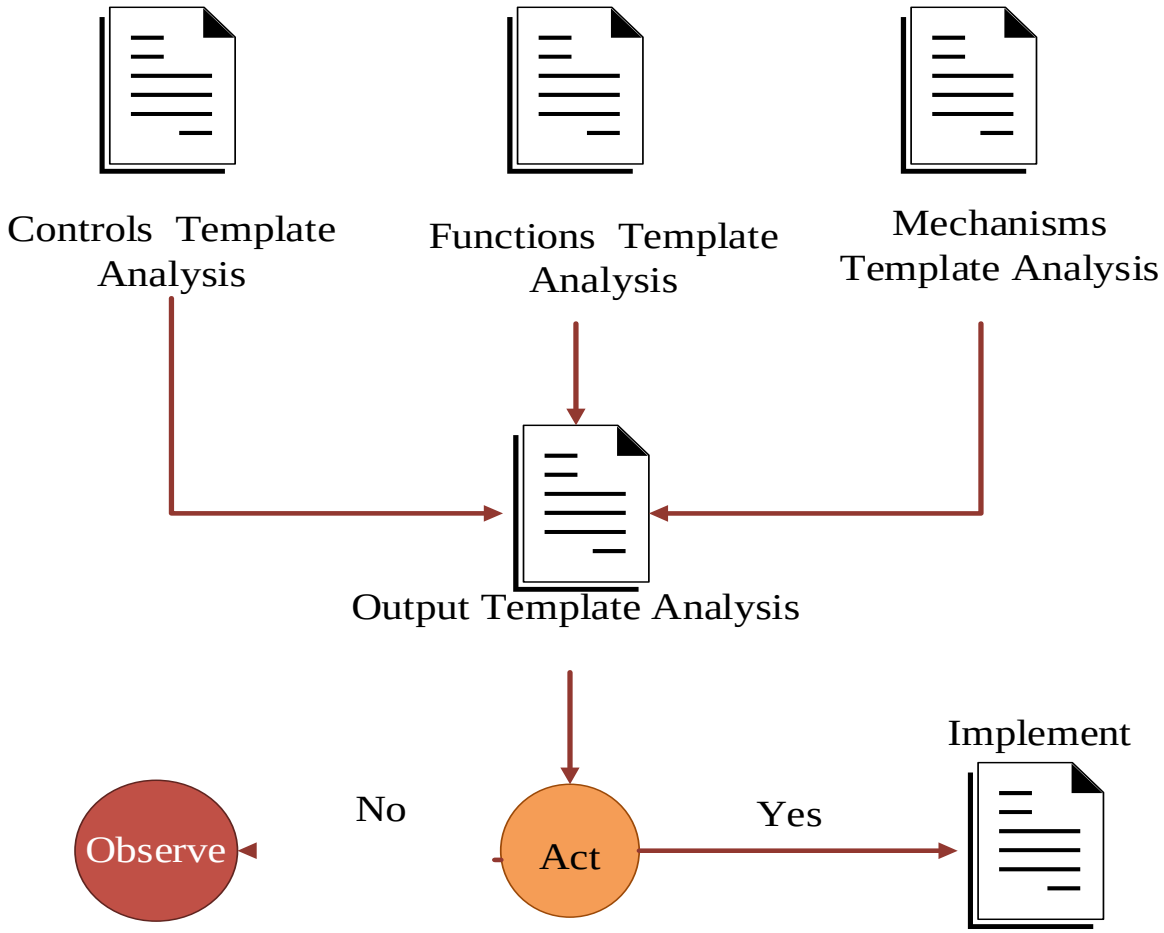



Figure 6.8 The Adaptive Action phase of the NCCBF model development

## 6.4 Further development of the National Cybersecurity Capacity Building Dimensions based on OODA'S Loop utilising the Spring Land Case Study

### 6.4.1 Dimension (D1): Build strategic capacity

According to the CCMM this dimension looks at the crucial steps required to implement and review national cybersecurity strategy capacity. The top level activity (D1) is represented using IDEF0 as shown in Figure (6.9).

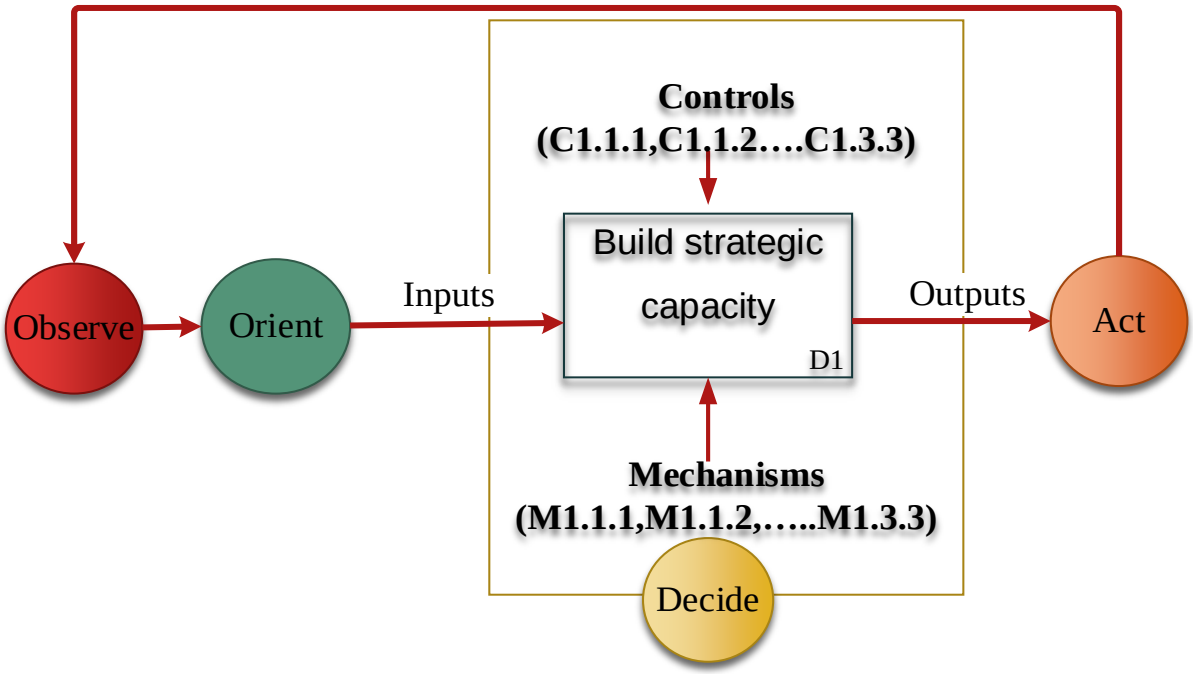



Figure 6.9 Top-level activity for D1

6.4.1.1 Oservervation phase for Dimension one (D1)

At this stage an input template analysis and IM techniques (Idea Writing (IW), Nominal Group Techniques (NGT) and Interpretive Structural Modelling (ISM)), were used to capture the challenges of NCB in the metaphorical Spring Land Case Study. The IW technique was employed to reveal the issues relating to a given trigger question, providing the participants with a forum to brainstorm and exchange ideas. The participants were divided randomly into three groups to discuss the question and to provide their views concerning the issues relating to cybersecurity in Spring Land. The trigger question employed was: *What are the current issues of cybersecurity capacity in Spring Land?*

After the session, the statements produced were numbered, organised and sorted into categories according to each of the CCMM dimensions. The ideas generated by the groups in response to the question are summarised in Table (6.1). In addition, a set of objectives was derived to support identified the key initiatives for the development of national cybersecurity capacity in the country using Nominal group technique (NGT) technique.

| Dimensions | Challenges and issues (Ben Naseir et al. 2019) |
|---|---|
| D1 | • D1-1. Lack of national cybersecurity strategy.<br>• D1-2. Lack of national risk management plan and threat of cyber space has not identified on the national or sectors level.<br>• D1-3. There is no national roadmap for Cyber Defence strategy.<br>• D1-4. Difficulties in implementing the cyber security strategy due to political issues and scarcity of resources for preparation of national cyber security blueprint (government funding and human resources).<br>• D1-5. Lack of public and private partnership. In addition, there are no government forums to share information.<br>• D1-6. There is no national crisis management protocol and Incident response plan for national critical infrastructure assets have not been prioritised.<br>• D1-7. There is no national cyber security framework to monitor the adoption of international cybersecurity standards in the government sectors. |

Table 6.1 Challenges of cybersecurity capacity of D1

The NGT was employed to generate, simplify, edit and obtain an initial rating for a set of objectives. At this stage, the participants were asked to select and vote for their top three objectives from the list for each dimension (1 = the least important, 3 = the most important). A total of 19 participants then voted on the objectives. A further outlying 7 of the participants failed to vote owing to security and sensitivity issues. After capture the most three objectives for this dimension, the Interpretive structural modelling (ISM) technique was applied. The ISM technique helped the participants to examine the inter-relationships between the elements gained through the NGT process and provided a structure for tackling its complexity (Checkland 1999; Trist 1981). In order to create a clear ISM, the objectives from the NGT stage were grouped according to similarities to facilitate the identification of the three most important objectives from each dimension. The three most important objectives for this dimension are organised using function template analysis (more details in **Section 6.3.1.3**).

6.4.1.2 Orientation phase for Dimension one (D1)

In this stage the maturity level of all factors of D1 using an the input template statement. Table (6.2) provides how the input template statement is used to capture the maturity level of certain factors related to this dimension. D1 refers to dimension one, D1.1 concerns the national cybersecurity strategy maturity level, D1-2 indicates the incident response capabilities maturity level, D1-3 refers to the critical national infrastructure (CNI) Protection maturity level and D1-4 indicates crisis management maturity level. Each factor, involves five stages of maturity (Start-Up (S-UP), Formative (F), Established (E), Strategic (S) and Dynamic (D). The lowest indicator implies a non-existent, or inadequate, level of capacity, and the highest indicates both a strategic approach, and ability to dynamically enhance environmental considerations, including operational, socio-technical, and political threats.

| Dimensions | Factors | Indicators | | | | |
|---|---|---|---|---|---|---|
| | | S-UP | F | E | S | D |
| D1 | D1.1 | | * | | | |
| | D1.2 | | | * | | |
| | D1.3 | * | | | | |
| | D1.4 | * | | | | |

Table 6.2 Maturity levels Indicators for D1

The outcomes of this stage show that the maturity level of this dimension can be classified from start-up to strategic stages. Despite the fact that there is no national cybersecurity strategy, certain factors are considered to be in either a formative or established level. For instance, the organisation leading the cybersecurity programme and national CERT in Spring

Land has been identified. Furthermore, one of the most significant findings to emerge from this assessment is that Spring Land does not have a blueprint for a cyber defence strategy in place as result of political fragmentation. Consequently, without any existing cyber defence strategy, Spring Land faces a big challenge in dealing with cyber threats from other states, and therefore the threat posed by terrorism, extremism and instability increases.This means that raising the level of maturity of these factors helps to fill certain gaps in the Spring Land's cybersecurity ecosystem.

6.4.1.3 Decision phase for dimension one (D1)

In this section the statement template were used to capture the functions, mechanisms and controls to improve the CCB in this dimension were chosen based on the existing national cybersecurity frameworks and the stakeholders' view from within the case study country in as discribed in **Section 4.3.3** (Ben Naseir et al. 2019). In this dimension the top three objectivies are as follows:

1. Adopt a national Cybersecurity framework and create collaborative model for include all stakeholders to write the national Cybersecurity strategy.

2. Establishment of a central committee for cybersecurity.

3. Create a national list of Critical National Infrastructure (CNI) assets and identify the risk priorities.

Based on the evaluation of the proposed framework in **Chapter 7,** these objectiove (functions) has been modifided and a function template was used to create these functions and establish the interaction between them statement is used as shown in Table (6.3).

The purpose of the NCS is to provide direction and framing for national policies and actions pertaining to cybersecurity over the medium-to-long (ENISA 2016; Bellasio et al. 2018; ITU 2018b). The NCS in the 5$^{th}$ Domain – Cyberspace is important because state interactions in cyberspace are characterised by uncertainty, rather than predictability of this era. To develop the NCS it is necessary to go through a number of mechanisms and controls that are described in the next section. Once developed the function will support other functions such as D1.2 and D1.3, because it will guide the preparation and enforcement of other functions. In

addition, it depends on national legal framework the outcome of dimension two in the NCCBF.

| Dimension ID | Functions ID and description (Activities ) | Interaction |
|---|---|---|
| D1. Build strategic capacity | D1.1 Develop NCS. | • Supports D1.2,D1.3<br>• Depends on D2 |
| | D1.2 Building a Risk management approach | • Supports D1.3<br>• Depends on D1.1 |
| | D1.3 Building a National Incident Response Capabilities | • Depends on D1.3, D2 |

Table 6.3: List of functions used in D1

Building a risk management approach helps to identify and prioritise the risks facing the Critical National (CI) assets and critical National Information infrastructure (CNI) (ENISA 2016; Bellasio et al. 2018; ITU 2018b). A different set of mechanisms and controls are used to develop a risk management approach and this is elaborated in the next section.

Building national incident response capabilities is another function used to build the CCB of the country. It allows government to identify national-level cyber incidents and coordinate a response to ensure that harm is contained, the attacker is no longer present, and the functionality and integrity of the network and system are restored (ENISA 2016; Bellasio et al. 2018; ITU 2018b).

To support these function or activities to achieve desired change a list of mechanisms and controls are created based on the existing literature and best practices. Table (6.4) shows how mechanisms and controls are defined and represents the justifications and rationale for the selected ones. For instance, to develop function (D1.1 Develop NCS), an establishment of a National Council for Cybersecurity with a clear mandate, appropriate statutory powers, and an organisational structure is required (M1.1.1). Organisational structure as described in **Section 2.8.2.1,** many countries around the world have established, or are looking to

establish, agencies or other administrative bodies to manage their cybersecurity strategy (Ciglic 2018; ITU 2018b). The rationale for creating the council is to perform a crucial function in coordinating across different organisations in the public and private sectors. Also, forming a strong leadership role at the highest level contributes to recognition of the NCS. To some extent, literature shows that, the national cybersecurity council will be expected to steer a complex environment that spans other government sectors, national legislatures, established regulatory authorities, civil society groups, public and private sector organisations, and international partners. It is also critical that the responsibilities of the national cybersecurity agency are distinct from those of other governmental groups involved in cybersecurity. In this research, based on the evaluation of the NCCBF, the "Organisational structure should include advisory committee and counter-terrorism committee and build capacity of these committees in field of cybersecurity in the country".

The roles and responsibilities can be defined using an assignment chart such as the RACI matrix that maps out every task, and assigns roles are Responsible for each action item, the personnel who are Accountable, and, who needs to be Consulted or Informed (CTO 2015). This matrix can be used with the Enterprise governance of IT, as defined through COBIT 5 (ISACA 2013), as a control tool (C1.1.1) to ensure adherence to best practice. After capturing the required functions, mechanisms and controls, we represent these activities using IDEF0.

| Mechanism ID | Rational | Control ID | Reference and Access |
|---|---|---|---|
| M1.1.1 Establish a national council | Performs a crucial function in coordinating across different organisations in the state. | C1.1.1, Regulatory framework ,assignment chart , Advisory group, counter-terrorism committee and EA governance | RACI matrix is open source.<br><br>COBIT 5 is not free, the proprietary rights are from ISACA, (www.isaca.org) |
| M1.1.2 Human Capital | To close the cybersecurity skills gap and to strengthening cybersecurity skills and competences in the state.<br><br>The dearth of cybersecurity professionals to address cyber risk, and a lack of education programs to train these professionals leads to a human capital crisis | C1.1.2 Cybersecurity Competency program | Cybersecurity Competency Model (NICE 2016). It is open source. |
| M1.1.3 Guiding principles | To guide the preparation and enforcement of cybersecurity | C1.1.3 International frameworks and national cybersecurity | ITU, ENISA, Microsoft and Commonwealth approach |

| | | | |
|---|---|---|---|
| | policies. | strategies | (Goodwin and Nicholas 2013; CTO 2015; ENISA 2016; ITU 2018b) Open source. |
| M1.2.1 Identify the Critical National (CI) assets and critical National Information infrastructure (CNI) | To develop measures and procedures for the protection of CNI and reduce the risk of cyberattacks. | C1.2.1 Good practices for the identification of CI sectors and CNI sectors | Checklist by Eric Luiijf and Marieke Klaver (Luiijf and Klaver 2019). Methodologies for the identification of Critical Information Infrastructure assets and services (Mattioli and Levy-Bencheton 2014) |
| M1.2.2 Risk assessment | To identify the threats to national security on cyberspace | C1.2.2 Risk assessment techniques (including threat assessment, vulnerability assessment and impact analysis). | Risk Management Framework from NIST<br><br>https://csrc.nist.gov/projects/risk-management/risk-management-framework-(RMF)-Overview |
| M1.2.3 Develop Military | To develop capabilities in both the cybersecurity and cyber defence | C1.2.3 Cyber defence doctrine | • Ormrod, D. & A. Turnbull. 2016. The cyber conceptual |

| | | | |
|---|---|---|---|
| capabilities | areas. | framework | framework for developing military doctrine. Defence studies. Vol 16(3) pp. 270-298.<br><br>• Klimberg, Alexander (Ed). 2012. National Cyber Security Framework Manual Tallinn: NATO CCD COE Publication.<br><br>• Robinson, Neil, Agnieszka Walczak, Sophie-Charlotte Brune, Alain Esterle, Pablo Rodriguez. 2013. Stocktaking study of military cyber defence capabilities in the European Union (milCybeCAP): Unclassified Summary. Santa Monica, UK: RAND Corporation. |

| | | | |
|---|---|---|---|
| M1.3.1Establishment of a National CSIRT | To react to computer security incidents those are deemed to be of national importance. A National CSIRT can also provide the government with a conduit for coherent, consistent messaging on cyber security issues. | C1.3.1 The National CERT Structure<br><br>And identify relevant stakeholders and legal framework. | • OAS (Organization of American States). 2015. Best Practices for Establishing a National CSIRT. https://www.sites.oas.org/cyber/Documents/2016%20-%20Best%20Practices%20CSIRT.pdf<br><br>• National/governmental CERTs - ENISA's recommendations on baseline capabilities (https://www.enisa.europa.eu/publications/national-governmental-certs-enisas-recommendations-on-baseline-capabilities) |
| M1.3.2 Define, document and | To define the steps that a CSIRT will follow to effectively counter a | C1.3.2 Incident response framework | Computer Security<br><br>Incident Handling Guide from |

| | | | |
|---|---|---|---|
| operate incident response processes and Maintain Trust Relationships. | cybersecurity incident. | | NIST, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf |
| M1.3.3Technical Excellence | To ensure that incidents are handled and organised effectively | C1.3.3 Cybersecurity Workforce Framework | Cybersecurity Competency Model (NICE 2016). It is open source. |

Table 6.4:list of mechanisms and controls for D1

After capturing the required functions, mechanisms and controls, we represent these activities using IDEF0 (see Figure 6.10).

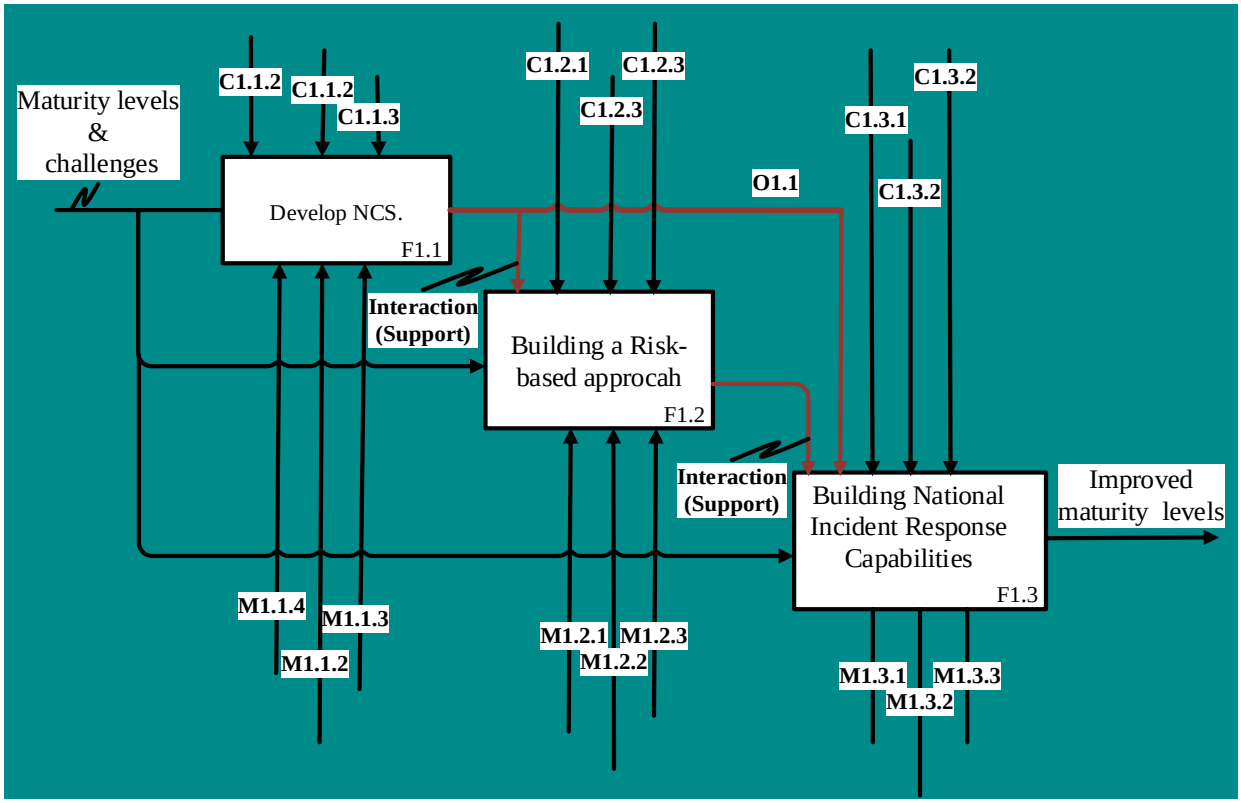



Figure 6.10: An IDEF0 representation for Dimension 1

6.4.1.4 Action phase for dimension one (D1)

As mentioned in **Section 6.3.4,** the output template statements were used to perform two major activities: 1) Find the gaps in the implementation process in each dimension, and 2) Measuring maturity levels improvement in each dimension. In this dimension, first of all the mechanisms and controls are cross-examined to the fullest for a cost-effective and find the gaps in the implementation process in this dimension. The literature of existing framework and best practices were used to review them. After reviewing the selected function, mechanisms and controls, the template analysis is used for measuring maturity levels improvement in this dimension. Due to time limitation during conducting of this study, this phase has not applied on real case.

These steps were used for the all dimensions of the proposed framework (NCCBF) and were not discussed in details. The next section provides a snapshot of the list of functions that created for other dimensions. The details of list of mechanisms and controls for each dimension can be found in Appendix (4).

## 6.5 Development of the Other Dimensions of the National Cybersecurity Capacity Building (NCCBF)

In this section, a snapshot of decision phase for dimensions 2, 3, 4, and 5. The list of functions that created for theses dimensions are presented. The details of list of mechanisms and controls for each dimension can be found in Appendix (5). The results of observation and orientation phases are captured in discussed in **Chapter 4** and **Chapter 5** and will not discussed in this section.

### 6.5.1 Dimension (D2): Build Cyber culture and society capacity

This section presents the main functions, mechanisms and controls that needed to build cybersecurity culture capacity for countries in transitional phase. These functions, mechanisms and controls will serve as input to the successful crafting of building a cybersecurity culture capacity for the grass root users of cyberspace in transitional phase countries. In addition, these functions, mechanisms and controls are considered part of the objectives of this study and will guide the researcher by way of depicting main issues to look at in the research.

The functions have been chosen based on the most important objectives that were created by various stockholders during the contextualising and evaluation of the NCCB in Spring Land as discussed in **Chapter 4, Section 4.2.3**. The mechanisms are the different types of resources, such as the cross-functional team, systems, and technology that used to support functions (activities) to achieve change. The controls are tools or checklists that ensure adherence to best practices such as the budget, knowledge, and regulations. The top level activity (D2) is represented using in Figure (6.11).

