TOWARDS A CAPABILITY MATURITY MODEL FOR A CYBER RANGE

A thesis submitted in fulfilment of the
requirement of the degree of

Masters of Science
of
Rhodes University

By Michael Joseph Aschmann

October 2020

Abstract

This work describes research undertaken towards the development of a Capability Maturity Model (CMM) for Cyber Ranges (CRs) focused on cyber security. Global cyber security needs are on the rise, and the need for attribution within the cyber domain is of particular concern. This has prompted major efforts to enhance cyber capabilities within organisations to increase their total cyber resilience posture. These efforts include, but are not limited to, the testing of computational devices, networks, and applications, and cyber skills training focused on prevention, detection and cyber attack response.

A cyber range allows for the testing of the computational environment. By developing cyber events within a confined virtual or sand-boxed cyber environment, a cyber range can prepare the next generation of cyber security specialists to handle a variety of potential cyber attacks. Cyber ranges have different purposes, each designed to fulfil a different computational testing and cyber training goal; consequently, cyber ranges can vary greatly in the level of variety, capability, maturity and complexity. As cyber ranges proliferate and become more and more valued as tools for cyber security, a method to classify or rate them becomes essential. Yet while a universal criteria for measuring cyber ranges in terms of their capability maturity levels becomes more critical, there are currently very limited resources for researchers aiming to perform this kind of work.

For this reason, this work proposes and describes a CMM, designed to give organisations the ability to benchmark the capability maturity of a given cyber range. This research adopted a synthesised approach to the development of a CMM, grounded in prior research and focused on the production of a conceptual model that provides a useful level of abstraction. In order to achieve this goal, the core capability elements of a cyber range are defined with their relative importance, allowing for the development of a proposed classification cyber range levels. An analysis of data gathered during the course of an expert review, together with other research, further supported the development of the conceptual model.

In the context of cyber range capability, classification will include the ability of the cyber range to perform its functions optimally with different core capability elements, focusing on the Measurement of Capability (MoC) with its elements, namely effect, performance and threat ability. Cyber range maturity can evolve over time and can be defined through the Measurement of Maturity (MoM) with its elements, namely people, processes, technology. The combination of these measurements utilising the CMM for a CR determines the capability maturity level of a CR. The primary outcome of this research is the proposed level-based CMM framework for a cyber range, developed using adopted and synthesised CMMs, the analysis of an expert review, and the mapping of the results.

Acknowledgements

This thesis is dedicated to my late father and mother who was in my life for six wonderful years, and my sister I never met, Rest In Peace, my thoughts are with you. Thank you to my Creator, He is always with me; my wife Natalie and my son James, who stood by me through my academic journey, thank you; my supervisor Professor Barry Irwin for the guidance, patience and direction he gave me; the staff of the Computer Science Department Rhodes University of Grahamstown South Africa for their support; my employer for the studying opportunity, and all the researchers who have published on this topic, and whose work has been referenced for this thesis, it is truly a privilege. To Dr Spalding Lewis my editor I thank you for your patience and quality of work, it is appreciated. It is for me a great privilege to write this thesis; it has been a learning experience. I have learnt on this academic journey that focus, effort and a will and determination will allow one to grow and complete the journey with one's head held high. I thank the Counsel for Scientific and Industrial Research (CSIR) Cyber Range team and I would further like to express my gratitude to all the participants in the CR evaluation questionnaire for their time and effort in making it a success.

Contents

List of Tables

List of Figures

Glossary of Terms

ALIVE Automatic Live Instantiation of a Virtual Environment

APT Advanced Persistent Threat

AWS Amazon Web Services

CCER Common Cyber Event Representation

CDX Cyber Defence Exercise

CIAD Cyber Immediate Action Drills

CIERT Cyber Incident Emergency Response Team

CMM Capability Maturity Model

CMMI Capability Maturity Model Integration

COA Cause of Action

COI Critical Operational Issues

CR Cyber Range

CSCMM Cloud Security Capability Maturity Model

CSIR Counsel for Scientific and Industrial Research

CTF Capture the Flag

CW Cyber Warrior

DARPA Defence Advanced Research Agency

DETER Cyber-Defense Technology Experimental Research

DLOD Defence Lines of Development

DOS Denial of Service

DOTMLPF Doctrine, Organisation, Training, Material, Leadership and Education, Personnel and Facilities

DPA Deep Packet Analysis

EPP Endpoint Protection Platform

FW Firmware

GNSS Global Navigation Satellite System

GPS Global Positioning System

GRC Governance, Risk and Compliance

GSM Global System for Mobile communication

HCI Hyper Converged Infrastructure

HW Hardware

IaaS Infrastructure as a Service

ICT Information and Communication Technology

IANA Internet Assigned Number Authority

IP Internet Protocol

IDS Intrusion Detection System

IPS Intrusion Protection System

IoT Internet of Things

IIoT Industrial Internet of Things

KSA Knowledge Skills and Abilities

LAN Local Area Network

LISI Levels of Information Systems Interoperability

IOC Indicator of Compromise

ISE Information Security Expert

LMS Learner Management System

MoC Measurement of Capability

MoE Measurement of Effects

MoM Measurement of Maturity

MoP Measurement of Performance

MoT Measurement of Threat

NATO North Atlantic Treaty Organisation

NCR National Cyber Range

NGCR Next Generation Cyber Range

NG Next Generation

NICT National Institute of Information and Technology

NOSC Network Operations Security Centre

OEM Original Equipment Manufactures

OS Operating System

OSI Open Systems Interconnection

PAID Policy, Application, Infrastructure, Data

PaaS Platform as a Service

POSTEDFIT Personnel, Organisation, Structure, Equipment, Doctrine, Facility, Information, Technology

PPT People, Processes and Technology

RMF Risk Management Framework

ROC Required Operational Capability

SaaS Software as a Service

SANReN South African National Research and Education Network

SCADA Supervisory Control and Data Acquisition

SIEM Security Information Events Management

SITL System in the loop

SOC Security Operations Centre

SSE System Security Engineering

SUT System Under Test

SW Software

T&E Test and Evaluation

TCP/IP Transmission Control Protocol /Internet Protocol

TTTPs Tools, Tactics, Techniques and Procedures

UDP User Datagram Protocol

URS User Requirement Specification

URSt User Requirement Statement

WAN Wide Area Network

ZA Zuid-Afrika

1 Introduction

A virtual platform to test cyber capabilities in real time is an increasing challenge, especially when it comes to proving that the cyber capabilities of a given organisation perform as designed. Organisational computational systems are under consistent cyber attack, both externally and internally (Protect, 2019), and the cyber domain is plagued with different and complex cyber threat vectors, all of which can impact on Information and Communication Technology (ICT) solutions. Moore's law suggests that cyber threats should increase exponentially with the proliferation of hardware, and historical trends recorded in the cyber domain confirm this (Deloitte, 2015). Further, cyber threats are becoming more and more sophisticated. In tandem with the exponential expansion of the Internet and the increasing complexity of organisational computational networks (Biscoe, 2018). Consequently, the security of computational information systems is no longer limited to the traditional use of a firewall, intrusion detection or prevention system; rather, the strength of security now comes from a mixture of specialist personnel, cyber resilience processes, product security, and consistent monitoring to ensure that a proactive approach is applied (Stefan *et al.*, 2014).

The testing and evaluation (T&E) of cyber products needs to be as accurate and predictive as possible to ensure that cyber products are able to fulfil their function and be secure from a cyber attack. Cyber threats are detected and created daily, thus the demand on cyber security related training is tremendous, especially with the cyber skills shortages globally. With the increasing cyber threat, a closed virtual or sandboxed cyber environment - a cyber range - in which an organisation can practice and test without running live cyber incidents on its live network, has become necessary for cyber training and experimentation (Beuran *et al.*, 2017).

A CR, as defined by the author for this thesis, is a managed closed sandboxed

and virtualised cyber lab environment in which modelling, simulating and emulating take place in an independent or federated deployment, to replicate and build cyber capabilities whether in people; through cyber training with multiple cyber scenarios augmenting cyber resilience or; in cyber processes that govern the cyber posture of an organisation or; in technology by undertaking research and development of computational cyber product, to emulate appropriate cyber defences and retaliatory means, through T&E with the utilisation and integration of different sensors and instrumentation. This definition for a CR is supported in more detail in Section 2.4. CRs have been in use for the greater part of fifteen years, in which time the CR model has been developed to operate on highly sophisticated technology platforms.

This thesis will address the need for a set of criteria to classify different levels of a CR and to determine a CR capability and maturity, and will propose a Capability Maturity Model (CMM) as the solution. Consequently, this thesis will address the following: defining a CR and determining the core capability elements in a CR in order to establish a firmer understanding of a CR capability. Once the capability is defined, a classification level schema for a CR is proposed, using a real network to determine sound baseline criteria. This development of CR levels will precede the main focus area of the research: a proposed Capability Maturity Model (CMM) for a CR. A synthesised approach is used to build the CMM for a CR. This choice is grounded in work already undertaken in multiple publications on CR capabilities and various maturity models, as discussed in Chapter 2. After the initial understanding of a CR and a proposed CMM for a CR a questionnaire was compiled and sent to identified CR experts to give inputs to the research of a CMM for a CR. The results are analysed and then used to modify initial classification levels, resulting in an upgraded version of a CMM for a CR. Finally, this thesis is concluded and revisits the problem statement and the research questions to evaluate to what extent this was accomplished.

Chapter 1 provides an overview of the research process and a description of the focus thereof. The introduction will describe the context of the research, followed by the problem statement in Section 1.1 that will define the focus for this research, followed by Section 1.2 which describes the research goals for the thesis. The Research Approach Section 1.3 describes the methodological approach and the research process. The Scope and Limits Section 1.4 defines areas of research covered in this study and points to work outside the scope of the project. The Research Contribution Section 1.5 will suggest potential use-cases for this research within the academic and private sectors. The chapter concludes by summarising the structure of the rest of the document.

1.1 Problem Statement

In the current cyber domain there is a growing necessity to ensure that the quality of cyber security as an entity is maintained. The complexity and the increased de-

mand for connectivity and information sharing in the cyber environment has caused a massive flow of data between users. In order to ensure that these diverse complexities in the cyber environment are secure, a platform to perform T&E on cyber products and cyber skills is imperative. There are multiple different types of CRs that can be utilised to T&E in terms of variety, capability, level of maturity and in complexity. In researching a CR capability and maturity level in order to develop a sound CMM for a CR, there is no single authoritative and detailed view to serve as a standard. Previous work published by Priyadarshini (2018) *"Features and Architecture of the Modern Cyber Range: A Qualitative Analysis and Survey"* describe the perimeters of an ideal CR; Spirent (2017) *"Operational Impact of Cyber Range Elements, Simulations and Realism"*, white paper describe a holistic view of CR capabilities, and Hwang and Bush (2015) *"Operational Exercise Integration Recommendations for DOD"*. CRs have indicated that the measurement of a CR is complex, particularly with respect to the Measurement of Effectiveness (MoE) and the Measurement of Performance (MoP). CRs are defined and used for different purposes in different organisations, making the identification of a global model for CR levels of capability maturity difficult, however this thesis will propose a baseline towards a CMM of a CR through a common consensus.

The primary problem for this thesis is the challenge of developing towards a CMM for a CR while considering literature and the dynamics of understanding the different views from CR experts on the interpretation of CR capabilities maturity levels. By focusing on the initial problem, the research allowed for the larger project goals to be solved - the construction of an acceptable baseline towards a CMM for a CR. In solving the primary problem the following research questions posed include:

1. How should the measures of capability maturity levels, using the CR core capabilities elements, be integrated towards a Capability Maturity Model for a CR?

2. What are the CR core capabilities and how should they be synthesised to derive CR capability levels?

3. How should the maturity of a CR be synthesised to derive CR maturity levels?

4. What is the outcome of results from experts to factorise in and formulate a baseline CMM for a CR?

1.2 Research Goals

CRs and their many applications have been widely researched in the academic community. A primary focus of these examinations is the comparison of a variety of CRs which have been developed globally, as per the Australian technical report "*A Survey of Cyber Ranges and Test Beds*" (Davis and Magrath, 2013). However, during the course of this project the researcher was unable to identify any hard evidence in open-source research information that focuses on a research view of a CMM for a CR.

The research for a CMM for a CR is novel, making this thesis a needed contribution to the academic conversation on CRs. The research goals compliment the research questions in achieving the primary problem of the project. The research goals are evaluated in section 8.2 to the degree to which they have been met. In order to address this lack of scholarship, the research goals to be posed by this examination include:

1. The primary research goal - defining the measures of capability maturity for a CR with their different elements and in determining viable levels. The focus is on defining the core capability and maturity elements for a CR, to provide an acceptable baseline towards a CMM for a CR. This will be determined by factoring in literature and results gained from an expert review.

2. The secondary research goals aided in reaching an understanding of the primary research goal:

   (a) Determining the CR core capabilities by analysing the relative importance thereof. The higher the relative importance, the more critical the core capability element, which informs the level of capability for a CR. By synthesising the proposed classified capability CR levels this enables the establishment of a baseline criteria for CR levels. An expert review will aid in determining a consensus for the core capability elements and synthesised capability levels for a CR.

   (b) Determining the maturity measures and levels by synthesising defined CMM models identified in literature, similarly an expert review will aid in determining a consensus for the maturity elements and synthesised levels for a CR.

   (c) Factorising in the results of the experts review into a modified CMM for a CR, by analysing the proposed capability maturity elements and levels in determining a consensus for a baseline modified CMM for a CR. The focus is to determine a CMM for a CR, by fully understanding the measures for CR capability maturity, to incrementally reach a certain standardised level that is agreed upon in the CR community as a whole.

1.3 Research Approach

The research described in this thesis focused on the development of a CMM for a CR to identify CR capability maturity at various proposed levels. A conceptual model was used, providing a useful level of abstraction in the development of a CMM for a CR. More generally, this project proceeded within a pragmatic and deductive approach to research - mixed methods testing existing theories, to the analysis of relevant literature on CRs and capability maturity models in order to synthesize current knowledge towards the development of an acceptable baseline towards a CMM for a CR. The

various facets and research activities addressed in this thesis are discussed for understanding the research process followed, link to the research objectives as in the generic research framework in Figure 1.1.

The background and initial research was a qualitative approach to first establish a theory and knowledge base for the cyber environment, CRs and CMM's to structure the specific knowledge gained into a logical flow. This was done through discussion with my supervisor and other knowledgeable members from a research institute, and through the evaluation of research and data acquired from various digital and print scholarly resources. With respect to the broader construction of the project, the choice was made to use a multi-method approach, dividing the research into different streams, with the results generated separately. A Forced Choice Pared Comparison analysis, also known as the Pairwise Comparison (Tsukida and Gupta, 2011) was utilised as a methodology, and during this process the relative importance of the core capability elements of a CR was determined. This formed the baseline for the initial understanding in the development of a CMM for a CR and the CR capabilities addressing the first secondary research goal.

Addressing the model an action research approach - diagnosing the primary research problem to develop a solution, with the goal of improving on professionalism within the cyber security environment was used. The practicality of this approach allowed the research to specialise on a specific data capture, which was used in tandem with previous academic research in step one to determine a baseline for CR criteria for capability maturity, classification levels, measurement criteria and the detailed measures proposed. This formed the baseline for the development of a proposed CMM for a CR addressing the both first and second secondary research goal.

A quantitative approach was used in order to acquire further practical data, a questionnaire using open ended questions was distributed to CR experts electronically using a google forms. The questions were derived from the literature study which were structured with the purpose to obtain answers to gaps identified in literature and an understanding of the views of CR experts, specifically focused on the proposed capability maturity for a CR. The participants for the questionnaire were recruited random from the international community of whom have written article's and journals on CR's, from the local Zuid-Afrika (ZA) community the participants were selected from the Counsel for Scientific and Industrial Research (CSIR) of whom have developed a CR or have been part thereof. A convenience sampling type was utilised with the minimum sample size for the questionnaire being seven with a maximum of thirty participants this was calculated by the amount of open source CR expert participants that were identified during the literature review. The limitations of the sampling were considered during the project due to the generalisation thereof. The number of the CR population is generally not known due to the nature of a CR, it is particularly difficult to obtain information from CR experts in some open and classified environments. Thirty initial requests for participation were sent out, which generated seventeen responses from CR expert participants. Following this, seventeen

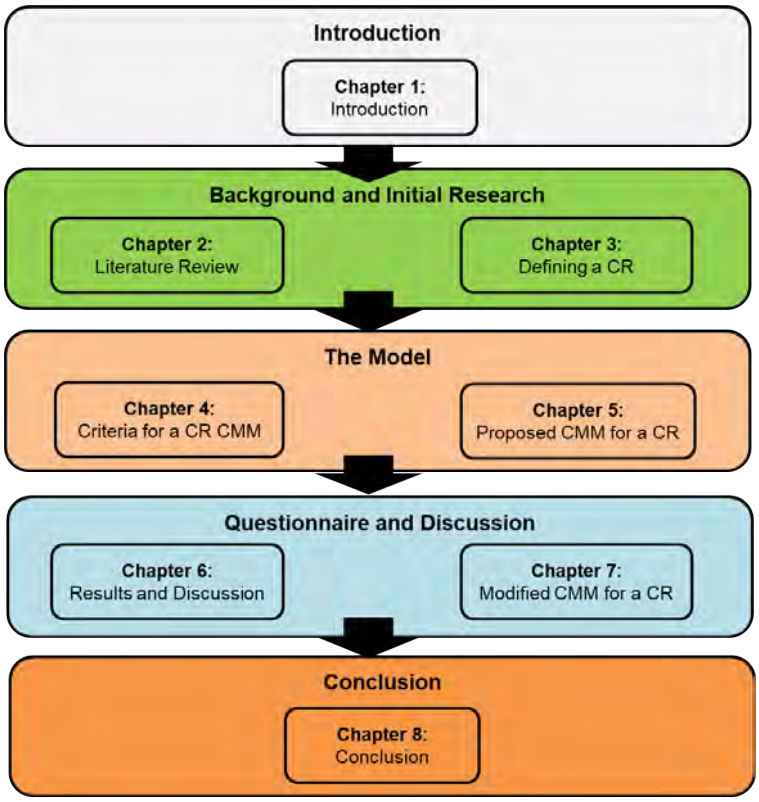


Figure 1.1: Generic Research Framework

questionnaires were sent out, with fourteen questionnaires received. The final ratio of participants was five international experts and nine local experts, of which five were from the same organisation. Data generated via questionnaire was analysed quantitatively, using the Likert approach. This formed the baseline for factorising in the experts review on the proposed CMM for a CR, addressing the third secondary research goal. The questionnaire went through the ethics committee of Rhodes University Grahamstown South Africa and was approved (trace-key number: CIS18-09, approved on 16 November 2018).

The results were captured, discussed and analysed from CR experts of which themes were generated. The data collection for the project included both primary and secondary data analyses, of which the research design was an exploratory study using text data analysis, content analysis, textual criticism, and a historical study to build towards the proposed modified CMM for a CR. This contributed to addressing the primary research goal by defining the measures of capability maturity for a CR with their different elements and viable levels, to provide an acceptable proposed CMM for a CR. The research framework in Figure 1.1 describes the generic research process that followed.

1.4 Scope and Limits

The scope of the thesis is the proposed research towards a CMM for a CR. The thesis covers the generic terms used in the cyber environment and their relevance to a CR in

order to add context to the terminology that is used. The capability maturity models used in literature are discussed to provide a more detailed understanding of the development of a CMM for a CR. This will lead to the composition of a CR in which the core capability elements for a CR and the relative importance thereof forms a baseline for CR classification levels. The capability development of a CR was determined to highlight the process to develop a CR through its life cycle. A selection criteria was then developed to form the baseline criteria for capability maturity levels of a CR, leading to the proposed measurement criteria, namely the Measurement of Capability (MoC) and Measurement of Maturity (MoM). These measurements are described according to their different elements in context towards a CMM for a CR. Following the development of the baseline criteria, further data acquired via questionnaire was analysed and used to determine necessary changes, which were then incorporated into a revised and modified CMM for a CR, which forms the primary result of this project.

While this thesis focused on the development and description of a CMM for CR, there are some aspects of this topic that were outside the scope of the project. These include the measurement and analysis of CRs from a quantitative view using a CR evaluation tool to evaluate a CR capability maturity against defined metrics. The legal applications of a CR are also not included in the thesis due to the challenging nature of different interpretations and opinions of cyber domain laws and rules of engagement. Finally, this thesis does not provide specific recommendations on the application of a CR. Most of the relevant CR documentation that is currently available as open-source, has been retrieved up until June 2019, and has been addressed in this thesis.

1.5 Research Contribution

The research described in this thesis is grounded in a high level approach to CRs, with a focus on identifying core capability elements and proposing a development process to build a working CMM for CRs. The research holistically generated a benchmark against a proposed criteria and classified capability maturity levels for a CR, which organisations can utilise. The levels for the measurements of capability maturity and their elements, in conjunction with the proposed CMM for a CR, can also be utilised to qualitatively evaluate the capability maturity of a CR to incrementally improve organisational CR levels. The outcome of the research will inspire future research in the development of an accepted CMM for a CR, as discussed in Section 8.4.

1.6 Document Structure

The remainder of the thesis is structured as follows:

1. Literature Review (Chapter 2): This chapter provides and introduces key con-

cepts that are covered in this thesis. Concepts addressed include an understanding of the cyber domain, cyber ranges, and capability maturity models. This chapter provides background and context, both on the current research landscape relating to CRs and also on the need for a CR. Finally, this chapter will also elaborate on other related work pertaining to the detailed operation and functioning of a CR.

2. Defining a CR (Chapter 3): This chapter provides an interpretative overview of the literature on CRs, with a particular focus on the CR design and system and the CR's core capability elements on a high level. A pairwise comparison was completed to determine a baseline for CR levels.

3. Criteria for a CR Capability and Maturity Model (Chapter 4): This chapter identifies measurement criteria, introducing the Measurement of Capability (MoC) and Maturity (MoM) for a CR, along with the proposed baseline criteria for CR levels and a process to evaluate a CR.

4. Proposed Capability Maturity Model for a CR (Chapter 5): This chapter defines the Measurement of Capability (MoC) and Maturity (MoM), and establishes the theory and concepts used to develop the first iteration of a CMM for a CR.

5. Results and Discussion (Chapter 6): This chapter provides the results of the data captured from the questionnaire distributed to CR experts and discuses the findings.

6. Modified Capability and Maturity Model for a CR (Chapter 7): This chapter describes the development of the modified CMM for a CR, outlining the ways in which the different results obtained from the expert review were used to develop a second iteration of modified classified capability CR levels and a CMM for a CR.

7. Conclusions (Chapter 8): This chapter provides a summary of the project, addressing the initial research question and how they were met, commenting on the significance of the research and findings, and outlining potential future work.

2

Literature Review

This literature review synthesizes research undertaken by a wide variety of scholars within the cyber domain and cyber range fields, providing necessary context for the main goal of this thesis - building a capability maturity model for a Cyber Range (CR), as described in Chapter 1. This chapter will discuss the key concepts for this thesis, with several definitions given to outline the cyber domain and how it integrates with the Cyber Range understanding. The general concepts of a CR and CMM will also be outlined for clarity.

Initial research utilised wide-ranging search criteria to identify relevant resources, and included any naming style of a CR or an association or conatation towards a CR and the following keywords: Cyber Range (CR), systems, capability, maturity, model, development, evaluation, measurement, metrics, criteria, evolution, core capability elements. Due to the relative lack of open-access scholarly resources on CRs, this thesis incorporated a wide variety of research into initial findings, with the majority of findings being peer-reviewed journals, proceedings, conference papers and presentations, technical reports, electronic blogs and webpages.

In Section 2.1 the cyber domain is defined with its attack vector groupings. Section 2.2 describes the cyber threat landscape in which a CR operates, and is followed by Section 2.3 where the dilemma of cyber security and information security is addressed. Section 2.4 provides a general overview of the CR. Section 2.5 discuses the modelling, simulation and emulation processes that are key to a CR. This is followed by Section 2.6, which describes the literature on models and CMMs in order to establish a baseline understanding on developing a proposed CMM for a CR. Section 2.7 provides a summary of the Chapter to highlight the key concepts.

2.1 The Cyber Domain

The cyber domain, as defined in the Finland cyber security strategy, is “an electronic information (data) processing domain comprising of one or several information technology infrastructures” Goverment of Finland (2013, pg 12). Within the cyber domain the utilisation of electronics (computational systems and devices) and the electromagnetic spectrum (wireless technologies) for the purpose of storing, processing and transferring data and information via telecommunications networks is effectively the core enablers for the cyber domain (Goverment of Finland, 2013, pg 12). The cyber domain can be described as multiple nodes connecting to other nodes using different protocols, allowing for digital binary packets to flow, which are displayed as data (text), voice or video to an incumbent (user). The cyber domain is directly associated with the cyber space, which is defined as “The interaction of people, software and services on the Internet with technology devices and networks connected to it, which does not exist in any physical form” (ISO Institute, 2012a, pg 4). Thus cyber domain and cyber space have a similar meaning and are often used together; in general, the cyber domain can be described as a man-made digital environment in which computational connectivity occurs with multiple devices using the Internet and World Wide Web (Denning, 2015). NIST (2013, pg 58) defines the cyber space as a “Global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers”. The dependency on the cyber domain and cyber space has become so vital that it can be described as a human right to be connected securely, however the cyber domain and cyber space is plagued with malicious code which is used to compromise nodes via many different methods. These methods have been divided into five different attack vector groupings, all of which attack computational infrastructure and devices in the cyber space and are defined below.