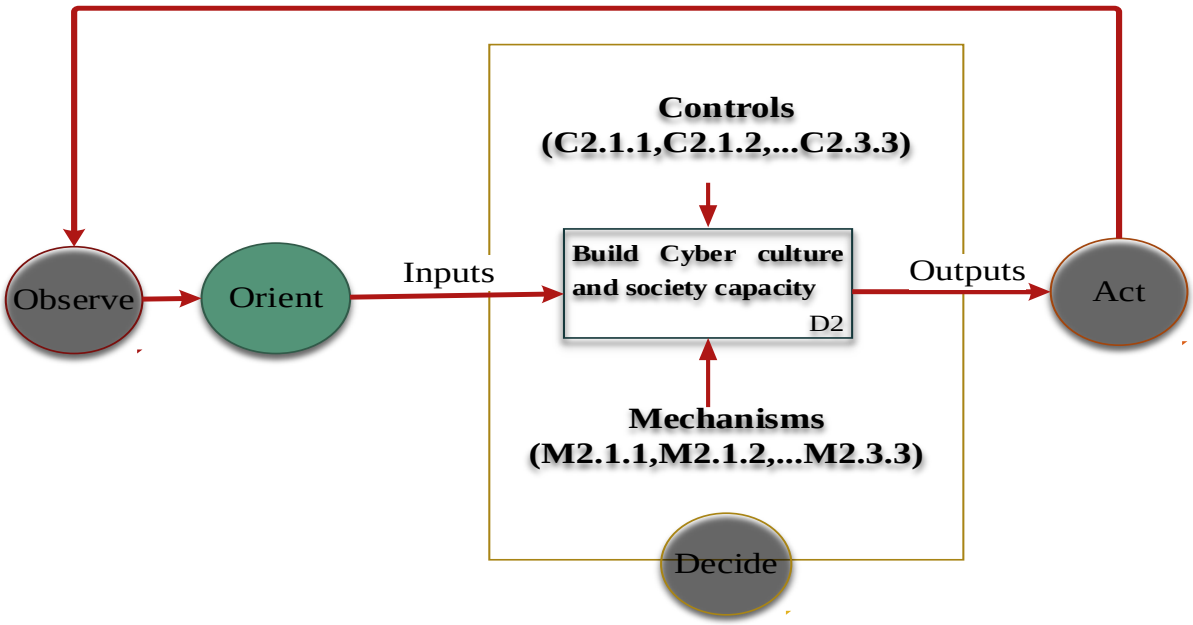



Figure 6.11: Top-level of D2

The list of functions for dimension two (D2) are captured using the function template analysis and presented in Table (6.5).

| Dimension ID | Functions ID and description (Activities ) | Interaction |
|---|---|---|
| D2. Build cyber cultural and society capacity | F2.1 Develop a national awareness program that is compatible with the current situation. | • Depends on F1.3,F2.2,F3.1,F3.3, and F5.1<br>• Supports F1.1 and F2.2 |
| | F2.2 Improve e-services, in order to promote the required level of trust. | • Depends on F2.1<br>• Supports F2.3 |
| | F2.3 Develop an evaluation criterion | • Depends F2.2 |

Table 6.5 : Functions list of dimension two (D2)

The list of Mechanisms and Controls for this dimension were captured using a template analysis and can be found in Appendix (5). After capturing the required functions,

mechanisms and controls, we represent these activities using IDEF0 as shown in Figure (6.12).

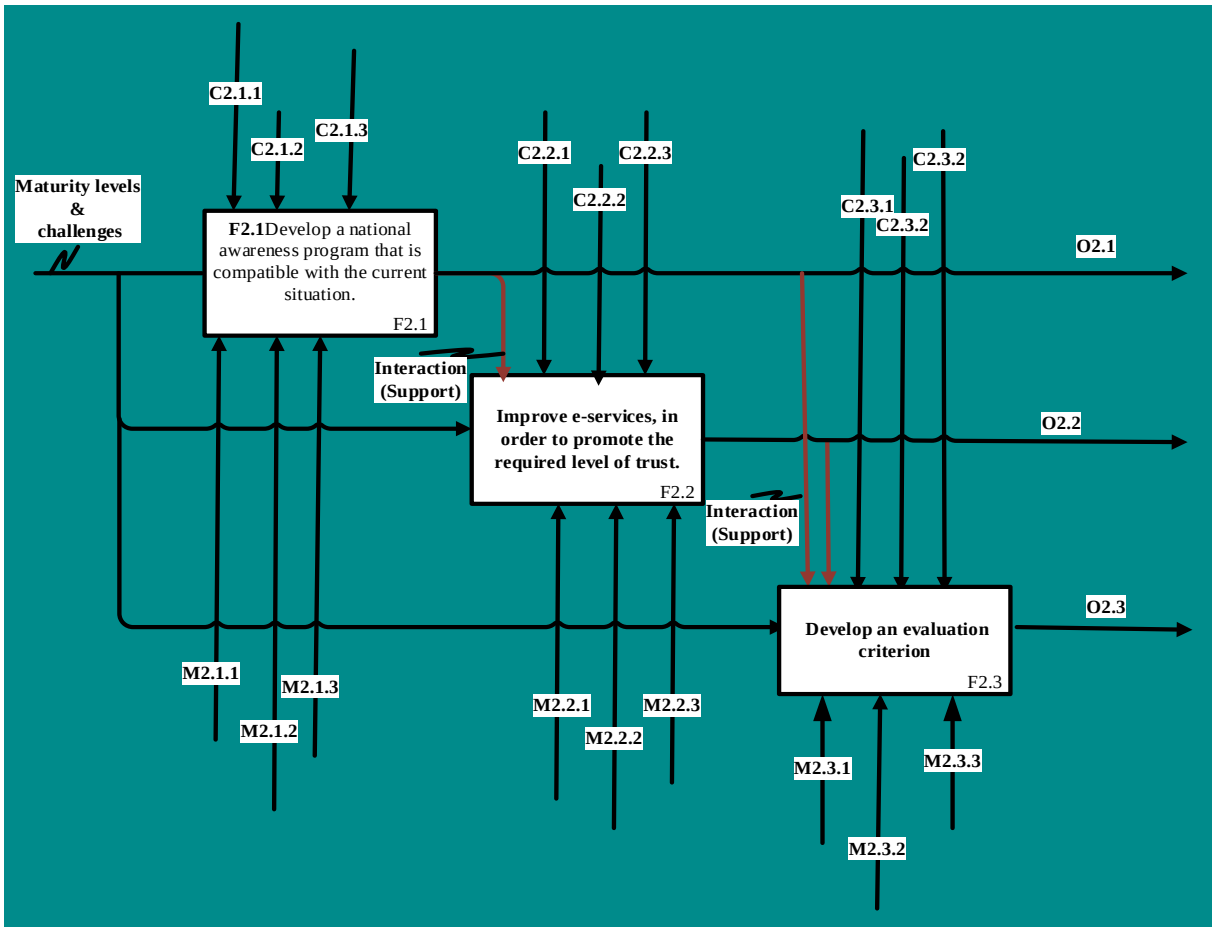



Figure 6.12 : An IDEF0 representation for Dimension 2

6.5.2 Dimension (D3): Build Cybersecurity Education, Training and skills

This dimension is used to deliver essential steps for cybersecurity education, training, and skills development. In this section, the main functions, mechanisms, and controls that needed to build cybersecurity Education, Training, and skills for countries in transitional phase are represented. These functions, mechanisms, and controls will serve as input to the successful crafting of building a cybersecurity skills capacity for the grass root users of cyberspace in transitional phase countries. In addition, these functions, mechanisms, and controls are considered part of the objectives of this study and will guide the researcher by way of depicting main issues to look at in the research. The top level activity (D3) is represented using in Figure (6.13).

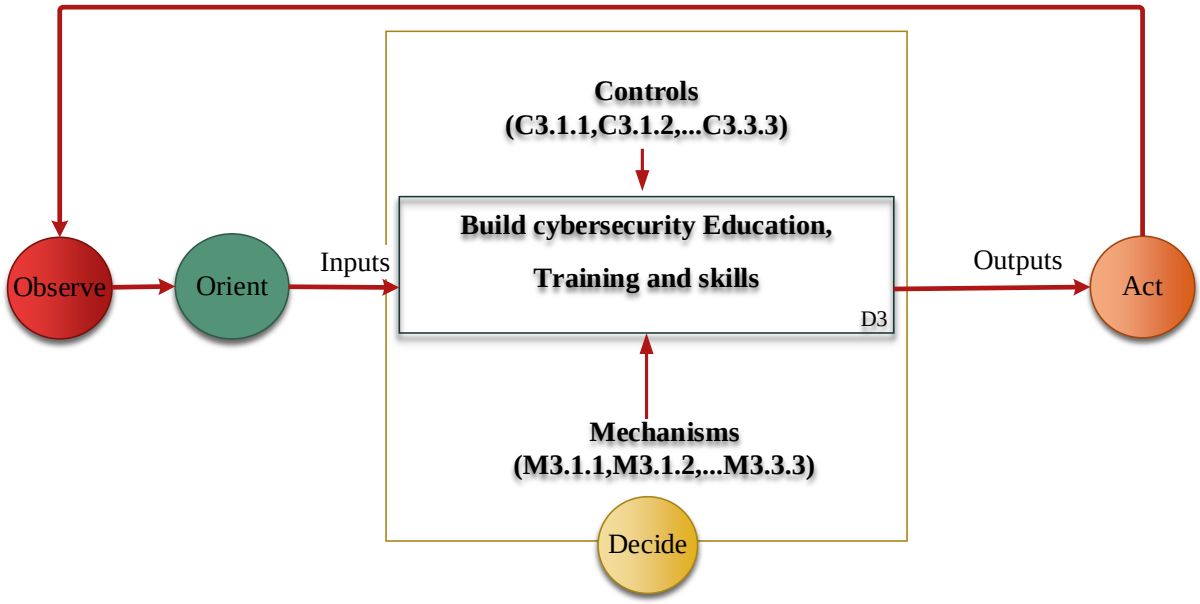



Figure 6.13 : The top level activity (D3)

The list of functions for dimension three (D3) are captured using the function template analysis and presented in Table 6.6.

| Dimension ID | Functions ID and description (Activities ) | Interaction |
|---|---|---|
| D3 Build cybersecurity Education, Training and skills | F3.1 Develop national cybersecurity education program. | • Depends on F3.2, and F3.3<br>• Supports F2.1 |
| | F3.2 Creating a certificate for national needs | • Depends on F1.1<br>• Supports F3.1and F4.3 |
| | F3.3 Defining tasks and required knowledge | • Supports F2.1and F3.1 |

Table 6.6 : Functions list of dimension three (D3)

The list of Mechanisms and Controls for this dimension were captured using a template analysis and can be found in Appendix (5). After capturing the required functions, mechanisms and controls, we represent these activities using IDEF0 as shown in Figure (6.14).

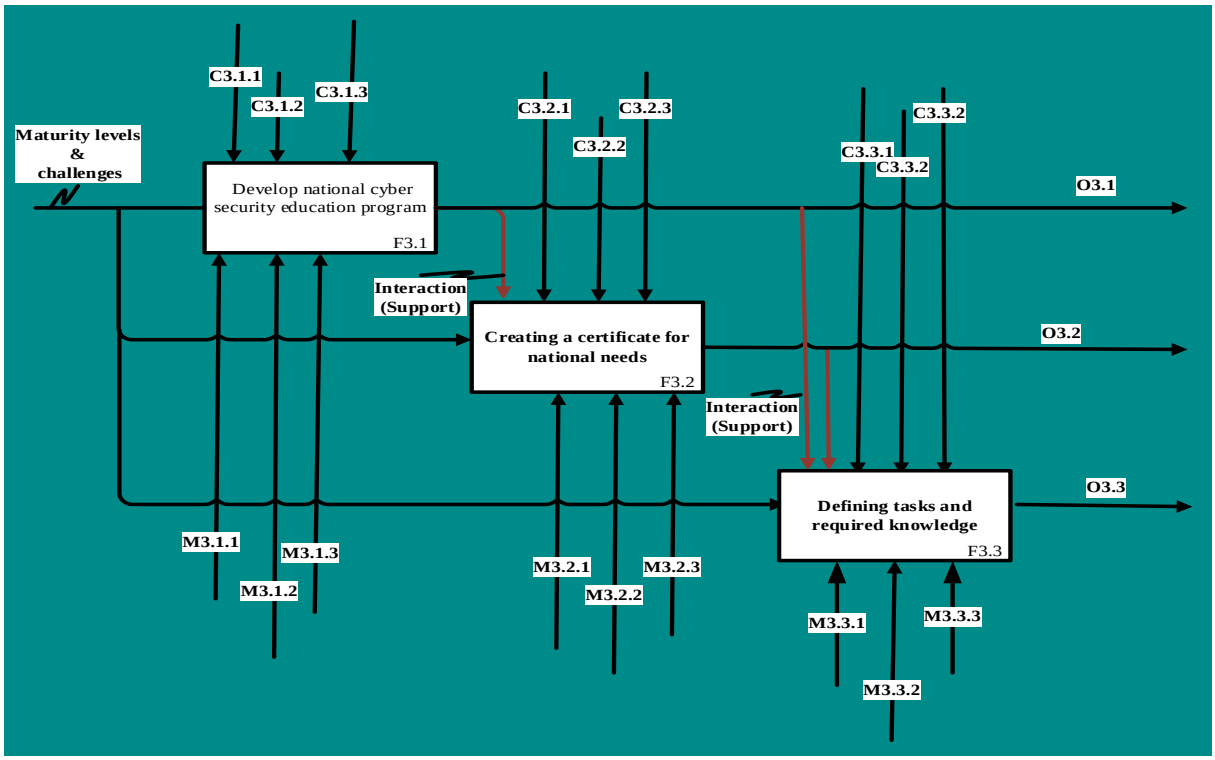



Figure 6.14 : An IDEF0 representation for Dimension 3

### 6.5.3 Dimension (D4): Build legal and regulations capacity

This dimension offers a different step required to form and update the national legislation and laws relating to cybersecurity. The top level activity (D4) is represented using IDEF0 in Figure (6.15).

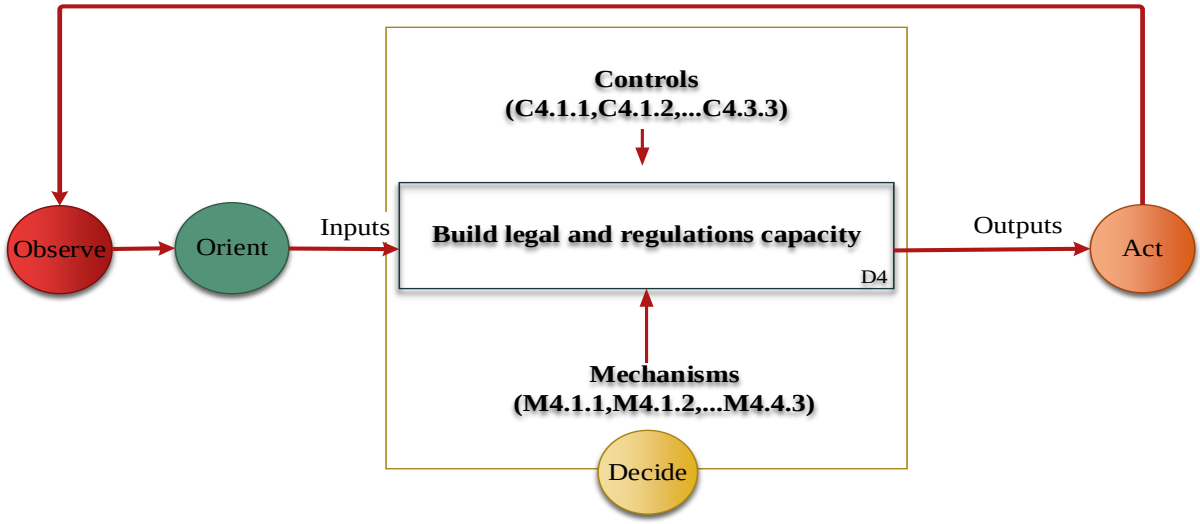



Figure 6.15 : the top level activity (D4)

The functions, mechanisms, and controls were captured using the template analysis that created in **Section 3.6.** The list of functions for this dimension is represented in Table (6.7).

| Dimension ID | Functions ID and description (Activities ) | Interaction |
|---|---|---|
| D4 Build legal and regulations capacity | F4.1 Development and adoption of relevant legislation supporting the policy that would enhance cybersecurity | • Depends on F4.2,F5.1 and F4.3<br>• Supports F1.1,F5.3 |
| | F4.2 Develop Criminal justice power | • Supports F1.1 and F4.1 |
| | F4.3 Establish effective informal cooperation mechanisms. | • Depends on F3.2, and F3.3<br>• Supports F2.1 |

Table 6.7 : Functions list of dimension four (D4)

The list of Mechanisms and Controls for this dimension can be found in Appendix (4). After capturing the required functions, mechanisms and controls, we represent these activities using IDEF0 as shown in Figure (6.16).

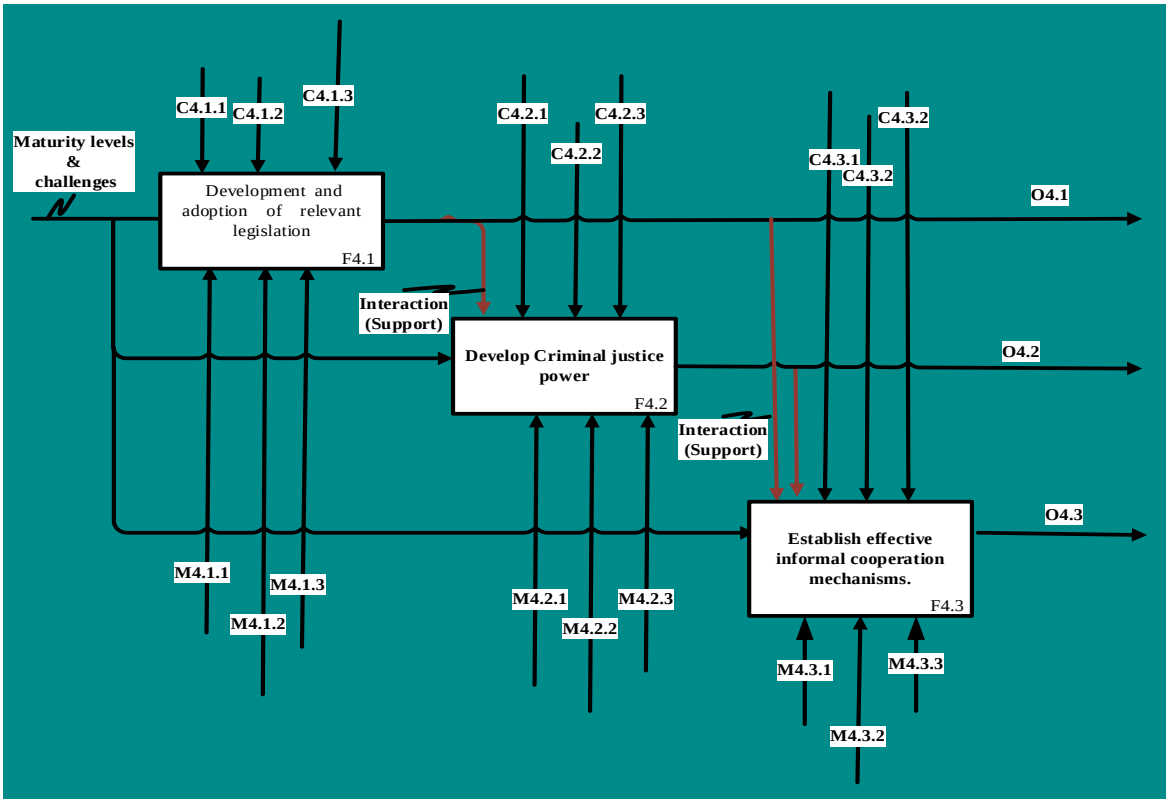



Figure 6.16 : An IDEF0 representation for Dimension 4

### 6.5.4 Dimension (D5): Build technical capacity

This dimension discusses the CCB steps that a country or organisation can implement to employ cybersecurity standards, and at least minimal adequate practices. The top level of this dimension is represented in Figure (6.17).

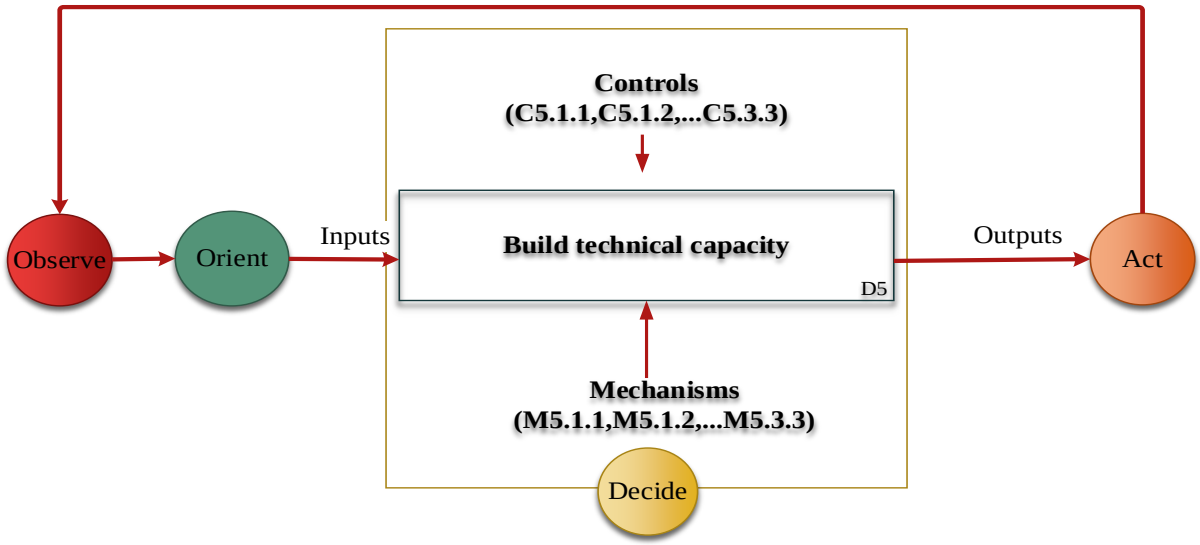



Figure 6.17 : the top level for Dimension 5

The list of functions that used in this dimension is described in Table (6.8).

| Dimension ID | Functions ID and description (Activities ) | Interaction |
|---|---|---|
| D5 Build technical capacity | F5.1 All stakeholders to adapt and adopt international standards. | • Supports F2.2,F4.1 and F5.2 |
| | F5.2 Build national resilience plan | • Depends on F5.1, and F5.2<br>• Supports F1.3 |
| | F5.3 Enhance physical security | • Depends on F4.1<br>• Supports F5.2 |

Table 6.8 : Functions list of dimension five (D5)

The list of Mechanisms and Controls for dimension five can be found in Appendix (5). The required functions, mechanisms and controls are represented using an IDEF0 modelling function as shown in Figure (6.18).

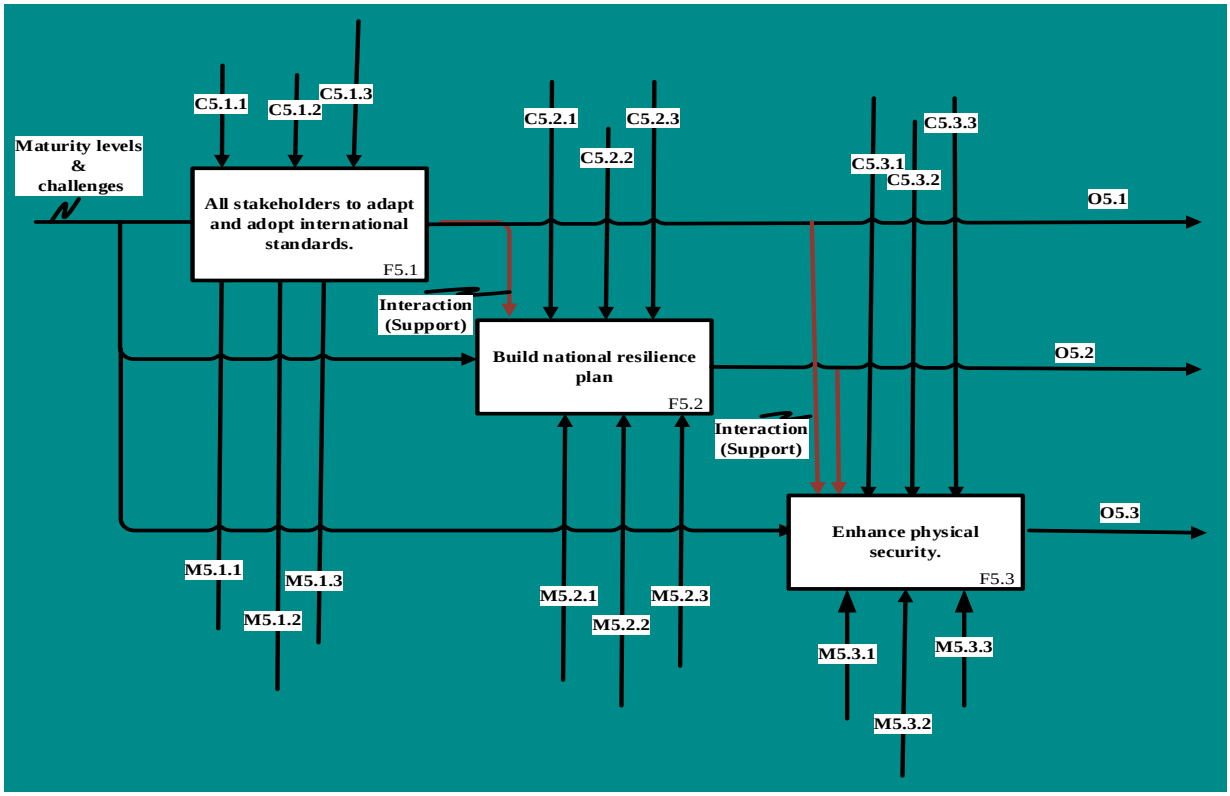



Figure 6.18: An IDEF0 representation for Dimension 5

After capture, all functions required for each dimension, the overall framework is represented in Figure (6.19) below.