The CR, which is a sandboxed and virtual cyber environment, models, simulates and emulates a part of the cyber space of a computational network. Cyber events using scenarios and narratives are developed for the different attack vectors to train cyber security personnel by ensuring computational networks are not vulnerable against the different attack vectors, as depicted in Figure 2.1.

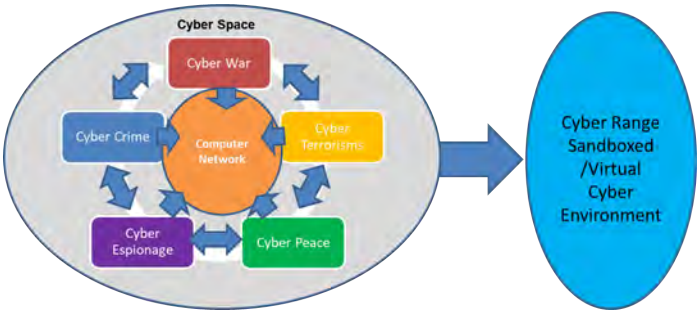


Figure 2.1: The Attack Vector Groupings in the Cyber Space linked to a Cyber Range

Cyber warfare, from a military perspective, is a war fighting capability in which warfare is conducted in the cyber space under the auspices of a cyber operation, against either another nation state, non-actors, or criminal organisations for the purpose of collecting information, disrupting, or destroying computational infrastructure or devices. Robinson *et al.* (2018) describe cyber warfare as, the use of cyber attacks with a warfare-like intent. In July 2016, NATO declared cyberspace an operational domain, calling it the 5th domain of warfare (Baldor, 2016). This was a significant historical development, and ensured that cyber warfare would be approached in the same way as military operations on land, sea, and air; from 2016 cyber space became an operational area, one which private and public environments must take cognisance of from a cyber resilience perspective. Thus from a private and public view cyber warfare can be viewed as a war against cyber criminals who penetrate computational networks of organisations and steal information, intellectual property or finances, affecting both the nation's economic sector and its citizens. Cyber warfare can be summed up as attacks using malicious code with intent on a computer network which contains information or a computer controls systems.

There are many different cyber tactics and techniques which use multiple different malicious tools to circumvent a computer network but all ultimately lead to data breaches and information loss, which can have multiple ramifications for a nation, organisation or business. Today cyber warfare is the reality, and it affects all humans and machines both from a behavioural level to a total shut down of any systems and services which utilize computational power and connectivity. Attacks of this nature are prevalent, especially as war fighting technology are integrated and the risk and the opportunity for a cyber attack increases proportionally, as described in the Metcalfe Law (Hwang and Bush, 2015).

Cyber terrorism, according to the the Oxford English Dictionary is the, "politically motivated use of computers and information technology to cause severe disruption or widespread fear in society" (Maurer and Morgus, 2014, pg 60). A real world example of this is the ways in which terrorist organisations use the Internet to support their recruitment, fundraising and propaganda activities, and use various forms of cyber techniques such as hacking, DDoS attacks, logic bombs, polymorphic and metamorphic malicious code to engage on their identified targets (DOD Republic of Korea, 2012, pg 10). "Terrorists are very aware of the potential of exploiting cyber systems due to their vulnerability and increasing human dependency on cyberspace" (Goverment of Canada, 2010, pg 5).

Cyber peace , as a concept, describes a state in which there is a balance in the maturity of cyber and information security and the adherence to legislation. This is a cyber environment where a complete non-threat cyber environment exists. The environment of cyber peace is one managed and configured accurately with all people, processes and technology coexisting as an entity to ensure that all cyber threats are eliminated and vanquished. Internationally, cyber peace is viewed as an arrangement where nations strive for a common good in the cyber space and are not in a

state of cyber threat towards each other (Robinson *et al.*, 2018). The United Nations (UN) approach to cyber peacekeeping is the application of cyber capabilities to preserve peace performed by a cyber peacekeeper - an individual who performs cyber peacekeeping activities. A cyber buffer zone refers to a network or site that is protected and monitored by peacekeeping forces, one where cyber attacks have been excluded (Robinson *et al.*, 2018).

Goverment of Austria (2013, pg 20) defines cyber espionage in essence as "spying within an IT system, dubbed digital spying". This is performed by collecting information through stealthy or covert cyber techniques without detection on a computational system. The aim is to obtain sensitive information, normally done by an intelligence agency or community not affiliated with a regular government, examples of which include non-state actors or criminal organisations. The Tallinn Manual defines cyber espionage Rule 66 as "any act undertaken clandestinely or under false pretences that uses cyber capabilities to gather or attempt to gather information with the intention of communicating it to the opposing party" (Schmitt, 2013, pg 159).

Cyber crime, as defined by the Qatar national cyber security policy, is any "misconduct or crime committed using technology" (Goverment of Quatar, 2014, pg 23). Cyber crime is also defined as anything that "comprises illegal attacks from cyber space on or through ICT systems, which are defined in penal or administrative laws", (Goverment of Austria, 2013, pg 21). In most cases, cyber criminals are motivated by financial gain, and the organisation and moving around of financial assets in a covert manner.

Cyber power is viewed as the disguising and exerting of power in cyber space by a nation or organisation in order to shape the experience of another nation or organisation (van Haaster, 2016). Cyber power consists of both physical attributes (as represented by Diplomacy, Information, Military and Economics (DIME)) and the cognitive levels pertaining to national power (Jansen van Vuuren and Leenen, 2018). Cyber power is important to understand, as it determines the stance of a nation with regard to the enhancement or development of their cyber capabilities to defend or attack. Cyber power will also enable a nation state or organisation to build capabilities and trained resources to effectively ensure certain cyber power abilities. Langer (2016) defines cyber power as "a society's organised capability to leverage digital technology for surveillance, exploitation, subversion and coercion in international conflict" (Jansen van Vuuren and Leenen, 2018). It is critical to note that a smaller organisation or nation with superior cyber ability compared to a stronger organisation or nation will have superior cyber power, which adds to their ability as a force, thus enabling a smaller or weaker organisation or nation to have a better defensive posture and deploy a large effect (Guzman, 2018).

Because cyber power includes both physical and cognitive elements, a CR should have the ability to be utilised to train cyber peace keepers, as part of cyber warrior or security experts training, to be best suited in their approach to ensure cyber peace. The use of CRs for cyber warfare training supports an understanding of the different

cyber techniques used by cyber terrorists and other criminal elements. CRs are critical for training cyber experts to identify a spying agent in a computational system and/or build on cyber skills in malicious code analysis, and can also be used to train cyber experts to use forensics tools to assist in the apprehension of cyber criminals. Developing on the capacity and capability of cyber warriors and security experts in the art of cyber defence, will incrementally increase an organisation or nation's cyber power.

Within a CR context, the sandboxing and virtualising of a cyber event is performed by different teams, as discussed in more detail in Section 2.4.4. These groups are allocated in a CR to function as different disciplines, however these can change depending on organisational naming conventions for their teams or entities. Damodaran and Couretas (2015) describe the following teams for a CR:

- Red team (Offensive participants, the attacker).
- Blue team (Defensive participants, the defender).
- White team (In control of the events in a CR).
- Green team (Ensures infrastructure support for the events).
- Grey team (Generates traffic in the CR for cyber events).

Priyadarshini (2018) adds two more teams to the CR: a Purple team, which is a collaboration of Red and Blue teams and is more focused on improving the gaps in the defensive and offensive operations, and a Yellow team, which is a human unintentional infection team, using human innocent clicks on malicious sites or links.

2.2 Cyber Threat Landscape

The cyber threat landscape is extremely wide due to its dynamic and multifaceted nature; with the extensive variety of methodologies for both attacking and defending targets and exploits, it can seem like an endless circle that is in constant evolution (Compute Scotland, 2015). Individual threats, however, can be defined by three common elements: there needs to be an intent, then an opportunity is created or available to exploit, and finally a capability that is not known (a typical Zero Day). While attack methodologies differ depending on the identified targets, and types of cyber attackers (non state actors, organised crime, and hacktivism, to name a few), threats typically involve the above three elements. An illustration of the cyber threat landscape, as depicted by Compute Scotland, can be seen in Figure 2.2.

Cyber targets are assets identified in a cyber environment that are focused on, either to be destroyed, captured or observed. Cyber defence measures designed to combat this include the following: a Network Operations Centre (NOC); a Security Operations Centre (SOC); a combination of the two which is referred to as a Network Operations Security Centre (NOSC) (Spirent, 2017); risk, identity and configuration management; and cyber awareness training.

In summary of the above, the cyber threat landscape is a vast maze of endless patterns of computational code, which makes cyber security very challenging. However, a greater understanding of the cyber threat landscape allows for cyber scenarios to be developed to teach cyber skills to future cyber warriors or security information experts, either to defend or attack a computational network.

Figure 2.2: Cyber Threat Landscape (Compute Scotland, 2015)

The Threat Analysis Group (2010) defined a threat as, "anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset". Thus, a cyber threat can be described as malicious code that compromises a vulnerability, either intentionally or accidentally, causes damage and destroys computational property or information. As stated in the Data Breach Investigations report by Verizon 2018, 94% of cyber security incidents fall into nine basic attack patterns: denial of service (DOS) attacks, privilege misuse, crimeware, web applications, lost and stolen assets, miscellaneous errors, everything else, cyber espionage, point of sale intrusions, and payment card skimmers (Verizon, 2018). Hwang and Bush (2015) describe in a cyber threat model, the terms used most frequently to delineate a threat include the following:

- Threat: a potential event, the occurrence of which may harm an asset.
- Vulnerability: the weakness or flaw that makes a threat possible.
- Attack: the action taken to exploit vulnerabilities.
- Adversary: the actor conducting the attack.

The evolution of cyber threats within cyber space is a huge concern within the global digital age; this is a result of the many different cyber-affiliated transgressions that take place on a daily basis - from nation states to criminal activities and rogue actions, the list is endless. Further, the ever-changing cyber threat landscape is also going through a maturity process, and threats are becoming more and more sophisticated and almost impossible to detect, as noted by multiple cyber security vendors and security reports within the cyber security realm. ENISA (2018) discusses a comprehensive threat landscape report which highlights the main trends captured in 2018.

Table 2.1: Threat Tier Structure (Defence Science Board Task Force, 2013)

Tier	Description
1	Users that rely on others to develop code and deliver mechanisms using known exploits.
2	Users with good knowledge to develop code and tools from known vulnerabilities.
3	Users who focus on the discovery and use of unknown malicious code to target Government and Corporations to steal data and sell it to criminal elements or nations.
4	Criminals or State Actors who are highly skilled and organised in teams to discover vulnerabilities and develop exploits.
5	State actors who can influence the design, development or manufacturing of products to enable exploitation of networks and systems of interest.
6	State with the ability to execute the full spectrum of Cyber capabilities in combination with military and intelligence to achieve a specific outcome politically, military or economically in scale.

While a threat assessment and its process is not covered in this thesis, this project will make use of threat tiers in the development of the proposed CMM for a CR. A threat tier is described as threats that are in distinctive levels and are categorized. The threat tiers are based on the adopted US Defence Science Board 2013 cyber threat taxonomy description (Hwang and Bush, 2015). This tier structure is based on threats which are measured according to the global cyber threat actors and their intent. The threat tier structure is outlined in Table 2.1.

As previously discussed, cyber defence is a major drive in nations and organisations, especially due to the global shortage of cyber skills noted in (Oltsik *et al.*, 2016). Godwin *et al.* (2014, pg 47) defines cyber defence as, "an organized capabilities to protect against, mitigate from and rapidly recover from the effects of cyber attack" and describes cyber defence capabilities as the ability to effectively Protect, Detect, Respond, and Recover, from a cyber attack; these capabilities are also central in Cyber Emergency Response Teams (CERTs). More generally, cyber defensive capability involves counteracting a cyber attack, the basic parameters of which are often called the five "D's" (Hwang and Bush, 2015):

- Deter an adversary from conducting an attack.
- Detect an attack and act against it.
- Deny: prevent an attack from being realised.
- Delay: slow down an attack.
- Defend: mitigate the severity of an attack.

Cyber defence in some cases is referred to as cyber security, however it is the application of cyber security that enables cyber defence in an organisation - this is discussed in more detail in Section 2.3. Being mindful of cyber defence and the application of cyber security with a clear understanding of cyber resilience is fundamental and is

defined by Bodeau and Graubart (2016, pg 1) as "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stress, attacks, or compromised cyber resources", by applying cyber awareness, policies and security mechanisms using people, processes and technology in harmony.

Cyber resilience is imperative for all cyber users, as it forms an incremental maturity in cyber security and thus allows for the ability to limit malicious cyber events within an organisation. Cyber resilience ensures an organisation's survivability (specific to data protection) against a cyber attack, no matter what the circumstances, but this is a tall order in itself (Conklin and Kohnke, 2018). The difference between cyber resilience and cyber security is that cyber resilience ensures absolute security and reliability of critical functions, which the organisation needs in order to continue to survive and carry out its mission. By contrast, cyber security is focused on the information assurance approach, based around creating and ensuring a protection perimeter and assuring all logical points, placing a higher demand on resources and maintenance service (Conklin and Kohnke, 2018).

Cyber resilience only focuses on the critical systems, because that is where the data is handled. Most intruders will want to obtain the data of an organisation. While there is a need to secure every computational logical point, the focus should be on ensuring survivability of an organisation's data to narrow the scope of a cyber attack. Cyber resilience requires a well-documented set of cyber penetrations (incidents) in an organisation's cyber space which are electronic and behaviour-based, and a recovery process if an attack was successful. This is to better prepare against and to ensure that a breach is not executed. An example of a system that can be implemented is a Security Information Events Management (SIEM) which is discussed in Section 4.4.5.

When considering cyber defence, security and resilience, the most challenging aspect of a breach within an organisation is cyber attribution. Irwin (2014, pg 101) describe cyber attribution in the following way: "the source(s) are identified, initially as an IP address, and then resolved using various methods to a source organisation". Wheeler and Larsen (2003, pg 1) define cyber attribution as "determining the identity or location of an attacker or an attacker's intermediary". Shamsi *et al.* (2016) divide attribution into two techniques, namely the technical and the human. Technical attribution can be seen as finding out the host from which the cyber attack or event originated, in which case the use of sophisticated techniques can be used. The human attribution is more complex, as humans can hide their identity, making it difficult to achieve positive confirmation. The three attribution steps as proposed by Shamsi *et al.* (2016):

- Step 1: Identification of the cyber weapon used.
- Step 2: Determining the origin of the attack, and
- Step 3: The identification of the actual (human) attacker.

Cyber offensive actions are in most cases classified - this is the weapon part of the

Figure 2.3: Cyber Kill Chain (Schmidt, 2013)

cyber domain. Godwin *et al.* (2014, pg 49) defines cyber offensive capability as, "a capability to initiate a cyber attack that may be used as a cyber deterrent". An offensive cyber capability will augment a nation's freedom of action in the cyber domain as discussed in Section 2.1, where cyber has become the 5th domain of warfare. The maintenance of cyber offensive capability is largely state funded - research and development within institutions in developing cyber offensive capability, whether national or private, are generally dependent on state funds.

In order to launch a cyber offensive, a cyber attack needs to be planned. There are multiple definitions for a cyber attack, but all are generally similar in nature - to take the Oxford Dictionary's definition, a cyber attack is "An attempt by hackers to damage or destroy a computer network or system". The Goverment of Canada (2010, pg 3) definition is, "the unintentional or unauthorised access, use, manipulation, interruption or destruction (via electronic means) of electronic information and the electronic and physical infrastructure used to process, communicate or store that information". A cyber attack is also related to an act in cyber space that could reasonably be expected to cause harm (Robinson *et al.*, 2018).

Cyber attack methodologies are based on attack trees, which are structured around solving a problem to reach an end state, which is ultimately the cyber attack method and technique itself. The Cyber Kill Chain is a model used widely across the cyber defence environment, and was initially developed by Lockheed Martin (Hutchins *et al.*, 2011). In this model, a specific cyber process is initiated that forms the reconnaissance of a target, which is followed by the development of a cyber exploit, the deployment of that exploit, the exploitation of the target, and finally the exiting and erasing of any traces from the specific target, as depicted in Figure 2.3. and also in Lockheed Martin (2015). CRs are integrated into the cyber threat landscape in a multitude of ways. A CR has the ability to emulate the cyber threat landscape by building basic attack patterns (as in Verizon (2018)) into its scenarios. This ability to model real-world cyber scenarios is one of the many reasons that the use of a CR is central to augmenting cyber resilience and developing the necessary skills to enable

the ability to perform attribution and allow for growth in the capacity to launch a cyber offensive action if and when required.

CRs have the ability to train cyber warriors (CWs) and white hat hackers to utilise exploitation cyber actions on certain identified targets in a computational network or system. This training allows for the use of pre-built scripts as payloads and/or the utilisation of cyber penetration tools, which are available as open-source on the Internet. In a CR, a Red team uses a variety of attack vectors and mechanisms, each implemented to suit the specific scenario or System Under Test (SUT). Attack vectors can include various malicious software (viruses, worms, spyware), phishing techniques, social engineering, fake and malicious webpages, embedded payloads in emails and document downloads, remote exploitation and privilege escalation techniques and various other cyber attack tactics and techniques using multiple exploitation tools to have the desired effect (ISO Institute, 2012b).

The ever-changing cyber threat is also going through a maturity process, as reported by multiple cyber security vendors and security reports across the cyber security realm. This evolutionary maturity of cyber threats has been a constant battle of updating and protecting cyber assets and data from cyber transgressors in all forms. Thus this will impact directly on the capability and the maturity of a CR. Given this context, it is pertinent to reiterate the fact that threat analysis and an environmental scan is paramount. This is to ensure that the level at which the CR is constructed is correct, as it must cater for mitigating those cyber threats to a nation and organisation which have been identified or are unknown in order to ensure that the ability to implement cyber security is at an acceptable standard and level.

A CR is obligated to cater for the requirements and specific cyber threats as set by the organisation it supports. Therefore an important and fundamental comparison between a functioning CR and the maturity of the cyber threat must ensure that they complement each other in that the one works with the other in a synergistic relationship. The identified challenge in this is that the unknown variants are not always captured, and the cyber risk must also be based on exploratory research and development to produce a result. The building of capabilities in the cyber environment, whether it be public, private or military in principle, will follow the same process, and as the CR evolves through its different stages, the capability of the CR will mature.

The products or technology that are used in a CR will ultimately reach their end of life or end of support, however the maintenance of the capability is still to be maintained throughout its life cycle, and the process should be recorded. The threat tier, as determined and categorised according to a level, will allow for a CR to be measured against standard threat tiers, which a CR must be able to accommodate. This use of a tiered system for classifying threats present in the cyber threat landscape gives a good overall view on what types of potential threats will need to be developed within a CR scenario or event and what capability it will need to operate effectively.

2.3 Cyber and Information Security

Any understanding of the difference between cyber security and information security requires clear definitions of each going forward. Cyber security is defined in ITU-T X 1205 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 organisation and user's assets" (ITU Institute, 2008, pg 2). Based on this definition, cyber security can be defined as all governance and technology used to protect an organisation from a cyber attacker.

ISO/IEC 27000 (2009) defines information security as "The preservation of confidentiality, integrity and availability of information in addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved" (ISO Institute, 2009b, pg 3). The Goverment of Montenegro (2013, pg 5) describes information security as "Information security is focused on data regardless of their form: electronic, printed and other forms of data". The most fundamental terminology that is widely utilised in the information security environment is the acronym CIA: Confidentiality - protection against unauthorised data disclosure; Integrity - protection against unauthorised data modification; and Availability - protection against denial of reliable data and services (Hwang and Bush, 2015).

There has been an increasing conceptual fusion over the past ten years of cyber security and information security, and they are often treated as equivalent. This fusion is emphasized by recent shifts in cyber security, which has begun to consider the securing of data as part of its domain (Stevens, 2016). However, it can be concluded that the main difference between cyber security and information security is that cyber security is focused on Governance, Risk and Compliance (GRC) and the technology needed to protect an organisation from a cyber attacker, with an additional more recent interest in securing data. Information security, by contrast, is focused on the data regardless of its form, using the principles of CIA. For a more detailed comparison of the variance in focal areas between these two fields, see Table 2.2.

Similar differences exist between a cyber warrior (CW) and an information security expert (ISE). A CW is described as a solider who is highly skilled in the cyber environment, trained to fight a cyber battle in cyber space both from a defensive and an offensive posture, and who engages in cyber warfare, whether for personal reasons or out of patriotic or religious belief. CWs come in different forms depending on their roles, but all deal with cyber security and information security in one form or another. It is important to remember that there needs to be a balance in the ways in which cyber warriors are utilised; a more detailed analysis of CW's different cyber skills and their economic benefit can be found in the cyber incentive balance.

A general understanding of an expert is an individual who has attained superior performance in a particular domain (Ericsson, 2008). An ISE is described as a highly skilled ICT person who monitors and ensures that there are no security or

Table 2.2: Cyber Security and Information Security Comparison (Knowww, 2017)

Description	**Cyber Security**	**Information Security**
Information in paper form		x
Confidentiality, Integrity and Availability (CIA) of information when using physical, administration or personal security		x
Protection of information and systems from unauthorised access, use, disclosure, disruption, modification, or destruction in order to provide CIA		x
Cyber warfare	x	
Negative social impacts of interaction of people, software and services on the Internet	x	
Online radicalisation	x	
Cyber stalking	x	
Critical infrastructure protection (for control systems)	x	
Part of the IoT security, where no processors are used (some controllers and passive IoT - Radio Frequency identification (RFID)	x	
Protection of organisation and user's assets	x	
CIA which may include authenticity and non-repudiation	x	x

information breaches within the computer system they are responsible for, all while working according to legislation and other best practices and policies. Information security has numerous areas of specialisation, including application security, network defence, intrusion detection, digital forensics and incident response endpoint protection, governance, risk and compliance. Therefore, one approach to determining whether someone is an ISE is to consider the extent to which that person has attained superior performance in one or more of these areas within the broader information security domain (Zeltser, 2017).

Functions determine what needs to be completed to ensure that the desired outcome is reached. Skills enable a human to accomplish their function, and skills are the underlying effect of knowledge put into practical use (Chapaev *et al.*, 2016). In ensuring that the skills competency level of an individual is maintained, a skill needs to be not only taught, but also practised over time. The age-old philosophy - that learning does not stop, but continues every day - is especially true of work in the cyber environment, where the landscape is in constant evolution and human skills need to be updated in the same way as software. A high level comparison were extrapolation and an interpretation of the variation of functions and skills for a cyber warrior and information security expert as presented in Table 2.3.

The cyber incentive balance argument is one of the more interesting debates in this field, and has been around since the earlier years of computer science, when the study of information security generally proceeded by trying to predict what an ad-

Table 2.3: Comparison of Functions and Skills: Cyber Warrior (CW) vs. Information Security Expert (ISE) (Fulp 2003; TechGenix 2018)

Attributes	**CW**	**ISE**	**Remarks**
		Cyber Skills	
Malware Analysis	x	x	Malware analysis both static and dynamic.
Specific Code specialist	x		Develops own specialist scripts of code.
Programming	x	x	Need an understanding of programming languages
Cryptography	x	x	Knowledge of different encryption techniques and cryptography analysis.
Network Infrastructure Specialist	x	x	Security knowledge of ICT Infrastructure and cloud services
Hardware (HW) Configuration	x	x	Ability to configure HW.
Analytic thinking	x	x	Ability to think outside the box.
Strategist	x		ICT Security long term effect.
Security Specialist	x	x	Knowledge of physical and logical ICT security.
Digital Forensics	x	x	Forensics of the digital footprint left on a computational device.
Cyber Threat Detection (Intrusion Detection)	x	x	Ability to maintain and Identify cyber incidents.
Reverse Engineering	x		Ability to dynamically and statically decouple SW.
Redundancy , Backup and Recovery	x	x	Ability to recover, implementing redundancy and backups
		Cyber Functions	
Data Analyst	x		Ability to analyse data in different formates.
Rapid response to a Cyber Threat (Incident Response)	x	x	Ability to Triage.
Maintenance of Network Health	x	x	Ability to maintain optimal performance of a computational system.
Threat, Risk and Security Analyst	x	x	Ability to analyse security risks and threats and act accordingly.
Defence in Depth	x		Ability to ensure a layered defence against cyber attackers on critical cyber national systems
Debugging Software	x		Finding flaws in the SW that is developed.