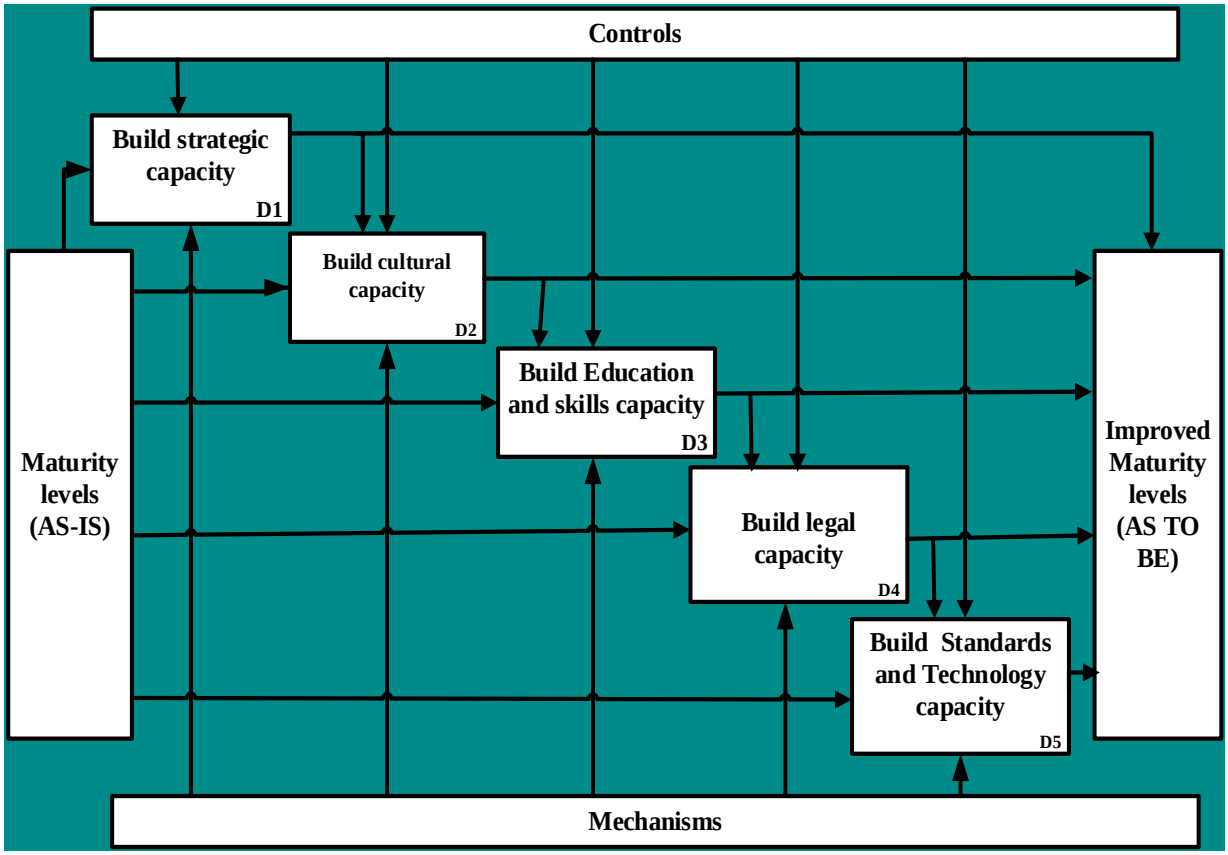



Figure 6.19 : The NCCBF Activities

## 6.6 Chapter Summary

The proposed National Cybersecurity Capacity Building Framework (NCCBF) for countries in a transitional phase addresses many issues, which were found lacking or not effectively implemented in their 5th Domain –Cyberspace. The Case Study amplified the concerns and issues of NCB within countries in a transitional phase. The design and development of the NCCBF artefact provides guidance and activities towards developing and building national cybersecurity capacity in several cybersecurity dimensions. The original dimensions are based on the Cybersecurity Capacity Maturity Model for Nations (CCMM), developed by Global Cybersecurity Capacity Centre in the University of Oxford through collaboration with international stakeholders. This CCMM model has been selected, because it successfully demonstrates the global effects of a Cybersecurity Capacity Building (CCB) solution - inclusive of all areas cybersecurity for building a robust cybersecurity platform does provide better GRC for the 5th Domain and effective security posture for a State's policies and

institutions. This model is offering a comprehensive analysis of CCB through five different dimensions: Cybersecurity Policy and Strategy; Cyber Culture and Society; Cybersecurity Education, Training, and Skills; Legal and Regulatory Frameworks; and Standards, Organisations, and Technologies.

The proposed framework's key functions, mechanisms and controls for each dimension and their rationality were identified and guided by IDEF0 modelling function. The framework also rely on existing national cybersecurity frameworks and best practices that countries in a transitional phase can adapt for building effective cybersecurity capacity. Moreover, the Hypothesis articulated and verified the interaction between all required activities to build cybersecurity capacities, which were, demonstrated when the NCCBF adapted the Observe, Orient, Decide and Act (OODA) model. For transitional States, the NCCBF will help countries to formulate and build their cybersecurity capacity in constantly changing environments.

The next chapter present focuses on the purpose and objectives of the evaluation of the proposed framework (NCCBF). In addition, provides the key findings from the evaluation and summarises the key performance and acceptance criteria of the proposed framework.

# 7. CHAPTER 7: EVALUATION OF THE FRAMEWORK

This chapter focuses on the evaluation of the proposed framework and the resolution of the Research Questions and its objectives. Can a collaborative research study bridge this gap? Will building capability to a transitional States be grounded in conducting, evaluating, and establishing resilience around a reliable National Cybersecurity Capacity Building Framework (NCCBF)? In answering the Hypothesis that, *there is a demonstrable gap (an extensive and vibrant chasm!) between the assurance of a stable, self-assured State that adheres to ISO Standards, Policies, Procedures and Good Practice, underpinned by security technologies, training and skills as opposed by States in a transitional phase that exhibit little Governance, Risk Management and Compliance of their 5th Domain -Cyberspace*. This chapter is proposed to achieve Objective 4 and Objective 5 of this thesis.

- Objective 4 – (S) To develop the NCCBF framework. (M) The NCCBF will be manged and guided by modelling functions techniques. (A) The framework will be attained through acceptance of NCCBF in the Spring Land National Defence. (R) Realistically NCCBF will be developed for National Security. (T) This will be ready by 2019.
- Objective 5 - (S) To evaluate the NCCBF for countries in a transitional stage. (M) The NCCBF will be evaluated against a set of criteria (Completeness, Correctness, Acceptability and the Overall Evaluation of the framework. (A) The NCCBF will be evaluated by conducting a focus group with experts from different countries including experts from countries that in transitional phase. (R) Realistically an enhanced NCCBF for countries in transitional stage will be developed. (T) The evaluation will be completed by 2020.

This chapter will demonstrate that Collaborative research has been able to bridge the gap with the proposed NCCB framework where our evaluation using various user experience and HCI techniques has been conducted and observations drawn. Focus group of subject matter experts from different countries including those from countries that are in a transitional phase was

conducted to ask and refine a set of requirements and questions which were developed to gather participants' views on the framework.

Given the design science method framework adopted in this thesis, the artefact developed in previous **Chapter 6** clearly closed the SMART milestones for Objective 4 in realistically delivering a timely framework and with the results presented at the 22nd International Conference on Enterprise Information Systems (Ben Naseir et al. 2020).

## 7.1 **Introduction**

This evaluation was developed to assess the proposed NCCBF framework. The validation and evaluation process according to Straub (1989)and Sperber (2004) are crucial to research. Kitchenham (1996), classified the evaluation activity into three main types objective, subjective and hybrid evaluations. In an objective evaluation, the focus is on identifying the benefits of the proposed design by evaluating its effects quantitatively, such as a reduction in time or a change in cost figures. In the subjective activity involves qualitatively evaluating the suitability of the method in terms of meeting the organisation's requirements. The hybrid type is a mixture of objective and subjective assessments.

In addition, Kitchenham (1996) had proposed another classification focuses on the three methods applied to evaluate an artefact. These methods are formal experiment, case study and survey method. In a formal experiment, the data can be collected statistically by involving participants in accomplishment the task. A case study is the second approach, can be conducted based on the standards and procedures of a similar project. This thesis utilises a case study evaluation method using focus group approach, as discussed in Section 7.2. The survey method the evaluation can be done through collecting data statistically from other associations or the contexts in which the project is applied.

## 7.2. Research Strategy

The plan of actions designed to achieve the research goal are called research strategy. The research strategy used for evaluating the proposed framework (NCCBF) is a focus group method following the University's ethics procedures. The motivation for choosing as research strategy was to obtain a broad set of expert opinions in the 5th domain. In addition, focus

group method offers a richer set of data compared to other qualitative approaches (Kitzinger 1995a). An introduction was given to participants highlighting some information about the framework and the purpose of this evaluation. The participants were asked to complete a participant agreement form before the commencement of the discussion. Furthermore, the researcher also prepared a form to profile the characteristics of each participant, such as their roles in their organisation or country and their years of experience. Related information is demonstrated in Section 7.3.

### 7.2.1 Participants' profile

Cybersecurity capacity building framework recommends the participation of different stockholders in building of state capacity in cyberspace. Cybersecurity capacity building requires a horizontal approach across different development policy fields, focusing on improving governance, protecting infrastructure, endorsing the rule of law and providing training and educations (Muller 2015). Therefore, a total of 13 experts in the field the cybersecurity as described in Table 23, taking each actor from different countries including experts from countries that in transitional phase were recruited, during a workshop session by using the focus group technique.

The participants were selected due to their contributions in their decision-making in security development from areas such as Defence, e-services, Private Sector, Banking, Regulations of ICT sectors, National cybersecurity agencies, Technical Advisor and capacity Buildings, High Education, and Integrated Digital application. The participants were recruited through personal and professional networks and they were selected based on their availability and convenience to participate in the study.

Critical topics such as cybersecurity capacity, as defined in this research, can be seen as challenging to discuss conveniently in some countries and organisations due to its effect on the state secrets. Thus, recruiting participants required a trust relationship between the researcher and the participants to effectively evaluate the proposed framework and gain more information about the research problem.

The researcher had attended the ITU Interregional Workshop for Africa and Arab regions on "National Cybersecurity Strategies", Tunis - Tunisia, 10-13 Dec. 2019 were the researcher evaluates the NCCBF (ITU 2019).

The rational of choosing this workshop for **Objective 5** was its convenience in the research timescale and the abundance of willing participants. First, the respectful ITU Interregional Workshop was designed to address mid to senior level management from policy makers, regulators, corporate executives and managers undertaking cybersecurity responsibilities in their respective organisations and countries. Second, the senior level management are specifically cybersecurity officials in charge of drafting ICT national policies and strategies (including from the legislative perspective) as well as the representative of the entities in charge of implementation of such policies, legal frameworks and regulations. Third, the workshop had provided many lessons learnt from different countries including countries in transitional phase. Fourth, the workshop had offered many activities to participants to gain more knowledge about national cybersecurity strategies and sharing experiences with other participants from other countries. These activities such as, hands - on exercise, National Cybersecurity Strategy Good practise and Lessons learnt from cybersecurity using the CCMM capacity maturity assessments, which applied in this study. Finally, it offers much savings in time and cost, and ensures a close contact and coordination with potential participants. Table (26) provides participants details in the evaluation study.

| No | Gender | Country | Category of Organisation | Sector | Job Description | Years of Experience | Response |
|---|---|---|---|---|---|---|---|
| **P1** | Male | Tunisia | Private | Cybersecurity | CEO | 7 years | Yes |
| **P2** | Male | Gambia | Public | Regulator (ICT, Multisector) | Head of IT and Regulations | 7 years | Yes |
| **P3** | Female | Palestine | Public | E- government | Director of Integrated applications | 9 years | Yes |
| **P4** | Female | Tunisia | Public | High Education | Teaching engineer | 25 years | Yes |
| **P5** | Female | Tunisia | Public | Finance | Technical Advisor and capacity Buildings | 10 years | Yes |
| **P6** | Male | Burkina Faso | Public | ICT sector | Auditing | 2 years | Yes |
| **P7** | Female | Somalia | Public | Government | Telecom Engineer | 1 year | Yes |
| **P8** | Male | Mauritania | Public | Cybersecurity | Head of IT security division | 12 years | Yes |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **P9** | Female | Syria | Public | Government | General manager | 7 years | Yes |
| **P10** | Female | Jordan | Public | Finance | Cybersecurity specialist | 3 years | Yes |
| **P11** | Male | Libya | Public | National cybersecurity authority | Director of planning and projects | 1 year | Yes |
| **P12** | Male | Tunisia | Public | National cybersecurity agency | CEO | 6 years | Yes |
| **P13** | Male | Oman | Public | Technology | Consultant | 10 | yes |

Table 7.1: Participants details in the evaluation study

## 7.3 Purpose and Objectives of the Evaluation

The main purpose of this evaluation is to validate each of the following: the framework, its main dimensions, functions, mechanisms and controls. At the time of the development of this evaluation, the aim was to meet the following objectives:

1. Completeness: the aim of this objective is to evaluate the level of completeness and self-explanation of the dimensions of the NCCBF and their descriptions. Thus, attention is paid to ensuring the completeness of the proposed functions, mechanisms and controls in terms of achieving the main goal of the NCCBF.

2. Correctness: this objective is aimed to find out which functions, mechanisms and controls in the proposed framework are unclear and whether need to be changed (i.e. amendment/addition/removal).

3. Acceptability: The focus here is on measuring the extent to which practitioners can benefit from the proposed framework in their organisation or country.

4. The Overall Evaluation of the framework including:

- Inclusive: this aimed to find out if the proposed framework involves as many stakeholders as possible or not.

- Coherent: this aimed to find out if the proposed framework recognises current International Standards, Protocols and Interoperability.

- Multi-Dimensional: this aimed to find out if the proposed framework includes Domestic and International Tools.

- Risk Based: this aimed to find out if the proposed mitigation functions, mechanisms and controls in accordance with the level of risk.

## 7.4 Sessions' Plan

The evaluation study of the NCCBF involves one meeting and two sessions: inductions session and evaluation session. The first session had taken approximately 30 minutes and the evaluation

had taken approximately 90 minutes with a break of 30 minutes in between. Figure 40 illustrates the protocol of these sessions.

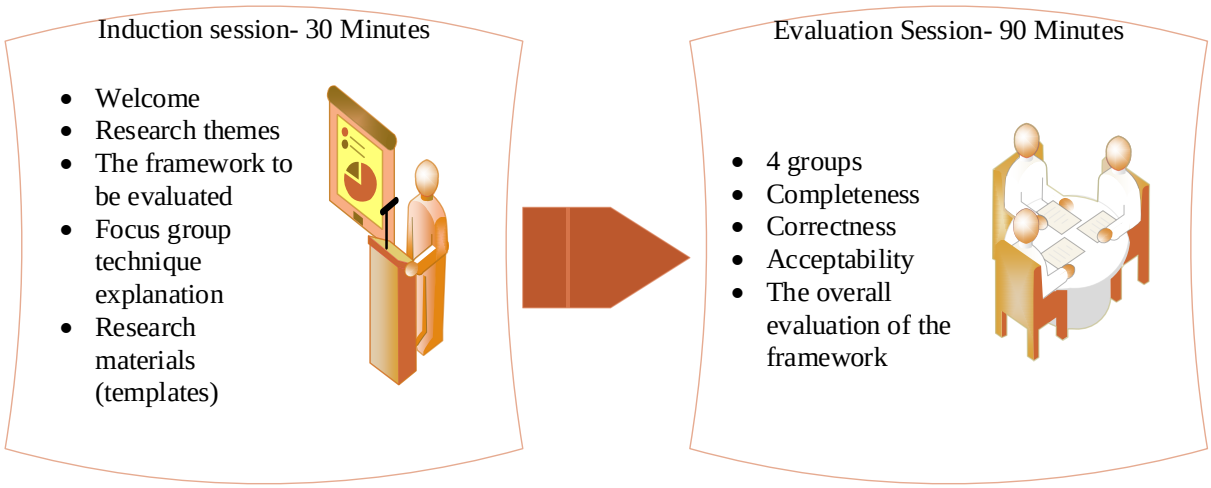



Figure 7.1 : PROTOCOL FOR EVALUATION SESSIONS

For each session, there will be a set of activities to be carried out in order, and questions to be discussed and answered, as follows:

1. **Induction session:** In this session, the participants were first welcomed. Using the MS PowerPoint the researcher then presented:

- The themes of research; in order to ensure that practitioners had the required level of understanding of the materials and documents that were given to each one. These materials including research overview, which contained Cybersecurity Capacity Maturity Model for Nations (CCMM) and the IDEF0 modelling language.

- The framework to be evaluated, the experts were given a brief presentation about of the NCCBF; In addition, plain text versions of the framework description were given with a set of questions used for the evaluations.

- Outlying the way by which this focus group research was to be conducted;

- The way the research materials (templates) are used for answers and comments. Experts were given a form with two questions about the completeness, four questions about the correctness, and two questions about the acceptability of the

framework. In addition, there was one question to evaluate the NCCBF based on a set of requirements was given to them. These questions are presented in Table 27.

| Activities | Questions | Notes |
|---|---|---|
| Completeness | • Which factors, mechanisms and controls are missing in this framework?<br>• Which factors, mechanisms and controls in this framework do you consider redundant? | |
| Correctness | • Which factors, mechanisms and controls are unclear to you?<br>• Which ambiguities are currently in this framework?<br>• What changes (i.e. amendment/addition/removal) to the artefacts do you suggest (labels, names, orders? Why? | |
| Acceptability | • Would you find it useful to use this framework to build a cybersecurity capacity for your organisation or country?<br>• Would you actually use this model? If not, what has to be changed? | |
| The Overall Evaluation of the framework | • To what extent do you think the framework is: (Please specify why, or why not using the sheet provided) :-<br>▪ Inclusive: Involves as many Stakeholders as possible.<br>▪ Coherent : Recognizes Current International Standards, Protocols and Interoperability<br>▪ Multi-Dimensional : Includes Domestic and International Tools<br>▪ Risk Based: Mitigation factors, mechanisms and controls in Accordance with the level of risk. | |

Table 7.2 : the Evaluation Questions

**2. Evaluation Session:** After the induction session, the experts were asked to form groups of 2 or 3 persons, resulting in 4 groups. The purpose of this session was to determine and examine how well the NCCBF artefact has addressed the practical problems explicated. The list of requirements and their definitions, against which the artefact was evaluated, have been presented in Section 7.4. The participants were asked

to write down their comments on the overall contribution of the artefact. These comments were openly discussed between the groups in order to come up with new ideas and recommendations for improving the artefact. The key finding from this session are discussed in following section.

## 7.5 Key findings from the Evaluation

The data obtained from the evaluation session were analysed qualitatively through content analysis. The researcher started by selecting appropriate texts from the templates of the evaluation session, analysing the texts, verifying their relation to the requirements categories, and finally presenting them as suggestions of change and improvement based on objectives of the evaluation discussed in Section 8.3 . These results are presented below in Table (7.3).

| Activities | Description | Number of Resp's | Related Dimension/ Phase |
|---|---|---|---|
| Completeness | Finical resources are missing in D1, it must be mentioned clearly and how to get the funding? | 8 | D1 |
| | Communication channel is missing | 7 | D1,D3,D4 |
| | Monitoring reporting mechanism is missing in D4 | 4 | D4 |
| | Legal framework should control D1 is missing | 13 | D1 |
| | Cooperation in case of instability and during the crisis, also think about actors outside the country that might support the state (good international cooperation). | 9 | D1,D4,D5 |
| | Performance measurement is messing and measuring capabilities after selecting functions, mechanisms and controls | 13 | All dimensions |
| | Evaluating the internal and external environment landscape in the AS-IS step is not enough. | 13 | All dimensions |
| Correctness | Add continues review of the model auditing. | 6 | D4 |
| | Create coordinated mechanisms with regional and international partners during crisis. | 13 | D1,D4,D5 |
| | Use risk management instated risk based approach in D1 and mirage M1.1.2 with M1.1.1. | 13 | D1 |
| | Add regional agreement mechanism. | 13 | D4 |
| | Add physical security policies in D5 and regional cooperation's. | 3 | D5 |
| | Add Big data sharing mechanisms (Regional and international) to D4. | 5 | D4 |

| | | | |
|---|---|---|---|
| | Change cybersecurity awareness-raising campaigns to cybersecurity awareness-raising program (M2.1.2). | 5 | D2 |
| | "Use a probabilistic graphical model to evaluate this framework such as, that Bayesian networks". | 1 | All dimensions |
| | "Use Performance measurement such as (KPI, Balanced Scorecard (BSC)) or other capabilities measuring frameworks". | 13 | Action phase |
| | "Organisational structure should include advisory committee and counter-terrorism committee and build capacity of these committees in field of cybersecurity in the country". | 13 | D1 |
| | "Use the development of the NCS as function not as a mechanism and swap it with "Establish a National Council". | 13 | D1 |
| | "Consider other methods to evaluate the internal and external landscape such as SWOT and PESTEL approaches". | 13 | Observation phase |
| Acceptability | "Yes it is useful and acceptable" | 10 | All dimensions |
| | "We liked how the capacity building in educations and private sectors has been defined and developed" | 2 | D2,D3 |
| The Overall Evaluation of the framework | All participants confirmed that the framework is inclusive, Coherent, multi-dimensional and risk based. | 13 | All dimensions |
| | "In our opinion this framework is Inclusive, Coherent, Multi-Dimensional and Risk Based because it based on a well know and internationally acceptable model (CCMM)". | 4 | All dimensions |

Table 7.3 : Key findings from the Evaluation

As presented in Table (7.3), some activities were missing. For instance, all of the experts mentioned that in the AS-IS step we should consider other methods to evaluate the internal and external landscape such as SWOT and PESTEL approaches. Also, eight of the experts clearly confirmed that the financial resources and how to obtain the funding are missing in the NCCBF. Moreover, nine experts confirmed that cooperation in case of instability and during crises is missing and we have to create coordinated mechanisms with regional and international partners. All experts mentioned that some activities should be added to the framework such as, performance measurements, auditing mechanisms to be added to legal capacity building.

Moreover, all of participants stated to use the NCS as function not as a mechanism and swap it with “Establish a National Council”. Another interesting point is that all of the participants stressed that the national council should include the advisory committee and counter-terrorism committee. Ten experts from thirteen, agreed that this framework is “useful and acceptable”. Two of them said that, they liked how the capacity building in educations and private sectors has been defined and developed. All of the participants acknowledged that the framework is inclusive, coherent, multi-dimensional and risk based. Four of them commented that in their opinion this framework is inclusive, coherent, multi-dimensional and risk-based because it is based on a well know and internationally acceptable model (CCMM).

## 7.6 Modification to the framework

This section summarises the main updates and amendments to the activities of the proposed framework. As described in the results in the previous section some suggested amendments suggested by the participants and the actions taken by the researcher are presented in Table (7.4). The new versions of the NCCBF dimensions were updated in the development section in **Chapter 6** while the previous version is present in Appendix 6.

| Amendments | No. of Resp's | Related Dimension/Phase | Action Taken |
|---|---|---|---|
| Add continues review of the model auditing. | 6 | D4 | Added |
| Create coordinated mechanisms with regional and international partners during crisis. | 13 | D1,D4,D5 | Added of D1,D4,D5. |
| Use risk management instated risk based approach in D1 and mirage M1.1.2 with M1.1.1. | 13 | D1 | Changed |
| Add regional agreement mechanism. | 13 | D4 | Added |
| Add physical security policies in D5 and regional cooperation's. | 3 | D5 | Added |
| Add Big data sharing mechanisms (Regional and international) to D4. | 5 | D4 | Added |
| Change cybersecurity awareness-raising campaigns to cybersecurity awareness-raising program (M2.1.2). | 5 | D2 | Changed |
| "Use Performance measurement such as (KPI, Balanced Scorecard (BSC)) or other capabilities measuring frameworks". | 13 | Output stage | Addressed |
| "Organisational structure should include advisory committee and counter-terrorism committee and build capacity of these committees in field of cybersecurity in the country". | 13 | D1 | Added |
| "Use the development of the NCS as function not as a mechanism and swap it with "Establish a National Council". | 13 | D1 | Swapped |
| "Consider other methods to assess the internal and external landscape such as SWOT and PESTEL approaches". | 13 | AS-IS step | Added in observation phase |

Table 7.4 Modification to the framework

## 7.7 Threats to Validity

The evaluation of the NCCBF in this chapter has the following threats to validity and some limitations. One was that the researcher has invited 20 participants from the workshop and the research material has been given to them. A total of 13 of the selected participants then attended the evaluation sessions, although seven of the participants failed to attend, owing to external commitments or issues. Second, the researcher was not able to demonstrate the proposed framework with the same participants due to the difficulty to arrange another separate meeting and get a consensus among all participants on the time of the two focus group meetings. The meeting was ultimately arranged in one focus group meeting on the same day at the same time. Third, some of participants failed to assess the IDEF0 modelling function template analysis such as (AS-IS) and (AS-TO-BE), due to lack of understanding the IDEF0 technique. This gave insight into the need to apply this artefact to another country with a set of experts from different domains.

## 7.8 Chapter Summary

This chapter has discussed the approach to the evaluation of the proposed framework (NCCBF) for countries in a transitional phase. This framework has been evaluated by 13 experts in the field the cybersecurity from different countries including experts from countries that in transitional phase, during an ITU workshop session by using the focus group technique and where the limitations of this evaluation study were also voiced and noted.

The evaluation demonstrated the valuable contribution of the NCCBF's at the United Nations organised event where it concepts, design principles, methodology and framework procedures were discussed in-depth as where the challenges in National Cybersecurity Capacity Building and the complexities associated with their builds. The results of evaluation including critical suggestions and procedural amendments were provided, and the finalised version of framework was adjusted based on their evaluation.

# 8. CHAPTER 8: CONCLUSION AND FUTURE WORK

This chapter summarises the findings and outcomes of the research. In addition, the research contributions to knowledge are defined as well as future work.

## 8.1 Key findings and outcomes

This thesis investigated the Cybersecurity Capacity Building (CCB) issues and challenges in countries that in a transitional phase. Building cybersecurity capacity has become increasingly a subject of global concern in both stable countries and those countries in a transitional phase. The following are the key research findings:

- National and international Research & Technology Organisations (RTOs) have developed a plethora of guidelines and frameworks to help with the development of a national cybersecurity framework. Although extensive research has been carried out on CCB, to our knowledge no single study exists which focuses on countries in a transitional phase. In addition, there are no efforts so far in linking existing frameworks and initiatives with benchmarking models, and thus this effort from the CCMM is presented (Hameed et al. 2018; Ben Naseir et al. 2020).

- Existing models and assessments of Cybersecurity Capacity Building (CCB) are successful in evaluating national levels of CCB in individual countries, however, the ability to aid countries in how to improve their cyber capacities is still lacking (Muller 2015).

- Many countries including countries in a transitional phase with poor infrastructure and poor governance are rapidly starting to establish their presence in cyberspace. However, this may provide a new breeding ground for organised crime, terrorism, and being used as an instrument for committing international cybercrime (Garlock 2018).

- The research findings indicate that countries in a transitional phase are vulnerable to cybersecurity risks, such as cybercrime and cyber terrorism, and that they lack of cybersecurity capacity areas such as; an adequate knowledge and awareness of cybersecurity, cybersecurity strategies and policies, technical controls, and incident response capabilities.

- Managing cyber risk to national critical infrastructure and information infrastructure is crucial in cyberspace. However, the results of this research show that many countries in a transitional phase lack of proper risk management process, lack of knowledge and skills in risk management.

- Existing literature highlighted that many countries in a transitional phase are facing numerous challenges in adopting e-services in, e.g., e-government (Ahmed et al. 2013; Karaim and Inal 2019), e-banking (Farag and Hilles; Elgahwash et al. 2014; MTMC 2016; Ward et al. 2017), e-commerce (Moftah et al. 2012; NISSA 2013; GCSCC 2017) and e-learning (Kitzinger 1995a; Warfield et al. 2002; Gill et al. 2008; Goldman 2010; Herrington and Aldrich 2013; DOE 2014; Hult and Sivanesan 2014). In addition, many of these countries suffer from the digital, and they are not able to deploy the appropriate ICT infrastructure for e-government deployment (Alshehri and Drew 2010; Forti et al. 2014). Government departments in some of these countries such as Spring Land are using different ICT tools, which make it difficult to centralise the services from various departments and avail to citizens through e-Government platform (Forti et al. 2014).

- The results show that countries in a transitional phase are facing many issues due to current political unrest and the austerity measures that affect local government. These issues such as, lack of funding has hindered most of the attempts of advancing cybersecurity including education (Symantec 2016). Muller (2015), stated that cybersecurity capacity is challenge in these countries due to many reasons including institutional stability, and building knowledge. Cyber education in these countries is concisely mentioned as a part of the discussion and as a crucial part of securing cyberspace (Muller 2015).

- Literature and body of knowledge show that no scholarly research has currently been done on countries in a transitional phase posture to implementing appropriate Cybersecurity Capacity Building frameworks. In addition, there are no studies addressing the factors that influence the development of a National Cybersecurity Capacity Building Framework (NCCBF) in a chaotic ecosystem.

Based on the research findings and analysis, a National Cybersecurity Capacity Building Framework (NCCBF) is proposed, highlighting the significant capacities necessary for improving cybersecurity in transitional phase countries. The NCCBF is inspired by a Design Science Research methodology (DSR) and guided by utilising modelling approaches. The OODA was used as a modelling baseline, selected for its simplicity and adaptability, OODA steps were used to construct and guiding the requirements of IDEF0. These steps were instantiated with the CCMM and finding from the conducted empirical studies and literature. Furthermore, the NCCBF has been evaluated by a focus group against a structured set of criteria. The evaluation demonstrated the valuable contribution of the NCCBF's in representing the challenges in the National Cybersecurity Capacity Building and the complexities associated with the build. It is hoped that the contribution of the qualitative studies and proposed framework in this thesis will benefit governments in transitional phase countries.

## 8.2 Research Contributions

This research contributes to both theoretical and practical understanding of national cybersecurity capacity in the context of transitional phase countries. The finding and outcomes of this study have numerous implications to academia, decision makers, cybersecurity practitioners, professionals, and general cyber space users as follows:

- Theoretically, this research contributed to the existing body of Cybersecurity Capacity Building research, mainly through problem space contextualisation. This has been done by filling the knowledge gap in understanding how countries in a transitional phase are managing cybersecurity capacity challenges and understanding the existing weaknesses in cybersecurity capacity domain in those countries. The outcomes highlighted in this research could influence the strategies and decisions on

an efficient framework which help to improve the contribution level of cybersecurity capacity for countries in a transitional phase.

- The research study has investigated the concept of national cybersecurity capacity framework and indices adopted by developed countries and international models and security standards to secure cyberspace and build cybersecurity capacities. These models were examined to understand their pros and cons and how could be adopted to enable countries in a transitional phase to transform their current cybersecurity posture by applying activities that reflect desired outcomes.
- This research involved active participants of expert and stakeholder utilising two qualitative studies. A significant contributing factor for this type of study closes the gap between academia and practitioners and creates the Knowledge Exchange Environment that will sustain Information Exploitation, Information Operations, and Digital Transformation for the NCCBF. According to Hevner et al. (2004), the artefact may enable the solution of an unsolved problem by either extending the knowledge base or applying existing knowledge in new innovative ways. For this research study, the variety of existing standards, guidelines, and practices based on criteria have been innovatively mapped t to address the research problem for understanding cybersecurity capacity building activities.

- The Macro-Development of a National Cybersecurity Capacity Building Framework (NCCBF) that secures the 5$^{th}$ domain for countries in a transitional phase.

## 8.3 Strengths and Limitations of the Research

Since the states around the world are facing similar cyber threats, developing a National Cybersecurity Capacity Building Framework to enhance National Security attracts more attention in recent years. The study's strength lies in the fact that this research fills the knowledge gap in understanding how countries in a transitional phase using Spring Land as a case study are managing and approaching Cybersecurity risks and threats. The study focuses on the strategic level challenges and develops a framework to overcome emerging Cybersecurity threats. The said framework will encompass convenient and efficient frameworks, which shall aid to contribute strongly to efficient Cybersecurity capacity for countries in a transitional phase.

In this research, adopting and adapting the Cybersecurity Capacity Maturity Model (CCMM) for Nation states developed a Common Operational Picture (COP) of the State-of-Art of the Spring Land Cyber defence and its threat landscape. The Interactive Management technique and Focus Group discussion are used in order to capture the required analysis framework for the National Cybersecurity Capacity Building Framework suitable for National security for countries in a transitional phase. This analysis is based on the Cybersecurity Capacity Maturity Model for Nations (CCMM) that was developed by the University of Oxford. While the research findings are limited to Spring Land, some generalisations are possible. In addition, other countries' Cybersecurity strategies, also existing global Cybersecurity frameworks, and Cybersecurity Capacity models are used as a base for the comprehension of the best practice around the world. The audiences of this research are decision makers, government officials, managers, and general employees participating in security development in Spring Land. Furthermore, the framework has been evaluated by international experiences from different countries including experts from countries that in a transitional phase.

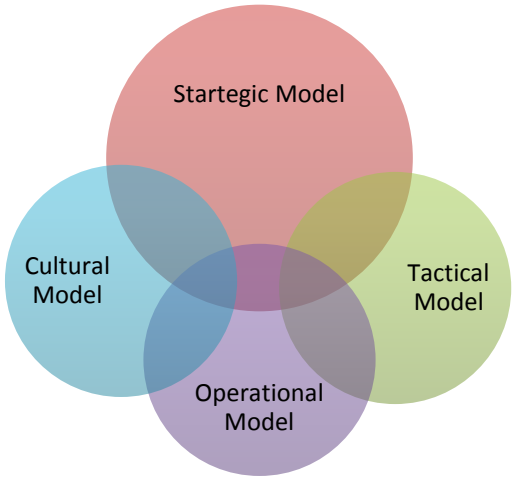



Figure 8.1: The scope of the research

This research is focused on the field of Cybersecurity Capacity Building for counties in a transition state using Spring Land as a case study. It is limited with respect to models applied in the study as it primarily concentrates on the strategic level and provides some of the indications for Tactical, Operational, and Cultural models as secondary elements. The case

study was limited to one state (Spring Land) at a given point in time and there is a lack of good data collection on cyber incidents and threats in Spring Land.

In addition, many efforts have been made to reduce research biases. However, this study recognise that certain research biases may have influenced the study results, such as participants are not understanding the questions or methods proposed in this study (Jackson 2015), the interaction between main functions in **Section** 4.2.4, was based on the judgment of the researcher which may influence the findings. Furthermore, the framework has been evaluated against a based on a set of requirements, but it has not been tested in a real-life environment as of yet.

## 8.4 Future work

Since this study is the first of its kind related to cybersecurity capacity building, there are many opportunities for future research on cybersecurity issues in countries that in a transitional phase. These opportunities such as the following:

- Conducting comparative studies to obtain a complete understanding of how stable or developed counties are managing and building their cybersecurity capacities.
- This research can be extended to evaluate the pertinence and usefulness of the proposed framework to other countries in addressing cybersecurity challenges.
- This research identified the critical success factors for cybersecurity capacity building for countries in a transitional phase by adapting CCMM dimensions. Therefore, it would be useful to explore and analyse these dimensions using other approaches such as Political, Economic, Social, Technological, Environmental and Legal (PESTEL) approach.
- The framework has been evaluated against a based on a set of requirements, but it has not been tested in a real-life environment as of yet. Therefore, further research can be considered including testing this framework in other countries.
- More research can be done to refinement the components of the framework such as using performance measurement techniques to monitor the performance of each dimension in the NCCBF. In addition, the Enterprise Architecture components can be adapted in the proposed CCB framework.

- The NCCBF provides five dimensions with concurrent and continuous functions for each dimension. The framework provides an easy to follow set of activities to build national cybersecurity capacity, however, a web tool can be developed to facilitate communication of these activities and outcomes across the country from the strategic to operations levels.

## 8.5 Conclusions

In this study, a National Cybersecurity Capacity Building Framework (NCCBF) is proposed to enable countries in a state of transition to transform their current cybersecurity posture by applying activities that reflect desired outcomes. The NCCBF provides the means to a better understanding of how NCCB can be defined and developed. The research findings showed that countries in a transitional phase are vulnerable to cybersecurity risks such as cybercrime and cyber terrorism.

As no previous studies have been conducted on countries in a state of transition, the research findings and results could influence the policies and decisions on building cybersecurity capacity in these countries.

## 8.6 Recommendations

Cyberspace has become an essential element in the development of modern economies. A robust cybersecurity capacity is vital for states to progress and advance in economic, political and social terms (Pawlak 2014; Muller 2015). Spring Land is beset with numerous challenges but needs to prioritise cybersecurity capacity to ensure it has the ability to react swiftly to protect its wellbeing and ensure continued economic growth and prosperity for its citizens. These issues have been raised due to political concerns and the scarcity of government funding and human resources to prepare a national cybersecurity blueprint. There are numerous recommendations arising from the research that could help the government to intervene in a constructive manner. These recommendations are articulated below:

1- Devise a National Cybersecurity Strategy (NCS)

A NCS should be considered by the government because state interactions in cyberspace are characterised by uncertainty, rather than predictability in this era. Therefore, by devising a NCS, the state is able to decide how to concentrate its efforts based on their relative strengths

and weakness. The strategy process should involve as many stakeholders as possible and centralise competence. Based on the existing frameworks in Section 2.8.2.1 and the proposed framework in Section 6.4.2, the strategy should be guided by numerous principles taken together in the development of the NCS. These guiding principles are: Risk-based; Outcome-focused; Prioritised; Practicable; Respectful of privacy and civil liberties; Globally relevant; and Appropriate set of policy instruments. In addition, a National Council for Cybersecurity with a clear mandate, appropriate statutory powers and an organisational structure must be established to develop the NCS. The rationale for creating the council is to perform a crucial function in coordinating various organisations in the public and private sectors. Also, demonstrating strong leadership at the highest level enhances recognition of the NCS.

2- Build a cyber defence doctrine

Cyber defence capabilities should be developed. This is essentially because cyber has become a tool for politics, espionage and military activities and cybersecurity has become a central topic for national and international security. The government recognising cyberspace as a warfare domain will enhance deterrence in air, space and cyberspace by enhancing the state's ability to attribute and defeat attacks targeting systems or supporting infrastructure (Pernik et al. 2016). To develop a cyber defence doctrine, several aspects should be considered by the government and these can be found in Section 2.8.2.2 and Section 6.4.2.

3- Develop national incident response capabilities

National incident response capabilities should be bolstered by establishing national computer security incident response teams (CSIRT) and ensuring that the technical, financial and human resources are adequate. In addition, it is necessary to establish clear processes and clearly defined roles and responsibilities. This research has found that Spring Land created a national computer emergency response team (CERT) but this is only working at the level of National Cybersecurity Authority (NCSA) departments. This is due to a lack of co-operation at the state level for various reasons including the lack of a national strategy, administrative complications, political orientations, poor awareness, and a lack of trust between all sectors (see Section 4.3.2 and Section 5.4.1).

Therefore, developing national incident response capabilities will help the government to establish a culture of risk assessment and crisis management to assess risks and devise methods to mitigate them. There are several existing guides that outline the activities required to establish a CSIRT (see Section 2.8.2.3 and Section 6.4.2).

4- Developing risk management and critical infrastructure protection capabilities

Developing a risk management approach should be considered by the government of Spring Land because it delivers a process that integrates security and risk management activities into the system development lifecycle. The risk-based approach to security control selection and specification considers the effectiveness, efficiency and associated constraints arising from the applicable laws, directives, executive Orders, policies, standards and regulations. In addition, it identifies the critical infrastructure (CI) assets and critical national information infrastructure (CNI) which are crucial for efforts to develop measures and procedures for the protection of CNI and reduce the risk of cyberattacks. Also, it is necessary to create a national list of CNI assets and identify the risk priorities. There are various sources of guidance and also different approaches available to develop these capabilities. More information can be found in Section 2.8.2.2 and Section 6.4.1.

5- Developing a national awareness programme

The government must develop a national awareness programme that is compatible with the current situation, targeting all of society to influence the implementation of secure behaviour online. This study has revealed that there is a lack of skilled people and campaigns actively raising awareness of cybersecurity to deal with incidents in government sectors. Consequently, the associated cybersecurity threats and vulnerabilities have been significantly increased (see Section 4.3.2 and Section 5.4.2). Therefore, establishing a formal national awareness programme can enable citizens, the public sector and private sector to develop a security-minded culture so that they behave securely in cyberspace. To develop such an awareness programme, the agency's awareness and training needs to be identified and an extensive awareness and training plan must be developed. This will require organisational buy-in as well as priorities to be established (see Section 2.8.2.4).

6- Creating a national cybersecurity education and workforce development framework

The government should consider cybersecurity education and workforce development as a part of a national capacity building strategy. This study has shown that Spring Land does not have any plans at the national level to enhance the efficiency of education or workforce development in the field of cybersecurity due to there being no financial resources allocated

for such purposes at the state level. In addition, there is no co-ordination between universities and private companies with regards to cybersecurity training and there are no plans to continue training government employees in cybersecurity (see Section 4.3.2 and Section 5.4.3). Therefore, the government should dedicate a national budget to harmonise cybersecurity education and research. Moreover, qualification programmes for cybersecurity should be developed to start amassing a cadre of professionals at the national and organisational level. Develop national cybersecurity education programme based on the existing frameworks will entail many steps. These steps will include the following: selecting the task owner and the audience for the cybersecurity education programme; mapping the existing cybersecurity education landscape and identifying gaps in provision; fostering research and development in cybersecurity; combining the education with practical training; and preparing the future cybersecurity workforce (McGettrick 2013; Newhouse et al. 2017; Bellasio et al. 2018). More information can be found in Section 2.8.2.5 and Section 6.5.2.

7- Drafting a legal framework

National laws and regulations related to cybersecurity and cybercrime should be drafted by the Spring Land government because the failure to establish a clear legal basis can lead to significant limitations on a country's ability to successfully secure cyberspace (Bellasio et al. 2018). The study has confirmed that no cyber- or ICT security-related legislation or regulations have been drafted by the Spring Land government (see Section 4.3.2 and Section 5.5.4). The government should develop a legal framework and ensure that the framework satisfies various principles such as the territoriality principle, the responsibility principle, national and international cooperation, and human rights. These principles outline fundamental concepts and areas that must be included or addressed in a comprehensive legal approach to cybersecurity as well as the need to raise awareness about existing legal difficulties involving cybersecurity (Tikk 2011). In addition, the government should develop and strengthen national capacities in law enforcement and cyber-related crime investigation as well as prosecutors and judges. More information about how to develop the legal framework can be found in Section 2.8.2.6 and Section 6.5.3.

8- Adhere to international cybersecurity standards

All governments and stakeholders in Spring Land have to adhere to common ICT security, technology, cybersecurity, and risk-management standards and protocols such as those

published by ISO and the International Electrotechnical Commission (IEC). This is because the scope of cybersecurity includes the protection of complex environments resulting from the interaction of persons, software and services on cyberspace by means of technology devices and connected networks (ENISA 2019). This research has found that military and political conflicts have greatly affected the resilience of infrastructure and exposed the telecommunications, electricity and water sectors to greater risk. In addition, there is no national agency or framework to monitor the implementation of standards, and minimal acceptable practices across all government sectors. There is also a lack of research centres in this field and poor co-operation between the public and private sectors with regards to training and skill development (see Section 4.3.2 and Section 5.5.5).

However, adhering to standardisations in cybersecurity would provide many benefits to the government and organisations of Spring Land. These benefits include: interoperability; reusability; knowledge development and cybersecurity awareness; harmonisation of terminology; consistency between different manufacturers, vendors and users; repeatability; performance checking; security evaluation; supply chain integrity and security (ENISA 2019). The government of Spring Land can utilise a range of general resources to build capacity in ICT security standards, cryptographic controls, cybersecurity standards, risk-management standards and audited assessment. These include standards derived from the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC); the International Telecommunications Union – Telecommunication Standardization Sector (ITU-T); the Internet Engineering Task Force, the Institute of Electrical and Electronics Engineers (IEEE); the World Wide Web Consortium; and the National Institute of Standards and Technology (NIST) (Bellasio et al. 2018). Further information can be found in Section 2.8.2.7 and Section 6.5.4.

These recommendations were derived from two qualitative findings (see Chapter 4 and Chapter 5) as well as existing frameworks which enabled the researcher to suggest relatively concrete recommendations. Enhancing national cybersecurity capacity will be more effective if it is structured and modelled under an overarching framework in a consistent way, as proposed in this research.

# 9. References


Abuzawayda, Y. I., 2016. Security Issues on Libya's E-Government. *Imperial Journal of Interdisciplinary Research*, 3 (1).

African-Union, 2014. African Union convention on cyber security and personal data protection. *African Union: Addis Ababa, Ethiopia*.

Ahmed, A. M., Moreton, R., Mehdi, Q. H. and Elmaghraby, A., 2013. E-government services challenges and opportunities for developing countries: The case of Libya, *2013 Second International Conference on Informatics & Applications (ICIA)* (pp. 133-137): IEEE.

Ajzen, I., 2002. Perceived behavioral control, self‐efficacy, locus of control, and the theory of planned behavior 1. *Journal of applied social psychology*, 32 (4), 665-683.

Aliyu, A. A., Bello, M. U., Kasim, R. and Martin, D., 2014. Positivist and non-positivist paradigm in social science research: Conflicting paradigms or perfect partners? *Journal of Management and Sustainability*, 4 (3), 79.

Alshehri, M. and Drew, S., 2010. Implementation of e-government: advantages and challenges, *International Association for Scientific Knowledge (IASK)* (pp. .).

AMC, 2017. *Cybersecurity Curricula 2017*. New York, NY: ACM, IEEE, AIS, IFIP.

Andreewsky, E. and Bourcier, D., 2000. Abduction in language interpretation and law making. *Kybernetes*, 29 (7/8), 836-845.

Appazov, A., 2014. Legal aspects of cybersecurity.

Appelbaum, S. H., 1997. Socio-technical systems theory: an intervention strategy for organizational development. *Management decision*, 35 (6), 452-463.

Archick, K., Ek, C., Gallis, P., Miko, F. T. and Woehrel, S., 2006. European approaches to homeland security and counterterrorism: LIBRARY OF CONGRESS WASHINGTON DC CONGRESSIONAL RESEARCH SERVICE.

Argomaniz, J., 2015. The European Union Policies on the Protection of Infrastructure from Terrorist Attacks: A Critical Assessment. *Intelligence and National Security*, 30 (2-3), 259-280.

Asadli, J., 2018. *PROPOSING ACTION PLAN IN CYBER SECURITY CAPACITY BUILDING FOR AZERBAIJAN.* Master Thesis (Master ). Tallinn University of Technology.

Avdoshin, S. M. and Pesotskaya, E. Y., 2016. Software risk management: using the automated tools. *Emerging Trends in Information Systems.* Springer, 85-97.

Avison, D. E., Lau, F., Myers, M. D. and Nielsen, P. A., 1999. Action research. *Communications of the ACM*, 42 (1), 94-97.

Azmi, R., Tibben, W. and Win, K. T., 2018. Review of cybersecurity frameworks: context and shared concepts. *Journal of Cyber Policy*, 3 (2), 258-283.

Bada, M., Creese, S., Goldsmith, M., Mitchell, C. and Phillips, E., 2014. Computer security incident response teams (CSIRTs) an overview. *Global Cyber Security Capacity Centre*, 1-23.

Bada, M., Sasse, A. M. and Nurse, J. R., 2019a. Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv:1901.02672*.

Bada, M., Von Solms, B. and Agrafiotis, I., 2019b. Reviewing national cybersecurity awareness in Africa: an empirical study.

Baker, M., 2013. State of cyber workforce development. *Software Engineering Institute, Carnegie Mellon University*.

Banathy, B. A., 1996. Information ‐ based design of social systems. *Systems Research and Behavioral Science*, 41 (2), 104-123.

Bandura, A., Freeman, W. and Lightsey, R., 1999. Self-efficacy: The exercise of control: Springer.

Baranowski, L. E. and Anderson, L. E., 2005. Examining rating source variation in work behavior to KSA linkages. *Personnel Psychology*, 58 (4), 1041-1054.

Barata, J., da Cunha, P. R. and Abrantes, L., 2015. Dealing with risks and workarounds: A guiding framework, *IFIP Working Conference on The Practice of Enterprise Modeling* (pp. 141-155): Springer.

Baskerville, R. L. and Wood-Harper, A. T., 1996. A critical perspective on action research as a method for information systems research. *Journal of information Technology*, 11 (3), 235-246.

Baxter, G. and Sommerville, I., 2011. Socio-technical systems: From design methods to systems engineering. *Interacting with computers*, 23 (1), 4-17.

Beesley, A. D. and Shebby, S., 2010. Evaluating Capacity Building in Education: The North Central Comprehensive Center. *Online Submission*.

Bellasio, J., Flint, R., Ryan, N., Sondergaard, S., Monsalve, C. G., Meranto, A. S. and Knack, A., 2018. Developing Cybersecurity Capacity: A proof-of-concept implementation guide.

Ben Naseir , Huseyin Dogan , Edward Apeh  and Raian Ali 2020. National Cybersecurity Capacity Building Framework for Countries in a Transitional Phase. *the 22nd International Conference on Enterprise Information Systems*. Science and Technology Publications. Available from: https://www.scitepress.org/PublicationsDetail.aspx?ID=0ngJLvAM5Mg=&t=1 [Accessed

Ben Naseir, M. A., Dogan, H., Apeh, E., Richardson, C. and Ali, R., 2019. Contextualising the National Cyber Security Capacity in an Unstable Environment: A Spring Land Case Study (pp. 373-382). Cham: Springer International Publishing.

Benbasat, I., Goldstein, D. K. and Mead, M., 1987. The case research strategy in studies of information systems. *MIS quarterly*, 369-386.

BenIbrahim, A., 2017. *Libyana Mobile Phone goes 4G LTE* [online]. Available from: https://www.libyaobserver.ly/tech/libyana-mobile-phone-goes-4g-lte [Accessed 24/04/2017].

Berendt, B., De Paoli, S., Laing, C., Fischer-Hübner, S., Catalui, D. and Tirtea, R., 2014. Roadmap for NIS education programmes in Europe.

Berger, P. L. and Luckmann, T., 1966. T.(1966). *The social construction of reality*.

Bhattacherjee, A., 2012. *Social science research: Principles, methods, and practices*.

Bigelow, B., 2019. What are Military Cyberspace Operations Other Than War?, *2019 11th International Conference on Cyber Conflict (CyCon)* (Vol. 900, pp. 1-17): IEEE.