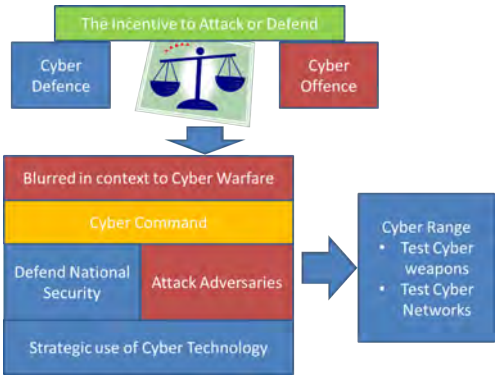


Figure 2.4: Cyber Incentive Balance to Defend or Attack

versary would do and worked off that assumption. This worked well as an approach for encryption, the design of algorithms, and to secure a computer networks and its communication (Moore *et al.*, 2010). The adversary, in this context, is viewed as a group or person wanting to gain unauthorised access to a computer system. This approach has not been viable with the rise of the Internet, as there are significant other needs that must be taken into account to secure a computer network; further, there is an economical view that must also be considered when working to secure a computer network. The economic value of securing information has allowed for a massive growth in the information security market, and this has lead to debates regarding the economical prospects for ISEs and whether there is a balance to be struck from an ethical perspective.

A central issue in the context of this debate is the fact that when defending a computer network, computer security experts are needed and vice versa when an adversary is attacking the computer network. Consequently, security has become a blurred environment, especially in a cyber warfare context (Moore *et al.*, 2010), a reality that has contributed directly to the rise of the cyber warrior, as discussed earlier. One can look to the US cyber command as an apt demonstration of this blurred environment with respect to cyber warfare. A cyber command needs to execute both defensive cyber action - as part of defending national cyber security - and offensive action - by launching cyber attacks against adversaries who intend to harm the cyber security of the nation. These cyber operations, as discussed in Section 2.3, are operations in which both defence and offensive cyber actions are performed. However this approach is a double-edged sword; in order to make strategic use of cyber technology to maintain national security, a CR can be used to test cyber weapons to maintain cyber offensive readiness and test cyber networks to secure and evaluate the networks, as shown in Figure 2.4. Figure 2. 4 highlights work undertaken in the position paper by Moore *et al.* (2010) which presents two scenarios:

- Scenario 1: A nation-state finds a vulnerability, does not make it known, and builds an exploit at the risk of its own civilians, one that can be exploited to their own purposes but is also potentially known to adversaries.
- Scenario 2: A nation-state makes the vulnerability known and secures its civil-

ian population from been exploited.

The logic behind these two approaches is that in Scenario 1, the nation state wants to not only build an exploit, but also stockpile that exploit for its potential use against an adversary. With this scenario, the nation-state will need to have highly trained CWs to defend against the vulnerability; these specialists will also need to be highly skilled to exploit that vulnerability on an adversary's computer systems. In this case, knowing about the vulnerability and maintaining it can give a highly-skilled cyber warrior force an advantage. Conversely, in Scenario 2 the nation-state makes the vulnerability known, securing their civilians but also securing their adversaries against exploitation.

This second scenario is more applicable to a nation-state that does not have well-trained CWs or the cyber capacity to defend itself against a cyber attack from an adversary. This then leads back to the question of what economical prospects there are for information security experts. A nation-state will need to determine what their stance is, whether it be based on pursuing a defensive posture or pursuing an offensive posture (Moore *et al.*, 2010). For obvious reasons both postures are applicable, however the dynamics of cyber skill levels, testing and evaluating capability, the nation's digital readiness, economic power and other factors need to be considered.

Cognisance must be taken of cyber culture, especially in any understanding of how humans are interacting via computational devices and computer networks with each other. Humans using computers have the ability to interact in anonymity, use a persona or simply pretend to be something else within a computer network. This leads to hacker culture, where an individual can operate under the umbrella of many faces, good, bad, white, dark. Hacker culture, as a concept, describes an environment where individuals come together to try to circumvent software and computational devices, working to identify methods to either crack or find vulnerabilities, with the end goal of either demonstrating that it can be done or using the vulnerability to their advantage (Strickland, 2017). However hackers are divided within the hacking community, as in any community; there are many competing dynamics and these dynamics lead to divisions, even though hackers are united in the more general goal of hacking computers.

Utilising a CR is a strategic way to integrate the training of CWs and ISEs in protecting computational systems while learning skills to either penetrate or exploit adversarial systems. There is a thin line between a military cyber operation and a public or private cyber security intervention due to laws of a given state. One of the main functions of the CR is to train CWs to defend and attack an adversary under the auspices of a military mandate, and to train ISEs to defend and follow appropriate legal processes to apprehend a cyber attacker. The CR should be able to test cyber weapons and cyber networks in a closed sandboxed and virtual environment. The impact of cyber and hacker culture on cyber training and the development of cyber scenarios must be understood in order to contextualize the many different attack vectors and Tools, Tactics, Techniques and Procedures (TTTPs) that are currently in

use.

2.4 A Cyber Range Overview

This Section will present a high-level view of a CR, as presented in current literature on CRs. There are multiple definitions for a CR, all of which centre on its abilities and functions and the specific purpose for which the CR is developed. From a military perspective, the use of the term "range" in this context - a piece of land which is used to practice using military capabilities to prepare military forces - underscores the way a CR is a virtual version of a military or industrial shooting range.

The basic understanding of a CR is a contained cyber environment that utilises and enables access to virtual computational networks, providing tools for learners to execute Capture the Flag (CTF) and Cyber Defence Exercises (CDX) (Ošlejšek *et al.*, 2018) as detailed in Section 2.4.4. The general composition of a CR is hardware (computational devices which enable a the CR), software (the operating systems and applications in the CR), firmware (the software to drive the computational devices), wetware (the people skills to operate and processes to operate and use the CR), traffic generated (generate IP/RF traffic and security threats), and scenario generator (to allow for cyber security event to be generated for a response).

A CR is important within System Security Engineering (SSE) and Risk Management Frameworks (RMF) (Cooper, 2018), as a response to cyber threats that are very prevalent, and to prove cyber security policy in systems. A CR also speeds up the evolution of cyber technology, both in computational performance and security due to the CRs flexibility, and its ability to provide quick identification of vulnerabilities within the cyber realm.

The core capability elements of a CR are identified and defined in Section 4.4. Ošlejšek *et al.* (2017) alludes to CRs having mainly four types of services that they offer: resource management, interaction of users with hosts, monitoring services, and learning and understanding of cyber security processes. Ultimately, there is no distinctive definition of a CR that can be firmly agreed upon, as a result of the many different purposes or different perceptions people focus on in defining a CR. This is discussed further in Section 6.2 with several key definitions outlined below:.

- USDOD (2018, pg 68) define a CR as "An event environment that supports cyber effects on information technology; weapons; C4ISR; and other network-enabled technologies for experimentation, testing, training, or exercising on a real or simulated network".

- European Cyber Security (2016, pg 100) define a CR as "A virtual environment typically built on top of standard hardware and used for multi-tenant hands-on training, experimentation, test and research in cyber security, supporting CDX's".

- NIST (2017, pg 1) define a CR as "An interactive, simulated representations of

an organization's local network, system, tools, and applications that are connected to a simulated Internet level environment. They provide a safe, legal environment to gain hands on cyber skills and a secure environment for product development and security posture testing".

A CR's main focus is on training and exercising different cyber events, due to the constantly evolving nature of the cyber threat landscape. A CR, as a training tool, can assist in the technical skill growth for CWs or a ISEs. A CR has more flexibility, in that it has the ability to test cyber competency in organisations, T&E and hardening cyber technologies used in computational networks from a cyber security view, and can also be used to plan, develop and test a response against a cyber-onslaught on a specifically-designed network infrastructure (Davis and Magrath, 2013). In this context of this thesis, a CR is defined as a closed sandboxed and virtualised cyber lab environment used to perform the following tasks:

- Model, simulate and emulate with high fidelity utilising computational systems in a distributed, federated or independent method.
- Replicate and build cyber capabilities, whether in individuals through cyber training with multiple cyber scenarios augmenting cyber resilience, in cyber processes that govern the cyber posture of an organisation, or in technology by undertaking research and development of computational cyber product.
- To emulate appropriate cyber defences and retaliatory means through testing, evaluation, verification, validation and certification, with the utilisation and integration of different sensors and instrumentation.

The context in which a CR can be utilised will vary depending on its various implementations in multiple clusters. A CR is part of the cyber ecosystem which enhances cyber security within these clusters, industries and private sectors. The CR application for different contexts as extrapolated and interrupted by the author from NIST (2015) and is described in Table 2.4. This context is a holistic representation, in which areas a CR can be applied to augment cyber capabilities, namely:

- The security cluster organisations, for example military (cyber warfare), police (cyber crime specific to forensics and attribution), intelligence agencies (cyber collection), and the Justice department (forensics).
- The Economic cluster, for example banking sector with specific focus on incident response.
- The research and development cluster, for example institutions, and universities focus on experimentation, T&E and verification in the cyber environment.
- The Industry sector focused on critical infrastructure.
- Telecommunications sector focused on ICT infrastructure, static, mobile, and terrestrial.

- Engineering sector focused on ICT in systems.
- Small Macro Economies (SMEs) focused on cyber resilience in companies and private usage.

Table 2.4: Cyber Range Applications in Different Contexts (NIST, 2015)

Cyber Security Training Exercises	**Testing Computational Products**	**Testing Cyber Payloads**	**Testing Computational Applications**	**Testing a Computational Designed Network**	**Other Testing**
Generate Cyber Events and Exercise Scenario on layer 1 to 7 (Open Systems Interconnection (OSI) stack on IP and RF platform.	Benchmarking the true products computational capability and behaviour on a network.	Using emulated methods to test Cyber Payload (Either defensively or offensively) behaviour before deployment.	Benchmarking the true SW and FW capability and behaviour on computational devices.	Confirming the computational design of a network for feasibility in a current network and setting up the configuration.	Other computational and war gaming simulations and emulations.
Cyber Events and scenarios on demand at high speeds, fidelity and the ability to distribute and or federate timorously.	Testing a baseline system and configuration with computational products before deployment into a network.	Testing of propriety SW as developed for a specific functionality or purpose for an organisation.	Benchmarking the true HW capability and behaviour on computational devices.	Testing of wired and wireless Infrastructure.	Exercising a Cyber Attack scenario on a war fighting physical battle platform grouping; Cyber Warfare.
Cyber CTF and CDX.	Testing of vulnerabilities on computational products.	Testing for detection of payload.	Testing of vulnerabilities in computational applications.	Testing of setting up the configuration.	Testing of research and development of new computational technology.

2.4.1 Brief History of Cyber Ranges

The JGN-X (Japanese Gigabit Network)[1] is a gigabit class network, large scale multi cast IPv6 environment, and advanced optical test bed network. It has been developed by the National Institute of Information and Communications Technology (NICT) in Japan since 1999 (NICT, 2016). NICT also collaborates with the large scale emulation environment, StarBED3, to enable a test bed for experiments, from emulation to a wide range of network experiments (NICT, 2016). One of the first concept CRs, which has been in operation since March 2004 and was used for academic testing for

[1]https://testbed.nict.go.jp/jgn/jgn-x_archive/english/info/what-is-jgn-x.html

medium scale-computer security testing, was the cyber-Defense Technology Experimental Research (DETER) test bed (Benzel *et al.*, 2007). The development of CRs really started to gain momentum from early 2009 to 2012, when the United States of America at the Defence Advanced Research Project Agency (DARPA) developed a National CR (NCR), which was handed to the US DOD Test Resource Management Centre (TRMC) in 2012 and then operationalised for US DOD cyber training and experimentation (TMRC, 2015). The USA NCR provides a large-scale Global Information Grid (GIG) infrastructure, in which technologies are tested in their current state and projections are made for the future. A CR must have the ability to test new network protocols, satellite, radio frequency (RF) communications, and mobile tactical and maritime communications (DARPA, 2008).

The USA DoD has a federated set of CRs called the "DOD Enterprise Cyber Range Environment" (DECRE3), which include the National CR (NCR), the DoD cyber security Range, the Joint Information Operations Range (JIOR), and the Joint Staff J6's C4 Assessments Division (C4AD) (Damodaran and Couretas, 2015). This is a joint CR environment that allows for multiple streams of cyber security training and testing and evaluating people, processes and technology within the cyber domain. Since 2012, multiple CRs have been developed that cater for military, public and private entities, and which are fully functional and powerful enough to deliver multiple capabilities in various methods. A selection of these are mentioned in Appendix A, however this is by no means the entire list of CRs globally. For a more complete survey of cyber ranges and test beds, see (Davis and Magrath, 2013).

2.4.2 Cyber Range Evolution

Older, more traditional CRs have extensive physical infrastructure and data centre needs; as a result, their reconfiguration involves a great deal of effort, can take time to change, and is a very involved task (Pridmore *et al.*, 2010). New CR are virtual, instantaneous, on demand, configured speedily, distributed and federated. They also have the ability to be provisioned and accessed through a cloud service provider using an Internet connection by using authentication credentials. For example, in the NCR, the concept of Flexible Automated Cyber Technology Range (FACTR) has been applied. FACTR consists of two core elements, namely a tool suite that has the ability to automate, construct and validate high-fidelity test beds using a common pool of resources, and a Cyber Scientific Methodology (CSM) that supports end-to-end cyber testing (Pridmore *et al.*, 2010). In a traditional CR resources are needed to run a cyber event, with an additional need of highly skilled specialists to develop, operate and maintain the necessary HW needed. Specialists are also needed to perform configuration and setup, to build the network and routing, and install cyber defensive tools, services, traffic generation and applications, all in support of the cyber event. This is a mammoth task which takes large amounts of planning, cost and time. The drive to increase in scaling the CR size and capabilities in order to have more realistic networks and generate more traffic has increased the complexity far more and

driven up CR operation and maintenance costs significantly. Hence the HW of a CR are consistent generally, but the network topologies, services and traffic will change depending on the specific cyber event being generated (Braje, 2016).

A primary challenge in this arena involves maintaining human capacity, or the cyber skills needed to operate, support and maintain a CR, especially if the CR is of a sizeable nature and federated. There are currently many collections of CRs maintained globally, and there is a drive towards federating CR between nations and militaries in order to optimise through collaboration the skills needed, the cyber scenarios, infrastructure and cyber tools. The CR as a concept can be seen to have developed in conjunction with the evolution of the cyber environment as T&E within the cyber environment has become more and more imperative.

The CR has grown exponentially from its humble beginnings as a computer test bed in which the testing of hardware and software was defined, developed, verified and certified for its purpose, under a specific specification and standard. Likewise, the cyber environment in the past few years has grown at a massive rate. A prime example of this is the Internet of Everything (IoE), which is growing exponentially and needs to be connected to the Internet continuously (Banafa, 2016). There are multiple different variations of CRs that have been developed in the commercial market environment and within government, especially in security departments throughout the world. Since then, CRs have broadened their horizons to keep as close to the hyper-real cyber environment - one emulated with high fidelity to give a hyper-real feel, as if living in the cyber space. The European Defence Agency is in the process of establishing one of the first cyber defence pooling and sharing projects as part of the CR federation project, which includes eleven European countries, with the lead being the Netherlands. This project is focused on closing capability gaps in the cyber domain with a federated CR (European Defence Agency, 2017). There are multiple different approaches in the utilisation of a CR, each of which fit a specific purpose for their different organisations, whether in the military, public or private cyber environments.

With this in mind, there is a definite increase in the demand for CRs, as stated by (Eborn, 2017): "To meet the growing demand for cyber vulnerability testing and training, the Defence Department's Test Resource Management Centre (TRMC) wants to set up and operate an integrated suite of facilities like the National CR". An example of this can be seen in the growth of the National CR (NCR), the Michigan Institute for Technology (MIT) CR, and the NATO (CCDCOE) CRs. Figure 2.5 reflects the author's view of the exponential growth of CRs over the past few years and the growth of cyber threats; from this it can be deduced that the need for CRs globally is increasing. In future, the focus of the traditional CRs will be augmented to provide a more focused view in Next Generation CRs (NGCR), which will be the next step in the CR evolution. There is a huge drive for NGCRs (Vill, 2018), which are more agile because they use higher computational performance and have the ability to respond to real-time cyber scenarios and or transgressions automatically through the

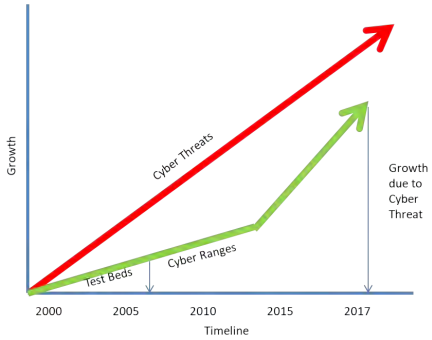


Figure 2.5: Growth of Cyber Ranges Globally

utilisation of Artificial Intelligence (AI) and Machine learning (ML) during Red and Blue teams training. The NGCRs are smarter families of systems (different systems having similar characteristics, namely CR capabilities), which are also integrated, distributed and federated (Spirent, 2017). Their abilities include the emulation of multimedia and audio services. Further, their graphical user interfaces (GUIs) are smarter and more user-friendly while also providing access to multiple use-cases. An example of this is the SMART GUI, in which the user is able to map Internet Assigned Number Authority (IANA) IP addresses by regions, emulate Global Navigation Satellite System (GNSS) and General Packet Radio Services (GPRS), along with 3/4/5G cellular networks, wireless families (802. 11 variations) network traffic (WEP, WAP2/3), Bluetooth short range wireless communication, and Next Generation Networks (NGN) devices (for example smart firewalls and switches).

Development Operations (DEVOPS) in private clouds is a growing environment, especially with respect to the development of cyber scenarios for a CR (Edwards, 2010). The ability to use data leaks as a concept within a CR is a possibility, as is the emulating of the "Quantum Internet" within a CR, based on quantum entanglement (a type of encapsulated encryption) (Wehner *et al.*, 2018). A final possibility is FOG computing or FOG networking, which is an architecture that a CR can utilise and which uses one or a collaborative multitude of end-user clients or near-user edge devices to carry out a substantial amount of storage (rather than stored primarily in cloud data centres) (European Cyber Security, 2016). It is also worth noting that the technologies in gamification are on the rise and can be utilised in Cyber Defence Exercise (CDX) and Capture the Flag (CTF) exercises to augment and create a better sense of a hyper-real cyber environment for cyber training.

The use of Artificial Intelligence (AI) methods such as Machine Learning (ML), which learns in different ways from the data created within the CR, will enhance the CR effectiveness and performance. ML is becoming a huge driving force in today's technology, in that systems are becoming more independent in nature. ML is also on the rise globally in different industrial platforms. Alpaydin (2010) explains the primes on which ML is based, using data or experience to program a computer to optimize a performance criterion. Murphy (2012) describe the goal of machine learning as the automatic detection of patterns in data to predict the future and other out-

comes. Bishop (1999) gives another view of pattern recognition, which focuses on the ways in which computer algorithms can be used to discover regularities in data.

Data - and a lot of it - is needed for ML to take place, and there are a number of different ML techniques that can be used. For a CR, ML can be applied in concept, and is an added benefit in the following method: data captured to form a pattern which can predict cyber threats. Capturing CW and ISE responses to identify failure points in their processes and skill development will generate a quicker response time and give a more accurate result, thus the quality of service (QoS) will improve in the CR. Another AI Method that can be used is affective computing, which is the machine equivalent to human emotional intelligence; this can be utilised to improve computer human interaction and interpret human activities and behaviours. For example, it can be used to detect human emotions, facial expressions, the way a person types text, and other human behaviours (Spacey, 2016). This method of AI will identify gaps in users' actions during a cyber event. Using ML will enhance the sustainability of the CR system health, and provide a higher turn-around time for testing multiple systems as in, work completed by Rege *et al.* (2018) namely, *"Predicting Adversarial Cyber Intrusion Stages Using Autoregressive Neural Networks"*.

2.4.3 Purpose and Types of a Cyber Range

A CR's main purpose for existence is the cyber threat landscape, as discussed in Section 2.2, with a primary focus on cyber training (CDX and CTF) of CWs in a military sense and ISEs in a civilian sense. Utilising a CR and generating cyber events augments cyber skills and processes to defend against cyber threats as part of the development of cyber resilience. Examples of these cyber events are corporate disaster recovery exercises, data breach exercises both in public and military, cyber skills assessment, cyber security awareness training, penetration testing exercises. Secondary focuses allow for the T&E and integration of any type of computational devices to determine functionality under cyber stressed conditions, and possible reactions under certain cyber scenarios. Finally, certain attack vectors determine how secure the ICT in a contained environment is. This service is referred to as Testing as a Service (TaaS).

For the utilisation of a CR there needs to be competent cyber skilled resources available to support operate and maintain a CR, and for this reason the CR resources should consist of a cyber test team, including highly valuable and highly cyber-skilled people to fulfil multiple services, namely end-to-end test support, test bed design support, cyber and test expertise, threat vector development, customised traffic generation, sensor and visualisation support, customised cloud support, custom data analysis, integration of custom assets software (SW), hardware (HW), wired and wireless, and remote Red and Blue team and other teams, as in Section 2.1 (TMRC, 2015). There are multiple other purposes for the application of a CR: testing critical infrastructure (Supervisory Control and Data Acquisition (SCADA) networks); as a test platform for HW, SW, and Firmware (FW); reverse engineering; testing cyber tools;

testing ICT projects for security testing on systems; testing of disaster recovery (Baham and Kisekka, 2015); testing of the Internet of Things (IoT); and the Industrial Internet of Things (IIoT); mobile environment testing and other ICT experimental testing; and the facilitation of forensics training.

The extensive list of purposes for a CR listed above demonstrate the need for skilled cyber resources to support, operate and maintain a CR. It is also important to note that the establishment of boundaries reflects the author's view as depicted in Figure 2.6 is central for the purpose of a CR. The ethics of a CR need to be defined in specific areas, which will then determine the application of the CR, for example;

- The testing capability for Governance, Risk and Compliance (GRC) in organisations focused on processes.
- The research and development capability to augment the CR evaluation as an instrument in a virtual environment.
- The providing of different cyber resilience training including cyber events and exercises.
- Cyber testing, evaluating verifying, validating and certifying of ICT as a whole.

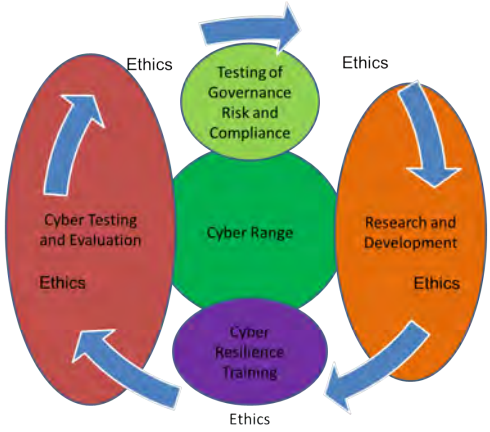


Figure 2.6: Boundaries of a Cyber Range with Ethics

The purpose and application of a CR will determine its ideal type and size for a given organisation, and whether the organisation will choose to either develop or go through an acquisition process. It is crucial that the requirements for a CR be formulated from the business drivers of an organisation in order for that organisation to position itself towards its cyber strategy and cyber resilience policies. There are various types and sizes of CR, all of which are implemented via different methods, namely the cloud and the stack methods. CRs which are more stack-based have a physical infrastructure that is on site. The following examples illustrate the stack-based CR: constructing a static facility for fixed small, medium and large CRs utilising computational HW and SW of which some examples are in Appendix A. A "CR in a box" is a

concept that allows for a CR to be portable in nature and provide Cyber training on the go (Bell, 2014).

CR in the cloud as a concept uses cloud services to provide CR on-demand services and storage utilising the cloud Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) for different public, private or military CRs, dependent on access and authorisation of use. Anything as a Service (XaaS) is an added concept, which refers to an increasing number of services that are delivered over the Internet rather than provided locally or on-site (European Cyber Security, 2016).

Edwards (2010) explains that the transition from products to services has impacted on SW development, as companies that develop SW and developers also operate on SW due to the cloud concept, in which SaaS is on all layers of the IT stack. Edwards (2010) also alludes to the fact that IaaS delivers on-demand virtual machines, networks, and storage. PaaS delivers on-demand databases, caches, workflow engines, and application containers. SaaS delivers on-demand functionality and can be applied to CR functionality, allowing customers to consume services based on demand, pay for them based on consumption, and relinquish responsibility for the masses of traditional stack-based CR infrastructure.

An example of a cloud service provider is Amazon Web Services (AWS)[2] and Microsoft Azure[3]. These providers are global cloud platforms that host services on the cloud to run applications, providing IaaS, SaaS, PaaS and storage. These services are able to create instances, virtual private clouds (VPC) to create networks, virtual storage, relation databases, DNS Scales according to demand, load balancing and automatic scaling. These services are paid for on demand or over a certain period.