Boas, G., Bischoff, J. L., Reid, N. L. and Taylor III, B. D., 2011. *International Criminal Law Practitioner Library: Volume 3: International Criminal Procedure*. Cambridge University Press.

Boehm, B. W., 1991. Software risk management: principles and practices. *IEEE software*, 8 (1), 32-41.

Boes, S. and Leukfeldt, E. R., 2017. Fighting cybercrime: A joint effort. *Cyber-Physical Security.* Springer, 185-203.

Boodhoo, R. and Purmessur, R. D., 2009. Justifications for qualitative research in organisations: a step forward. *The Journal of Online Education (New York)*.

Boyd, J. R., 1996. The essence of winning and losing. *Unpublished lecture notes*, 12 (23), 123-125.

Braun, V. and Clarke, V., 2006. Using thematic analysis in psychology. *Qualitative research in psychology*, 3 (2), 77-101.

Brechbühl, H., Bruce, R., Dynes, S. and Johnson, M. E., 2010. Protecting critical information infrastructure: Developing cybersecurity policy.

Broome, B. J. and Keever, D. B., 1986. Facilitating Group Communication: The Interactive Management Approach.

Bryman, A., 1984. The debate about quantitative and qualitative research: a question of method or epistemology? *British journal of Sociology*, 75-92.

Bryman, A., 2016. *Social research methods*. Oxford university press.

Bryson, J. M., 2018. *Strategic planning for public and nonprofit organizations: A guide to strengthening and sustaining organizational achievement*. John Wiley & Sons.

Burrell, G. and Morgan, G., 1979. Two dimensions: Four paradigms. *Sociological paradigms and organizational analysis*, 21-37.

CabinetOffice, 2010. Strategic framework and policy statement on improving the resilience of critical infrastructure to disruption from natural hazards: Cabinet Office London.

Campion, M. A., Campion, J. E. and Hudson Jr, J. P., 1994. Structured interviewing: A note on incremental validity and alternative question types. *Journal of Applied Psychology*, 79 (6), 998.

Capers, I. B., 2018. Criminal Procedure and the Good Citizen. *Columbia Law Review*, 118 (2), 653-712.

Carey, J. W., 1993. Linking qualitative and quantitative methods: Integrating cultural factors into public health. *Qualitative Health Research*, 3 (3), 298-318.

Carr, M., 2016. Public–private partnerships in national cyber-security strategies. *International Affairs*, 92 (1), 43-62.

Caruso, J., 2002. Combating Terrorism: Protecting the United States. *testimony of JT Caruso, Deputy Executive Assistant Director, Counterterrorism/Counterintelligence Division, FBI, before the House Subcommittee on National Security, Veteran Affairs, and International Relations, Washington DC, March*, 21, 122.

Cavelty, M. D., 2014. Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. *Science and engineering ethics*, 20 (3), 701-715.

Cerezo, A. I., Lopez, J. and Patel, A., 2007. International cooperation to fight transnational cybercrime, *Second international workshop on digital forensics and incident analysis (WDFIA 2007)* (pp. 13-27): IEEE.

Cerullo, V. and Cerullo, M. J., 2004. Business continuity planning: a comprehensive approach. *Information Systems Management*, 21 (3), 70-78.

Charmaz, K. and Belgrave, L. L., 2007. Grounded theory. *The Blackwell encyclopedia of sociology*.

Choo, K.-K. R., 2011. The cyber threat landscape: Challenges and future research directions. *Computers & Security*, 30 (8), 719-731.

Christakis, A. N., 1985. The national forum on nonindustrial private forest lands. *Systems Research and Behavioral Science*, 2 (3), 189-199.

Cichonski, P., Millar, T., Grance, T. and Scarfone, K., 2012. Computer security incident handling guide. *NIST Special Publication*, 800 (61), 1-147.

Ciglic, K., 2018. *Cybersecurity Policy Framework A practical guide to the development of national cybersecurity policy*. Microsoft.

Clarke, C., 2009. Paths between positivism and interpretivism: An appraisal of Hay's via media. *Politics*, 29 (1), 28-36.

Coram, R., 2002. *Boyd: The fighter pilot who changed the art of war*. Hachette UK.

Craig, A., 2018. *Risk Management for Cybersecurity: Security Baselines*. Microsoft

Creswell, J. W., 2013. *Research design : qualitative, quantitative, and mixed method approaches* [Non-fiction]. Los Angeles, Calif. : SAGE, 2013.Fourth edition, international student edition.

Cronin, C., 2014. Using case study research as a rigorous form of inquiry. *Nurse Researcher (2014+)*, 21 (5), 19.

CSFI, C. S. F. I., 2011. *Project Cyber Dawn - Libya* [online]. Available from: http://stefanomele.it/public/documenti/222DOC-395.pdf [Accessed 25-04-2016].

CTO, 2015. *Commonwealth Approach for Developing National Cybersecurity Strategies: A Guide to Creating a Cohesive and Inclusive Approach to Delivering a Safe, Secure and Resilient Cyberspace*. London, UK.: Commonwealth Telecommunications Organisation (CTO)

Cyberkov, 2016. *Hunting-libyan-scorpions* [Available from: https://cyberkov.com/hunting-libyan-scorpions/ [Accessed 15-11-2016].

CyberSeek, 2016. *Hack the Gap: Close the cybersecurity talent gap with interactive tools and data* [online]. Available from: https://www.cyberseek.org/pathway.html [Accessed 07-08-2019].

Danermark, B., Ekstrom, M. and Jakobsen, L., 2001. *Explaining society: an introduction to critical realism in the social sciences*. Routledge.

DCMS, 2018. *DEVELOPING THE CYBER SECURITY PROFESSION IN THE UK.*

De Vaus, D. A., 2001. *Research design in social research*. Sage.

Demchak, C., Kerben, J., McArdle, J. and Spidalieri, F., 2015. CYBER READINESS INDEX 2.0.

Denning, D. E., 2001. Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy. *Networks and netwars: The future of terror, crime, and militancy*, 239, 288.

Dennis, A., Jones, R., Kildare, D. and Barclay, C., 2014. Design Science Approach to Developing and Evaluating a National Cybersecurity Framework for Jamaica. *The Electronic Journal of Information Systems in Developing Countries*, 62 (1), 1-18.

Denscombe, M., 2014. *The good research guide : for small-scale research projects* [Book]. Fifth edition. edition.: Milton Keynes : Open University Press, 2014.

Denzin, N. K. and Lincoln, Y. S., 2000. *Handbook of qualitative research* [Non-fiction]. Thousand Oaks, Calif. ; London : Sage Publications, 2000.

2nd ed.

DeRouen Jr, Karl Goldfinch and Shaun, 2012. What makes a state stable and peaceful? good governance, legitimacy and legal-rationality matter even more for low-income countries. *Civil Wars*, 14 (4), 499-520.

Dey, P. K., Kinch, J. and Ogunlana, S. O., 2007. Managing risk in software development projects: a case study. *Industrial Management & Data Systems*.

DiCicco‐Bloom, B. and Crabtree, B. F., 2006. The qualitative research interview. *Medical education*, 40 (4), 314-321.

DoD, 2008. *Defending a New Domain* [online]. the U.S. Department of Defense. Available from: https://archive.defense.gov/home/features/2010/0410_cybersec/lynn-article1.aspx [Accessed 16/06/2018].

DOE, U. S. D. o. E., 2014. *Cybersecurity Capability Maturity Model Version 1.1* (15/10/2017).

Dogan, H., 2013. *Managing knowledge for capability engineering* [https://repository.lboro.ac.uk/articles/Managing_knowledge_for_capability_engineering/9544058]. Loughborough University.

Dogan, H., Pilfold, S. A. and Henshaw, M., 2011. The role of human factors in addressing Systems of Systems complexity, *2011 IEEE International Conference on Systems, Man, and Cybernetics* (pp. 1244-1249).

Donaldson, S. E., Siegel, S. G., Williams, C. K. and Aslam, A., 2015. Mapping Against Cybersecurity Frameworks. *Enterprise Cybersecurity.* Springer, 231-239.

Doody, O., Slevin, E. and Taggart, L., 2013. Focus group interviews. Part 3: analysis. *British Journal of Nursing*, 22 (5), 266-269 264p.

Dorfman, M., 2007. *Introduction To Risk Management And Insurance*. 9 edition.: Pearson (1650).

Draganidis, F. and Mentzas, G., 2006. Competency based management: a review of systems and approaches. *Information management & computer security*.

Druckman, J. N., Green, D. P., Kuklinski, J. H. and Lupia, A., 2006. The growth and development of experimental research in political science. *American Political Science Review*, 100 (4), 627-635.

Dudovskiy, J., 2016. *The Ultimate Guide to Writing a Dissertation in Business Studies: A Step-by-Step Assistance* [Available from: http://research-methodology.net/about-us/ebook/ [Accessed 20/05/2017].

Dunn, M., 2005. Centre for Security Studies, paper prepared for WSIS thematic Meeting on Cyber security: Geneva.

Ehrenfeld, J. M., 2017. WannaCry, Cybersecurity and Health Information Technology: A Time to Act. *Journal of Medical Systems*, 41 (7), 104.

El-Guindy, M., 2013. *21 Century Cyber Threats and the Middle East Dilemma* [online]. Available from: https://www.academia.edu/5522905/Middle_East_Cyber_Security_Threat_Report_2014 [Accessed 18/04/2016].

Elgahwash, F. O., Freeman, M. B. and Freeman, A., 2014. Improving online banking quality in developing nations: A ;Libyan case: i6doc.com.

ENISA, 2010. *Baseline Capabilities of National/Governmental CERTs (Part 2 Policy Recommendations).*

ENISA, 2011. *Inventory of Risk Management / Risk Assessment Methods*

ENISA, 2013. *National-level Risk Assessments: An Analysis Report* Panagiotis TRIMINTZIOS, ENISA, Razvan GAVRILA, ENISA.

ENISA, 2015. *National/governmental CERTs - ENISA's recommendations on baseline capabilities*

ENISA, 2016. NCSS Good Practice Guide,Designing and Implementing National Cyber Security Strategies. Available from: https://www.enisa.europa.eu/publications/ncss-good-practice-guide [Accessed 10/08/2017].

ENISA, 2019. *Standardisation In Support Of The Cybersecurity Certification*.

Eracar, Y. A. and Kokar, M. M., 2014. Using UML and OCL for representing multiobjective combinatorial optimization problems. *Journal of Intelligent Manufacturing*, 25 (3), 555-569.

European, 2018. *General Data Protection Regulation (GDPR).*

Evans, K. and Reeder, F., 2010. *A human capital crisis in cybersecurity: Technical proficiency matters*. CSIS.

Fakhoury, R. and Aubert, B., 2015. Citizenship, trust, and behavioural intentions to use public e-services: The case of Lebanon. *International Journal of Information Management*, 35 (3), 346-351.

Farag, O. M. and Hilles, S. M., Evaluate the e-banking services on North Africa Bank: Case of Tripoli branch.

Farrell, R. and Hooker, C., 2013. Design, science and wicked problems. *Design studies*, 34 (6), 681-705.

Finn, R. L., Wright, D. and Friedewald, M., 2013. Seven types of privacy. *European data protection: coming of age.* Springer, 3-32.

Forti, Y., Bechkoum, K., Turner, S. and Ajit, S., 2014. The adoption of e-government in Arab Countries-The case of Libya, *Proceedings of the 14th European conference on e-government: ECEG* (pp. 319-327).

Fred, S., 2015. *DCAF HORIZON 2015 WORKING PAPER No. 7 : On Cyberwarfare* [online]. Available from: https://www.google.co.uk/search?sourceid=chrome-psyapi2&ion=1&espv=2&ie=UTF-8&q=The%20Basic%20Building%20Blocks%3A%20Cyberspace%2C%20Cyberpower%2C%20Cyberwarfare%2C%20and%20Cyberstrategy&oq=The%20Basic%20Building%20Blocks%3A%20

Cyberspace%2C%20Cyberpower%2C%20Cyberwarfare%2C%20and%20Cyberstrategy&aqs=chrome..69i57j69i60.1544j0j8 [Accessed

Gabriel, D., 2013. *Inductive and deductive approaches to research* [Available from: http://deborahgabriel.com/2013/03/17/inductive-and-deductive-approaches-to-research/ [Accessed 30/06/2017].

Galley, P., 1996. „Computer terrorism: what are the risks?". *Science, Technology and Society Swiss Federal Institute of Technology*.

Garlock, K., 2018. *Maturity Based Cybersecurity Investment Decision Making in Developing Nations.* The George Washington University.

Gcaza, N., von Solms, R. and van Vuuren, J. J., 2015. An Ontology for a National Cyber-Security Culture Environment, *HAISA* (pp. 1-10).

GCSCC, 2017. *Cybersecurity Capacity Maturity Model for Nations (CMM)* [online]. University of Oxford: Available from: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20Version%201_2_0.pdf [Accessed 25/10/2016].

GCSCC, 2019. *The Gambia: Cybersecurity Capacity Review 2018*.

Gerber, T., Theorin, A. and Johnsson, C., 2014. Towards a seamless integration between process modeling descriptions at business and production levels: work in progress. *Journal of Intelligent Manufacturing*, 25 (5), 1089-1099.

Gercke, M., 2016. Understanding cybercrime: a guide for developing countries.

Gill, P., Stewart, K., Treasure, E. and Chadwick, B., 2008. Methods of data collection in qualitative research: interviews and focus groups. *British dental journal*, 204 (6), 291.

GLACY, 2014. *Good practice study Cybercrime reporting mechanisms*. France.

Glock, C. Y. and Bennett, J., 1967. *Survey research in the social sciences*. Russell Sage Foundation.

Goldman, H. G., 2010. Building secure, resilient architectures for cyber mission assurance. *The MITRE Corporation*.

Goodman, R. M., Speers, M. A., McLeroy, K., Fawcett, S., Kegler, M., Parker, E., Smith, S. R., Sterling, T. D. and Wallerstein, N., 1998. Identifying and defining the dimensions of community capacity to provide a basis for measurement. *Health education & behavior*, 25 (3), 258-278.

Goodwin, C. F. and Nicholas, J. P., 2013. Developing a National Strategy for Cybersecurity: Microsoft Press.

Gordon, S. and Ford, R., 2006. On the definition and classification of cybercrime. *Journal in Computer Virology*, 2 (1), 13-20.

Graham, L., 2017. *Cybercrime costs the global economy $450 billion: CEO* [Available from: https://www.cnbc.com/2017/02/07/cybercrime-costs-the-global-economy-450-billion-ceo.html [Accessed 15/03/2017].

Gray, D., Allen, J., Cois, C., Connell, A., Ebel, E., Gulley, W., Riley, M., Stoddard, R., Vaughan, M. and Wisniewski, B. D., 2015. *Improving Federal Cybersecurity Governance Through Data-Driven Decision Making and Execution*. CARNEGIE-MELLON UNIV PITTSBURGH PA PITTSBURGH United States.

Greenwood, D. and Levin, M., 1998. An introduction to action research Thousand Oaks: Sage Publication Inc). p.

Grierson, J., 2017. *UK hit by 188 high-level cyber-attacks in three months* [Available from: https://www.theguardian.com/world/2017/feb/12/uk-cyber-attacks-ncsc-russia-china-ciaran-martin [Accessed 23/08/2017].

GSF, 2020 *The Government Security Profession career framework* Government Security.

Guiling, L. and Xiaojuan, Z., 2011. Research on the risk management of IT project, *2011 International Conference on E-Business and E-Government (ICEE)*.

Gumperz, J. J., 1981. Conversational inference and classroom learning. *Ethnography and language in educational settings*, 3-23.

Guo, S. and Stradiotto, G. A., 2014. *Democratic transitions: Modes and outcomes*. Routledge.

Haller, J., Merrell, S. A., Butkovic, M. J. and Willke, B. J., 2010. *Best practices for national cyber security: Building a national computer security incident management capability*. CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST.

Hameed, F., Agrafiotis, I., Weisser, C., Goldsmith, M. and Creese, S., 2018. Analysing trends and success factors of international cybersecurity capacity-building initiatives.

Hammarberg, K., Kirkman, M. and de Lacey, S., 2016. Qualitative research methods: when to use them and how to judge them. *Human reproduction*, 31 (3), 498-501.

Hammersley, M. and Atkinson, P., 1983. Ethnography principles in practice tavistock. *London, England*.

Heath Kelly, C., 2013. Counter‐Terrorism and the Counterfactual: Producing the 'Radicalisation' Discourse and the UK PREVENT Strategy. *The British Journal of Politics & International Relations*, 15 (3), 394-415.

Herrera, V. V., Ramos, A. V. and Lastra, J. L. M., 2012. An agent-based system for orchestration support of web service-enabled devices in discrete manufacturing systems. *Journal of Intelligent Manufacturing*, 23 (6), 2681-2702.

Herrington, L. and Aldrich, R., 2013. The future of cyber-resilience in an age of global complexity. *Politics*, 33 (4), 299-310.

Herzog, P., 2010. OSSTMM 3-The Open Source Security Testing Methodology Manual: Contemporary Security Testing and Analysis. *ISECOM-Institute for Security and Open Methodologies*.

Hevner, A. R., March, S. T., Park, J. and Ram, S., 2004. Design science in information systems research. *MIS quarterly*, 75-105.

Hipp, V., 2017. *Cyberattacks threaten our national security and economy* [online]. Available from: http://www.foxnews.com/opinion/2017/05/17/cyberattacks-threaten-our-national-security-and-economy.html [Accessed

HMG, 2009. Technical Risk Assessment.

HMGovernment, 2016. *NATIONAL CYBER SECURITY STRATEGY 2016-2021* HM Government

Ho, J. K.-K., 2014. Formulation of a systemic PEST analysis for strategic analysis.

Hohmann, M., Pirang, A. and Benner, T., 2017. Advancing Cybersecurity Capacity Building. *Global Public Policy Institute (GPPI)*.

Hu, C., Pazaki, H. and Velander, E., 2014. Evaluating global education at a regional university: A focus group research on faculty perspectives. *Theory in Action*, 7 (1), 65.

Hult, F. and Sivanesan, G., 2014. What good cyber resilience looks like. *Journal of business continuity & emergency planning*, 7 (2), 112-125.

Hussein, R., Mohamed, N., Ahlan, A. R., Mahmud, M. and Aditiawarman, U., 2010. An integrated model on online tax adoption in Malaysia, *European, Mediterranean & Middle Eastern conference on information systems* (pp. 12-13).

IDEF0, 1993. *Integration Definition for Function Modeling (IDEF0).* Department of Commerce, National Institute of Standards and Technology, Computer Systems Laboratory.

infoDevWorldBank, 2009. *e-GOVERNMENT PRIMER*. Washington, DC: infoDev/World Bank.

InternetWorldStats, 2017. *Internet usage and Population Statistics* [online]. Available from: http://www.internetworldstats.com/africa.htm#ly [Accessed 01/04/2017].

ISACA, 2013. Cybersecurity Nexus: Transforming Cybersecurity: Information Systems Audit and Control Association (ISACA) Illinois, USA.

ISO27002, 2005. BS ISO/IEC 27002: 2005 Information technology—Security techniques—Code of practice for information security management: ISO.

ISO31000, 2009. Risk management — Principles and guidelines. Available from: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en [Accessed 19-09-2019].

ISO, 2012. *ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity* [Available from: http://www.iso27001security.com/html/27032.html [Accessed 05/06/2016].

ISO/IEC29147, 2018. Information technology — Security techniques — Vulnerability disclosure. Available from: https://www.iso.org/obp/ui/#iso:std:iso-iec:29147:ed-2:v1:en [Accessed 12-03-2019].

ITU, 2009. Understanding Cybercrime: A Guide for Developing Countries.

ITU, 2014. *Global Cybersecurity Index* [online]. Available from: http://www.itu.int/en/ITU-D/Cybersecurity/Documents/WP-GCI-101.pdf [Accessed 29-05-2017].

ITU, 2015. *Global Cybersecurity Index & Cyberwellness Profiles* [online]. Available from: http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf [Accessed 10/03/2016].

ITU, 2017a. *Global Cybersecurity Index* [online]. Geneva: the International Telecommunication Union (ITU). Available from: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf [Accessed 20-10-2018].

ITU, 2017b. *Index of Cybersecurity Indices*. Geneva: The International Telecommunication Union (ITU)

ITU, 2018a. *Global Cybersecurity Index 2018*. Geneva: The International Telecommunication Union (ITU)

ITU, 2018b. *Guide to Developing a National Cybersecurity Strategy* [online]. Geneva, Switzerland: International Telecommunication Union (ITU). Available from: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf [Accessed 25/10/2019].

ITU, 2019. *ITU Interregional Workshop for Africa and Arab regions on "National Cybersecurity Strategies"* [online]. Available from: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/NCS-GCI-workshop-AFR-ARB-2019.aspx [Accessed 10-11-2019].

Jackson, S. L., 2015. *Research methods and statistics: A critical thinking approach*. Cengage Learning.

Jacobs, P. C., Von Solms, S. and Grobler, M. M., 2017. Towards a national cybersecurity capability development model.

Jasper, S. and Wirtz, J., 2017. Cyber Security. *The Palgrave Handbook of Security, Risk and Intelligence.* Springer, 157-176.

Johannesson, P. and Perjons, E., 2014. *An introduction to design science*. Springer.

Johnson, G., Scholes, K. and Whittington, R., 2008. *Exploring corporate strategy: text & cases*. Pearson Education.

Johnson, G. and Whittington, R., 2009. *Fundamentals of strategy*. Pearson Education.

Juell-Skielse, G. and Perjons, E., 2009. Improving E-government through benefit analysis and value modeling, *2009 33rd Annual IEEE International Computer Software and Applications Conference* (Vol. 1, pp. 332-339): IEEE.

Karaim, N. A. and Inal, Y., 2019. Usability and accessibility evaluation of Libyan government websites. *Universal Access in the Information Society*, 18 (1), 207-216.

Kaspersky, 2017. *IT threat evolution Q1 2017. Statistics* [online]. Available from: https://securelist.com/analysis/quarterly-malware-reports/78475/it-threat-evolution-q1-2017-statistics/ [Accessed 30-05-2017].

Kerbaj, R., 2017. *Russia steps up cyber - attacks on UK* [Available from: https://www.thetimes.co.uk/article/russia-steps-up-cyber-attacks-on-uk-rl262pnlb [Accessed 23/08/2017].

Kim, D.-H., Ahn, B.-J., Kim, J.-H. and Kim, J.-J., 2009. The strategic approach using SWOT analysis to develop an intelligent program management information system (iPMIS) for urban renewal projects, *Computer Sciences and Convergence Information Technology, 2009. ICCIT'09. Fourth International Conference on* (pp. 320-324): IEEE.

Kitchenham, B. A., 1996. Evaluating software engineering methods and tool part 1: The evaluation context and evaluation methods. *ACM SIGSOFT Software Engineering Notes*, 21 (1), 11-14.

Kitzinger, J., 1995a. Qualitative research. Introducing focus groups. *BMJ: British medical journal*, 311 (7000), 299.

Kitzinger, J., 1995b. Qualitative research: introducing focus groups. *Bmj*, 311 (7000), 299-302.

Klaver, M., Luiijf, H. and Nieuwenhuijsen, A., 2011. RECIPE: Good practices manual for CIP policies, for policy makers in Europe.

Klimburg, A., 2012. National cyber security framework manual.

Kortjan, N. and von Solms, R., 2012. Cyber security education in developing countries: A South African perspective, *International conference on e-Infrastructure and e-Services for developing countries* (pp. 289-297): Springer.

Kortjan, N. and Von Solms, R., 2014. A conceptual framework for cyber-security awareness and education in SA. *South African Computer Journal*, 52 (1), 29-41.

Kothari, C. R., 2004. *Research methodology. [electronic resource] : methods & techniques* [Bibliographies Non-fiction Computer File]. New Delhi : New Age International (P) Ltd., Publishers, c2004.2nd rev. ed.

Kovács, G. and Spens, K. M., 2005. Abductive reasoning in logistics research. *International Journal of Physical Distribution & Logistics Management*, 35 (2), 132-144.

Kritzinger, E., Bada, M. and Nurse, J. R., 2017. A study into the cybersecurity awareness initiatives for school learners in South Africa and the UK, *IFIP World Conference on Information Security Education* (pp. 110-120): Springer.

Krone, T., 2005. High tech crime brief. *Australian Institute of Criminology, Canberra, Australia, ISSN*, 3413, 2005.

Kshetri, N., 2019. Cybercrime and Cybersecurity in Africa: Taylor & Francis.

Kumar, R., Dhanpathi, H., Basu, S., Rubello, D., Fanti, S. and Alavi, A., 2008. Oncologic PET tracers beyond [^ sup 18^ F] FDG and the novel quantitative approaches in PET imaging. *The Quarterly Journal of Nuclear Medicine and Molecular Imaging*, 52 (1), 50.

Kvale, S., 1994. Ten standard objections to qualitative research interviews. *Journal of phenomenological psychology*, 25 (2), 147-173.

Lachaud, E., 2020. ISO/IEC 27701: Threats and opportunities for GDPR certification. *Available at SSRN*.

LaFond, A. and Brown, L., 2003. A guide to monitoring and evaluation of capacity building interventions in the health sector in developing countries.

Lawler , E. E., 1986. *High-Involvement Management. Participative Strategies for Improving Organizational Performance*. ERIC.

Lewis, J. A. and Timlin, K., 2011. *Cybersecurity and cyberwarfare: Preliminary assessment of national doctrine and organization*. UNIDIR.