Priyadarshini (2018) has classified the types of CR as follows: Military, Defence and Intelligence focused on the cyber warfare capability; Education, focused on the idea of "CR for education" - a collaborative effort between military, industry, and research institutes based on cloud-based CRs; Enterprise and Commercial CRs from vendors specific for commercial organisations to train in cyber defence activities; Service providers that offer CR services; open-source CRs providing free access to learn cyber security skills and law enforcement, focused on application testing for responding to cyber crime and forensics. The European Cyber Security (2016) describe two types of CR, namely open ranges - to involve more participants in the exercises, trainings, testing, experimenting and so forth in a collaborative manner - and closed black box ranges - for parties that need a closed environment to conduct classified trainings or testing.

The federation solutions for CRs allow for the utilisation of capacity and capability of other CRs, which while providing cost savings for an organisation will also require a high integration of systems capabilities. The federation of CRs' minor hardware can be procured to maintain the storage space or speeds needed for the CR. Challenges to the development of a traditional CR include a lengthy procurement and configuration

[2]https://aws.com/

[3]https://azure.microsoft.com/en-us/

time and effort in getting the stack operational. The traditional CR is more of a silo infrastructure and requires a large workforce to deploy, monitor and manage. There has been a significant shift in focus from the traditional stack CR to a Hyper Converged Infrastructure, which includes software-defined infrastructure containers within a CR, and to making use of cloud services providers to host CR cyber events. For any organisation considering the balance of funds versus operational capability, a determination must be made if it is feasible to continue to develop a certain type and size of CR, or whether it is more beneficial to procure or pay for CR services.

2.4.4 Training and Skilling in a Cyber Range

Cyber skills will need to be defined by the purpose and task that the cyber skill needs to perform in the CR. Thus the cyber skills level will need to be determined from the complexity or basic needs of the cyber environment the participants are exposed to. The fundamental skills that are generally required for a CR to operate include cyber strategic and operational management; cyber security; cyber analysis (with its subsets malware, threat, and risk); networking (physical and virtual); cyber scenario planner, designer and developer; computer programming skills in various languages; and mobile and web application developer. This list is of course dependent on the purpose of the CR. Oltsik *et al.* (2016) indicated that the cyber security skills shortage has increased exponentially, rising from 23% in 2013 to 25% in 2014 and 28% in 2015. Most recently, Enterprise Strategy Group (ESG) stated that in 2018 that 51% of organisations have a problematic cyber security skills shortage, implying that the cyber security skills gap is getting worse (Oltsik, 2018). The European Cyber Security (2016) alludes to allowing stakeholders to utilise CRs in a shared and secure manner for integration and collaboration for cyber security training, especially cyber training exercises, as these can solve some challenges in the CR domain.

Information Systems Security Association (ISSA) and ESG have warned organisations who are trying to defend against increasing threats and comply with the implementation of regulatory demands with a cyber security team that is understaffed and lacking advanced skills (Security, 2017). Mavroeidis and Bromander (2017) state that security analysts and incident responders need the right skills to recognize attacks before performing defence efforts. Cyber skills is a concern in multiple organisations and the demand thereof has increased; training to augment cyber resilience is therefore an imperative in organisations to ensure good cyber governance.

Testing response time for a cyber incident or event is vital for a CW's or ISE's effectiveness against a threat, and the correct cyber competencies and ability to work under pressure will enable a short response time. it is imperative to understand what is needed to train cyber security personnel in the current era of complex cyber attacks; to understand a cyber attack requires an understanding of different techniques and forms of malware, namely polymorphic, metamorphic, hybrid, worms, viruses, trojan, file-less malware and many more. It is also crucial to understand how an attack was executed, what to look for, and how to stop it. Time versus the cy-

ber activity is another important consideration in training, as time will be needed to firstly train users in the beginning of a cyber activity to obtain a certain level of cyber skill. As learning takes place, time needs will then decline. Consistently monitoring the time that learning takes is an effective method in which one can pace the amount of time needed for training in a CR.

Ošlejšek *et al.* (2018) allude to two main cyber exercises: Capture the Flag (CTF) and Cyber Defence Exercise (CDX). A Capture The Flag (CTF) exercise is an exercise in which users practice attack skills while executing a single task at a time in an incremental approach to obtain hidden flags in a cyber scenario. A cyber scenario for a CTF is developed on different layers, from basic to highly advanced, for users to attack or defend using both tools provided locally or online. This aim of the exercise is to simulate a cyber environment where participants can execute cyber actions to solve cyber challenges and gain as many flags as possible.

A CDX is a more complex and closer to real-world cyber events scenario, in which there are several cyber issues and events to maintain at a given time. A CDX is a well-planned and coordinated event which needs highly-skilled people in multiple different cyber domains, namely cyber security, education law and media. Within the CDX there are specific teams in the exercise beginning with the Blue team, which defends systems from the Red team, which attacks the Blue team's systems with a specific goal in mind. The White team controls scores and implements rules for the orchestrated cyber event by injecting different cyber incidents which changes the cyber attack or changes the configuration of a server on the Blue team's system. The Green team maintains the infrastructure and other assets in the CR (Ošlejšek *et al.*, 2018).

For a CTF or CDX exercise to function at an acceptably realistic level, the type and size of the CR needs to be considered. Similarly, Brundage *et al.* (2018) describe the practice of Red teaming, in which a "Red team" composed of security experts or members of the organisation deliberately plans and carries out attacks against the systems, processes, policies and practices of an organisation (with some limitations to prevent lasting damage), while an optional "Blue team" responds to these attacks. These exercises explore what an actual attack might look like in order to better understand and improve the security of the organisation's systems and practices. Damodaran and Couretas (2015) also states that there are different teams that are allocated in a CR to function as different disciplines; these can change depending on the organisation's naming convention for their teams or entities.

Kick (2014) has stated that cyber exercises that are conducted should have a "Hot Wash Session". This is a session for discussing lessons learned, including where to improve on the exercise conducted and potential areas for skills improvement for the CWs or participants. Based on this output, a training program is suggested, and is to be made viable so that improvements on a re-run of the exercise can be performed. Table 2.5 illustrates the generic process steps for a cyber event: planning and preparation, allocation of resources and a dry run in testing the cyber event, and

the execution and analysis thereof, with a final step of sanitising the CR. The Detec-

Table 2.5: Generic Process Steps for Conducting a Cyber Event

Ferguson *et al.* (2014) **Suggested steps for NCR**	Damodaran and Couretas (2015) **Suggested steps**	Ošlejšek *et al.* (2018) **Adopts four phases for a cyber scenario or event**
Define the test is a planning cycle that needs to be confirmed, to ensure that the test or the evaluation is what is required to be completed.	Planing the cyber event, (gathering the requirements, designing for a specific goals that is to be achieved.	Preparation Phase: This is phase where planning takes place over many months in which the outcome is the detailed scenario, the rules, scoring system, and the infrastructure deployed
Allocate resources for the cyber event that needs to take place.	The deployment (creating a virtual environment) within a physical stack or cloud infrastructure in which a System Under Test (SUT) is being tested.	Dry run Phase: This is testing the planned detail scenario.
Configure the hardware and software that needs to be utilised in the test or the evaluation.	The execution (start the cyber event).	Execution Phase: This is when the participants play the CDX
Run the test, with the support of the allocated resources according to the test or evaluation plan.	Analysis and evaluate the event and assess the performance of the cyber event.	Evaluation Phase: This is the phase in which all aspects of evaluation is executed, this is also done on all phases and especially during the CDX to aid in the improvement, and lessons learnt
Obtain the results captured and do analysis, complete a report give feedback and augment the event if needed and log in a data base.		
Sanitize the resources used for the cyber event, to be ready for the next cyber event.		

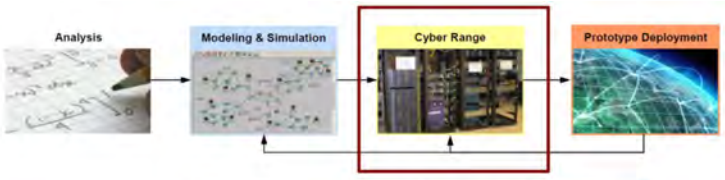
tion Maturity Level model as proposed by Stillions (2014) describes the maturity of an organisation based on their ability to act upon given threat information. Threat information include Indicators of Compromise (IOC), Tools, Tactics, Techniques and Procedures (TTTPs) of an actor, threat intelligence reports, and so forth (Mavroeidis and Bromander, 2017). This model can be adapted for skilling CR users in terms of handling threat information and responding to a cyber incident.

Governments, public, private and military personal in today's complex cyber en-

vironment need to have a basic knowledge of cyber security. For this reason, the author suggests Cyber Immediate Action Drills (CIAD) are to be implemented within the basic education structures of society. This can be compared to the basic first aid course that is taught generally in schools. CIAD is a fundamental building block within the educational curriculum to use in every day life when using the cyber space with computational devices. Here are some basic CIADs that can be implemented as a quick win: (as per author reference): avoid opening an email that is suspicious and not identified or trusted, enable spam filters, update anti-virus, update operating systems and firmware, back up files off-site, and store cryptography keys on another device, amongst others. The relevance of this in a CR is to get foundational cyber awareness implemented across an organisation.

2.5 Modelling, Simulation and Emulation for a Cyber Range

A CR will need to model, simulate and emulate cyber activities at a level of fidelity - high or low - depending on the amount of nodes that are virtualised in a contained environment, to enable a close-to-hyper-real cyber environment. Most CR events are sandboxed and not connected to a live network or the Internet. Modelling, simulation and emulation will save costs when creating and practising certain cyber events and testing in a CR. Figure 2.7 provides some guidance for choosing a cyber event environment, as drawn by USDOD (2015, pg 61): by analysis, modelling and simulation, emulation or prototype development, of which a CR has the ability to maintain the last three environments described.



	Analysis	Modeling & Simulation	Cyber Range	Prototype Deployment
Fidelity	Low	Low	Moderate to High	High
Scalability	High	High	Moderate	Low
Cost	Low	Low	Moderate	High
Repeatability	N/A	High	Moderate to High	Low
Program Phase	Early	Early	Mid-term	Mid-term to Late

Figure 2.7: Cyber Event Environment (USDOD, 2015)

2.5.1 Modelling

Modelling is using a mathematical formula or representation to copy a system in the same method the system would operate to predict an outcome or a result. Models allow us to reason about a system and make predictions about how a system will behave (Astrom and Murray, 2010). An example of a modelling tool is Riverbed[4], which can model systems and simulate their behaviour.

[4]https://www.riverbed.com/

2.5.2 Simulation

Simulation in general is to pretend that one deals with a real object while really working with an imitation, and is useful for studying a system's behaviour. In a CR the simulation is a computer model of the simulated reality, for example a power supply system in which Programmable Logic Control (PLC) are modelled and are then simulated as part of a power plant system to observe the PLC behaviour. Arsham (2015) compares this to a flight simulator, which is a model for flying an aeroplane, and is implemented on a computational platform on a computer, showing on the screen the controls and what the "pilot" sees from the cockpit. Mammadov (2017, pg 6) describe simulation as "a tool that, given an input, uses mathematical modelling or software techniques to generate an expected output based on what the model is supposed to be simulating". Calheiros *et al.* (2013) suggests that simulations rely on models of software and hardware for evaluation, implying that a model needs to be developed for simulation to be effective for evaluation.

Simulation as a whole requires less hardware resources than emulation for experimentation due to developers using models and applications to simulate whole systems. Thus, simulation does not have scalability limitations, as is the case with emulation, however simulation results are as accurate as the model of the software submitted to the simulator, so accurate modelling is key in simulation (Calheiros *et al.*, 2013). Thus, simulation simulates a system's behaviours, similarly to the real system, using models dependent on its accuracy, therefore not according to a system's rigid rules. Henninger *et al.* (2008) describe the Live, Virtual, Constructive (LVC) simulation terminology that is utilised to classify kinetic CR simulations which has been adopted in CRs, in which live and virtual simulation provides a better level of fidelity in CR than a constructive simulation. Damodaran and Couretas (2015) has described these terminologies as follows:

- Live simulation: operate on and with actual systems and protocols. Due to being a closed contained environment, live simulation is considered simulation because the scenario is simulated and attacks are not conducted against a live cyber threat.

- Virtual simulation: physical assets may interact with limited or representative system models and visa versa.

- Constructive simulations are limited or representative asset models.

In the context of a CR, simulation imitates the cyber events of a real-world cyber threat in a closed environment. Some examples of simulation software platforms used in CR include Metova[5], Cyberbit[6], Tintri[7] and others (Priyadarshini, 2018).

[5]https://cybercents.com/
[6]https://www.cyberbit.com/
[7]https://www.tintri.com/

2.5.3 Emulation

Mammadov (2017, Pg 6) describe an emulator, as a "tool that actually performs the actions in between the input and output stages of the process that yield in the desired output". Davis and Magrath (2013, pg 5) describe emulation as "the process of mapping a desired experimental network topology and software configuration onto the physical infrastructure of the CR". Emulation emulates a system that behaves exactly like the system must in the real world, with all the system rules, in a emulated environment using SW, for example EXate[8], CORE[9] and others. Calheiros *et al.* (2013, Pg 596) states, "emulation uses the actual software deployed in a model of the hardware infrastructure". Emulation is also more suited to be utilised once an application software prototype is available, however emulation has limitations specific to scalability and hardware constraints or the difficulty in generating large and realistic workload (Calheiros *et al.*, 2013). Schiess (2001, pg 1463) present the following analogy:

> "Emulation is the marriage or combining the two worlds of two distinct disciplines, namely the simulation and controls designs, (controlling SW of the system), to effectively achieve 'virtual world'".

Emulation ensures that the behaviour of the real ICT system is copied, implying that an emulator tries to duplicate the inner workings of the device in real time and emulates physical HW and SW of a system. The emulator SW allows for the full functionality of the hardware and its original SW code in the emulator. An emulator can be used for large ICT systems; the balance of true results will need to be weighed, however the results are very accurate as there is no approximation. The use of having a System in the Loop (SITL) and/or the Operator-in-the-loop (OITL) in cyber events that are emulated will allow for a more mature assessment approach that includes decision making and human performance within a CR.

2.5.4 Fidelity

Lewis *et al.* (2012) indicates that simulators perform at low or high fidelity depending on how closely they represent real life. All network components, such as switches and virtual hosts, behave in a highly predictable way while they operate in HW. When these components are emulated, the behaviour of these components should be close to the real way the component operates in real time, this is where the high and low fidelity during emulation takes place. The term "network invariant" (Heller, 2013) describes the delay that is inherent in a real network and is to be considered when determining low or high fidelity.

To achieve network invariant, the emulator needs to consider and calculate the error during an emulation run so that the network invariant for a network can be emulated as close to a real time cyber environment as possible. Fidelity is viewed as

[8] https://www.scalable-networks.com/exata-network-emulator-software/
[9] https://www. nrl.navy.mil/itd/ncs/products/core/

the ability to ensure that the emulation performed in a CR is as close to the hyper-real network environment to ensure that the factor of "network invariants" is considered during the emulation of nodes. In ensuring high fidelity, the number of nodes provisioned are to be considered - as more nodes are emulated, fidelity will decrease. Achieving a high level of fidelity with its complexities is a key consideration for a CR to be as accurate and close to a real-time environment as possible.

2.5.5 Hyper Real Environment for a Cyber Range

Bonanni (2006, pg 130) describe hyper-reality as "distributed computing interfaces that weave existing environments with additional channels of sensory feedback to enhance everyday activities without confusing users". Making use of virtual reality, augmented reality, tangible interfaces and ambient displays add new channels of digital information to the "real world" without overwhelming users (Bonanni, 2006). By ensuring the quality of simulated content by being more illusionary, where virtual reality is at one extreme and reality at the other, hyper-reality can be seen as extending the spectrum of how "real" an experience feels by superimposing sensory simulation based on the existing environment. Hyper-reality is seen as a condition in which what is real and what is fiction are seamlessly blended together. Some famous theorists of hyper-reality and hyper-realism include Jean Baudrillard, Albert Borgmann, Daniel J. Boorstin, Neil Postman and Umberto Eco. In Figure 2.8, an adapted synthesised view is depicted, from virtual to hyper reality.

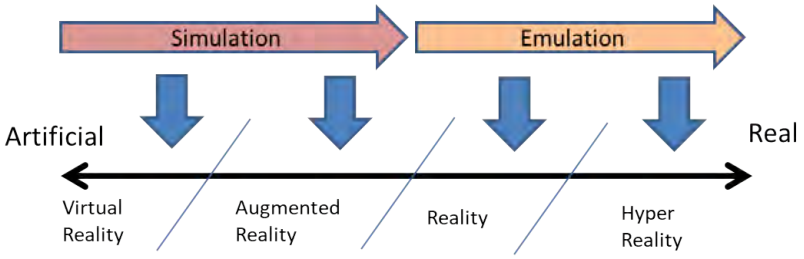


Figure 2.8: Virtual to Hyper Reality as synthesised. After Bonanni (2006)

Baudrillard (1988) suggests that hyper-reality is a result of simulation, utilised to replace actual objects and experiences. Using the science of emulation and high fidelity and the ability to create a hyper-real environment is key to ensuring that the CR has the ability to perform as it would on a real computational network. A hyper-real environment can be described as an environment that matches the real cyber world through the utilisation of computational devices and instrumentation to enhance the emulated environment. Reality within the cyber environment is difficult to achieve in more methods than one, for example creating a cyber space that is a replica of the current Internet environment.

The reality is that within a CR the creation of a real-world cyber event will never be completely accurate, or as if it were live; this is due to the massive amount of diverse errors, packet flow, up and down time of multiple applications and services

all executing and running at once (network invariants). This is why the drive for an as-close-to reality solution for a CR is so challenging. Hence the hyper-real cyber environment is plagued with different "network invariants" and cyber challenges.

2.6 Capability Maturity Models

Mateski *et al.* (2012, pg 10) describe a model as, "something used to represent or explain the operation and mechanism of something else, or a simplified representation of something else". Thalheim and Tropmann-Frick (2015, pg 604) describe a model as being a "well-formed, adequate, and dependable artefact that represents origins and must be commonly accepted by its community of practice". In layman's terms, a model is an abstract view of a concept that highlights the main details of the concept. Models are one of the main instruments in scientific research, and they are considered to be the third dimension of science (Thalheim, 2013). Models have two kinds of meaning, namely referential meaning, which establishes an interdependence between elements and the origin ('what'), and functional meaning based on the function of an element in the model ('how') (Thalheim and Tropmann-Frick, 2016). Johnson and Henderson (2002, pg 26) define the conceptual model as a "high-level description of how a system is organized and operates". Thalheim (2012, pg 86) alludes to the fact that a "conceptual model enhance models with concepts that are commonly shared within a community who are involved in the modelling process". Johnson and Henderson (2002, pg 28) applies this rule: "if it is not in the conceptual model, the system should not require users to be aware of it".

Conceptual modelling is a widely applied practice with a large body of knowledge, and concepts are the basis for concept modelling. They specify our knowledge by indicating what objects are, and what properties objects have, thus one of the main reasons for using a model is to provide a solution to a problem (Thalheim, 2010). Conceptional modelling aims at the creation of an abstract representation of the situation under investigation, or rather the method users employ to think about it (Thalheim and Dahanayake, 2015).

There are strategic, tactical and support layers to consider when developing a model, however as in Figure 2.9, the concept of modelling in it narrowest sense is synthesis, which lives in the tactical layer. The modelling properties describe the purpose and characteristics of the model; the modelling activities describe the actions for developing a model including work product, scope, resources, goals, intentions, time span, restrictions, and obligations; and the modelling constructs describe the need for a common understanding in the community (CR community) of language, application and engineering that is used in the model.

Salah *et al.* (2014) have proposed an evaluation template for a maturity model. The template highlights that a maturity model includes three components: reference model, or the fundamental elements that are to be assessed; performance scale, which used by the assessor to rate the fundamental elements, and assessment procedure,

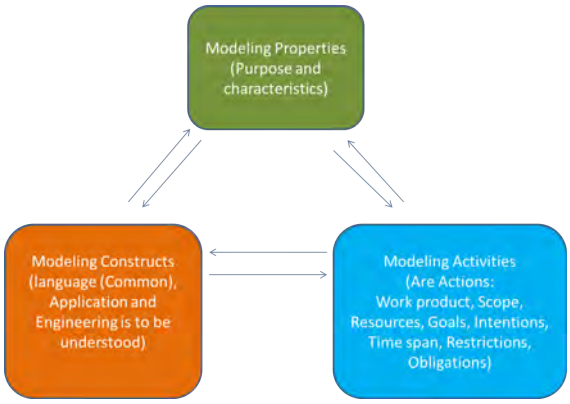


Figure 2.9: Modelling in the Narrow Sense as synthesised. After Thalheim (2010)

which is a guide that has a maturity recording sheet, levels, performance and help tips. These components are then evaluated accordingly as per a maturity model.

Maturity model have structured levels that allow for improvement in effectiveness, and anyone that moves through these structured levels becomes more capable (Fowler, 2014). Caralli *et al.* (2012, pg 3) describe a maturity model in its simplest form as a "set of attributes that represent progression in a particular domain which is mostly determined by levels". The outcome of a maturity model provides a standard to benchmark against and delivers a roadmap to guide improvement. Thus by guiding improvement, when an evaluation has taken place on an organisation's processes, the outcome of the evaluation is redirected to the "Plan, Do, Check, Act" cycle to validate that improvement has taken place (Caralli *et al.*, 2012).

The importance of a benchmark is that the benchmark must be validated practically by empirical data and measured accordingly, thus each level in the maturity model must be more mature than the previous step, based on the evaluation of the processes, practices and methods which are scored against a clear set of best practices and standards. Thus if the CR has achieved the determined attribute the CR has then achieved the benchmarked maturity of a certain level, keeping in mind that levels are not to be skipped.

Caralli *et al.* (2012) has also elaborated on the essential components to a maturity model that are imperative for its structural form. These are: the levels - different levels to progress through during a CR's evolution; the domain areas - the CR domain of which a domain is regarded as a "process area"; the attributes - the core content of the process areas; and the appraisal and scoring methods, which are used to facilitate evaluation using a common standard of measurement. Scoring methods can apply weights or values on certain data collected for a certain attribute, with attributes weighted or valued higher than others depending on the approach. The "Plan, Do, Check, Act" cycle assists in improving the level, once weighted or scored, to progress to the next level. A depiction of the components that are essential to a maturity model is shown in Figure 2.10.

Caralli *et al.* (2012) indicates that there are three different types of maturity models. First, the progression model, which represents simple progression of attribute

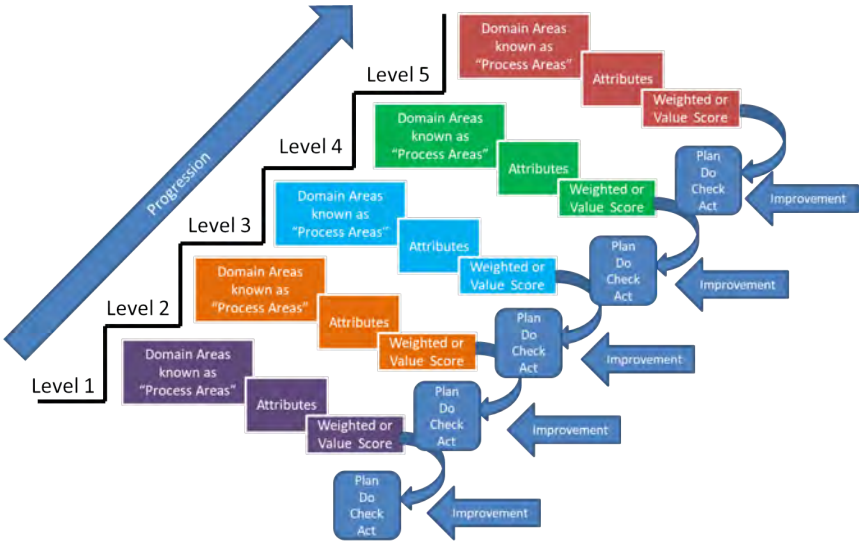


Figure 2.10: Components of a Maturity Model as synthesised. After Caralli *et al.* (2012)

maturity. Second, the CMMs, also known as "Process Models", which represent an organisation's capabilities with the processes and mature culture they use to reach a certain level of maturity. Curtis *et al.* (2009, pg16) describe a CMM as, "An evolutionary improvement path from an ad hoc, immature process to a disciplined, mature process with improved quality and effectiveness". Finally the hybrid model, which is a combination of the progressive model's characteristics and the CMM's (Caralli *et al.*, 2012). However note that insufficient results may be derived from these models due to their abstractness, which is a general flaw in most CMMs. For this thesis the type of maturity model used is the CMM or process model. There are multiple CMMs that have been developed and defined over the years, and some of the most utilised and well-known are discussed below.

2.6.1 Capability Maturity Model

The Capability Maturity Model (CMM) for software is primarily focused on and utilised to determine software capability maturity. It provides guidance on processes for developing and maintaining software and on how to evolve toward a culture of software engineering and management excellence (Paulk *et al.*, 1993):

- **Level I:** Initial: The software process is characterized as ad hoc. There are very few processes that are defined, and success is more of an individual effort.
- **Level II:** Repeatable: Basic project management processes are established and the necessary process disciplines are in place from previous projects that were successful.
- **Level III**: Defined: The SW process for management and engineering activities are documented, standardized, and integrated into a standard software process. All projects use the same SW standards documentation.

- **Level IV**: Managed: Detailed measures of the SW process and product quality are collected and are quantitatively understood and controlled.

- **Level V**: Optimizing: Continuously improving the process through quantitative feedback and other innovations and ideas on technology.

2.6.2 Capability Maturity Model Integration (CMMI)

Capability Maturity Model Integration (CMMI) initially is a combination of three predecessor models namely *"Capability Maturity Model for Software"*, *"Systems Engineering Capability Model" and "Integrated Product Development Capability Maturity Model"* (CMMI Team, 2010). CMMI provides characteristics of best practices to give guidance to an organisation to improve its processes, quality and efficiency, covering activities such as, hardware and software development from inception to maintenance throughout its life cycle, to reach a certain maturity (CMMI Team, 2010). Its main driver shows an organisation what to do to improve, but not how to do their processes (Constantinescu and Iacob, 2007). CMMI is a process improvement model which conforms to the ISO/TS 9000 standard, which is an international quality standard using the quality management principle - the process approach ISO Institute (2016) - in which both entities complement each other. CMMI is not an implementation but rather an application of concepts to reach (Fowler, 2014) maturity from a process perspective.

The three CMMI concepts provide guidance to organisations; these are Development, Acquisition and Services which form the core CMMI Process Area (PA). The CMMI PA, which is not a process description but rather areas of interest that are common for all three concepts which, when performed collectively, satisfy a set of goals for process improvement Kulpa and Johnson (2008). CMMI for development is a reference model that covers activities for developing both products and services, covering the product's life cycle from conception to maintenance. The emphasis is on the work necessary to build and maintain the total product (CMMI Team, 2010). There are two representations, namely staged and a continuous structure (levels III and II are the same). Continuous representation focuses on capability, allowing an organisation to focus on a specific process to augment the capability or organisation's objective. Continuous representation includes the following levels: Level 0: Incomplete (inconsistent performance); Level I: Initial (addresses performance issues); Level II: Managed (identifies and manages progress); Level III: Defined (focus on achieving performance objectives). The Staged representation focuses on overall maturity of an organisation's process, improvement and achievement across multiple process areas to improve incrementally throughout an organisation Kulpa and Johnson (2008). This is discussed in more detail in Section 5.2.2. The levels for the CMMI Staged representation are:

- **Level I**: Initial: Processes are not structured and are reactive.

- **Level II**: Managed: Basic processes and controls are present, focused more on a project based process which is reactive in nature.
- **Level III**: Defined: Standardizes processes and controls are present throughout.
- **Level IV**: Quantitatively Managed: Quantitative techniques measure the standardized processes.
- **Levels V**: Optimizing: Focus on continuous improvement to strive for excellence and added value to the improved processes.

2.6.3 Levels of Information Systems Interoperability (LISI)

The Levels of Information Systems Interoperability (LISI) model is a reference model and process for testing interoperability between information systems. This improves interoperability between information systems and can be utilised to link different levels of CRs and CR systems in themselves (Kasunic, 2001). When combined with the maturity levels, the acronym PAID - which references the interoperability attributes of the LISI Model, namely Policy, Application, Infrastructure, Data - becomes the LISI Capability Model. The maturity levels for LISI are as follows (Chie, 2001):

- **Level I**: Isolated, which is manually implemented for interoperability with removable media or manual configuration.
- **Level II**: Functional is peer to peer interoperability connected for basic two method communication.
- **Level III**: Connected is distributed interoperability, namely Local Area Network (LAN).
- **Level IV**: Domain is integrated interoperability, namely Wide Area Network (WAN).
- **Level V**: Enterprise is universal interoperability, connected to multiple topologies and heterogeneous systems levels.

2.6.4 Cyber Security Capability Maturity Model (CSCMM)

The Cyber Security Capability Maturity Model (CSCMM) indicates different levels of cyber security capability and the maturity of an organisation (Oxford University, 2014). The maturity of this model can be used to determine the levels of cyber resilience that need to be implemented in a CR. This has been broken down into five levels of capability maturity, namely:

- **Level I**: Start-up: At this level there is limited to no cyber security.
- **Level II**: Formative: Some cyber security features have begun to be formulated.

- **Level III**: Established: Elements of cyber security are in place and working in that cyber security is functional and defined.
- **Level IV**: Strategic: A decision on priorities for cyber security is determined, focused on and put in place.
- **Level V**: Dynamic: There are clear cyber security mechanisms in place to augment a cyber strategy in terms of the threat environment, and there is a scene of responsibility within the organisation towards cyber security.

2.6.5 People Capability Maturity Model (PCMM)

The People CMM is focused on implementing practices that continuously improve a workforce by managing, developing, motivating and retaining a workforce with reference to the business objectives using best practices (Valdez *et al.*, 2008, pg 76). Curtis *et al.* (2009, pg 5) describes that people CMM as "a proven set of human capital management processes to improve a work force". The model has five distinct levels in which people maturity can be improved, this is discussed in more detail in Section 5.2.1. The levels for the People CMM are:

- **Level I**: Initial: Skills are not certified and are haphazard in nature.
- **Level II**: Managed: Implementing basic workforce practices.
- **Level III**: Defined: Development of structured workforce practices and rewards for people.
- **Level IV**: Predictable: Capability management and continuously improving workforce practices.
- **Level V**: Optimizing: People are striving for performance excellence, optimising the workforce.

2.6.6 Capability Maturity Model Comparison

Comparing the CMM, CMMI-Dev, LISI, CSCMM and the People CMM, discussed above, one can clearly see an alignment in the maturity levels. The underlining baseline in the comparison of the CMMs is that it is clear that there are five levels in each model: Level I Initial, Level II Managed, Level III Defined, Level IV Quantitatively Managed, Level V Optimised. This general view is directly associated with the CMMI-Dev view of levels. All of the models complement each other and can be utilised for a proposed CMM for a CR to measure its capability maturity on five different levels. Thus the CMM, CMMI-Dev and People CMM are appealing to be synthesized and adopted using a staged representation structure for a proposed CMM for a CR. A comparison of the CMMs is depicted in Table 2.6. An analysis of cyber security models was completed in work by Le and Hoang (2016), namely *"Can Maturity Models Support Cyber Security"* is also referred to in determining the different maturity levels.

Table 2.6: Capability Maturity Model Comparison

Capability Maturity Models	Focus Area	Level I	Level II	Level III	Level IV	Level V
CMM	Software Process	Initial	Repeatable	Defined	Managed	Optimised
CMMI - Dev	Processes	Initial	Managed	Defined	Quantitatively Managed	Optimised
LISI	Interoperability	Isolated	Functional	Connected	Domain	Enterprise
CSCMM	Cyber Security	Start Up	Formative	Established	Strategic	Dynamic
People CMM	Workforce	Initial	Managed	Defined	Predictable	Optimised

2.7 Summary

Chapter 2 established the baseline definitions for the cyber domain, the cyber threat landscape and its elements, which have a relevance to establish a CR for specific purposes. A comparison of cyber and information security established the differences thereof and gave a description of the skills and functions of a cyber warrior and information systems expert. A CR overview established context for the understanding of a CR, the origin of the concept of a CR, its different purposes, function, and utilisation to form a firm base of understanding of a CR. The next generation CRs have been discussed to give insight into the future focus of CRs. The concepts of modelling, simulation and emulation were discussed to allow for better understanding of their uses in a CR, with the understanding of fidelity and a hyper real environment.

From literature on models and the CMMs that were identified it was established that a conceptual model type is more appropriate, which will provide a level of abstraction in a conceptual approach to the development of a capability maturity model for a CR. A combination of CMMs that have been discussed are adopted and synthesised to develop a proposed CMM for a CR. It was also established that most CMMs have five levels, which are adopted accordingly as an incremental approach. The main focus for this thesis is to form a baseline for the development towards a CMM for a CR. The literature review identified no formulated CMM for a CR, standardized measurement for a CR, standard classification of a CR on different levels, or common CR definition. This literature review is the departure point to determining a proposed CMM for a CR.

Chapter 3 will build on from the literature in defining a CR, highlighting the high level architecture, the CR as a system and defining the core capability elements of a CR and their relative importance. A real network is introduced to benchmark a baseline to emulate a CR on a specific proposed level. The functional attributes and capability elements of a CR are proposed to portray the complexity of enabling the capability development of a CR.

3
Defining a Cyber Range

In Chapter 2 a literature review was completed which focused on describing the holistic picture of the cyber domain, the CR as a concept and the generic CMMs in literature, which forms the baseline understanding for the development of a CMM for a CR.Chapter 3 focuses on determining the core capability elements of a CR and establishing their relative importance. In Section 3.1, a holistic architecture provides the establishment of a foundation for the design and development of a CR. Section 3.2 looks at the CR as a system to allow for Section 3.3 to define the core capability elements of a CR; this flows into Section 3.4 which presents a Paired Comparison analysis and determines the relative importance of the core capability elements to determine proposed CR levels. In Section 3.5 a real network's data was captured to form a baseline for a CR level. Section 3.6 addresses the capability development of a CR according to a process which is discussed, establishing a view on the capability life-cycle of a CR. Section 3.7 provides a summary of the chapter.

3.1 Cyber Range Architecture

Architecture focuses on abstraction, as the skeleton of a system is used to visualise the big picture, indicating the plan for the structure of a system, and what the system must do (Spacey, 2017). A CR is developed according to an operational viewpoint, the type of cyber operations it is to maintain, organisational objectives, and the missions that are to be performed. The more realism in a CR the better the effect when performing certain cyber-related events. An established operational view allows for a system viewpoint to be established; the system viewpoint links to the systems that are used to achieve the operational view, hence understand which node or subsystems are linked or related.

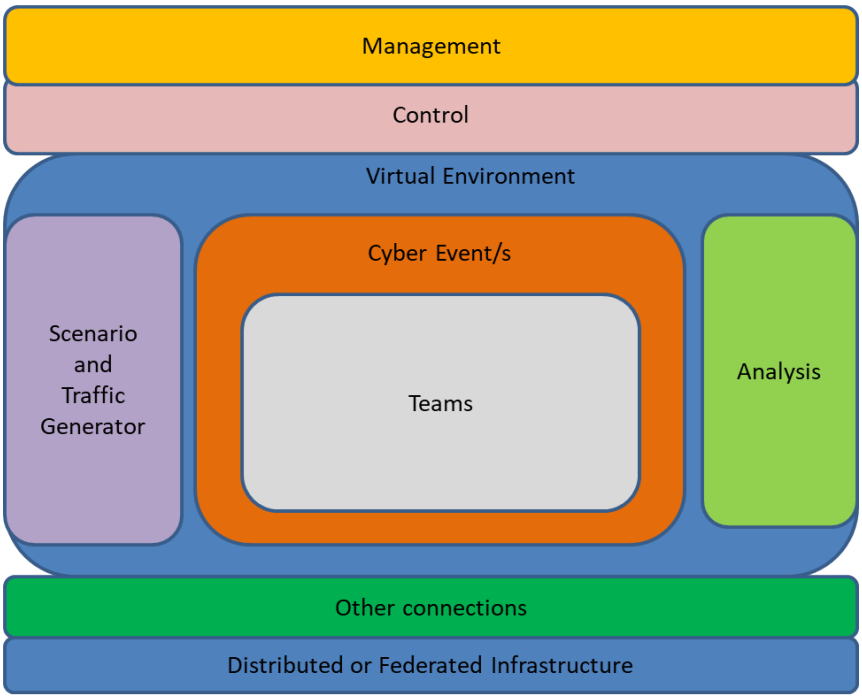


Figure 3.1: High Level Cyber Range Architecture

There are many architectural models that are documented in literature and can be adopted to form a CR architecture. Two architecture models are briefly discussed below, namely an open and closed architecture. An open architecture model allows for different hardware (HW) and software (SW) components to be added within the design of a system. A closed architecture model is manufactured for a specific system and is not compatible with other SW or HW (Levison, 2019), hence if one component changes it changes the entire system. This type of architecture is mainly used in closed systems that are interdependent. In comparing the two architectures, the open architecture is a more prescribed approach to use due to its flexibility, based on allowing a CR to evolve. Hwang and Bush (2015) also indicates some other models that are utilised for a CR:

- Monolithic model serves all user bases, due to a stand-alone high-level virtual interface over other computational hardware systems.
- Distributed model: allows a system using technology to be more flexible, by physically separating subsystems and enabling the exchange of resources through standard interfaces over networks.
- Federated models allow a system to utilise capabilities of other systems on demand, and enables interoperability to share information and allow resources to be augmented using computational processing.

As an observation, distributed and federated model is a more viable implementation method for a CR. Mosleh *et al.* (2016) has indicated to move away from a monolithic model to a distributed model to allow for flexibility.

The high level CR architecture, as in Figure 3.1, is comprised of five main areas, namely management, control, virtual environment, other connections and distributed or federated infrastructure. The management area is divided into two approaches: first, the administrative management of the CR, which is predominantly focused on resource from a technical perspective, and the life cycle of the CR. The second approach is the management of cyber events focusing on generating cyber events for training and T&E of computational products from a research and development view. The control environment is controlling the CR cyber events and activities that are performed in the CR from an operational viewpoint by allocating resources and assets.

The virtual environment enables the cyber events to take place by hosting them, either in a containerised or a cloud environment, to accommodate different cyber events. The virtual cyber event are either modelled, simulated or emulated, of which IP or RF traffic is generated and teams are allocated accordingly. Analysis is performed on the cyber event by utilising different sensors to collect and measure data to determine the effect of the event. A platform that allows other connections such as instrumentation is optional to implement, and can augment the effectiveness or performance of the CR depending on the cyber event. The distributed or federated infrastructure (either utilising a stack or cloud infrastructures) provides users access to the CR and the utilisation of resources and assets in other CR.

By utilising the high level architecture of a CR as a concept, a design can be determined. Designing a system is fundamental and creates a plan to develop something specific, as determined in the architecture, enabling the designing of specific core components for a system based on how the system will work (Spacey, 2017). The core capability elements of a CR are the subsystems for a CR system, which have an impact on the design of the CR and which are discussed in Section 3.3. The design for a CR system must consider the CR's operational environment and engineering process approach, as in Figure 3.2, where the external environment refers to those systems the CR needs to interact with without hampering its own operation. The environment is where a CR system executes its function and purpose. The CR system indicates how the design should look to fulfil its purpose and the capabilities that are expected. The CR subsystem includes the core components needed for a CR to function as a system. The CR user is the user's ability to operate the full complement of the CR functions in a user-friendly manner. There are however two different users that will use a CR system, namely application and administrative users. The application users, who use the services of the CR system, will utilise the CR system to perform a specific function or task without having any technical expertise or understanding of the system itself. Administrative users configure the operations and maintenance of the CR system and provide systems testing and training for the CR application user.

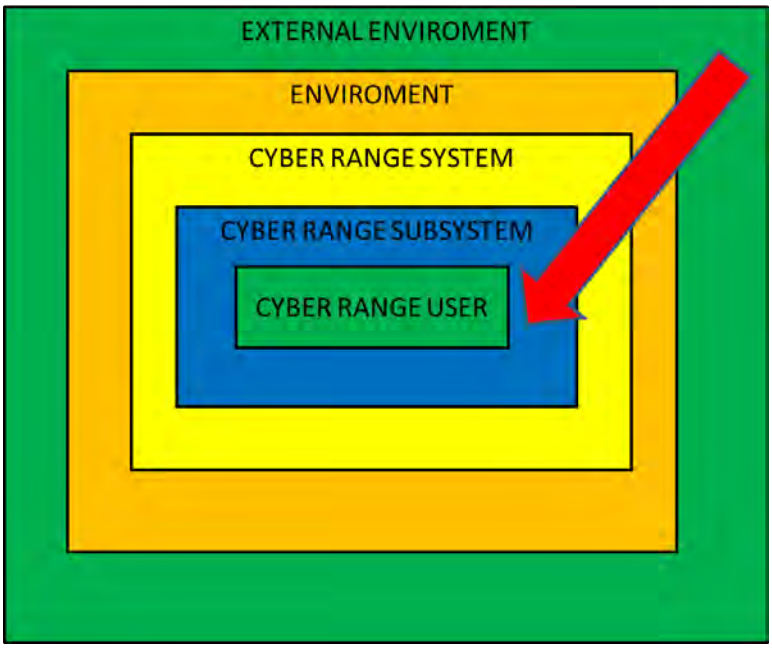


Figure 3.2: Cyber Range Operational Environment Engineering Process

3.2 Cyber Range as a System

The CR requirements are to be understood in the context of the purpose of the CR and its expected outcome. A modular and scalable approach to the development of a CR is a logical view to implement. This is due to technological changes, upgrades and the integration with other capabilities. Firstly, a feasibility study including a technical, economical and operational study must be completed to determine whether to develop, procure or outsource CR services (stack or cloud infrastructure). When procuring a CR system the requirements are to be met according to the product's specifications and the criteria that are needed to suit the needs and purpose of the CR. The criteria for a CR are discussed in Section 4.1.

In the development of a system there are certain principles that are to be considered. Bentley and Whitten (2007) have proposed the principles of system development as follows: get the system user involved, use a problem solving approach, establish phased activities, produce documentation throughout the development, establish standards, manage the process and projects, justify information systems as a capital asset, do not be afraid to cancel and re-scope, divide and conquer and design systems for growth. These principles can be adopted when developing a CR.

A system is divided into two broad areas, namely functional , which is what the system will do, how it will do it, under what conditions, and what other systems are involved with the operation. Similarly, the physical is what the system's components will look like and be used for from a detailed technical specification, and how they will integrate with each other. A system is much more than just an integration of components; it addresses the fundamental model of People, Processes and Technology (PPT) focusing on resources, material, facilities, data, HW and SW. The CR system is

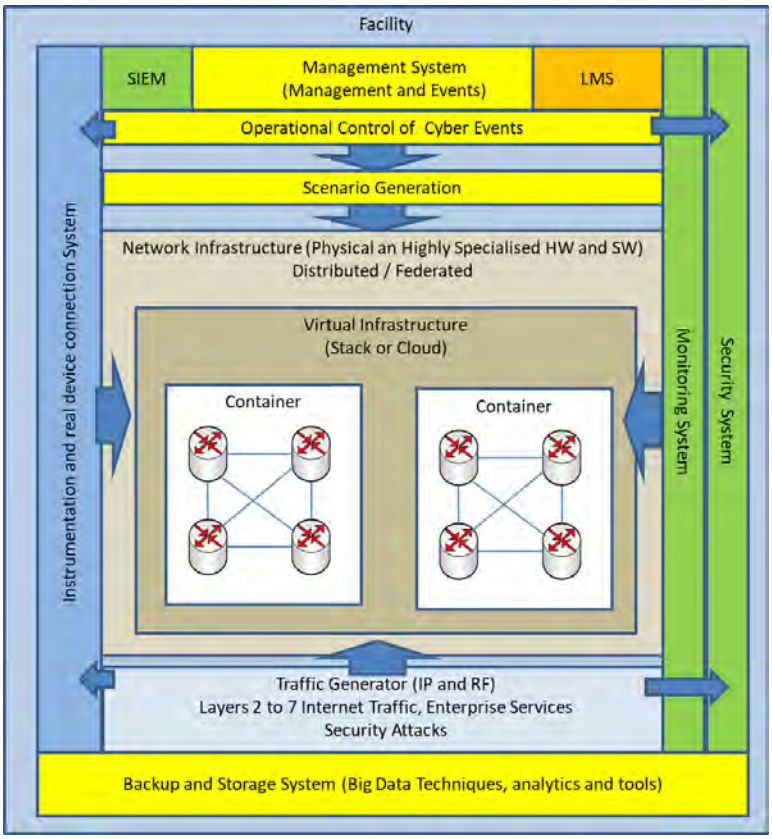


Figure 3.3: Cyber Range System and Sub-Systems

designed to provide the desired operational environment, and to achieve the desired functionality and performance. Figure 3.3 illustrates a proposed CR system and sub-systems which will form the building blocks for the CR core capability elements.

3.3 Core Capability Elements for a Cyber Range

The core capability elements for a CR are identified elements that a CR requires to function as a system. The mapping and justification thereof are based on a review of relevant literature and the general composition of a CR, as discussed in Section 2.4. The core capability elements are further defined to create context for CR capabilities as a collective. Not all capabilities are implemented in a CR, as this depends on the purpose the CR is to fulfil. However determining the core capability elements allows for a baseline to be established to formulate CR-specific capability requirements. Priyadarshini (2018) has proposed an ideal CR with perimeters that are essential in a CR. The relevant importance of the qualitative values determined are as follows.

- **Very High:** Infrastructure, Scenarios teams, Simulation Environment, Tools, Automation, Performance, High Fidelity and Intellectual Property.
- **High:** Virtual Private Networks (VPN's) and cloud infrastructure.
- **Medium:** Seats, Virtual Cloned Networks (VCN's).

- **Low:** People involvement.

This research has assisted in defining the core capability elements for a CR for this thesis. The core capability elements have been broken down for understanding. Utilising the core capability elements, a Pairwise Comparison analysis was used to determine the relative importance of the elements to determine different CR levels, as in Section 3.4. The bases for determining the core capability elements are used in the measurement criteria for a CR, as in Section 4.5. The results of the CR core capability element are discussed in Section 6.1.1 which has aided in acquire a consensus from CR experts. The core capability elements in the context of this thesis are defined as the subsystems for a CR. The high-level descriptions of the core capability elements for a CR are listed in Table 3.1.

3.3.1 Management System

To manage a CR with all its functions and capabilities is complex in nature, thus it is imperative for a management system to be implemented in a CR. A CR management system is the central operational hub of the CR, and must have the ability to allocate, distribute and configure resources, manage cyber events, develop processes, manage administrative aspects of the CR, and train human resources. The management of a CR can be divided into two parts: CR management through out the CR's life cycle, and cyber events management, which manages cyber events through their life cycles. A computational management system ensures that the system is controlled as per its purpose and configuration according to the operational needs (Buyya *et al.*, 2000).

CR management functions that are applicable to managing the technical life cycle of the CR include the configuration of ICT systems, administering access permissions and managing the security system for authentication and access control to the CR, management of on-demand services for rapid implementation of cyber events, managing the integration with other CR systems, database management and digital documentation, knowledge management in the CR, management of resources training, and the Quality of Service (QoS) the CR provides. The implementing of CR policies, operating processes, and standard working procedures for the CR is key in ensuring standard practices are adhered to. The content of training material and manuals for operating the CR, whether for an exercise or the CR itself, are to be managed accordingly. Managing the CR events as per requirements for users is dependent on the cyber event, which is fundamental in a CR.

Cyber event management in a CR is the ability to design, plan, develop, execute and provision a cyber event. Utilising the necessary tools and capabilities to give an effective and efficient cyber event which is cyber mission focused and operationally realistic. When developing a cyber event, a Red and Blue environment is established to accommodate realistic cyber capabilities that simulate and emulate these environment. Sensors are to be deployed to monitor and send data back to the management system to be analysed using metrics to measure the users responses accurately. Sensors for the CR are discussed in Section 4.4.3.

Table 3.1: Cyber Range Core Capability Elements

Core Capability Elements	**Description**
Management System	Main hub of the CR, used to issue and establish different platforms to host cyber activities in the CR, to create sessions and cyber exercises, to allocate resources, to ensure the optimal operation of the CR, and to have a view of the complete CR network and activities.
Learner Management System	Allows for people to interact with a computational system in relation to lessons or outcomes that need to be performed in the CR.
Monitoring System with Sensors	To monitor cyber activities of people and the processes used based on establishing statistics, to establish lessons learnt in the CR.
Health Monitoring System with Sensors	To monitor the health status of the CR with health sensors to indicate status, failure or faults in the CR.
Security System	The ability to execute both physical and logical security in a CR.
Security Incident Events Management (SIEM)	To ensure event correlation and the ability to analyse malicious activity according to SIEM functions.
Back Up and Storage Capability	To store and replay cyber activities when required and to maintain a history and storage of data captured in the CR.
Threat Library Capability	Library in which all types and families of cyber malicious code are stored.
Scenario Generator Capability	Set of cyber scenarios of cyber attacks that have been created, reference or recorded. Real time cyber scenarios are injects to cyber events.
Big Data Capability	Methodology to store data in huge amounts due to CR activities.
Traffic Generator Capability	Ability to generate digital Internet Protocol (IP) traffic and Radio Frequency (RF) traffic realistically at high volumes.
Network Infrastructure	Physical high speed computational and networking processing capability for a CR.
Virtual Infrastructure	Ability to emulate, simulate and model virtually, and the ability to create SW defined converged infrastructure, with high fidelity nodes, and provision networks on demand in a short space of time.
Software Operating Systems	Ability to host multiple operating systems within the CR, whether licensed, open-source or proprietary.
Software Applications	Ability to hold multiple SW, cyber security and offensive tool set applications within the CR, whether licensed, open-source or proprietary
Redundancy	Mirrored back-to-back system implementation of a CR.
Real Device Connectivity	Capability to connect real hardware devices to execute testing or for utilisation in a cyber event.
Instrumentation connectivity capability	Ability to connect specific cyber instrumentation to augment a CR.
Facility	The housing of the physical CR which is dependent on size and functionality being it a fixed facility or mobile in nature.