Libicki, M. C., 2011. The strategic uses of ambiguity in cyberspace. *Military and Strategic Affairs*, 3 (3), 3-10.

libyaobserver, 2016. *Hakers attack libya's civil registry database* [Available from: https://www.libyaobserver.ly/tech/hackers-attack-libyas-civil-registry-database [Accessed 20-02-2017].

Lincoln, Y. S. and Guba, E. G., 1985. *Naturalistic inquiry*. Vol. 75. Sage.

Luiijf, E. and Klaver, M., 2019. Resilience approach to critical information infrastructures. *Critical Infrastructure Security and Resilience.* Springer, 3-16.

Luiijf, H. and van Schie, T., 2017. A Good Practice Guide on Critical Infor-mation Infrastructure Protection. *European CIIP Newsletter, march-june, 1, 11, 21-22*.

Luiijf, H., van Schie, T., van Ruijven, T. and Huistra, A., 2016. The GFCE-MERIDIAN good practice guide on critical information infrastructure protection for governmental policy-makers.

Lutz, F. W., 1981. Ethnography: The holistic approach to understanding schooling. *Ethnography and language in educational settings*, 51-63.

MacColl, I., Cooper, R., Rittenbruch, M. and Viller, S., 2005. Watching ourselves watching: ethical issues in ethnographic action research. *Proceedings of the 17th Australia conference on Computer-Human Interaction: Citizens Online: Considerations for Today and the Future*, Canberra, Australia. 1108447: Computer-Human Interaction Special Interest Group (CHISIG) of Australia. 1-4.

Mack, L., 2010. The philosophical underpinnings of educational research.

Mackay, R. and Horton, D., 2002. *Capacity Development Planning, Monitoring, and Evaluation: Results of an Evaluation*.

Manz, C. C. and Stewart, G. L., 1997. Attaining flexible stability by integrating total quality management and socio-technical systems theory. *Organization Science*, 8 (1), 59-70.

Marshall, B., Cardon, P., Poddar, A. and Fontenot, R., 2013. Does sample size matter in qualitative research?: A review of qualitative interviews in IS research. *Journal of Computer Information Systems*, 54 (1), 11-22.

Matania, E., Yoffe, L. and Goldstein, T., 2017. Structuring the national cyber defence: in evolution towards a Central Cyber Authority. *Journal of Cyber Policy*, 2 (1), 16-25.

Matsubara, M., 2014. Countering Cyber-Espionage and Sabotage: The Next Steps for Japanese–UK Cyber-Security Co-operation. *The RUSI Journal*, 159 (1), 86-93.

Mattioli, R. and Levy-Bencheton, C., 2014. Methodologies for the identification of Critical Information Infrastructure assets and services. *ENISA Report*.

McCusker, K. and Gunaydin, S., 2015. Research using qualitative, quantitative or mixed methods and choice based on the research. *Perfusion*, 30 (7), 537-542 536p.

McGettrick, A., 2013. Toward effective cybersecurity education. *IEEE Security & Privacy*, 11 (6), 66-68.

McGettrick, A., Cassel, L. N., Dark, M., Hawthorne, E. K. and Impagliazzo, J., 2014. Toward curricular guidelines for cybersecurity, *Proceedings of the 45th ACM technical symposium on Computer science education* (pp. 81-82).

MCIT, 2013. *Egypt ICT Strategy 2012-2017* [online]. Available from: http://www.mcit.gov.eg/Publication/Publication_Summary/660/ICT_ [Accessed

Michie, S., Van Stralen, M. M. and West, R., 2011. The behaviour change wheel: a new method for characterising and designing behaviour change interventions. *Implementation science*, 6 (1), 42.

Microsoft, 2016. *Microsoft Security Intelligence Report* [online]. Available from: https://www.microsoft.com/security/sir/default.aspx [Accessed 30-05-2017].

Minnameier, G., 2010. The logicality of abduction, deduction, and induction, *Ideas in action: Proceedings of the applying peirce conference* (pp. 239-251): Nordic Pragmatism Network Helsinki.

Miron, W. and Muita, K., 2014. Cybersecurity capability maturity models for providers of critical infrastructure. *Technology Innovation Management Review*, 4 (10), 33.

Moftah, A., Sheikh Abdullah, S. N. H. and Hawedi, H. S., 2012. CHALLENGES OF SECURITY, PROTECTION AND TRUST ON E-COMMERCE: A CASE OF ONLINE PURCHASING IN LIBYA. *International Journal of Advanced Research in Computer and Communication Engineering*, 1 ( 3), Moftah, AbdulghaderSheikh Abdullah, Siti Norul HudaHawedi, Hadya.S.

Mohamed and Abdulmajid H, 2017. E-Government as a Tool for Stability and Socio-Economic development in Post-Conflict Libya. *African Journal of information systems*.

MTMC, 2016. *2016-2019 National Cyber Security Strateg* [online]. Ministry of Transportation, Maritime and Communication Available from: http://www.udhb.gov.tr/doc/siberg/UlusalSibereng.pdf [Accessed 15/10/2017].

Muegge, S. and Craigen, D., 2015. A design science approach to construct critical infrastructure and communicate cybersecurity risks. *Technology Innovation Management Review*, 5 (6), 6-16.

Muller, L. P., 2015. Cyber security capacity building in developing countries: challenges and opportunities.

Muniz, J., McIntyre, G. and AlFardan, N., 2015. *Security Operations Center: Building, Operating, and Maintaining Your SOC*. Cisco Press.

Myers, M. D., 1997a. Qualitative research in information systems. *Management Information Systems Quarterly*, 21 (2), 241-242.

Myers, M. D., 1997b. Qualitative Research in Information Systems. *MIS Quarterly*, 21 (2), 241-242.

NCSA, 2013. *National Cybersecurity Authority* [online]. Available from: https://nissa.gov.ly/ [Accessed 16/03/2016

].

NCSC, 2016. *Risk management guidance.* National Cyber Security Centre

NCSC, 2019. *Introduction: Incident Response overview.*

Newhouse, W., Keith, S., Scribner, B. and Witte, G., 2017. National initiative for cybersecurity education (NICE) cybersecurity workforce framework. *NIST Special Publication*, 800, 181.

Newmeyer, K. P., 2015. Elements of national cybersecurity strategy for developing nations. *National Cybersecurity Institute Journal*, 1 (3), 9-19.

NICE, 2016. *NICE Framework, National Institute of Standards and Technology* [online]. Available from: https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework [Accessed 18-11-2019].

NISSA, 2013. *The National Information Security and Safety Authority (NISSA)* [online]. Available from: http://en.nissa.gov.ly/ [Accessed 15/03/2016].

NIST, 2012. *Guide for Conducting Risk Assessments* National Institute of Standards and Technology.

NIST, 2014a. Framework for Improving Critical Infrastructure Cybersecurity. Available from: https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf [Accessed 10/05/2016].

NIST, K. D., 2014b. Risk management framework overview: NIST, FISMA and RMF overview.

Noran, O., 2003. UML vs IDEF: An ontology-based comparative study in view of business modelling, *Proc. 6th In International Conference on Enterprise Information Systems, Porto, Portugal* (Vol. 3, pp. 674-682).

Obama, B., 2013. Executive Order—Improving Critical Infrastructure Cybersecurity.[Online] The White House, February 12, 2013.

Obama, B., 2015. Proclamation 9357--Critical Infrastructure Security and Resilience Month, 2015. *Daily Compilation of Presidential Documents*, 1-2.

OECD, 2015. Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document. Available from: http://dx.doi.org/10.1787/9789264245471-en [Accessed 18/05/2016].

Olesen, V., 1994. Feminisms and models of qualitative research. *Handbook of qualitative research*, 158, 174.

Oltramari, A., Ben-Asher, N., Cranor, L., Bauer, L. and Christin, N., 2014. General requirements of a hybrid-modeling framework for cyber security, *2014 IEEE Military Communications Conference* (pp. 129-135): IEEE.

Onwuegbuzie, A. J. and Byers, V. T., 2014. An exemplar for combining the collection, analysis, and interpretations of verbal and nonverbal data in qualitative research. *International Journal of Education*, 6 (1), 183.

Ormrod, D. and Turnbull, B., 2016. The cyber conceptual framework for developing military doctrine. *Defence Studies*, 16 (3), 270-298.

Othman, A., Pislaru, C., Kenan, T. and Impes, A., 2013. Analysing the effectiveness of IT strategy in Libyan higher education institutes. *International Journal of Digital Information and Wireless Communications (IJDIWC)*, 3 (3), 114-129.

Ozanne, J. L. and Hudson, L. A., 1989. Exploring diversity in consumer research. *ACR Special Volumes*.

Pahl, N. and Richter, A., 2007. SWOT Analysis. Idea, Methodology And A Practical Approach.

Passeri, P., 2017. *Cyber Attacks Statistics* [online]. Available from: http://www.hackmageddon.com/category/security/cyber-attacks-statistics/ [Accessed 28/08/2017].

Patton, M. Q., 1990. *Qualitative evaluation and research methods*. SAGE Publications, inc.

Paul Nicholas and Kaja Ciglic, 2017. *Building an effective national cybersecurity agency*. United State: Microsoft Corporation.

Pawlak, Patryk Barmpaliou and Panagiota-Nayia, 2017. Politics of cybersecurity capacity building: conundrum and opportunity. *Journal of Cyber Policy*, 2 (1), 123-144.

Pawlak, P., 2014. *Riding the Digital Wave: The impact of cyber capacity building on human development*. EU Institute for Security Studies.

Pawlak, P., 2016. Capacity building in cyberspace as an instrument of foreign policy. *Global Policy*, 7 (1), 83-92.

Pernik, P., Wojtkowiak, J. and Verschoor-Kirss, A., 2016. National cyber security organisation: United States. *NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia*.

Petter, S., Khazanchi, D. and Murphy, J. D., 2010. A design science based evaluation framework for patterns. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, 41 (3), 9-26.

Peursum, L., 2015. *The building blocks for a cyber security strategy.*

Pinsonneault, A. and Kraemer, K., 1993. Survey research methodology in management information systems: an assessment. *Journal of management information systems*, 10 (2), 75-105.

Prichard, J. J. and MacDonald, L. E., 2004. Cyber Terrorism: A Study of the Extent of Coverage in Computer Science Textbooks. *Journal of Information Technology Education: Research*, 3, 279-289.

Purdy, G., 2010. ISO 31000: 2009—setting a new standard for risk management. *Risk Analysis: An International Journal*, 30 (6), 881-886.

Razzaq, A., Latif, K., Ahmad, H. F., Hur, A., Anwar, Z. and Bloodsworth, P. C., 2014. Semantic security against web application attacks. *Information Sciences*, 254, 19-38.

Remenyi, D. and Williams, B., 1998. *Doing research in business and management: an introduction to process and method*. Sage.

Richardson, C., 2012. Bridging the air gap : an information assurance perspective: University of Southampton.

Roman, R., Alcaraz, C. and Lopez, J., 2007. The role of wireless sensor networks in the area of critical information infrastructure protection. *Information Security Technical Report*, 12 (1), 24-31.

Rotenberg, M. and Jacobs, D., 2013. Updating the law of information privacy: the new framework of the European Union. *Harv. JL & Pub. Pol'y*, 36, 605.

Ruona, W. E., 2005. Analyzing qualitative data. *Research in organizations: Foundations and methods of inquiry*, 223, 263.

Sabillon, R., Cavaller, V. and Cano, J., 2016. National Cyber Security Strategies: Global Trends in Cyberspace.

Sahyoun, K., 2015. *Cyber jihad and cyber terrorism: A real threat to governments* [online]. SyndiGate Media Inc. Available from: http://search.ebscohost.com/login.aspx?direct=true&db=edsgin&AN=edsgcl.416951066&site=eds-live&scope=site [Accessed

Samarati, M., 2017. Cyber crime cost UK businesses £29 billion in 2016. Available from: https://www.itgovernance.co.uk/blog/2016-cyber-security-breaches-cost-uk-businesses-almost-30-billion/ [Accessed 23/08/2017].

Saunders, M., Lewis, P. and Thornhill, A., 2009. *Research methods for business students*. Fifth edition. edition.: Harlow : Financial Times Prentice Hall,2009.

Scarfone, K., Benigni, D. and Grance, T., 2008. Cyber security standards. *Wiley Handbook of Science and Technology for Homeland Security*, 1-10.

Schell, C., 1992. The value of the case study as a research strategy. *Manchester Business School*, 2, 1-15.

Schjolberg, S. and Ghernaouti-Helie, S., 2011. A global treaty on cybersecurity and cybercrime. *Cybercrime Law*, 97.

Schware, R., 2005. *E-development: From excitement to effectiveness*. The World Bank.

SE-Institute, 2017. *Skills Needed When Staffing Your CSIRT*. Software -Engineering -Institute

Segura-Serrano, A., 2015. *Cybersecurity: Protection of Critical Information Infrastructures and Operators' Obligations*. Vol. 6.

Segura Serrano, A., 2015. Cybersecurity: towards a global standard in the protection of critical information infrastructures. *European Journal of Law and Technology*, 6 (3).

Seuring, S. and Müller, M., 2008. From a literature review to a conceptual framework for sustainable supply chain management. *Journal of cleaner production*, 16 (15), 1699-1710.

Shackelford, S. J., Proia, A. A., Martell, B. and Craig, A. N., 2015. Toward a Global Cybersecurity Standard of Care: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices. *Tex. Int'l LJ*, 50, 305.

Shafqat, N. and Masood, A., 2016. Comparative Analysis of Various National Cyber Security Strategies. *International Journal of Computer Science and Information Security*, 14 (1), 129.

Shahabadkar, P., 2012. Deployment of interpretive structural modelling methodology in supply chain management–an overview. *International Journal of Industrial Engineering & Production Research*, 23 (3), 195-205.

Shashi, J., 2016. *State, Society and National Security: Challenges and Opportunities in the 21st Century*. World Scientific.

Sims, J. W., 2011. *Cybersecurity: The Next Threat to National Security*. MARINE CORPS COMMAND AND STAFF COLL QUANTICO VA.

Singer , P. W. and Friedman, A., 2014. *Cybersecurity and cyberwar: what everyone needs to know* [online]. Available from: https://news.asis.io/sites/default/files/Cybersecurity_and_Cyberwar.pdf [Accessed 19 Apr 2016].

Smith, W., 2019. A Comprehensive Cybersecurity Defense Framework for Large Organizations.

Sperber, A. D., 2004. Translation and validation of study instruments for cross-cultural research. *Gastroenterology*, 126, S124-S128.

Stentoft Arlbjørn, J. and Halldorsson, A., 2002. Logistics knowledge creation: reflections on content, context and processes. *International journal of physical distribution & logistics management*, 32 (1), 22-40.

Stewart, D. W., Shamdasani, P. N. and Rook, D. W., 1990. Focus groups: Theory and practice. Applied social research methods series. *Focus groups: theory and practice applied social research methods series*.

Strachan and Anna, 2017. *Factors affecting success or failure of political transitions*. K4D Helpdesk Report. Brighton, UK: Institute of Development Studies.

Straub, D. W., 1989. Validating instruments in MIS research. *MIS quarterly*, 147-169.

Strauss, A. and Corbin, J., 1998. Basic of Qualitative Research; Technique and Procedures for Grounded Theory". Sage Publication.

Strauss, A. and Corbin, J. M., 1997. *Grounded theory in practice*. Sage.

Strauss, A. L., 1987. *Qualitative analysis for social scientists*. Cambridge University Press.

Švábenský, V., Vykopal, J. and Čeleda, P., 2020. What Are Cybersecurity Education Papers About? A Systematic Literature Review of SIGCSE and ITiCSE Conferences, *Proceedings of the 51st ACM Technical Symposium on Computer Science Education* (pp. 2-8).

Svennevig, J., 2001. Abduction as a methodological approach to the study of spoken interaction. *Norskrift*, 103, 1-22.

Symantec, 2016. *Cyber crime and cyber security trends in Africa Report*. Symantec.

Symantec, 2017. Petya ransomware outbreak: Here's what you need to know. Available from: https://www.symantec.com/connect/blogs/petya-ransomware-outbreak-here-s-what-you-need-know [Accessed 12/07/2017].

Tagert, A. C., 2010. Cybersecurity challenges in developing nations.

Tikk, E., 2011. Ten rules for cyber security. *Survival*, 53 (3), 119-132.

Tong, A., Sainsbury, P. and Craig, J., 2007. Consolidated criteria for reporting qualitative research (COREQ): a 32-item checklist for interviews and focus groups. *International journal for quality in health care*, 19 (6), 349-357.

Tongco, M. D. C., 2007. Purposive sampling as a tool for informant selection. *Ethnobotany Research and applications*, 5, 147-158.

Trimintzios, P., 2017. Cybersecurity in the EU Common Security and Defence Policy (CSDP). *Challenges and risks for the EU. Brussels: Scientific Foresight Unit (STOA), European Parliamentary Research Service, European Parliament*.

Trist, E., 1981. The socio-technical perspective: The evolution of socio-technical systems as a conceptual framework and as an action research paradigm: New York: Wiley & Sons.

Tsironis, L., Gentsos, A. and Moustakis, V., 2008. Empowerment the IDEF0 modeling language. *International Journal of Business and Management*, 3 (5), 109-118.

UK-CERT, 2015. Cyber-security Information Sharing Partnership (CiSP).

Ullman, R. H., 1983. Redefining security. *International security*, 8 (1), 129-153.

United-Nations, 2018. *Capacity-building* [online]. Available from: https://academicimpact.un.org/content/capacity-building [Accessed 19-09-2019].

UNODC, 2019. *Legal Frameworks and Human Rights, the role of cybercrime law.*

US-CERT, 2016. *Cyber Resilience Review (CRR)*.

Vaismoradi, M., Jones, J., Turunen, H. and Snelgrove, S., 2016. Theme development in qualitative content analysis and thematic analysis.

Vaismoradi, M., Turunen, H. and Bondas, T., 2013. Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study. *Nursing & health sciences*, 15 (3), 398-405.

Von Solms, R. and Van Niekerk, J., 2013. From information security to cyber security. *computers & security*, 38, 97-102.

Wahyuni, D., 2012. The research design maze: Understanding paradigms, cases, methods and methodologies.

Walker, R., 1981. On the uses of fiction in educational research. *Practising Evaluation, Driffield: Nafferton*.

Walsham, G., 1995. The emergence of interpretivism in IS research. *Information systems research*, 6 (4), 376-394.

Ward, J., Dogan, H., Apeh, E., Mylonas, A. and Katos, V., 2017. Using Human Factor Approaches to an Organisation's Bring Your Own Device scheme, *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 396-413): Springer.

Warfield, John N and Cárdenas, A. R., 2002. *A handbook of interactive management*. Iowa State Press.

Warfield, J. N., 1974. Toward interpretation of complex structural models. *IEEE Transactions on Systems, Man, and Cybernetics*, (5), 405-417.

Warfield, J. N. and Cárdenas, A. R., 2002. *A handbook of interactive management*. Ames: Iowa State University Press.

Weber, A. M., 2003. The Council of Europe's Convention on Cybercrime. *Berkeley technology law journal*, 18 (1), 425-446.

WEF, 2017. *Guidance on Public-Private Information Sharing against Cybercrime*. Geneva, Switzerland: World Economic Forum.

Weforum, W. E. F., 2018. *The Global Risks Report 2018*. Geneva: World Economic ForumGeneva.

Williams, M., 2003. *Making sense of social research*. Sage.

Wilson, C., 2005. Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. CRS Report for Congress. Congressional Research Service-The Library of Congress.

Wilson, M. and Hash, J., 2003. Building an information technology security awareness and training program. *NIST Special publication*, 800 (50), 1-39.

Wong, L. P., 2008. Focus group discussion: a tool for health and medical research. *Singapore Med J*, 49 (3), 256-260.

WorldBank, 2017. *Combatting Cybercrime : Tools and Capacity Building for Emerging Economies*. 1818 H Street, NW, Washington, DC, 20433; USA; : The World Bank, .

Yang, S. C. and Wen, B., 2017. Toward a cybersecurity curriculum model for undergraduate business schools: A survey of AACSB-accredited institutions in the United States. *Journal of Education for Business*, 92 (1), 1-8.

Yates, P. D., 1987. Figure and section: Ethnography and education in the multicultural state. *Interpretive Ethnography of Education: at home and abroad*.

Yin, R. K., 2004. *CASE STUDY METHODS* [online]. 2004. Available from: http://www.cosmoscorp.com/Docs/AERAdraft.pdf [Accessed 10/05/2016].

Zager, R. Z., John, 2017. OODA loops in cyberspace: A new cyber-defense model. *Journal Article| October*, 20 (11), 33pm.

Zareen, M. S., Akhlaq, M., Tariq, M. and Khalid, U., 2013. Cyber security challenges and wayforward for developing countries, *2013 2nd National Conference on Information Assurance (NCIA)* (pp. 7-14): IEEE.

# 10. Appendices

Appendix (1): Participant Agreement Form to Confirm the Interactive Management workshop and Focus Group Meeting for contextualise the challenges of cybersecurity capacity in Spring Land and assess the its maturity levels.

Full title of project: National Cybersecurity Capacity Building Framework for counties in a Transitional Phase (Using Spring Land as a case study).

Name, position and contact details of researcher: Mohamed Ben Naseir, PhD Researcher, Bournemouth University.

Name, position and contact details of supervisor Dr. Huseyin Dogan, Dr. Edward Apeh and Professor Raian Ali

Please Initial or Tick Here

| | |
|---|---|
| I have read and understood the participant information sheet for the above research project. | |
| I confirm that I have had the opportunity to ask questions. | |
| I understand that my participation is voluntary. | |
| I understand that I am free to withdraw up to the point where the data is processed and become anonymous, so my identity cannot be determined. | |

| | |
|---|---|
| During the interview, I am free to withdraw without giving reason and without there being any negative consequences. | |
| Should I not wish to answer any particular question(s), I am free to decline | |
| I give permission for members of the research team to have access to my anonymised responses. I understand that my name will not be linked with the research materials, and I will not be identified or identifiable in the outputs that result from the research.<br>I give permission for members of the research team to use my identifiable information for the purposes of this research project. | |
| I agree to the audio recording that will be taken as part of the interview. | |
| I agree to take part in the above research project. | |

Name of Participant Date Signature

_____ _____ _____

Name of Researcher Date Signature……

*This form should be signed and dated by all parties after the participant receives a copy of the participant information sheet and any other written information provided to the participants. A copy of the signed and dated participant agreement form should be kept with the project's main documents which must be kept in a secure location.*

Appendix (2): Interviewer details

1- Name:

2- Contact details

3- Under which category does your organisation belong?

Public ☐ Private ☐

4- Under which sector does your organisation belong?

5- Describe your position in your organisation?

6- How long have you worked in field of information and Cybersecurity?