An integrated cyber events tool suite supports the cyber event management, and includes tools that support cyber scenarios, a scenario generator, and assistance for cyber event planning. It also defines and manages resources required for a cyber event, and automatically builds, verifies, and sanitises the CR to support the full cycle of cyber event development (Hwang and Bush, 2015).

3.3.2 Learner Management System

A Learner Management System (LMS) allows a learner to interact with a computational system through lessons or evaluations that need to be performed. The LMS also displays the learners efforts and compliance to a set curriculum in a formal or informal manner. Hence a LMS is a software application for e-learning in which courses and education programs can be customised (Elite, 2019). For learning to take place there is a need for a cognitive balance between practical application and theoretical ability to be performed by an individual in order to accredit the individual efforts and skills (Chapaev *et al.*, 2016).

A conceptual framework for modelling cognitive complexities in a CR in an operating environment - which highlights the cognitive complexities, tasks difficulties and workload - can be utilised in conjunction with the LMS in assessing the cognitive complexities experienced by CR users (Antonio *et al.*, 2019). Within a CR the LMS should be structured according to a structured growth learnership program that caters from a basic entry level to the most advanced level for each individual. Developing a curriculum for a LMS is a process that is to comply with the Education Training and Development (ETD) standards of a specific nation. Compliance with formal cyber certifications will need to be formulated in accordance with international certifying authority.

Reith *et al.* (2018) states a LMS forces a linear progression of material coupled with an evaluation system. Reith *et al.* (2018) also alludes to a possible rethink of an LMS, as suggested in the framework "Rethinking USAF Cyber Education and Training". The LMS assists in allowing trainees to become accustomed to the cyber environment through learning multiple different cyber-related learning outcomes. Similarly, it allows trainees to link up to different LMS sessions to build on and develop their cyber skills. Access to the LMS is also a widely-utilised system with wide-reaching abilities to not only augment CR events but also as a platform for cyber resilience.

The LMS system should be maintained consistently to keep up with the ever-changing cyber environment. Other approaches that can be implemented to augment learning in a CR include gamification, which allows for a sequenced cyber game to play out with participants needing to execute certain functions in the game to reach an objective or stage linked to a scoring system. The CR LMS system allows training content, such as cyber lessons and training material applicable to different levels of cyber training, the ability for users (learners) to interact with cyber lessons as part of the CR computer-based exercises (not the CTF or CBX), and the ability to interact

with other CR LMS's using distributed cloud-based technologies (Reith *et al.*, 2018).

3.3.3 Sensors for a Cyber Range

Sensors are a vital component in a CR, as they allow for the CR to be monitored in various aspects. The metrics that are collected will aid in giving certain results pertaining to the effect and performance of human and machine interaction in a CR. Sensors in a CR are deployed to collect system and events data; this is stored in a database, and analysis of the data with machine learning techniques allows for situational awareness of a CR to take place (Labuschagne and Veerasamy, 2017). Franke and Brynielsson (2014) state that data from the sensors can be fed to a data fusion process that enables situational awareness and aggregation for a CR. The situational awareness information of a CR triggers a response, either automatic or manual, however false positives and negatives are to be considered when taking appropriate action to the response.

An example of this is the National Cyber Range (NCR), which is instrumented with traffic generators and sensors collecting network traffic and data from local and distributed nodes (Ošlejšek *et al.*, 2017). Another example of this is the utilisation of Artificial Intelligence (AI) to gather data with sensors or software solutions in the CR network or networks (Pahi *et al.*, 2017). Sensors can be used to measure the performance of the CR in the following areas: packet flow, health of the system, security of the system and multiple other users, or effectiveness (by monitoring peoples' behaviour in a cyber event).

An example of technology which has access to a large amount of the aggregated data are the automotive sensors, which are capable of collecting and transmitting information derived from personal behaviours (Simon and Graham, 2017). Sensors, in layman's terms, can act as a warning to circumvent a critical failure, allowing for improvement in effectiveness and performance due to the subsequent analysis of the sensors' output. Sensors are specific to a function that needs be performed, and there are a multitude of sensors that can be implemented in a CR. The following list is a high-level view of sensors for a CR.

1. Monitor System: Monitoring sensors need to be deployed on multiple nodes to be able to monitor user behaviours while in a CDX (human interaction, where the human clicks using a mouse). These sensors are able to monitor ports and IP address connections over a period of time (intrusion detection sensor); all this statistical data is captured to evaluate the event from both the users' interactions and the computational actions and ability. It also enables analysis of user performance while executing cyber events, the generation of statistical data on the performance of users, the monitoring of the computational actions performed by the users per an event, and the keeping of a score which displays the user's performance.

2. Health Monitoring System: The understanding of the health of a ICT system

pertains to the sensors that indicate whether the ICT system is operating at optimum. The health of a CR as a system needs to be monitored to ensure proactive maintenance to the CR. The health system must monitor the general well-being of the CR.

3. Instrumentation and Connectivity Capability: Real device connectivity to perform a System in the Loop (SITL) test is a useful method to ensure that the device or System Under Test (SUT) is tested accurately in a CR. Instrumentation in the CR environment can be described as tools or cyber sensors that deliver results or that can augment and enable shortages within a CR capability. Instrumentation usage in a CR depends on the application, thus a mixture of instrumentation sensors are a best fit for a CR. Adding instrumentation to a CR will enable it to have a better real-time feel for the user. Below are some examples of instrumentation that can be plug-ins into a CR:

   (a) Network telescope (which is a network sensor) allows a user to observe if there are any anomalies in IP ranges which are not being used. These telescopes are deployed within a public subnet or other subnets which hosts no services or normal traffic, with the main function to capture and analyse traffic that flows in specific subnets (Moore *et al.*, 2004). This will allow for a CR to utilise a network telescope, to aid a Blue team (defensive team) to observe specific subnets to detect anomalies such as a DOS attack, IP and port scanning to name a few (Irwin, 2011).

   (b) Honeypots are described as "a system (for example, a Web server) or system resource (for example, a file on a server) that is designed to be attractive to potential crackers and intruders and has no authorized users other than its administrators" NIST Institute (2013, pg 86). Honeynets are extensions of a honeypot system that can emulate entire virtualised networks (Irwin, 2011). High interaction monitoring systems are also described as a high interaction honeypot, which is a darknet monitoring system that detects darknet packets by attempting to connect back to the suspicious host system to allow for exploitation to take place to capture the injected malware samples for analysis (ISO Institute, 2012b). These are useful in a CR to monitor any traffic that is detected in a scenario and to analyse malware that is injected into a cyber event.

   (c) NetFlow is the name given to a series of protocols developed by Cisco, which are used to record metadata about a connection (Claise 2004; Cisco 2019). Herbert (2018, pg 15) discribes NetFlow as, "a means of logging network flows which passes through a flow monitoring device in a communications pair's route". As an example, the information recorded by these protocols include, but is not limited to, what IPs were involved in a connection, what ports were used, the number of bytes sent, the number of flags raised, and the duration of the connection. NetFlow differs from Deep

Packet Analysis (DPA) in that DPA analyses each packet within a communication, whereas NetFlow only concerns itself with generating a log about a communication. The benefits of using both approaches is that the one augments the other, in that NetFlow identifies the problem area and DPA drills in deeper to solve the attribution. NetFlow is also a unidirectional logger that analyses the packet traffic in one direction. This means that in a communication between two end-points, a NetFlow log will be generated for all data sent from the first host to the second, and another NetFlow log will be generated for all data sent from the second host to the first. NetFlow is a near real-time system in that it creates logs after a communication is complete. This severely limits its ability to respond to a network event while the event is occurring. The typical data that will be collected on a specific problem area will be IP address, flags, ports and services. A NetFlow system operates holistically in the following method: a publisher is started up which tells the process modules (PM) what it needs processed; the PMs then communicate to the collectors - hardware components - that collect NetFlow data which is needed on a specific network.

(d) Cyber security instrumentation, of which there are many examples, including NESSUS[1], NexPose[2] and OpenVAS[3].

(e) Performance instrumentation, which is specific to computational devices, is used to establish an accurate performance level, for example oscilloscope, wave propagation instrumentation and other electronic scientific measurement instrumentation.

3.3.4 Security System

In a CR the containment and the maintenance of the sandboxed and virtual environment is key for both a stack or cloud implementation of a CR. All sub-system components have functions which need protection mechanisms to allow for the sub-components to function and fulfil their purpose without compromising the CR system as a whole. The security architecture for a CR should be integrated as part of the design from the start to ensure that the protection of the CR is segmented in different authorisation layers. The security system must visualise the component behaviour through a security interface, and feedback status is to be provided to the CR management system. The acceptable risk appetite for a CR from a security perspective is to be considered, and what risk reduction activities are necessary to mitigate the risks. To address this, CR risk management process are to be documented. The "black swan theory", which focuses on a surprise event that is not predicted and has a major impact on an organisation (Summers, 2012), must be taken into account, in that cyber event exploits are to be contained in a CR, so as not to leak on the Internet

[1] https://www.tenable.com/products/nessus/nessus-professional/
[2] https://www.rapid7.com/products/nexpose/
[3] http://www.openvas.org/

and or other distributed CR networks.

The risk appetite is to be confirmed through conducting a complete security threat and risk analysis on the sub-system components of a CR from a security functionality and assurance perspective. A consideration of the cost verses the risk appetite is to be defined for the CR, addressing whether in each case it would be better to accept the risk or procure security controls, which can over capitalize the CR sub-system or complete system. A residual risk will also need to be considered for corrective actions to be implemented, for a security failure of a sub-system or system. Consistent changes in technology and the approaches of malicious actors will need to be considered in securing sub-systems in the CR. A way to address this involves a consistent security maintenance plan to support the evolving CR. Authentication and non-repudiation for access to the CR is fundamental to a security system and is to be implemented accordingly.

Perimeter and application firewalls between the Internet and a distributed network are to be configured to filter ingress and egress traffic and allow for deep packet inspection (Spirent, 2017). Intrusion detection and prevention systems, the utilisation of encryption to secure connection, and Endpoint Protection Platforms (EPP), which provide malware protection of endpoints are to be centrally managed. Security standards implementations are also to be considered for a CR. When participating in a CDX, a Blue team perspective operating in a CR requires security tools to detect, isolate and block security attacks and exploits from Red teams. The CR is to cater for various different cyber categories of security classifications within a security system, namely unclassified, restricted, confidential, secret and top secret cyber events.

The physical protection of a CR is also to be considered in the light of potential physical breaches, such as theft and the utilisation of CR without appropriate authorization. Other functions for a CR security system include the following: the ability to contain a security incident in the CR, the ability to enable encryption internally and externally; the separation and containerisation of CR cyber events; the implementation of cyber security standards in the CR as adopted by an organisation; the logical security for access to CR services within the CR; the ability to ensure data integration for the CR; the physical security of the CR and the visual monitoring; authentication and access control implementation; degaussing or sanitising exposed systems in the CR facility or Lab after utilisation; and finally the ability to enforce and ensure the security classification of CR events.

3.3.5 Security Information Events Management (SIEM)

A SIEM is employed to display the data collected by network and security systems (Spirent, 2017). The SIEM is a vital capability in the security environment in that the SIEM will monitor and confirm security compliance within an organisation, and is a benefit to a Security Operations Centre (SOC). SIEM will have the capability to receive feeds from sensors and sources in a network, namely routers; servers, switches, Intrusion Protection Systems (IPS), Intrusion Detection System (IDS), and

other sources within a network. The sources will give logs in which the events that take place on the sources are logged. Event correlation will then be executed to link events together and to monitor if there is a cyber security incident or an Indicator of Compromise (IOC).

If there is a cyber incident in which the event shares a certain signature or pattern with a malicious act, a red flag is indicated and a triage process is activated to analyse the event, which is categorised according to its risk it poses to a network , and a response will then be generated to contain or eliminate the malicious event (NIST Institute, 2012). Typically in a SIEM there are different capabilities, including log collection and processing, searching and reporting, real time monitoring, incident management, threat intelligence and user behaviour analytics. Utilising these capabilities together supports the viability of an organisation's network security (Subhalakshmi, 2018). Karlzén (2009) states that a SIEM provides a centralised log analysis, hence identifying errors on networks, and providing policy monitoring and identity management. In a CR the SIEM will aid in allowing CR technical staff to prioritize workload due to the SIEM generating events or alarms. A SIEM in most cases deploys a SW agent that is installed to collect data to either pull the data at a specified time or pull the data from devices to the SIEM for analysis (Coetzee, 2015). It is worth noting that the next generation SIEM applications have allowed for developers to write their own SIEM apps (Spirent, 2017).

3.3.6 Back Up Storage Capability

A back-up system is fundamental in any ICT system, and is essential especially in cyber events to replay the event, allowing users to learn from mistakes made or to augment the process used in the event. Having a replay ability also enables the CR to maintain a history, whether as logs or the cyber event itself, and store data captured in the CR itself. Back-up systems are normally designed to have a on-site and off-site functionality according to best practices. Rabinovich *et al.* (2018) has eluded to different back-up techniques that can be utilised to reduce storage size to a central server, which can be applied in a CR. Another method of backup storage is SW defined storage, which allows for a shared pool of storage in which servers have a SW layer implemented to provide separate storage (Sreenivasamurthy, 2018). Cloud storage is mostly used globally as a service, and is an added benefit to a CR, especially when utilising a cloud service provider to provision a CR and during cyber events. From a security viewpoint the data that is stored in a back-up site is to be tamper proof, with logs of all changes or deletions kept, data integration maintained, and accurate clocking of the metadata.

Back-up storage, from a practical viewpoint for a CR, is to provide back-up on-site and off-site: the importance of this is to ensure the consistency and reliability of the CR. Encryption techniques are to be implemented to ensure secure storage of data within the CR as well as the validation and management of digital signatures, keys and hashes. Organisational procedures on secure data disposal are to be implemen-

ted accordingly within the CR management of databases (Jones *et al.*, 2017). The use of portable external backup storage devices is to be managed and be maintained according to CR security processes.

3.3.7 Big Data Capability

Big Data, as the name suggests,deals with large quantities of data, and requires different approaches, techniques, analytical and statistical tools, processes and architectures (Grobelnik, 2012). This is a fundamental part of a CR due to the masses of data that are generated from the events management, cyber scenario generator, execution of the CDX and CFT exercises, and from computational test and evaluation. Big Data refers to the 3Vs, namely volume, velocity, and variety, where volume is the amount of data, velocity is the speed data is processed, and variety is the number of different types of data sources (Su, 2012). Grobelnik (2012) describe the key enablers for the growth of sufficient data as the increase of data storage capacities, computational processing power and the availability of data on demand.

A big data platform in a CR will enable and maintain the V3 in a CR. By using datasets in a CR to capture multiple cyber event data and applying AI methods specific to Deep Learning, an algorithm can be trained using the CR data sets (Hurley, 2018). Using big data techniques, tools and processes will augment the CR capability in decision-making on various levels regarding the management of a CR. Adding to this, big data will benefit the cyber threat library and scenario generator capability. This will also allow for the CR to have the ability to have accurate and relevant information specific to identifying the gaps in the CR events, supporting the systems' ability to function optimally. Using big data methods to collect, analyse, visualize and share information (Labuschagne and Veerasamy, 2017) is essential in any CR for future implementation of smart CR systems. An example of big data techniques and tools used in a CR is the CyberVAN using the Apache Hadoop[4] family (Ošlejšek *et al.*, 2017).

3.3.8 Threat Library

There are multiple CRs that utilise threat feeds from shared platforms to receive feeds and download threats from malicious code laboratories from different vendors and open-source crowd-sourcing malicious code sites. Using threat intelligence techniques in analysing data and detection of cyber threats is vital to the development of a threat library. The known and unknown cyber threats and vulnerabilities of computational HW and SW are to be stored with their signatures, and must include a set of standard definitions and descriptions, namely a threat agent library (Mavroeidis and Bromander, 2017). A national threat library is beneficial - having a centralised threat database for the utilisation of the threat library for CRs and for utilisation in research on cyber threats provides the ability to cross-reference families of cyber

[4]https://hadoop.apache.org/

threats and to determine the threat signatures of non-state actors.

These benefits will enable the CR to generate real to hyper-real cyber threats in an event or in the T&E of computational devices. In the development of a threat library, the library will need to be contained in different threats vaults, and access control mechanisms will need to be implemented. The threat library must have the ability to populate the library with cyber threats, feeds from malware labs or crowd-based labs in real time, due to the ever changing threat environment in cyber space. Cyber threat signatures are to be confirmed either as a proprietary threat contained for research purposes or families or signatures of cyber attackers, and this is to have a cross-reference capability and a database where each threat is categorised as high, medium or low.

Examples of directories and repositories that add value to a threat library include NIST's National Vulnerability Database repository (NVD)[5] and MITRE, which has many threat directories that can be utilised, namely Common Platform Enumeration (CPE)[6], Common Weakness Enumeration (CWE)[7], Common Attack Patterns Enumerations and Classifications (CAPEC)[8] and the Adversarial Tactics, Techniques and Common Knowledge (ATT&CK)[9], and endless other sources. Mavroeidis and Bromander (2017) describes the directories and repositories as connections that aid in the collaboration and identification of threat actors, TTTP's and identities. Threat libraries form an integral back-end part of the security attacks that a traffic generator provides in a CR. The threat library is depicted in Figure 3.4 with the scenario generator.

3.3.9 Scenario Generator

A scenario generator forms an integrated part of the cyber events management system of a CR, and can provision VMs based on random cyber scenarios (Schreuders *et al.*, 2017). Cyber scenario are based on past events or events which are not recorded, current trends and statistical data and historical facts that have occurred or that are predicted to occur in the future. This assists in the conceptualisation of a cyber event that an organisation can be confronted with. In planning a cyber scenario, all possible occurrences pertaining to a specific event are to be considered. A cyber scenario library is a repository in which cyber scenarios are kept which are either developed, recorded or predicted. For instance, a real-time cyber event can be logged in a SIEM, from which the scenarios can be extracted and developed further for a CDX or CTF exercise, enabling participants to test their cyber security skills to prevent, detect and respond to a cyber attack. Figure 3.4 shows a basic layout of a cyber threat and scenario library. For cyber scenario development to be effective there needs to be an in-depth knowledge of the operational view of the cyber domain, the threats, and

[5]https://nvd.nist. gov/
[6]https://cpe.mitre.org/
[7]https://cwe.mitre.org/data/
[8]https://capec.mitre.org/
[9]https://attack.mitre.org/

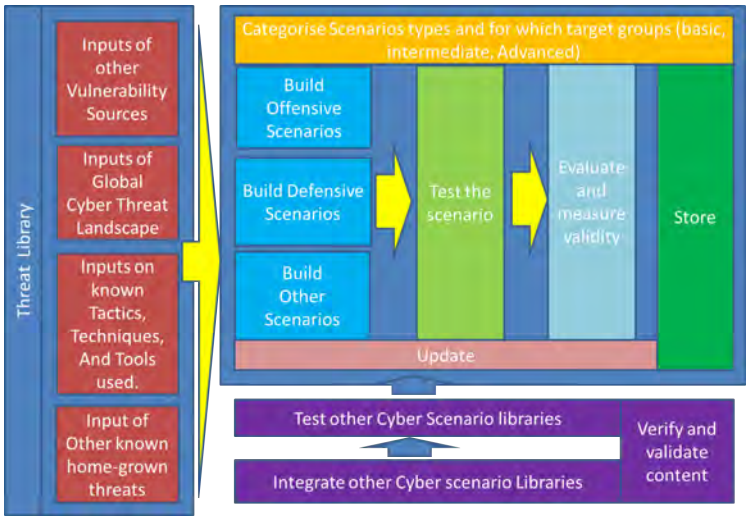


Figure 3.4: Cyber Threat and Scenario Library

how a cyber operation should be performed to provide and create realism in a CR. The goal is to train as realistically as possible to accomplish a certain cyber mission. Before the deployment and implementation of a cyber scenario an assessment of the entire cyber scenario must be undertaken to confirm that the scenario satisfies and imitates a close-to-real-world cyber environment. This is an important part of the validation process for the cyber scenario library. Cloppert (2009) suggests that when developing a cyber scenario, the "Kill Chain Methodology" can be utilised. The steps for conducting a cyber event, as discussed in Section 2.4.4 in Table 2.5, are linked to the general process for developing a cyber scenario. The link is that the cyber event will run multiple cyber scenarios where the cyber scenarios are to be tested before deployed in a cyber event. The general development steps for a cyber scenario include;

1. Step one: perform an environmental analysis to consider all relevant cyber trends, environments and cyber threats globally.

2. Step two: decide on a target and draft a probable plan for the use of different cyber offensive and defensive TTTPs for different cyber topology, systems and computational devices.

3. Step three: identify possible vulnerabilities in the target, and harden or soften security accordingly.

4. Step four: develop a cyber threat, either a proprietary cyber attack or known vulnerability.

5. Step five: test and evaluate the scenario to confirm that it satisfies the required objective as set.

6. Step six: implement changes if needed, re-evaluate and then validate and capture the scenario in the scenario generator repository.

Scenario development is an intellectual process. The scenario developer needs to be creative and imaginative and have a sound cyber security background with experience in the cyber field, and have the ability to cognitively apply his or her mind to how and with what TTTPs a non-state actor or a cyber criminal would act. Other considerations include the CR capabilities, which include the skill level of the participants, the time needed to develop and perform the scenario, the tools needed and the ability to implement injects to the cyber event. The NATO CR, located in Tallinn Estonia, has a digital library which allows for a shared development and storage environment for cyber security exercises, and includes texts, images, video, configuration files, scripts, executables, virtual machine images, and so forth (Estonian Ministry of Defence, 2017). Utilising a shared digital library will save costs in developing cyber scenarios.

The most common types of cyber scenarios which can be developed include but are certainly not limited to: Distributed Denial of Service (DDOS) on computational systems, IoT, IIoT and mobile platforms, privilege escalation, extracting information, webpage defacement, man in the middle, evil twin, kill command, shadow shell, phishing, ransomware, social media exploits, critical information infrastructure (CII) attack on SCADA networks, and scenarios to simulate social engineering attacks on humans or a targeted workforce. The OWASP[10] top ten application security risks, as identified for 2017, are injection, broken authentication and session management; sensitive data exposure; XML External Entities (XXE); broken access control; security misconfiguration, Cross-Site Scripting (XSS); Insecure deserialization, the utilisation of components with known vulnerabilities, and insufficient logging and monitoring of organisations computational networks. These are typically the type of cyber attacks that are implemented in a CDX or a CTF exercise scenarios.

3.3.10 Traffic Generator

A traffic generator can be divided into two categories, namely generating digital and radio frequency (RF) traffic in a simulated and emulated environment and simulating security attacks. Generating IP traffic on a network is vital in a CR, as this allows for a simulated and emulated environment to take place. It also allows for network invariants, to a certain extent, in a virtual environment. Holistically, traffic generators are utilised to model or simulate IP /RF traffic on a network via communication packets and payloads that would be produced by computational devices on a network (Edgar and Manz, 2017). High-fidelity traffic generators take the real behaviour of a network, both of the computational devices and users behaviour, and emulates this traffic, providing for a more real-life feel in a network that is being used in a CR (Edgar and Manz, 2017).

The traffic generator generates datagrams on layers 2 to 7 of the Open Systems Interconnection (OSI) stack. This includes Internet Protocol (IP) traffic that is a realistic representation of the Internet traffic organisations would generate, for ex-

[10]https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

ample social media traffic, multimedia video traffic, unsolicited IP packets (.onion), connection-oriented TCP/IP, connectionless UDP traffic, and other stateful application protocols within a network. The generator is to emulate traffic for hundreds of the Internet Assigned Number Authority (IANA) country codes (Spirent, 2017), as well as generate mobile application traffic and enterprise services such as email, database and voice services. Other traffic to be generated includes satellite signals, such as Global Navigation Satellite Systems (GNSS), Internet of things (IoT), as well as critical infrastructure industrial systems used in SCADA networks. Updating traffic generators with reference to protocols, newer technology services and so forth is essential to maintain accuracy.

Security attacks (cyber attacks) are to be generated to exploit clients, servers and services on all OSI stack levels that are simulated and emulated. The security attacks are to include all variations, types and families of malicious code, which include exploits in the Common Vulnerability Environment (CVE)[11], Denial of Service (DOS), deployment of botnets, fuzzing technologies for Zero Day exploits, mobile application vulnerabilities, other vulnerabilities for IoT, and critical infrastructure and GNSS. Using the security attacks, the traffic generator allows for computational products to be tested in a system in the loop test, confirming performance and security. The updating of the security attacks is vital for a traffic generator to stay within a minimal relative lag period in terms of the new global cyber security threats.

All CR fundamentally are to include a traffic generator, and the purpose of the CR will determine the size and specifications for the traffic generator. However, a standard traffic generator that can operate using the minimum requirement for the number of clients and servers that are simulated or emulated is to be implemented.

3.3.11 Physical Network Infrastructure

Legacy stack infrastructure for a CR, which are traditionally HW orientated by using physical HW and loading virtual SW for cyber events and tests, are hugely costly. However the need for high-speed computational and networking processing capability is essential in a CR to route Internet and other network traffic between nodes and is required to enable a CR infrastructure. Some HW examples of this are routers and switches, servers, devices supporting IPv4 and IPv6 network protocols, security devices, firewalls IDS, IPS and other peripherals used in SCADA systems. The performance of HW and its use should maximize the potential for implementing a virtual environment in a CR; this is critical, as most cyber events are sandboxed and virtual. The physical HW infrastructure must accommodate and implement multiple virtual machines in a relatively short period of time. The HW set up of the infrastructure for a CR is to be modular, scalable and flexible in nature with a network segregation ability.

The physical infrastructure according to the specification for a CR capability should comply with the CR design and architecture, configuration of the CR network and

[11]https:// cve. mitre. org/

configuration management. The setup of the CR network is to be simple and managed to allow for the infrastructure to route traffic, isolate networks and block devices accordingly (Spirent, 2017). The maintenance and support of the physical CR HW, the performance of infrastructure, and the devices are mapped according to CR purpose and standards. Quality of service (QoS) on the infrastructure is critical to ensure accuracy within the CR network. Conway (2018) describe the drive for digital transformation, and the innovation of hybrid infrastructure and SW defined solutions which are to be used to upgrade physical infrastructure.

3.3.12 Virtual Infrastructure

Virtual Infrastructure for a CR is a critical core element, due to a CR being a sandboxed and virtualised environment. Virtualisation using virtual machines (VM) is better suited to a CR due to the VM being safer and isolated; testing can thus be more sophisticated. Therefore while the sandbox approach is flexible, it will not be as accurate in results as virtualisation (Priyadarshini, 2018). When using virtual tools to simulate and emulate a network for a specific cyber event or test, the main outcome is to design network topologies with high fidelity nodes in a speedy setup. Heller (2013) reiterates that within the virtual infrastructure the virtualisation is to be of a high fidelity - this is of great importance within a CR environment.

Sreenivasamurthy (2018) describe hyper convergence as a pool of computation, memory and storage in a single platform that makes storage available natively within a hyper-visor. A hyper convergence model, which varies the computing and storage to provision resources accordingly, is a newer and more cost-effective solution for a CR. A SW defined converged infrastructure is a compilation of SW defined servers, storage, and infrastructure containers (Sreenivasamurthy, 2018). A SW defined infrastructure allows for containment, isolation, portability, automation and security using a crypto key per a container. Utilising SW defined infrastructure in a CR enables infrastructure orchestration, which is a simple drag and drop activity. The simplicity of drag and drop functionality can create and configure infrastructure on demand, and has the ability to deploy and rapidly clone an infrastructure with its devices at the push of a button, all while keeping the original devices in their original and native state.

With the utilisation of a SW defined converged infrastructure the benefits include the following: cost savings - there is less HW infrastructure needed - it is faster and scalable, and it can provision an infrastructure of multiple nodes in a short space of time. One of the other views in using SW defined converged infrastructure is a SW defined military application, where it is possible to emulate different military platforms ships, aircraft, tanks and vehicles ICT systems by creating cyber attack scenarios to experiment with what vulnerabilities there are in the platforms ICT within a CR. This can be augmented with other examples, such as SCADA networks, SMART cities, autonomous cars and drones. Cloud-based technologies like SaaS, PaaS and IaaS also allow for the flexible provisioning of virtual infrastructure nodes for a CR.

Priyadarshini (2018) alludes to CRs that are utilising hyper-visors such as ESXi, which are unfortunately not supported on certain cloud infrastructures. Most current CRs have implemented a cloud infrastructure and virtual private networks (VPN), and a limited few CRs have implemented Virtual Clone Networks (VCN) (Priyadarshini, 2018). Using virtualisation, VMs can be deleted and provisioned in any form or manner according to the desired event that is needed (Spirent, 2017).

3.3.13 Software for a Cyber Range

Software (SW) for a computational system is essential for the system to operate (Garrido, 2011). The two components of SW are discussed holistically, namely Systems SW - Operating System (OS) and SW Applications. Globally, there are multiple different types of OS that are utilised and installed in CRs, ranging from the popular OS Linux[12] to a Microsoft Windows platform[13] utilising various different versions and releases. Adding to this are proprietary OS versions that are independently developed in organisations. From a SW development perspective, upgrades throughout the life-cycle are to be managed according to a standardised SW development process. Open-source SW development is widely utilised due to costs, however careful consideration of this is to be made so as to implement SWs that are fit for the purpose of the CR.

Virtual SW is a fundamental and essential part of enabling a CR to emulate OS and provision multiple networks in a small space of time. There are multiple virtual SW applications that are utilised in CR, with the most common virtual SW utilised being VMware[14] (Fusion and Workstation), Oracle VM Virtual Box[15] and other Linux based virtualisation SW (such as Red Hat virtualization). There are multiple other virtual SW that are utilised in a CR and are discussed in work by Davis and Magrath (2013), which highlights SW utilised in academic, military and commercial CRs. In customising SW for a CR, the approach of Development and Operations (Devops), which is a combination of SW development and operations, enables a collaborative effort in SW construction (Edwards, 2010). Some Devops tools are Ansible[16] which is a development configuration tool similar to Chef[17] and Puppet[18], which have been applied in CRs and can be applied easily and seamlessly to the management and configuration of virtual nodes.

Examples of vulnerability SW tools utilised in CRs include OpenVAS[19], NESSUS[20], and Forensics tools such as (Forensic Tool Kit (FTK)[21]). There are multiple open-source tools and software hacking peripherals that are similarly utilised in a

[12]https://www.linux.org/
[13]https://www.microsoft.com/
[14]https://www.vmware.com/
[15]https://www.virtualbox.org/
[16]https://www.ansible.com/overview/devops/
[17]https://www. chef. io/devops-tools/
[18]https://puppet. com/solutions/devops
[19]http://www.openvas.org/
[20]https://www.tenable.com/products/nessus/nessus-professional
[21]https://accessdata.com/products-services/forensic-toolkit-ftk

CR, namely Pwn Pad[22], Wifi Pineapple[23], and USB Rubber ducky[24]. Other SW that is widely utilised in a tool box for cyber security testing and evaluation includes Kali[25], Black Arch[26], Maltigo[27], and multiple other SW security testing tools. Other SW utilised for modelling, simulation and emulation are discussed in Section 2.5. When utilising SW applications in a CR, the following considerations are to be taken into account: licensing related to cost, upgrading and testing of the SW, development of proprietary SW related to its sustainment over time and cost through its life cycle, and finally the risk of SW failure and the impact thereof on the CR effectiveness and performance.

3.3.14 Redundancy

Redundancy for a CR can be debated due to its virtualisation either in a cloud-based or stack infrastructure. The concept of IaaS can be utilised depending on the cloud service provider and the imaging of the virtual instances. The redundancy of the physical computational processing platform can be mirrored as a back-to-back system that is updated regularly to ensure redundancy in case of data loss -if a CR system gives errors or a failure. This will depend on the cost and feasibility of the implementation, and on whether a CR is distributed and can use other computational processing platforms. Considering a mirrored back-to-back system for a CR must take into account the different power distribution, SW appliances, critical servers, Core LAN HW (routers, switches), boundary HW (gateways for distribution and federation), and data links. These pointers are to be configured according to the identified CR. Redundancy works together with backup systems in that the course of action is to restore the system or applications to their original state, especially when conducting cyber war gaming or a cyber event (Fox *et al.*, 2018).

3.3.15 Facility

The facilities for a CR are to comply with its type, purpose and size according to national occupational health standards. There can be other layouts that are appropriate for the type and size of the CR that is required, as discussed in Section 2.4.3. CR facilities differ according to its purpose and method for accommodating users, either by utilising a small room or remote container to a cloud service provider, which links users in remotely through VPNs, or the traditional computational stack infrastructure facilitating a static testing and training environment. A static facility concept layout of a CR, as adopted from TMRC (2015) is depicted in Figure 3.5 and described below:

[22]https://www.pwnieexpress.com/mobile-line-shift-to-aopp
[23]https://www.wifipineapple.com/
[24]https://shop.hak5.org/products/usb-rubber-ducky-deluxe
[25]https://www.kali.org/
[26]https://blackarch.org/
[27]https://www.paterva.com/

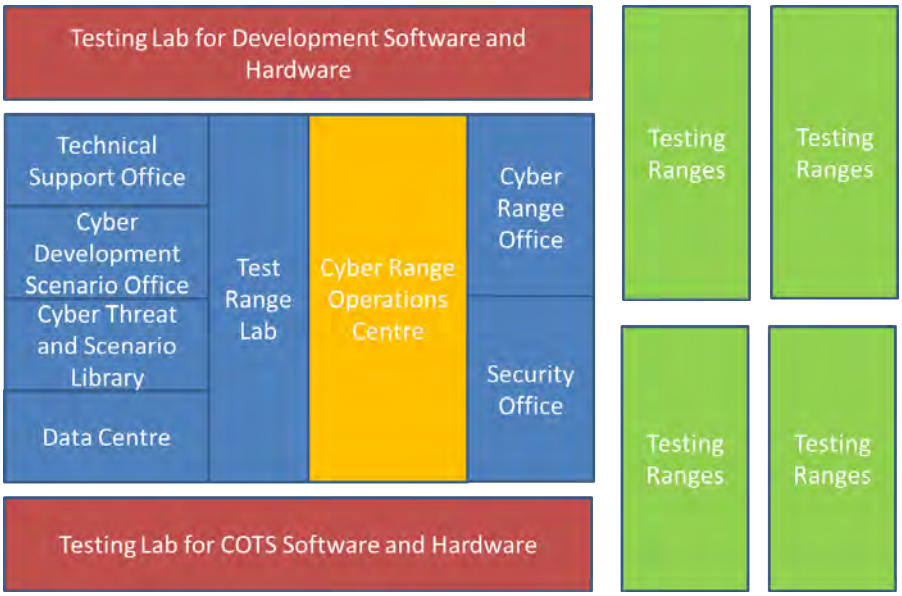


Figure 3.5: Proposed Concept Layout Cyber Range Facility

- CR operations centre: Overall situational awareness of the CR, implementing cyber scenarios and monitoring the overall view of the performance of the test ranges.
- Technical support office: All related technical support for the CR (setting up of cyber events, CDX, CTF, degaussing and sanitising hardware).
- Cyber development scenario office: Development of cyber scenarios for different cyber events.
- Cyber threat and cyber scenario library: Housed in a secure data centre.
- Test range lab: Testing of the initial cyber event for a specific network or technology.
- CR office: Administration of personnel and booking of cyber events and/or requirements for testing and evaluation.
- Security office: Administration of security testing with the testing lab for Commercial off the Shelf (COTS) and Military off the Shelf (MOTS) products, FW, HW and other SW.
- Test ranges: Dependent on size and number of users to be trained in a CR.

3.4 Cyber Range Pairwise Comparison

A "world-view" is a generalised view of the world and how individuals and objects are related and fit into the world, with reference to the view-holder's beliefs, socio-political, moral and aesthetic ideals, and the principles by which they know (Spirkin,

1983). 'The principles by which they know' is the premise from which the argument is based by using experience, understanding of literature and observations of a CR.

The author has utilised the world-view methodology and the Forced Choice Paired Comparison Analysis, which is also known as Pairwise Comparison (Mindtools, 2018), to determine the relevant importance between two different CR core capability elements. This evaluation was reviewed by experts, as in Section 6.4. Based on this understanding, these methods were used to determine the relevant importance of core capability elements for proposed CR capability levels I to V, namely limited, low, medium, high and ultimate. The relevant importance was determined with the capability levels in mind, with the top five core capability elements forming the basis of the level that is being compared. This was done to get an output to minimize bias and manipulation. This technique of analysing is used in engineering requirements and other environments, and enables one to work out the importance of a number of options relative to one another to decide on the relevant importance of the core capability elements . To analyse the Pairwise Comparison data, there are different models that can be utilised, namely Thurstone's model, which states that when a person judges whether A is better than B, they draw a realization from A's quality distribution and a realization from B's quality distribution, and then choose the option with the higher quality. Bradley and Terry introduced an alternate model, also known as the Bradley Terry Luce Model (BTL) (Tsukida and Gupta, 2011), which differs from the Thurstone model in that it uses Gumbel random variables for the quality of each option Tsukida and Gupta (2011). For this thesis the Thurstone model was utilised to derive the higher quality.

The Pairwise Comparison analysis tables are included in Appendix D,where the four different CR levels (with level V being multiple level IVs), were determined according to the proposed CR capability levels, namely Limited, Low, Medium, High and Ultimate, as captured in Sections 4.2 and 4.3. The scores for the analysis were Low = 1, Medium = 2, High = 3. The score was calculated to give a result which was rated from highest to lowest relative importance. The results are not perfect, however for the purpose of justifying the relative importance of the core capability elements for the different CR levels, the Pairwise Comparison allows for a result to be determined. The results that were captured using the Pairwise Comparison analysis are depicted in Table 3.2.

The tables are incrementally displayed, starting from a level I CR cascading up to a level IV CR, and level V is a presented as multiple level IVs. The core capability elements that are determined in CR level I are by default part of level II and so forth. As can be seen, the top five core capability elements are allocated into the different CR capability levels. The rationale behind this result is that there needs to be a baseline established for CR capability levels, however the fundamental critical core components are to be implemented, as discussed in Section 3.3. The analysis of the relevant importance for a CR as per expert review is presented in Section 6.1.2. The overall relevant importance for the CR capability levels is depicted in Table 3.3.

Table 3.2: Relevant Importance Cyber Range levels I to IV

Relative Importance CR Level I	
1	Software Operating Systems
2	Network Infrastructure (Physical)
3	Software Applications
4	Management System
5	Traffic Generator Capability
6	Scenario Generator Capability
7	Virtual Infrastructure
8	Security System
9	Back Up Storage Capability
10	Threat Library Capability
11	Real device Connectivity Capability
12	Facility
13	Instrumentation connectivity capability
14	Redundancy
15	Monitoring System with sensors
16	Learner Management System
17	Health Monitoring System with Sensors
18	Security Incident Events Management (SIEM)
19	Big Data Capability

Relative Importance CR Level II	
1	Virtual Infrastructure
2	Scenario Generator Capability
3	Real device Connectivity Capability
4	Facility
5	Threat Library Capability
6	Back Up Storage Capability
7	Instrumentation connectivity capability
8	Monitoring System with sensors
9	Instrumentation connectivity capability
10	Learner Management System
11	Redundancy
12	Health Monitoring System with Sensors
13	Security Incident Events Management (SIEM)
14	Big Data Capability

Relative Importance CR Level III	
1	Instrumentation connectivity capability
2	Redundancy
3	Monitoring System with sensors
4	Back Up Storage Capability
5	Learner Management System
6	Security System
7	Health Monitoring System with Sensors
8	Big Data Capability
9	Security Incident Events Management (SIEM)

Relative Importance CR Level IV	
1	Security System
2	Big Data Capability
3	Health Monitoring System with Sensors
4	Security Incident Events Management (SIEM)

Table 3.3: Relevant Importance for Cyber Range Capability levels

Relevant Importance as per paired Comparison	CR Levels	CR Core Capability Elements
1		Software Operating Systems
2	Level I	Network Infrastructure (Physical)
3		Software Applications
4		Management System
5		Traffic Generator Capability
6		Virtual Infrastructure
7	Level II	Scenario Generator Capability
8		Real device Connectivity Capability
9		Facility
10		Threat Library Capability
11	Level III	Instrumentation connectivity capability
12		Redundancy
13		Monitoring System with sensors
14		Back Up Storage Capability
15		Learner Management System
16	Level IV	Security System
17		Big Data Capability
18		Health Monitoring System with Sensors
19		Security Incident Events Management (SIEM)
20	Level V	Multiple Level IV CR's

3.5 Case Study SANReN

The real network data capture of the South African National Research and Education Network (SANReN[28]) was used as an inspiration to form a baseline in determining a level III for a CR. The reason for this was to utilise a sizeable real network as the midpoint for creating a baseline criteria for classifying CR levels based on the network's capabilities. From these network capabilities, the levels are incrementally adjusted for lower and higher levels. The SANReN was used to gather technical results based on throughput, speeds, latency and other data as a real-time view of an

[28]http://www.sanren.ac.za/

ICT network in order to quantify the analysis of networks to be implemented in a CR at different levels. The SANReN is comprised of a core national backbone, backbone extensions, back-hauling from submarine cable, several metropolitan rings, and link extensions. The logical view of the SANReN network is depicted in the Figure 3.6. By

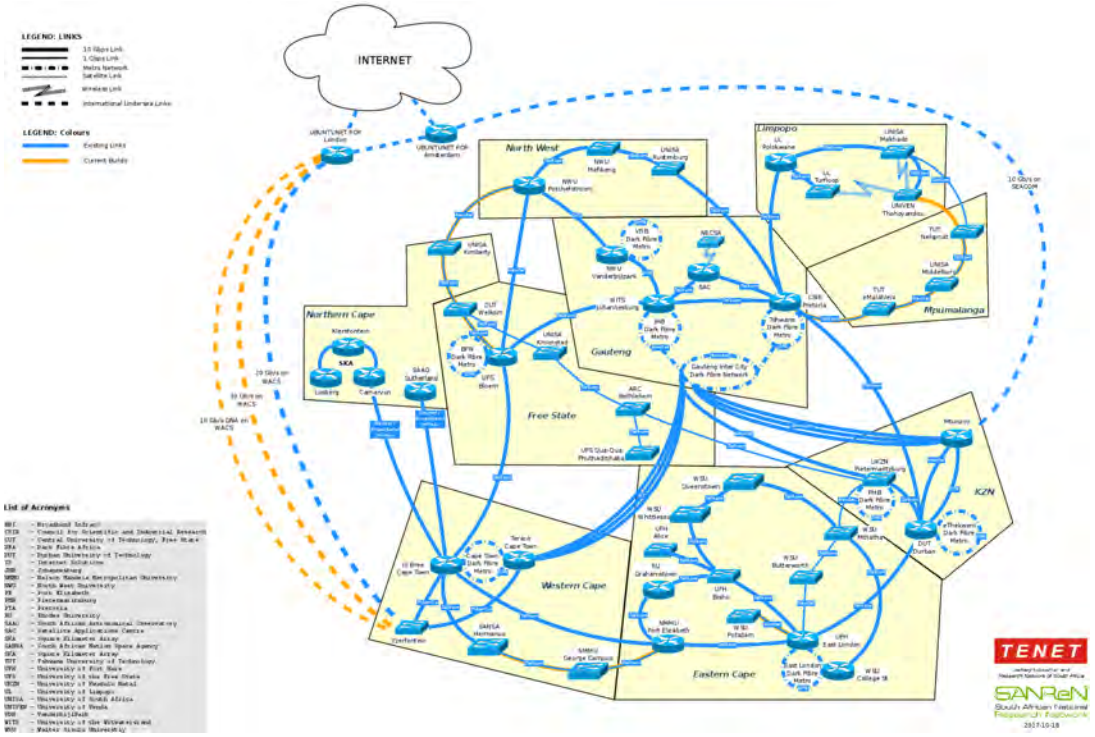


Figure 3.6: SANReN Logical View (SANReN, 2018)

attaining the results of the relative importance of the core capability elements and establishing proposed CR capability levels, the results of the data received from the SANReN allow for a network to be emulated in a CR in a realistic manner to establish a benchmark of a real network. The rationale for this is to provide an example of an organisation's real network topology, which can be emulated in a CR depending on its capability. The data that was gathered from the real network was done through the implementation of sensors that were deployed on the network through a project that is envisaged to be implemented to monitor the SANReN. Data captured from the SANRen was received on 29 June 2018 for the period 12 April to 21 May 2018.

1. Hosts (divided into two parts)

   (a) Full stack of physical hosts. The SANReN total IPs in IPv4 range from /15 to /24 with a total of IPv4 addresses 5 757 440. However, due to the live nature of SANReN, getting the exact number of hosts is challenging due to users joining and leaving the network on a continuous basis. The IPs which are active was determined in a given hour on a normal work day.

   (b) Per hour, on average, 789 667 unique internal IP addresses were observed, which connect to 3 897 504 unique IP addresses externally. However, in

Table 3.4: Top 20 Generic Services Running on SANReN 12 April to 21 May 2018

Port	Protocols	Flows	Port	Protocols	Flows
443	HTTPS (TLS/SSL)	3. 9B	6666	IRC(U) Internet Relay Chat	184. 7M
80	HTTP	2. 4B	3545	CAMAC Equipment	168. 4M
445	Samba - SMB(server message blocker)	1. 5B	6060	Unique	163. 8M
53	DNS	1. 4B	81	Host 2 Name Server	145. 6M
23	Telnet	1. 2B	2323	3D-Nfsd (IOT devices)	137. 2M
22	SSH	701. 5M	6881	Bit Torrent	131. 8M
123	Network Time Protocol	548. 7M	143	IMAP (Email)	120. 8M
3309	TNS ADV	305. 4M	51413	Unique	110. 1M
0	Not a valid port	304. 1M	8083	Unique	94. 7M
8080	HTTP	213. 7M	41543	Unique	92. 8M

general there are approximately 1.2 million users and there are approximately 1.8 million devices connected to the internal SANReN network.

(c) Traffic generated generally in one month is approximately 50.61 petabytes of traffic flow travelling between the SANReN and external networks in one month.

(d) Total network capacity is 3 292 Gbps, and at the time this data was received the current utilised capacity was 240 Gbps (only 7.3% utilised).

(e) Services running on the SANReN at the time this data was received are illustrated in Table 4.1; this is the type of traffic that needs to be generated within a CR.

2. The number of servers was unknown due to the SANReN not owning, operating or controlling servers on the network, however there can be multiple at any of the end points.

3. The network itself:

(a) End points are approximately 1.8 million internal endpoints in the backbone, the back haul is dependent on the link, which varies between 100GB/10GB/1GB links, and the core backbone routers are approximately 239, of which 231 are situated at research institutes and university sites.

(b) Throughput on average to each site as per above SANReN logical view is 3.7 Gbps.

(c) Latency, National Latency (response time): < 50 ms (Telnet) and International Latency (response time < 260 ms (Telnet)).

The SANReN will be utilised as an implementation scale type level III network to formulate a start baseline for the CR levels. This is the type of infrastructure that is to be emulated, and traffic generated in a level III CR (medium CR) is used as a baseline to categorise the different levels of a CR, as in Section 4.3.

3.6 Capability Development for a Cyber Range

Developing a capability starts off with a reason why the capability is needed. In most cases, this is derived from a strategy which gives direction for the future. For a capability to be developed requires an understanding of what the capability must achieve to fulfil certain objectives and effects. In the development of a CR there are two main areas which are focused on, namely the functional attributes and the capability elements. Functional attributes are functions that the capability needs to fulfil with reference to the effects that the capability must achieve (Thaba, 2017). The functional attributes of a CR are suggested as follows: cyber fire power, Command and Control (the management) of a CR, mobility of a CR, information flow in a CR, the protection (security) within the CR, the level at which the CR should operate, the funds available for the development of the CR and the sustainment over the CR's life cycle. Capability elements, or system elements, are the elements that the capability requires in order to operate (Thaba, 2017). The capability elements of a CR can be associated with the acronym POSTEDFIT, as described by Smith and Oosthuizen (2011); Botha and De Vries (2012) and Thaba (2017), which suggests which elements are needed to sustain the CR capability in an organisation. A CR, according to POSTEDFIT, is described as follows:

- **Personnel** - the teams that are utilised to ensure that the functioning of the CR exercises.
- **Organisation** - what organisation the CR will be associated with.
- **Structure** - how the CR will be structured with personnel.
- **Training** - what training is required to operate the CR and what training is provided in the CR.
- **Equipment -** what is needed to build, develop and maintain the CR.
- **Doctrine** - what processes and rules apply when using the CR and how the will be CR utilised.
- **Facility** - how sufficient must the facility be and what should be in the facility.
- **Information** - how will the information be shared and communicated in the CR.
- **Technology** - what technology is needed and what is needed to be researched and developed for a CR.

There are two other well-documented capability elements; firstly, the US Department of Defence uses an acronym DOTMLPF, which stands for Doctrine, Organisation, Training, Material, Leadership and Education, Personnel and Facilities (Defense Acquisition University, 2005). The British defence force uses Defence Lines of Development (DLOD) which include Concepts and Doctrine, Equipment, Information, Infrastructure, Interoperability, Logistics, Organisation, Personnel and Training (TRAK-Community, 2010). These capability elements can also be adopted to aid in the development of a CR capability.