Appendix (3): Multi-Dimensional National Cybersecurity Question Set and Results of the Spring Land Security Posture

| Dimensions | Rational for Indicator Selection (Awareness & Assessment) |
|---|---|

| | |
|---|---|
| D1 Cyber security policy and strategy | What is our current national strategy for cyber security?<br><br>Who is driving Cyber Security in the Libyan Homeland Security program? [1]<br><br>Are there any national incident response plans?<br><br>Who is in charge of IM?<br><br>Is there a coordination mechanism for incident response at the national level? [2]<br><br>Are the critical national infrastructures defined?<br><br>Is risk analysis used to determine potential threat impact to the national critical infrastructure?<br>Can you ID any crisis management activities standards and/or guidelines?<br><br>Have any been identified and implemented at the national level?<br><br>Is there an existing framework for managing cyber defence at the national level?<br><br>Is there a plan to organise assured system redundancy and communications among stakeholders?<br>Can you ID any crisis management activities standards and/or guidelines?<br><br>Have any been identified and implemented at the national level?<br><br>Is there an existing framework for managing cyber defence at the national level?<br><br>Is there a plan to organise assured system redundancy and communications among stakeholders? |

| | |
|---|---|
| D2 Cyber culture and society | Are we conducting cyber security awareness activities for the critical services? How?<br><br>What are the cybersecurity issues currently been addressed and what is the degree of importance of each issue?<br><br>Are there any standard, policies and security measures to promote trust in e-services<br><br>Is there legislation or regulations detailing privacy protection? |
| D3 Cyber security education, training and skills | Are training needs been identified at a national level?<br><br>Is there any education strategy to develop our Cybersecurity skills?<br><br>Is there an adequate budget allocation?<br><br>Is there a continuous training plan for our skills development?<br><br>Do Enterprise Boards and their executives within private and state-owned companies understand the Spring Land cybersecurity issues? |
| D4 Legal and regulatory frameworks | Is there any cyber related legislation or regulation?<br><br>What does the content of the regulation aim to achieve?<br><br>How do we respond to challenges of anonymity and attribution?<br><br>Do we differentiate the sets of rules to protect systems and<br>data types<br>Critical Infrastructure<br>Proprietary<br>Information<br>Personal<br>Data<br><br>Do we have a problem of jurisdictional fragmentation? |

| | |
|---|---|
| D5 Standards, organisations, and technologies | Are there any existing standards and practices do you adhere to?<br><br>Do we have a Cyber Security Standards at the national level for:<br>Government Agencies<br>Industries<br>Citizens<br><br>Is our national Infrastructure Technology effectively managed, monitored and evaluated based on international standard?<br><br>Do we have any insurance practises or third party mitigation? |

Appendix (4): Transcription of focus group discussion

1- Cybersecurity policy and strategy Indicators

| | |
|---|---|
| What is our current national strategy for Cybersecurity? | In 2016, a general strategy was adopted for the work of the National Authority for Information Security and Safety. The first objective was to build a national framework for cybersecurity and we have made great strides at the strategic level and technical level. Currently we are at the operational level and expectations during the year, the strategy will be ready .The work plan was divided into several stages: The study and the stages of consultation, both internal and external, and working with all stakeholders directly and indirectly targeted at all citizens levels of public and private sectors.<br>We have classified all of the major sectors such as the banking sector, and we used for that the Central Bank of Spring Land, as a direct stakeholder and a coordinator for the banking sector in Spring Land as a whole. We also identified the General Authority for Communications and Information as it is an incubator of the main sector. As a whole, you can say that we have taken into account the organized sector of all parties. After that, the proposals will be taken from all parties, whether directly or indirectly. We will provide the strategy at the local level in the Arab countries and the international level in several international organizations. You can say we are in the START UP level<br>INT: Who are the direct and indirect actors? Is it possible to get a copy of these bodies?<br>For example: the direct is: the Council of the Prime Minister and currently involved in the government of reconciliation<br>The banking sector is the Central Bank of Spring Land, and this does not prevent the bank from establishing a special sector task force to assist the Commission in studying the strategy. The telecommunications sector is represented by the General Authority for Communications and the Spring Land Holding Company for |

| | |
|---|---|
| | Telecommunications because they are the main regulator for the telecommunications sector. NCSA operates under the General Authority for Communications. We have prepared a proposal for conducting work teams in all the telecommunications bodies and administrations to help us write the strategy and participate directly from some sectors to formulate and write strategy<br>Another part is workshops to get suggestions and feedback from a particular sector. And for the energy and water (the National Oil Corporation, the General Company for Electricity and Water which come from the source called the industrial river project) and the rest of the government sectors and part of the tasks of the draft strategy to identify the remaining sectors that can be extracted in a stage of the stages, for example, the health sector in Spring Land is now depends on the paper system, and we will do a survey and examine these sectors to find out and that they can provide us with their opinions and, of course, their feedback is necessary as a strategic project.<br>The private sector has been contacted with several civil society organizations including the Spring Land Internet Society, the Technical Society and some other civil bodies, but the country's security situation and political conditions affected their interaction with the authorities especially after 2014, where they were actively involved in reviewing the laws with government agencies and providing advice, but work was getting less dramatically. We have a security, military and intelligence sector that will have a direct role in writing the strategy. There is another part that has not been decided yet, is the proposed strategy to be the general security sector, the military, the intelligence, the civil or the work of a sub under our supervision, so it is a strategy for the security and military sector and a strategy for the civil bodies. The subject is still complex and decision is not taken yet, there are some differences because we are still in the data collection phase. This point is |

| | |
|---|---|
| | postponed it to the next stage but you might be able to help us through the research you are working on and help us with your point of view. |
| Who is driving Cybersecurity in the Spring Land National security program? | NCSA leads the security of information and cybersecurity in Spring Land and there is no body or group related to cybersecurity in Spring Land, and the Authority has a decision to establish from the prime minister, it has the mandate of the Spring Land state at the international and regional level. But some sectors have no idea or awareness of dealing with this body In general we can say that we are in a strategic level with lack of financial support because of the political situation, it can be said that we are in a strategic level, but there is a weakness stopping all projects of the organisation. We need a higher status of cybersecurity. |
| Are there any national incident response plans? Who is in charge of IM? | There is a clear plan, but we are still in the process of gathering information and not doing the actual work. In general, the focus of the strategy will be to raise the level of awareness and the establishment of the network of relations for the exchange of information between the main sectors through the plan to respond to events at the level of the state and between the sectors will be the outline of the strategy and the proposed timetable between 3 and 5 years, and it will be updated after the proposed period, and building up the Spring Land state's public and private institutions will and linked to the course and a general emergency response plan will be set up for the Spring Land state in full and will include everyone with the specification of the security sectors. The security and military sectors will be involved and take their security point of view, but cooperation at the moment is quite difficult due to lack of awareness and differences of opinion and mentality.<br>We have meetings with some security agencies such as intelligence office, so that the strategy is general and the details do not belong to anyone and that the constitutional declaration of the state is the reference to write strategy We have a general strategy of the state |

| | |
|---|---|
| | and a specific strategy for each sector such as the banking sector is different from other sectors as its priority is to protect the citizens data from the financial aspect, reversing the state strategy that is focused on raising awareness, especially in cybersecurity, and a strategy for each sector will be established after the completion of the overall strategy<br>Director of Spring Land-CERT, We, currently, have a strategy of response at the level of the authority, but at the level of the state does not exist, and it is one of the objectives of the organisation, so we can say that we are in the start up stage, but because of the lack of a strategy of the state, it cannot be employed to other parties.<br>Director of the awareness department: through meetings with all sectors, we found a difference in the structures, some have an information security unit and some others do not have, the only party is the Central Bank of Spring Land that has a special department on this thing, and its future leaders is the unification of the establishment of state institutions in relation to cybersecurity and administrative organization and to formulate the strategy to find who is implementing it.<br>The Authority pays a great deal to set up a CERT team in each side to communicate with the authority directly to avoid administrative complications.<br>Director of CERT, In general, we have a national accreditation to represent the Spring Land in the world, but there is no national plan, and also, the communication channel between the sectors is very weak due to the fear of dealing with each other for several reasons; including obstruction of administrative procedures suffer from lack of information sharing between all sectors, political orientations and poor awareness. As an organization we are in a strategic level, Moreover, Spring Land is a member of several international organizations such as the Organisation of The Islamic Cooperation – Computer Emergency Response Teams (OIC-CERT); Africa |

| | |
|---|---|
| | CERT; and has pan to get a membership in the global Forum of Incident Response and Security Teams (FIRST) by 2019. Furthermore, NCSA had a good corporation with Oman-CERT and Tunisia – CERT. |
| Is there a coordination mechanism for incident response at the national level? | There are some international work carried out by the Centre and we participated in the response and find solutions on a global level and there are reports with this regard, but at the national level, cooperation is weak, for example when you want to solve a problem within the state, there are complex and long procedures, for example we received a message from the State of Brazil because we are a member of OIC- CERT IN Malaysia and we were informed through it, we dealt with this matter and found a source of cyber-attack from an institution in Spring Land whose server was exploited as a source of phishing, and another example is a communication from the bank of America that there is a source of cyber-attack from inside an institution in Spring Land, and we dealt with it and solved.<br>We can say generally that the international cooperation is high, due to the existence of international concerns to cyber risks, but at the national level, it is weak and cooperation is based on the personal relations between the authority and some other government sectors. Some incidents have been solved and dealt with by the cert team within Spring Land as well.<br>For example, LTT was hacked and subscribers' databases were hacked and published. The authority had a major role in dealing with this event, conducting RISK ASSESMENT analysis and detecting the gaps in their E-CARE SYSTEM, and Huawei was informed of the gaps.<br>We have a plan in place, headed by the director of the CERT centre, the authority will become a member of the FIRST organization from the beginning of 2019 through an invitation from Africa Cert and the Organization of Islamic Cooperation.<br>In general, international cooperation is much better than local |

| | |
|---|---|
| | cooperation. |
| Are the critical national infrastructures defined? | Head of internal auditor office: In the aspect of Critical National Infrastructure (CNI) Protection, Spring Land is extremely in low scale and the government has not issued a list of (CNI). In general, the physical security has a negative impact on CNI and there no clear processes to reveal who is in charge of protect all sectors, except the telecommunication sector. Here, there is a point, what do you mean by Critical national infrastructure?<br>Spring Land has the problem that our communications are advanced, and at the same it is not. On the one hand, advanced in the Spring Land state<br>The telecommunications critical infrastructures is good and even its protection is fairly good because it is supervised by some important companies such as Spring Land, Al-Madar and LTT. On the other hand, the other sectors, which have electricity and water, are isolated network so if there will be a risk, it would be internal, and there won't be an external risk.<br>In general, there is no provision or classification, and we seek to do it after the formulating a strategy and identifying and assessing risks.<br>National strategy for risk assessment is currently unavailable and are not specified or rated, For example, in a certain period, specifically in the project of the Artificial River, we tried to do a similar thing, but there were not an awareness of the dangers of the Internet risks. This was in the previous regime.<br>And finally, we tried to be more focused, and people are busy with workshops on SCADA security, and the authority gives some lectures on awareness of the subject of SCADA security. Then, The answer was unexpected, they told us that SCADA system is off for a year or more, because all the links and points of connection in Spring Land were stolen, thinking that they were copper wires to sell them. |

| | |
|---|---|
| | In general, the physical security is very impressive, so there is no a view. The one I mentioned earlier the property of the sovereign systems backbone of Spring Land and the connections that are happening from the physical aspect, who is protecting them? I can say frankly that you can access the vital centres easily, because of the fact that it is supervised and leaded by untrained and not qualified people, and they have not got the sense of responsibility in terms of security and awareness, and they can be penetrated and you can enter using fake cards or a valid card and you can access and reach to the system and control it. For example, and the telecommunications sector, which is considered as the most important one, because they are considered as the main communications of the state, but with a little social engineering, you can find yourself inside the CERT or the sector.<br>But there is a considerable interest within the telecommunications sector in the field of physical security to protect Spring Land's telecommunications infrastructure. But at the level of the state, we are in a start-up level. Director of Spring Land-CERT. |
| Is risk analysis used to determine potential threat impact to the national critical infrastructure? | There is no national framework for analysing and identifying risks and threats, we could say that we are still in the start-up-level. |
| Can you ID any crisis management activities standards and/or guidelines? | Currently, Crisis management is not related to the National authority for information security and safety. There are currently efforts to establish a centre, and we are working on it. The proposal is submitted to the Prime Ministers Council to build a homeland crisis centre (National Crisis Management Centre). This centre will use all the details of the issue of crisis management. It is possible to show you the proposal after we finish this workshop.<br>This proposal was approved by the president and is supposed to be |

| | |
|---|---|
| | issued in two or three months and the decision will be made about the centre and start work. But it is not in the tasks of NCSA.<br>There is a plan, which in fact come out from the authority and we noticed its importance. But it is not in the establishing decision, and its subject is overlapped with many parties. We provided advice to some parties, so that they build an authority in Spring Land interested in this major and the plan covers all aspects, including cybersecurity in cooperation with the Crisis Management Centre at the Arab University. We can say we are in START-UP LEVEL. |
| Have any been identified and implemented at the national level? | There are some strategies to assess the current situation, but of course, now we are providing logistical support to the proposed crisis management centre and the important needs to get started. We are still in the stage of researching the administrative management and we are researching the subject of its work areas and how it works before we announce it and appear in the strategic work. There is nothing on the ground at the moment, so we can say we are in START-UP LEVEL |
| Is there an existing framework for managing cyber defence at the national level? | With regard to Cyber Defence, there is no national strategy, but there is a sort of high level cooperation between the authority and the Ministry of Defense, and at the personal level of the higher departments or senior leaders in both institutions. But there is no technical or strategic communication or joint workshops as a result of the status of the Ministry of Defense under the current situation and the war. We have a cyber defense plan for the Spring Landstate as a whole, and it has no relation with the army at that stage, later on, the army role will begin. As I told you, we haven't had any cooperation with the Ministry of Defense and the Ministry of Interior, especially the Ministry of Defence because of the situation of the ministry itself and the conflict and problems are happening. And also that it has been long time with no a recognised ministry, so we could not do anything. But we are trying and in the process of thinking in a new vision that it is closer to reality, so we will be |

| | |
|---|---|
| | having the National Operations Centre and merging with SOC. Moreover, there are several countries seemed to be starting heading to this direction. So as a summary, we can consider that CERT and cyber threat intelligence as one centre, and we are in the START-UP LEVEL because we have no defence strategy.. |
| Is there a plan to organise assured system redundancy and communications among stakeholders? | As a part of the authority's strategy is the business continuity plan, but has not yet started work, it means you can say as an existing vision and start simple work as a collection of information and data, but as a service in the project, still not started yet, and it is part of the authority's strategy in 2017/2018, and it will be extended for two years, God willing. It is approved by the Commission and you can have a copy of the establishment decision. So you can say that we are in the START-UP LEVEL.<br>We have held several meetings with some telecom companies to urge them to conduct business continuity recovery in each organization. The main telecommunications companies in Spring Land have responded and will make a plan in 2018 as a result of the awareness and pressure exerted by the Authority in this field and in absolute cooperation.<br>We put forward the idea in principle and coordinated with them that they bring some of the international institutions that have been recommended by the state to help us in terms of complete and best continuity recovery plan. And of course the banking sector and commercial banks and the Central Bank of Spring Land have a business continuity recovery plan, but At the state level, there is not. Originally, e-services in Spring Land is weak, Therefore, how the business continuity plan works. For example, the national authority is acting freely in the telecommunications sector, acting in a way of simple freedom in the banking sector and acting more freely in the oil and gas sector. Thus, every sector we gain trust for a while, but the authority is considered as an umbrella for applying future plans, and we can say that we are in Formative LEVEL |

2- Cyber Culture and Society Indicators

| | |
|---|---|
| Are we conducting Cybersecurity awareness activities for the critical services? How? | Director of the Awareness Department: According to the strategies of the Commission, we are still in the planning stage, and we have two plans for awareness, including the national program to raise awareness of the dangers of information security and in general cybersecurity and it is ready, but there is a lack of financial resources allocated to this area. However, with voluntary initiatives and efforts by the Commission, we have carried out some programs with several parties targeting the general staff to spread the Cybersecurity culture. One of the things that have been focused on is the increase in the use of internet by citizens of all age groups, for example, social networking sites in Spring Land specifically. We have prepared a range of lectures to raise awareness from 8 to 10 different topics such as social networking, cloud computing, information security, Internet stuff, personal computer security, spam, ransom viruses, how the terrorists hide their online activities, privacy protection in the digital community. Some of these lectures are processed in the form of posters and publications written in Arabic. Of course, providing material in Arabic language even on the level of our meeting and participation in some conferences held in cooperation with the Organization of the Islamic Cooperation (OIC). Most of the Arabic countries are having the lack of the providing the awareness materials in Arabic language, Oman is one of them. The Commission has written topics affecting everyday life in the Spring Land community and printing a number of topics. We have contacted many of them, some have agreed and welcomed the idea, and some have rejected the need for that, and pointed IT department to be responsible for awareness, as well as the lack of understanding of the risks and cyber-consequences of decision makers in most institutions. We cooperated extensively with the telecommunications and oil sector such as the Petroleum Training |

| | |
|---|---|
| | Institute and some technical colleges in Tripoli such as Ben Ashour Institute for Electronics, Ghout Al-Shaal Institute, the Technical College of Tripoli University, and the National Number Project, and we have held several programs and events, including participation in the open week program or open month at universities by delivering lectures about awareness for the students.<br>There is an initiative targeting the technical colleges, especially as they do not have specialized departments in this field to graduate specialists in the field of information security, and most of the departments are focusing on computer technologies such as programming and hardware, and there is no explicit interest in information security, and even if there is any, it would just be some educational materials giving an introduction about information security. The initiative's idea is to create an interactive professional relationship between the mentors and students of graduate projects in universities and higher institutes (trainees) in order to guide them to the field of information security and safety in an early stage, and develop their skills to have suitable job opportunities.<br>Some of the lectures were about searching what is information security and what are the main pillars of information security, and this initiative was continued for about two years. The first year was targeted 5 students from the Faculty of Electrical Engineering, University of Tripoli, and the second year from Ghoot Al-Shaal Institute and the Faculty of Information Technology at University of Tripoli due to lack of abilities and the political situation. The commission focused the work in the city of Tripoli with some initiatives and contributions from other areas, but they were very weak. Moreover, The commission used social networking sites such as Facebook to spread awareness.<br>In general, the national awareness project has another part with a 5 to 10 year time frame for the Global Child Protection Program, as well as there are contributions from civil society organizations on |

| | |
|---|---|
| | education and some private companies such as a security company. A summary of the awareness project to be implemented by conducting lectures, workshops and meetings, not only for children but also for children, but for who is looking after them too. The authority is trying to apply international standards from ITU, and we have a written implementation plan to launch the program. We can say that we are in the star-up |
| What are the cybersecurity issues currently been addressed and what is the degree of importance of each issue? | Awareness programs focused on cybersecurity in general, including e-services such as letters to catch on the social network to increase the amount of the withdrawal of bank cards in foreign currency of $ 50, a large number of citizens' bank accounts have been hacked through suspicious and fake pages on the social networks due to lack of awareness. We have focused heavily on catching, spamming and the dangers of Android phone applications, which most of them are fake, such as the Caller ID app "Truecaller", which steals the balance of phone calls by making international calls from the user's phone without his knowledge and the use of mobile phones is a major target of malware attacks, and this a big problem in Spring Land. There was an investigation by a security body in cooperation with the Commission, and the result was discovered that a group of organized crime supported by external parties and for unknown reason, which is likely to be political, especially in Tripoli and the group is targeting certain individuals, and some of these group's members are arrested. Other sources of attacks have been discovered, some institutions have signed beginners because of the low cost to prepare websites for the sectors suffering the design changes and gaps, and lack of awareness of institutions. For example, there is a Spring Land institution that I cannot mention its name due to the confidentiality of the subject has lost millions of dinars, and when they investigated that, that found that there is no log management system (LOG MANGMENT). There are no organisations that have CRITICAL SECURITY CONTROLS, LOG |

| | |
|---|---|
| | AND EVENT MANGMENT, BATCH MANGMENT, and Disaster recovery plans apart from telecommunication companies. Most of the organisations suffer the security by design issues, and the attacks that it suffers from for this reason. The commission has the goal of educating citizens and raising awareness of the IT staff in the institutions because of the lack of skilled ones and the lack of the awareness, and paying attention to information security. Some institutions have huge budgets and rely on commercial programs. They are cracking some programs to save money, which opens several changes to the system. We found that one of the organisation part of botnet after the commission received a report from the Spam House and also some of the institutions of the international community to support Spring Land, they are providing some servers and systems for some institutions free programmer and equipped, but unfortunately, with a lack of knowledge and lack of awareness, it is used and causes the penetration of this institution without notifying, and they monitored several incidents of this kind for the data of the prime minister and the Supreme Commission for Elections in previously, but these problems were overcome and resolved. We can say that there are initiatives, and we are at the start up level. |
| Are there any standard, policies and security measures to promote trust in e-services | The level is very poor, there is no interest in applying international standards and we noticed through the workshops over-persistence in social networking sites such as Facebook. Spring Landsociety, whether technical or ordinary, does not have the awareness of the risks caused by the problem of the high level of trust in sites because of the lack of their awareness and not aware of the risks.<br>Spring Land has been considered as a target of e-hunting, there are hackers inside and outside Spring Land. These hackers are creating fake pages for banks to register your data in foreign exchange services or activation of Visa card services or increasing the withdrawal limit. Most of these people, unfortunately, from within |

| | |
|---|---|
| | the banking institutions in cooperation with people outside Spring Land and the reason there are no public key structure and digital certificates and there is no awareness on this matter. Creating the public key is one of the authority's strategies, but due to the lack of the sources and potential, we have not started yet. Awareness is aiming to focus on citizens, leaders and communication engineers in the sectors.<br>In addition, lack of awareness of information security within institutions. For example, when any organization provides an online service or social media, they are not interested in providing a clear picture to the user or citizen, the most important thing that it has a page on Facebook. The institutions are supposed to educate the user about these things and the authority can participate in that.<br>Another question was asked: Is Spring Land subjected to attacks from other countries, especially you have been addressed the existence of internal and external threats?<br>Yes, some countries use some institutions as a source of botnet. It has been dealt with after receiving communications from a cooperating state, and it is hacked while another penetration of a public entity will not be named because of their contract with a third party to design and implement its own system, which is the same one who penetrated them. We have the state of Nigeria, which is targeting Spring Land a lot, as well as China. In the past, there were two problems and most of the Internet providers in Spring Land are aware of that, and a commission of inquiry has been set up. Also, there was an electronic attack from Egypt, and the purpose of the attack is not known.<br>It is also noted that most of the telecom companies rely on foreign companies as a third party, mostly Chinese, to prepare and supervise all services, and the Spring Landside does not do anything, except X company. There were several violations noticed, and after investigation, it has been found that the Spring Landside does not |

| | |
|---|---|
| | have the ability to manage the records and they only be satisfied for keeping all records with third party. Sources of major threats from major countries such as China, America and Russia.<br>Have you recorded any breakthroughs in the oil sector?<br>Yes, especially ransom viruses. The biggest targeted sectors are oil, banks and telecommunications. We give the example of a bank in Spring Land, according to reports issued by them, exposed to more than 53 attacking attempts from America, it's been found recently that an employee was working in the bank and moved to America and was identified. They communicated with the competent authorities in America. We also have service systems such as the national number system, the civil registry and the passports that provide online service, which suffers from loots of problems in design and hosting data without protection. |
| Is there legislation or regulations detailing privacy protection? | There are only initiatives, but due to the absence of the legislator, because of the political circumstances since year 2014, these laws are not issued. It is not specific about cybercrimes, it is for the electronic transactions include the Electronic Crimes Law in general and not detailed and it is close to the laws are being used in the Arab world. The Ministry of Justice, Spring Land Chamber of Commerce, and the Ministry of Interior concluded that only in the preparation stage. |

3- Cybersecurity education, training and skills Indicators

| | |
|---|---|
| Are training needs been identified at a national level? | There are no plans at the state's level in defining the required educational curricula in cybersecurity. |
| Is there any education strategy to develop our Cybersecurity skills? | There are no plans at the national level in the area of raising the efficiency of education in the field of cybersecurity, part of the of the authority's strategies, but we have not started yet, and we require more cooperation with the Ministry of Education and we noticed that the replies are only from some colleges and |

| | |
|---|---|
| | universities and they use in the teaching some of materials about an introduction to the definition of information security.<br>The topic was discussed with some authorities to prepare detailed curricula in information security and the possibility of opening a new educational department in this field. The topic was discussed with the Dean of the Faculty of Information Technology, as it is known before Ghout Al-Shaal, the idea was welcomed. In an urgent manner to promote cybersecurity at higher institutes. We are in Start-Up level |
| Is there an adequate budget allocation? | There are no financial allocations for it at the state's level |
| Is there a continuous training plan for our skills development? | There are no plans at the level of the state in the field of raising the efficiency of employees in public and private sectors, except some plans from the Authority to prepare a plan to train the staff and try to make it a reference to other parties, but most of the parties are not interested. The authority, participated in some workshops and international cyber drill and several international conference in Tunis, Qatar and the cyberspace evaluation's conference in Amman and attending the annual meetings of the Organization of the Islamic Cooperation (OIC), accompanied by training courses to improve the efficiency of our employees. |
| Do Enterprise Boards and their executives within private and state-owned companies understand the Spring Land cybersecurity issues? | For public sector, telecom operators have an awareness of the seriousness of the subject. Some of them are seeking to issue a strategy for cybersecurity of the company led by some banking sectors, and it is considered In the private sector as a bit better one, but in general, it is not satisfactory in both sectors.The awareness is existing but there are no real initiatives and there is no plan in the field of raising the efficiency of employees in public and private sectors. |

4- Legal and regulatory frameworks Indicators

| | |
|---|---|
| Is there any cyber related legislation or regulation? | There is no legislation or regulation except an initiative to issue Electronic Transaction law and Electronic Crime law. This initiatives are not issued yet due to jurisdictional fragmentation due to political instability |
| What does the content of the regulation aim to achieve? | The e-Commerce Chamber of the Ministry of Economy in cooperation with some specialized companies from Korea prepare a proposal aims generally to issue an electronic crimes law to conduct electronic government transactions and services in cooperation with the authority and the participation of the former committee. Spring Land has signed on an international protocol for child with the Internet |
| How do we respond to challenges of anonymity and attribution? | There is an electronic crimes unit in the Ministry of the Interior that deals with this type of crimes by applying other laws relating to that. |
| Do we differentiate the sets of rules to protect systems and data types<br>• Critical Infrastructure<br>• Proprietary Information<br>• Personal Data | There is no laws related to protect systems and data |
| Do we have a problem of jurisdictional fragmentation? | Yes, due to the political conflict, as we mentioned earlier. We can say we are still in a start-up level. |

5- Standards, organisations, and technologies Indicators

| | |
|---|---|
| Are there any existing standards and practices do you adhere to? | There is an attempt to start the project of implementing international standards, but we have a lack of the resources and expertise in the public and private sectors, as well as the issues related to evaluation, which is problematic for the two sectors, but the Authority is seeking to qualify experts in this field and to grant licenses to some private entities by the Authority to |

| | |
|---|---|
| | provide this service with the established policies. |
| Do we have a Cybersecurity Standards at the national level for:<br>• Government Agencies<br>• Industries<br>**1.Chapter 1** C itizens | There is no national framework or organisation to monitor the adaption of international standards. There is only an acceptable cooperation between some of the major sectors, such as petroleum, telecommunications, and banking. |
| Is our national Infrastructure Technology effectively managed, monitored and evaluated based on international standard? | Currently, there is no any organization, but there is some future plans of the authority. There is a lack of research centres in this field. However, there is a research centre that is not directly specialized in cybersecurity. It is preparing a technical research related to e-commerce, communication and information infrastructure related to the open market to be established in Benghazi city. In fact, there was a communication with the authority to participate in the preparation of the strategy, but due to the security and political situation, they stopped these attempts. |
| Do we have any insurance practises or third party mitigation? | There is a vision from the Authority for the participation of the private sector in this major, but unfortunately, even the private sector suffers from a lack of expertise, and it is not one of the authority priorities at the present time. |

**Appendix 5** the Mechanisms and controls template analysis for dimensions (2,3,4,and 5) of the NCCBF

1. Mechanisms and controls template analysis for Dimension 2.

| Mechanism ID | Rational | Control ID | Reference and Access |
|---|---|---|---|
| M2.1.1 Behaviours change | To influence the adoption of secure behaviour online. | **C2.1.1** Behavior Change Techniques ( behavior change wheel) | Behaviors change wheel (Michie et al. 2011), open source |
| M2.1.2 Cybersecurity awareness-raising campaigns | To help the country in achieving cybersecurity goals. | **C2.1.2** Guiding principles ( Outcome focused- Prioritised- Identify target group | (https://pdfs.semanticscholar.org/9ea6/28ec868e9c3347b0ff93cf61e5453e74ada0.pdf) ( RAND Europe analysis) (https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/2015%20OAS%20-%20Cyber%20Security%20Awareness%20Campaign%20Toolkit%20%28English%29.pdf) |
| **M2.1.3** Promote information sharing | To reduce the threats and vulnerabilities of cyber space. | **C2.1.3** Reporting mechanisms framework. | Good practice study Cybercrime reporting mechanisms (GLACY 2014). |
| **M2.1.4** Organise a national cyber-security month, week or day | To engage the public, and private- through events and initiatives | **C2.1.4** Provide a sufficient budget and human resources | Global awareness raising campaign, STOP.THINK.CONNEC, US National Cyber Security Awareness Month |

| | | | |
|---|---|---|---|
| | | | (NCSAM), open sources |
| **M2.2.1** Develop a strategic plan for e-government | To implement e-government effectively. | **C2.2.1**Governance, infrastructure, policy and outreach | World bank (Schware 2005), (infoDevWorldBank 2009), open source |
| **M2.2.2** Launch and continuously develop government e-services | To deliver the best online services for people. | **C2.2.1** Embed the application of security measures in their design and running | (infoDevWorldBank 2009), open source |
| **M2.2.3** Develop national privacy framework | To protect information and personal data. | **C2.2.2** Privacy framework | ISO/IEC 27701:2019 (Lachaud 2020), OECD. 2013. The OECD Privacy Framework. Paris: OECD, General Data Protection Regulation (GDPR) (European 2018) |
| **M2.3.1** Define benchmarks, success indicators for initiatives and publish periodically. | To monitor and evaluate the initiatives. | **C2.3.1** Monitoring and Evaluation guidelines. | Performance measurement and key performance indicators. |

2. Mechanisms and controls template analysis for Dimension 3.

| Mechanism ID | Rational | Control ID | Reference and Access |
|---|---|---|---|
| **M3.1.1** Develop national cybersecurity education and cybersecurity modules in schools and universities. | To form basic cyber skills into the State's labour force. | **C3.1.1** Curriculum Guidelines | https://www.acm.org/education/curricula-recommendations, open source |
| **M3.1.2** Foster research and development in cybersecurity | To address emerging challenges of cyberspace and reinforce State's research in the area of cybersecurity. | **C3.1.2** Provide a sufficient budget and other resources. | National strategy |

| | | | |
|---|---|---|---|
| **M3.1.3** Combine the education with practical training | To close the cybersecurity skills gap among all organisations and preparing the future cybersecurity workforce. | **C3.1.3** Alignment of curricula and training with demand for skills. | CyberSeek, open source (CyberSeek 2016) |
| **M3.2.1** Set the professional standards for cyber practitioners | To build the State cross-cutting knowledge, skills and power to boost all cybersecurity objectives. | **C3.2.1** professional certification bodies | CIISec Skills Framework, open source. |
| **M3.2.3** Creating the competences of the private sector | To improve the competences of the private sector. | **C3.2.2** Frameworks and standards for private sector | Cyber Essentials' - standards/ requirements and Certification for SME (UK) & 'Référent en cybersecurity' guide with standards by ANSSI (France), open sources |
| **M3.3.1** Establish a cybersecurity career awareness campaign targeting educators, students, parents, administrators, and counsellors | To increase career awareness and sustain young and public commitment in cybersecurity activities | **C3.3.1** Knowledge frameworks, job descriptions and professionalisation | National Cybersecurity Workforce Framework 2.0' by the National Initiative for Cybersecurity Education (US), open sources |
| **M3.3.2** Promote training for human resources already in the workforce | To determine if the cybersecurity capabilities are satisfying the operations during cyber crises. | **C3.3.2** Conduct cyber drills and exercises | ITU guidance. Open source |

3. Mechanisms and controls template analysis for Dimension 4.

| Mechanism ID | Rational | Control ID | Reference and Access |
|---|---|---|---|
| **M4.1.1** Substantive law. | Substantive law outlines the rights and responsibilities of legal subjects. | **C4.1.1** Balance security with privacy and data protection (Fundamental human rights) | (https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/the-role-of- |

| | | | |
|---|---|---|---|
| | | | cybercrime-law.html) ( ITU Toolkit for Cybercrime Legislation) |
| **M4.1.2** Procedural law. | To defines the process that followed to apply substantive law. | **C4.1.2** Law enforcement, prosecution and the courts. | https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/the-role-of-cybercrime-law.html) (ITU Toolkit for Cybercrime Legislation), open source. |
| **M4.2.1** Law enforcement procedural powers. | To ensure the effectiveness and fairness of criminal justice systems. | **C4.2.1** national capacity in law enforcement. | https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/the-role-of-cybercrime-law.html) (ITU Toolkit for Cybercrime Legislation), open source. |
| **M4.2.2** Procedures regarding electronic evidence. | Enhance the forensic capabilities | **C4.2.2** national investigation and the prosecutor's power. | The United Nations Office on Drugs and Crime *(*UNODC*)* guidelines, open source |
| **M4.3.1** Form national and an international cooperation. | To ensure effective collaboration on cybersecurity in state and worldwide. | **C4.3.1** Information sharing platform (common, specific guidelines, Encourage information exchange). Mutual legal assistance treaties (MLATs). | Information sharing in the international fight against cybercrime (WEF (2017). African Union Convention on cybersecurity (African-Union 2014) |
| **M4.3.2** Develop a cybersecurity policy | To identify all obligatory cybersecurity requirements and | **C4.3.2** Cybersecurity standards. | Standards for IT and |

| | | | |
|---|---|---|---|
| | controls with which it must comply. | | cybersecurity from British and International Standards (https://www.bsigroup.com/en-GB/Cyber-Security/Standards-for-IT-and-cyber-security/) |
| **M4.3.3** Responsible disclosure | To protect national assets and risk associated with exploiting vulnerabilities. | **C4.3.4** Responsible disclosure frameworks | ISO/IEC 29147:2018. It is not free, the proprietary rights are from the International Organization for Standardization (ISO) |

4. Mechanisms and controls template analysis for Dimension 5.

| Mechanism ID | Rational | Control ID | Reference and Access |
|---|---|---|---|
| **M5.1.1** Create a national risk assessment, crisis management, and auditing framework | To identify the key risks and their consequences. | **C5.1.1**Establish a national risk management Centre. | NIST Special Publication 800-39, open source |
| **M5.1.2** Adopt cybersecurity and risk-management standards and promote their adoption across the public and private sectors. | To identify baseline ICT security, | **C5.1.2** Apply International standards | ISO 31000, Risk management. It is not free, the proprietary rights are from the International Organization for Standardization (ISO) |

| | | | |
|---|---|---|---|
| **M5.1.3** Embed security-by-design, in buying technology or install software from overseas | To ensure that technologies and systems are designed and fabricated securely. | **C5.1.3** Security architecture, Security by default principles | https://www.csa.gov.sg/~/media/csa/documents/legislation_supplementary_references/security_by_design_framework.pdf), open source |
| **M5.2.1** Internet infrastructure resilience plan | To ensure the continuity of Internet infrastructure services against any destruction. | **C5.2.1** Standards for IT security and critical infrastructure | Requirements for Network Resilience and Recovery form ITU, open source |
| **M5.2.2** Business continuity plan | To deal with potential cyber threats to a state and enable operation of national systems before and during the execution of disaster recovery. | **C5.2.1** Resilience Frameworks | ISO 22301:2019(en) Security and resilience - Business continuity management systems — Requirements. It is not free, the proprietary rights are from the International Organization for Standardization (ISO) |

| | | | |
|---|---|---|---|
| **M5.3.1** Technical security controls | To avoid, detect, or minimise security risks to physical assets, information, computer systems, or other assets. | **C5.3.1** Security controls framework | U.S. Federal Government information security standards (NIST Special Publication 800-53), open source. ISO 27001 controls list from ISO. |

Appendix 6 – the NCCBF version 1

1.Dimension 1: Cyber security policy and strategy

| **Dimension ID and description** | **Factors ID and description** | **Mechanism ID and description** | **Control ID and description** |
|---|---|---|---|
| **D1Build strategic capacity** | **D1.1** Establish a National Council for Cybersecurity. | **M1.1.1** Clear mandate and appropriate statutory powers | **C1.1.1** Regulatory and corporate governance compliance ( ITIL®, ISO 20000 and ISO 27001) |
| | | **M1.1.2** An organizational structure | **C1.1.2** Stakeholders approach ( Partnership and collaboration) |
| | | **M1.1.3** Human Capital | **C1.1.3** Cybersecurity Competency program |
| | | **M1.1.4** Develop national Cybersecurity strategy. | **C1.1.4** Guiding principles |
| | **D1.2** Building a Risk-Based Approach | **M1.2.1** Identify the Critical National (CI) assets and critical National Information infrastructure (CNI) | **C1.2.1** Good practices for the identification of CI sectors and CNI sectors |
| | | **M1.2.2** Identify the threats to national security on cyberspace | **C1.2.2** Risk assessment (including threat assessment, vulnerability assessment and impact analysis). |
| | | **M1.2.3** Develop Military capabilities | **C1.2.3** Cyber defence doctrine framework |
| | **D1.3** Building a National Incident Response Capabilities | **M1.3.**1 Establishment of a National CERT | **C1.3.1** The National CERT Structure. |
| | | **M1.3.2** Establish Incident Registry<br>Platform for reporting and sharing of incidents and Maintain Trust Relationships. | **C1.3.2** Relevant stakeholders and legal framework |
| | | **M1.3.3** Technical Excellence | **C1.3.3** Cybersecurity Workforce Framework |

2. Dimension 2: Cyber culture and society

| Dimension ID and description | Factors ID and description | Mechanism ID and description | Control ID and description |
|---|---|---|---|
| **D2 Build cyber cultural and society capacity** | **D2.1** Develop a national awareness program that is compatible with the current situation. | **M2.1.1** Behaviors change | **C1.1.1** Behavior Change Techniques ( behavior change wheel) |
| | | **M2.1.2** cybersecurity awareness-raising campaigns | **C1.1.2** Guiding principles |
| | | **M2.1.3** Promote information sharing and Effectively communicate the benefits of paying attention to threats and vulnerabilities | **C1.1.3** Cooperation framework |
| | | **M2.1.4** Organise a national cyber-security month, week or day in order to engage the public, and private- and public-sector partners through events and initiatives | **C1.1.4** Provide a sufficient budget and human resources |
| | **D2.2** Improve e-services, in order to promote the required level of trust. | **M2.2.1** Develop a strategic plan for e-government | **C1.2.1** Governance, infrastructure, policy and outreach |
| | | **M2.2.2** launch and continuously develop government e-services | **C1.2.1** Embed the application of security measures in their design and running |
| | | **M2.2.3** Protect information and personal data | **C1.2.2** Privacy policy |
| | **D2.3** Develop an evaluation criterion | **M2.3.1** Define benchmarks, success indictors for initiatives and publish periodic | **C1.3.1** Monitoring and Evaluation guidelines |

3.Dimension 3: cybersecurity Education, Training and skills

| Dimension ID and description | Factors ID and description | Mechanism ID and description | Control ID and description |
|---|---|---|---|
| **D3 Build cybersecurity Education, Training and skills** | **D3.1** Develop national cyber security education program | **M2.1.1** Develop national cybersecurity education and cyber security modules in schools and universities. | **C2.1.1** Curriculum Guidelines ( https://www.acm.org/education/curricula-recommendations) |
| | | **M2.1.2** Foster research and development in cyber security | **C2.1.2** Provide a sufficient budget and other resources. |
| | | **M2.1.3** Combine the education with practical training and Preparing future cyber security workforce | **C2.1.3** Alignment of curricula and training with demand for skills. ( CyberSeek) |
| | **D3.2** Creating a certificate for national needs | **M2.2.1** Set the professional standards for cyber practitioners | **C2.2.1** professional certification bodies ( NCSC Certified Cyber Professional (CCP) scheme) |
| | | **M2.2.3** Improving the competences of the private sector | **C2.2.2** Frameworks and standards for private sector Example: 'Cyber Essentials' - standards/ requirements and Certification for SME (UK) & 'Référent en cybersecurity' guide with standards by ANSSI (France) |
| | **D3.3** Defining tasks and required knowledge | **M2.3.1** Establish a cyber security career awareness campaign targeting educators, students, parents, administrators, and counsellors | **C2.3.1** Knowledge frameworks, job descriptions and professionalisation Example: 'National Cybersecurity Workforce Framework 2.0' by the National Initiative for Cybersecurity Education (US) |
| | | **M2.3.2** Promote training for human resources already in the workforce | Conduct cyber drills and exercises |

4.Dimension 4: legal and regulations

| Dimension ID and description | Factors ID and description | Mechanism ID and description | Control ID and description |
|---|---|---|---|
| **D4 Build legal and regulations capacity** | **D4.1** Development and adoption of relevant legislation supporting the policy that would enhance cybersecurity | **M4.1.1** Substantive law. | **C4.1.1** Balance security with privacy and data protection (Fundamental human rights) ( ITU Toolkit for Cybercrime Legislation) Substantive law defines the rights and responsibilities of legal subjects, which include persons, organizations, and states. Sources of substantive law include statutes and ordinances enacted by city, state, and federal legislatures ( statutory law), federal and state constitutions, and court decisions (https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/the-role-of-cybercrime-law.html) |
| | | **M4.1.2** Procedural law. | **C4.1.2** Law enforcement, prosecution and the courts. |
| | | **M4.1.3** Jurisdictional law | **C4.1.3**Territoriality, nationality, protection and universality. |
| | **D4.2** Develop Criminal justice power | **M4.2.1** Law enforcement procedural powers. | **C4.2.1** national capacity in law enforcement. |
| | | **M4.2.2** Procedures regarding electronic evidence. | **C4.2.2** national investigation and prosecutor's power. |
| | **D4.3** Establish effective informal cooperation mechanisms. | **M4.3.1** Form national and an international cooperation. | **C4.3.1** Information sharing platform (common, specific guidelines, Encourage information exchange) . Mutual legal assistance treaties (MLATs). Information sharing in the international fight against cybercrime (WEF (2017)). |
| | | **M4.3.2** Develop a cybersecurity policy | **C4.3.2** cybersecurity standards. |
| | | **M4.3.3** Responsible disclosure | **C4.3.4** Responsible disclosure frameworks |

5.Dimension 5: Standards, organisations, and technologies

| **Dimension ID and description** | **Factors ID and description** | **Aspects** | |
|---|---|---|---|
| | | **Mechanism ID and description** | **Control ID and description** |
| **D5 Build technical capacity** | **D5.1** All stakeholders to adapt and adopt international standards. | **M5.1.1** Create a national risk assessment, crisis management, and auditing framework | **C5.1.1**Establish a national agency |
| | | **M5.1.2** Identify baseline ICT security, cybersecurity and risk-management standards and promote their adoption across the public and private sectors. | **C5.1.2** Apply International standards |
| | | **M5.1.3** Embed security-by-design, in buying technology or install software from overseas | **C5.1.3** Security architecture, Security by Default principles ( https://www.csa.gov.sg/~/media/csa/documents/legislation_supplementary_references/security_by_design_framework.pdf) |
| | **D5.2** Build national resilience plan | **M5.2.1** Internet infrastructure resilience plan | **C5.2.1** Standards for IT security and critical infrastructure |
| | | **M5.2.2** Business continuity plan | **C5.2.1** Resilience Frameworks |
| | | | |
| | **D5.3** Enhance physical security. | **M5.3.1** Technical security controls | **C5.3.1** Accreditation Authority |
| | | | |

**Appendix (6) A Letter sent to the Participants to invite them to participate in the Evaluation of the NCCBF.**

Dear Sir/Madam,

My name is Mohamed Ben Naseir. I am a PhD candidate at the Faculty of Science and Technology, at Bournemouth University. As part of my PhD research at Bournemouth University, I am conducting an empirical study in the area of Cybersecurity focusing on National Cybersecurity Capacity Building Framework (NCCBF) for countries in a transitional phase to facilitate a better understanding and representation of a real-world problem from an enterprise perspective. I would like to cordially invite you to participate in my study since your profile and background makes me interested in your views on the research topic, and any further insights would be greatly appreciated.

Participation is anonymous, thus, no one will know what you have answered. This setting allows respondents to be free of any bias and hesitance when accepting to participate in the study. Your help is of high importance to provide a pragmatic view on Cybersecurity problem in different countries.

If you agree to participate in my study, you are invited to join us in focus group meetings. There will be almost one meeting to demonstrate and evaluate the Cybersecurity focusing on National Cybersecurity Capacity Building Framework (NCCBF) for countries in a transitional phase against a set of requirements.

For the detailed information about the research and participation, please find the attached file and confirm your participation by replying back to me for arranging further details, if necessary.

Kind regards,

Mohamed Ben Naseir
PhD Candidate
Faculty of Science and Technology, Bournemouth University
Office number: Poole House, 521.
Mob: +44 7478458144
Email: mnaseir@bournemouth.ac.uk

Appendix 7: Interviewer details of the evaluation of the NCCBF

1- Personal details :

| Name: |
|---|

2- Contact details

| Email: |
|---|

3- Under which category does your organisation belong?

| Public ☐ rivate ☐ |
|---|

4- Under which sector does your organisation belong?

| |
|---|

5- Describe your position in your organisation?

| |
|---|

6- How long have you worked in this position?

| |
|---|

Appendix 8- A Sample of Templates Filled by the Participants in Evaluation Focus Group Sessions

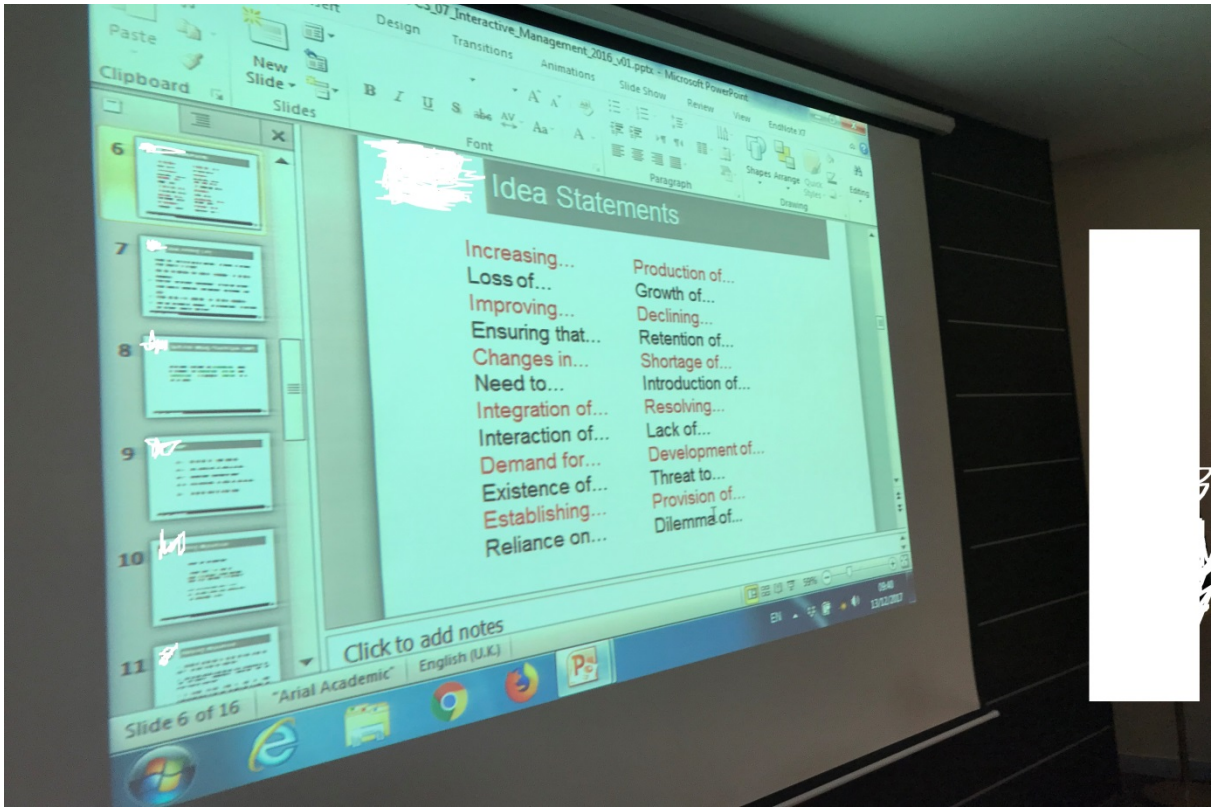
| Activities | Questions | Notes |
|---|---|---|
| Completeness | • Which factors, mechanisms and controls are missing in this framework?<br>• Which factors, mechanisms and controls in this framework do you consider redundant? | → IND 1: Financial resources also lacking.<br>→ In case of unstability in the country during the implementation process, also think about actors outside the country.<br>→ Cybercriminality is to be taken into account as a factor. |
| Correctness | • Which factors, mechanisms and controls are unclear to you?<br>• Which ambiguities are currently in this framework?<br>• What changes (i.e. amendment/addition/removal) to the artefacts do you suggest (labels, names, orders? Why? | No - comment |
| Acceptability | • Would you find it useful to use this framework to build a cybersecurity capacity for your organisation or country?<br>• Would you actually use this model? If not, what has to be changed? | In my point of view, this model is acceptable. |
| The Overall Evaluation of the framework | • To what extent do you think the framework is: (Please specify why, or why not using the sheet provided) :-<br>• Inclusive: Involves as many Stakeholders as possible.<br>• Coherent : Recognizes Current International Standards, Protocols and Interoperability<br>• Multi-Dimensional : Includes Domestic and International Tools<br>• Risk Based: Mitigation factors, mechanisms and controls in Accordance with the level of risk. | This framework is inclusive, coherent, multi-dimensional and risk-based because it rely on, it is based on a correct existing framework (CMM) and it doesn't bring ~~incertitude~~ inconsistency. |

Kim

| Activities | Questions | Notes |
|---|---|---|
| Completeness | • Which factors, mechanisms and controls are missing in this framework?<br>• Which factors, mechanisms and controls in this framework do you consider redundant? | → Add Active Risk Nangement (Sectors)<br>→ Add Continuous review of the model and monitoring<br>→ Assets inventories → timescale for actions |
| Correctness | • Which factors, mechanisms and controls are unclear to you?<br>• Which ambiguities are currently in this framework?<br>• What changes (i.e. amendment/addition/removal) to the artefacts do you suggest (labels, names, orders? Why? | |
| Acceptability | • Would you find it useful to use this framework to build a cybersecurity capacity for your organisation or country?<br>• Would you actually use this model? If not, what has to be changed? | ~~The~~ country is working on a framework for the county. This framework |
| The Overall Evaluation of the framework | • To what extent do you think the framework is: (Please specify why, or why not using the sheet provided) :-<br>  • Inclusive: Involves as many Stakeholders as possible.<br>  • Coherent : Recognizes Current International Standards, Protocols and Interoperability<br>  • Multi-Dimensional : Includes Domestic and International Tools<br>  • Risk Based: Mitigation factors, mechanisms and controls in Accordance with the level of risk. | YES<br>I liked How capacity building has been defined and developped |

| Dimension ID and description | Factors ID and description | Mechanism ID and description | Control ID and description |
|---|---|---|---|
| D1<br>Build Strategic capacity | D1.1. Establish a National Council for Cybersecurity | M1.1.5 Allocate relevant financial resources | |
| | | | |
| | | M1.1.3 | C1.1.2 Stakeholders approach (Partnership and collaboration); strong participation of National manpower abroad → Expertise; Volunteers; etc. |
| | | | |
| D2<br>Build cyber cultural and society capacity | D2.3 Develop strong international participation<br>↳ already in D4.3. | M2.3.1 International cybersecurity events. | |
| | | M2.3.2. Partnerships. | |
| | | | |
| D4.<br>Build legal and regulations capacity | D4.2. | Cybercrimes? | |
| | | | |
| | | | |

Appendix 9- Sample of photos from the IM workshop


Idea Statements
Increasing... Loss of... Improving... Ensuring that... Changes in... Need to... Integration of... Interaction of... Demand for... Existence of... Establishing... Reliance on...
Production of... Growth of... Declining... Retention of... Shortage of... Introduction of... Resolving... Lack of... Development of... Threat to... Provision of... Dilemma of...
Click to add notes
Slide 6 of 16

Appendix 10- Sample of photos from the evaluation sessions of the NCCBF