After the development of a capability, the full life-cycle capability management will need to be implemented to ensure that the capability is updated due to changing environments. PPT need to embrace the changing environment. With this in mind, the development process for a CR capability will evolve as the cyber environment changes. The main focus in developing a CR is viewed as an effect-based approach to enable the CR to fulfil its purpose and ensure that the functional attributes and capability elements are appreciated for the CR development. However, this will only be satisfied up until the next major cyber threat, this will then lead to a heightened motivation to improve, thus increasing the maturity level through the CR's evolution.

The capability development process for a CR is based on the IDEF 0[29] functional modelling method, in that the model needs an activity that has an input, a mechanism, a control and an output which becomes an input for the next activity. Figure 3.7 illustrates the holistic approach for the capability development generic process for a CR.

Within the capability development process, there must be a cyber security strategy that gives direction. In the strategy there are multiple considerations that must be taken into account, thus the threat analysis - as part of an environmental scan of both external and internal environments - must be quantified and understood, hence the focus on the cyber domain (5th Domain of Warfare) with specific goals, objectives and missions that need to be achieved, as described Section 2.1.

The capability development starts as a higher level concept as part of identifying the national cyber maturity and identifying the cyber gaps. In identifying the gap, a Required Operational Capability (ROC) will be developed, addressing what capability needs to be developed, this is known as the Conceptual stage, and is the input to the Technical Building stage. In this stage the requirements to build a CR are drafted in a User Requirement Statement (URSt), which will give input to the functional and system requirements (the system is divided further to sub-system and component level), allowing for a plan to be drafted as input to a User Requirement Specification (URS) for the CR. The specifications will cater for an array of specific features, taking into account specific needs (HW and SW) and core capability elements for the CR system. The requirements and the specification phase is the main crux for maturity of a CR, as this forms part of determining the level of CR capability maturity and will direct the technical development of the CR in its design.

[29] http://www.idef.com/idefo-function_modeling_method/

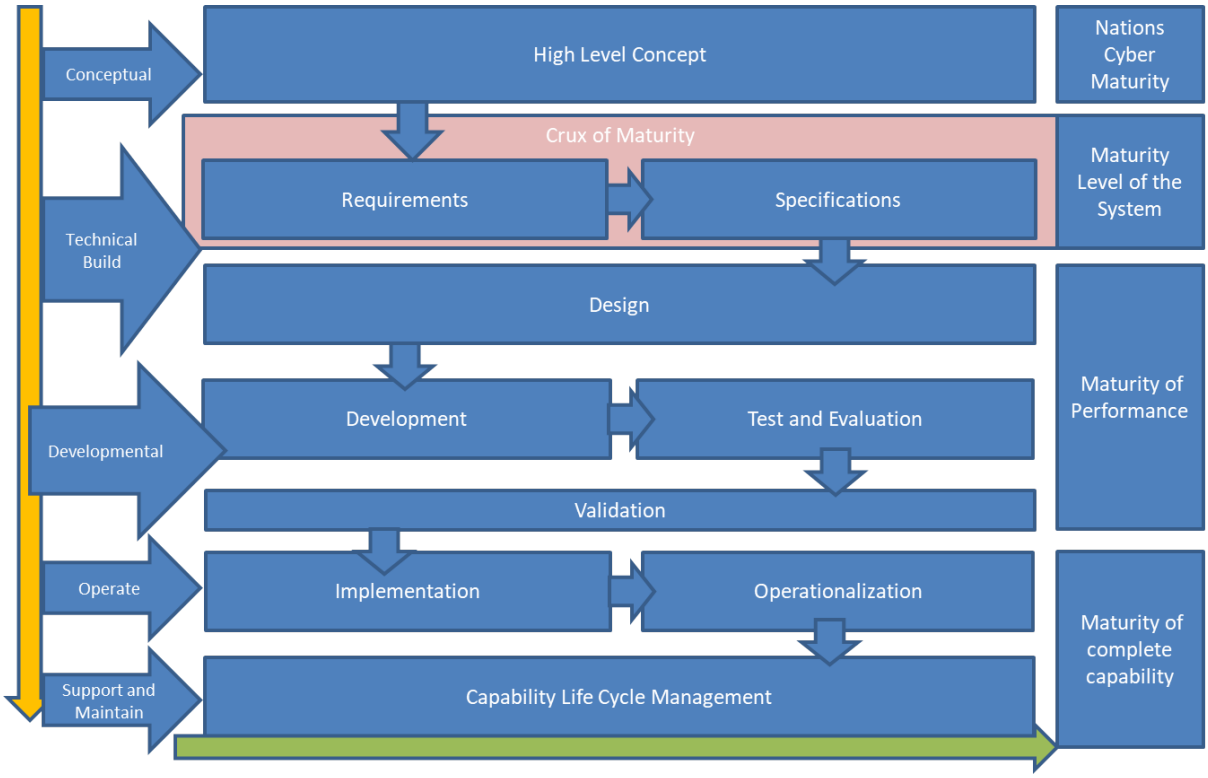


Figure 3.7: Generic Capability Development Process for a Cyber Range

The design phase must have an initial concept design, which must comply with the requirements, and the detailed design must comply with the specifications. Once the design is accepted it forms the input to the Developmental Stage in developing the CR itself. Before the development of the CR, the acquisition phase must be approved; this is a determining factor in the level of capability maturity once the CR is operational. After the development of system artefacts, Proof of Concepts (POC) and the integration of the sub-systems for the CR will lead to rigorous testing and evaluation (T&E) of the CR to ensure that the requirements, specifications and design have been satisfied. Once the T&E is analysed, the results are given either a pass or fail score. If there are rectifications needed this is adjusted and a complete T&E is redone. This is to ensure that there is quality assurance. Validating the CR against the ROC and measuring the CR in a real-time cyber event ensures the CR functionality. Once validation is completed, the capability maturity can be determined and the CR will enter the Operate Stage. This stage is where a CR is implemented in an organisation and operationalised. In these phases the CR will implement the CR capability elements with the processes and procedures that were developed during the Development Stage. This is to accommodate the organisation in terms of the operation of the CR, and with this the maturity of the complete capability is determined. Throughout the CR capability life-cycle management and midlife upgrade cycles, the capability will evolve through the CR's effectiveness, performance, threat, people, processes and technology (Research and Development). The continuous improvement of the capability is key to adhere to the higher level concept of the CR as directed by the cyber

security strategy of an organisation or nation.

3.7 Summary

This chapter established an understanding in defining a CR, taking into account the architecture, the design approach and a concept design for a CR. The CR core capability elements were defined for clarity. The utilisation of a world view methodology and a Pairwise Comparison analysis established a baseline for the relative importance of the core capability elements according to proposed CR levels. A data capture of the SANReN was used as an inspiration for a network topology to form a baseline for a CR level III capability, from which the levels were either incrementally increased or decreased to allow for the development of a proposed criteria for classified CR levels. An understanding of the functional attributes and capability elements for a CR was discussed. A capability development process was established to create a process that can be utilised to develop a CR, taking into consideration the different stages of development and capability maturity. Chapter 4 discusses the establishment of a selection criteria and a proposed baseline criteria for CR capability maturity levels and classified CR levels, and the measurements for a CR.

4

Criteria for a Cyber Range Capability Maturity Model

In Chapter 3 the defining of a CR was discussed, highlighting the architecture of a CR as well as the CR as a system. The core capability elements of a CR were defined, in which a Pairwise Comparison analysis was completed to determine the relevant importance thereof. This enabled the development of a proposed baseline for CR levels; the capability development process gave a holistic view, outlining the process to develop a CR through its development cycle and establishing an understanding of the CR's functional attributes and capability elements, all of which form the basis for Chapter 4.

Chapter 4 focuses on determining a baseline selection and measurement criteria for a CR CMM. In Section 4.1, the selection criteria for a CR are determined to give a high level view on CR criteria, while in Section 4.2 a proposed set of baseline criteria for a CR are given to establish levels. Section 4.3 proposes criteria for the classified CR levels, while Section 4.4 highlights standards that can be utilised for a CR. Section 4.5 will discuss the measurement criteria for a CR, such as the Measurement of Capability (MoC) and Measurement of Maturity (MoM), followed by Section 4.6 which briefly discusses the evaluation of a CR. Section 4.7 gives a summary which highlights the main discussion points raised.

4.1 Selection Criteria for a Cyber Range

The selection criteria for a CR is based on the ability of a CR to perform what it is required to achieve, as per a certain requirement derived from an organisation. Using a criteria allows for a baseline measurement to be formed, either for the development

or procurement of a CR. The formulation of generic criteria for a CR is complex in nature due to the diversity of different CR types and purposes. One source that has developed a proposed criteria for a CR is the National Institute for Cyber Education (NICE) (Adams, 2019) as shown in Table 4.1.

Table 4.1: NICE Proposed Criteria for CR (Adams, 2019)

Criteria for a CR	**Description**
Purpose	For the training of cyber education skills to cater for beginner to advanced levels, either by self paced or simulated real-time experience as defined by a job function. These functions are linked to a workforce development framework which guides the assessment of cyber skills. This is achieved by either obtaining result of the training or assessing the process used by the trainees.
Capability	The content that the CR can deliver which is linked to objectives that are to be achieved. Some examples are CR learning material (presentations, audio, video), lab exercises (virtual machines, physical hardware, lab guides and references), group exercises (Red vs. Blue) and CDX /CTF.
Accessibility	Users ability to access the content either by remote, on-site, on device and the network requirements needed for instance bandwidth and security policies.
Scalability	The CR ability to accommodate more users or different types of content by infrastructure scaling with physical workstations (type and cost) and the CR delivery scaling using resources, facilities and either deploying on premises or through a cloud provider.
Customizability	Ability to alter the content to suit the cyber event requirements such as security metrics, the effort is involved in scenario development the customization thereof.
Usability Administration	Managing and adding users (Manual vs. Self-provisioning), cyber events scored (Results vs. Process) and user's access to integrated LMS.
Mapped to a Workforce Development Framework	Mapping to Knowledge Skills and Abilities (KSA's) and report generation according to the content which is delivered.
Realism Abstract vs. Real Measures	Fidelity of the training environment compared to the actual operating environment.

The criteria in Table 4.1 have aided in formulating the selection criteria for a CR from a holistic view and in developing a method of measuring the capability of a CR

from a performance and effectiveness view. The selection criteria have been derived and formulated from the understanding of a CR and its functions, as presented in Chapter 2. Based on this understanding, the selection criteria focuses on the main areas that are to be considered for a CR. Thus, selection criteria for a CR include the following:

- CR to be measurable against technical specifications and standards as per the functional requirement set.
- Specific for its purpose as defined in the design.
- Relevant and verifiable to the goals it is to achieve.
- Economically viable considering capacity, capability development and sustainment over time.
- Flexible and modular in nature over its life-cycle as a system.
- CR service on demand to generate cyber events, learning material and results in a short space of time.
- High computational performance, Quality of Service (QoS) and high fidelity in a virtual environment.
- CR management and ease of use for the implementation of CR activities, including competency in cyber skills.
- Ability to generate different levels of threat tiers tolerant with the ability to maintain malicious code libraries.
- An interoperable, intelligent, and integrated CR system with the ability to be distributed and federated with other CRs.
- Ability to collect data from users of a CR for analysis of a user's performance during a cyber event.

In comparing the above selection criteria with the proposed criteria from NICE, it was established that the focus is predominantly on CR performance and ability to provide quality cyber skills training. Key for both sets of criteria is the ability of the CR to provide quality cyber content to develop users' cyber skills in a cyber development environment (with high fidelity and accuracy), and to generate cyber event timeously and with the relevant ease of access. Both of these criteria allow for the development measures that are to be considered for a CR capability maturity.

4.2 Proposed Baseline Criteria for Cyber Range Levels

CR levels are fictitious in nature for the purpose of this research due to CRs being considered a closed to confidential environment, however they are used as a baseline

to illustrate a basic to a highly advanced CR using the literature to substantiate the different levels, as discussed in Section 2.6, in which the most common number of levels for capability maturity is five .

For the duration of this thesis, the CR levels are used in measuring the capability maturity of a CR. The CR levels are more of an evolutionary process, in that the CR level will consistently evolve and adapt with technology to reach the desired purpose or performance goal. When developing a CR, the end state, or what the CR needs to perform effectively,is a vital consideration throughout the CR's project development life cycle and as the CR evolves to different levels, as portrayed in Table 4.1.

4.3 Proposed Criteria for Classified Cyber Range Levels

Due to the lack of classified levels currently present in the relevant literature, the proposed levels are novel. In the development of a proposed criteria for classified CR levels as in Appendix B, the approach was to utilise the results of the relevant importance of the core capability elements as in Section 3.4, which was based on the Pairwise Comparison analysis. The utilisation of real network data capture (SANReN) as in Section 3.5 was used as an inspiration for a level III CR to create a baseline from which to incrementally increase and decrease the levels accordingly. The rationale of developing a proposed criteria for classified CR levels is based on forming a baseline to allow for a distinction between different CR levels and the ability to measure a CR. It also allows for an incremental view of a CR's capability maturity. This has been determined by five specific levels that indicate the following:

- Description of the CR.
- Core capability elements that are critical requirements for a CR.
- The capabilities focused on a proposed required performance.
- The maturity is focused on the level of maturity of the People, Processes and Technology in a CR.
- The threat tier level a CR can maintain.

4.4 Standards for a Cyber Range

Standards are specific and technical in nature to guide the achievement of a certain requirement, whereas a baseline is more mapped to accepted industrial standards, hence a standard gives a baseline for the minimum compliance requirement (Gregg, 2005). Standards are important to ensure integration, interconnectivity, interoperability and security due to the vast and different ICT technologies. Within a CR the core capability elements with their different components need to utilise ICT and international security standards to allow for the CR to be comparable with industrial

Table 4.2: Proposed Criteria for a CR Levels

Level	Capability	Maturity
I	**Limited**: Initial cyber security training on an isolated simulated network with limited hosts and limited cyber scenarios, limited legacy stack infrastructure.	**Basic**: Initial: People have basic cyber skills, processes are not structured and are more reactive, the technology has a basic maturity.
II	**Low**: More focused on testing and evaluation of basic cyber projects, cyber processes and cyber security training, with a modelling, simulating and emulating capability for medium cyber scenarios with a legacy stack infrastructure and limited hyper convergence infrastructure.	**Intermediate**: Managed: People have intermediate cyber skills, basic processes and controls are present, and more reactive in nature, Technology is of a more focused nature for the initial CR capability maturity.
III	**Medium:** The focus is on cyber resilience, testing and evaluation of computational products, with limited research and development, with a modelling, simulating and emulating capability for advanced cyber scenarios but with limited federation capability which is virtual, instantaneous and on demand for limited stakeholders, with a legacy stack and a functional hyper convergence infrastructure.	**Fully Functional**: Defined: People are more certified and trained, processes are standardised and controlled and are present throughout the CR, and technology is of a higher functional mature nature.
IV	**High**: More advanced focus on cyber resilience and cyber testing, with a more research and development closed-source focus, with a modelling, simulating and emulating capability for highly advanced cyber scenarios and wider federation access capability which is virtual, instantaneous and on demand for limited stakeholders on a national level with an advanced hyper convergence infrastructure.	**Advanced**: Quantitatively Managed: People are at an advanced level of analytic cyber skills level, processes are qualitatively measured and are used to standardized processes, and technology is of an advanced maturity.
V	**Ultimate**: Focused on quality cyber resilience and highly advanced cyber testing with high research and development closed-source focus for multiple stakeholders with a modelling, simulating and emulating capability for ultra highly advanced cyber scenarios which is virtual, instantaneous and on demand, testing cyber capabilities with sophisticated instrumentation, with national and global federation, and with a highly advanced hyper convergence infrastructure.	**Highly Advanced**: Optimizing: People have highly advanced cyber skills, processes are focused on continuous improvement to strive for excellence to improve the processes, and technology is of a highly advanced maturity.

baseline standards. A CR is to be flexible to adjust to an adopted set of standards depending on its purpose.

An example of work that has been done in standardisation for CRs is the Lincoln Laboratories. They have proposed a single descriptive language that all CRs can utilise for a CR event, from which ontologies have been built, named the Common Cyber Event Representation (CCER). The CCER is used to describe networks and standardise networks for use in a CR. The data of the CCER is then fed into a CR tool called Automatic Live Instantiation of a Virtual Environment (ALIVE), which is a range build out application. This then feeds into the Lincoln adaptable real time information assurance test bed (LARIAT) application for traffic generation and control of the range (Braje, 2016). This standardisation addresses the gap in the lack of rapid virtual network reconfiguration SW for use in CRs in general. The standardisation of using a common data source for cyber events will greatly lower costs for other CRs, and the use of a single descriptive language that can be shared globally can enable interoperability and events reuse (Braje, 2016).

Common Criteria, as described by Mead (2013), enable objective evaluation to validate that a particular product or system satisfies a defined set of security requirements or perimeters. Best practices, on the other hand, is described as a concept in which the best of specifications and applied practices are a culmination of different standards and implementations from experience and expert views. A combination of standards, Common Criteria and best practices can be implemented in a CR to give a holistic guideline that can be utilised for measuring a CR. These list of standards presented below is not exhaustive, but provides a guideline that can be adopted for a CR. The rationale behind the selection of these standards is a focus on cyber terminology and technical and security training guidelines that a CR can implement.

- **NIST Special Publication 800-115 (2008)** provides a technical guide to information security testing and assessment covering the basic technical aspects of conducting information security assessments (NIST Institute, 2008), which can be utilised in the security testing of computational devices in a CR.

- **ITU-T X. 1205 (2008)** provides an overview and defining of cyber security, threats and vulnerabilities and the application of security dimensions and security layers (ITU Institute, 2008) which can be utilised for for cyber event planning in a CR.

- **ISO/IEC 15408-1 (2009)** provides a common set of security functionality and assurance measures (ISO Institute, 2009a) which can be utilised in a security evaluation to measure a System Under Test (SUT) in a CR.

- **IEEE 802. 1X (2010)** provides and specifies common architecture, functional elements, and protocols that provide authentication and secure communication between clients attached to the same LAN (IEEE Institute, 2010). This can be utilised when provisioning networks for cyber events due to the implementation

of the standard in real networks. This can also be utilised for a distributed CR, or between CR VLAN's.

- **ISO/IEC/IEEE 42010 (2011)** addresses the creation, analysis and sustainment of architectures of systems (ISO Institute, 2011a), which can be used for CR architecture for the development of a CR system.
- **ISO/IEC 25010 (2011)** provides specific measuring and evaluating of systems and software from a product quality view using the product quality model (ISO Institute, 2011b). This standard can be used in the development of CR systems, utilising the product quality model to measure and evaluate products.
- **ISO/IEC FDIS 27032 (2012**) provides guidance for improving the state of cyber security (ISO Institute, 2012a), which can be utilised when developing CR training content.
- **NIST Special Publication 800-61 (2012) Revision 2** provides guidance in the handling, analysis and response determination for Computer Security Incidents (NIST Institute, 2012), which is useful in the training that a CR provides for cyber incident handling.
- **NIST 7298 Revision 2 (2013)** Glossary of Key Information Security Terms is a guideline for terminology that can be utilised to standardise terminology used in a CR (NIST Institute, 2013). Another glossary that can be utilised is the Cyber Range Interoperability Standards (CRIS) Cyber Range Lexicon Version 1.0, which was created to form standard terminology for cyber activities. This standard, can still be utilised as part of a best practices approach (Damodaran and Smith, 2015).
- **Draft NIST Special Publication 800-181 (2016)** National Initiative for Cyber Security Education (NICE) Cyber Security Workforce Framework (NCWF), provides a framework for cyber security education, training, and workforce development (Newhouse *et al.*, 2016). The framework can assist in developing content processes for the training application in a CR.

4.5 Measurement Criteria for a Cyber Range

Frost (2000) states the meaning of measure as "a specific observation characterizing performance". Black *et al.* (2008, pg 2) describe a measure as, "a solid objective attribute, for example a percentage or length of time". Abbadi (2006) alludes to measuring, as a quantitative method in which some object is measured by its quantity against a standard of a specific dimension. Hence a measurement is an agreed-upon attribute, according to a standard or specific observation of performance using a quantitative method.

Hwang and Bush (2015) at the Massachusetts Institute of Technology Lincoln Laboratory, who gave a recommendation for measuring a CR, indicated that there

are two prominent approaches to measure a CR, namely Measurement of Effectiveness (MoE), and Measurement of Performance (MoP). Hwang and Bush (2015) argues that a MoE is a top-down approach, is mission critical, and is measured in a qualitative approach. MoP by contrast is a bottom-up approach, is technology focused, and is measured in a quantitative approach. However, a mixed method research approach to capture the breath and depth of the CR measurement is ultimately best suited. By using the mixed method, multiple methods and data sources are utilised for measuring, which allows for triangulation that can identify aspects from different viewpoints using different methods. This can be very complex and time-consuming, and can become unclear in solving discrepancies (FoodRisc, 2016). The mixed method for measuring a CR will allow for the strengths of both a qualitative and quantitative method to augment each other, with a more complete and comprehensive understanding of measuring a CR to give an accurate result.

Kiemele *et al.* (1997) defines a metric as, "an objective indicator or measure which facilitates process improvement", which can be adjusted to facilitate people, process or technology improvement. Merriam Webster (2018) defines a metric as, "a standard of measurement". Hence a metric is expressed by a unit of measurement; for example, a metre is a metric that measures lengths. Mateski *et al.* (2012, pg 9) states that, "a metrics allow us to measure attributes and behaviours of interest", for example the performance of a CR when in test, or the effectiveness of the CR in emulating cyber events. Metrics facilitate decision making and can be applied by an operator to improve performance (Black *et al.*, 2008). Mostly, a metric is a quantitative measure of the degree to which a system, component or process possesses a certain attribute.

In a CR, metrics are especially designed to characterize the capabilities, performance, risk, or security of the SUT. A security metric looks at mission-relevant adversarial threats and mission-critical system assets (Hwang and Bush, 2015). In general, metrics for a CR identify a certain unit of measure, such as gigabit per second, millisecond, and other ICT units of measurement. The opinion of Black *et al.* (2008) is that an organisation should first select metrics, and then determine what measures it can employ that support those metrics to improve performance. Different measures using metrics for different CR levels are to be standardised and established for a CR to be quantitatively measured. This allows for milestones to be achieved, allowing for progression to another level. This also establishes a benchmark from baselines that are taken from the real operational cyber environment, which can be used to determine capability maturity of a CR. Formulating measures and metrics for a CR is a huge task in itself, and involves consolidating standards of measures accepted by the CR community and experts alike. However, these measures and metrics will enable a CR to be classified according to levels of capability and maturity.

Software automated collection methods using a quantitative measure are a more effective and accurate method than that of the traditional manual method, for example surveys or evaluation forms, which are less accurate and provide more of a qualitative measure of collecting data . An example of data collected using a SW

automation collection method is the time a cyber warrior (CW) takes to solve a cyber event in a given scenario. The measurement will indicate what processes, tools, and scripts were used to solve the cyber scenario, providing a step-by-step analysis of the actions performed (Labuschagne and Grobler, 2017). The data capture from logs of the cyber events that have been executed in the CR over a certain time period can be utilised to measure the CR's effectiveness with reference to the time to configure, provision or generate new cyber events, and execute a SUT evaluation. The accuracy of metrics is vital, and is dependent on the accuracy of the measurement determined by the organisation for its CR. With this, the measures are to be well-defined to not have any ubiquity. Donovan *et al.* (2015) stated in his lessons learnt that the current CRs have sufficient capabilities to capture many general measures of performance, however specialised tools and instruments are needed to measure effect.

The measurement of a CR for this thesis is based on two distinct categories, namely capability and maturity, which are measured to determine a proposed level of capability maturity for a CR. While no scored index or metric for the measurement of a CR is defined as this is outside of the scope of the thesis, a conceptual baseline to measure a CR is discussed. These categories - the MoC and MoM - are utilised to measure a CR from a multiple dimensional view to allow for a more objective and complete measure. The baseline measures are discussed in more detail in Sections 5.2 and 5.3.

Briefly, the first category MoC is composed of three elements, namely Measurement of Effect (MoE), Measurement of Performance (MoP) and Measurement of Threat (MoT). These elements with their specific defined levels allow for the overall level of the CR capability to be determined. The identified elements are prominently utilised in determining capability in a system. The second category, MoM, includes three elements, namely People, Processes and Technology. As with the MoC, these elements with their specific defined levels will allow for the overall level of the CR maturity to be determined. The identified elements are predominantly utilised to drive successful change, focused on the maturity of a CR through defined levels. The following subsections (4.5.1 and 4.5.2) give a holistic description of these two categories

4.5.1 Measurement of Capability (MoC)

In literature, different methodologies are used to measure the capability of a system's ability, effect and performance. The capability of a CR is measured in accordance with the identified CR core capability element within the elements for the MoC:

1. **Measurement of Effect (MoE):** The sub-categories measured are the operator's cyber skills, CR ability to capacitate a single or multiple cyber operational tasks, CR ability to adapt to different cyber environment scenarios, CR ability to manage cyber activities' effectiveness with different levels of cyber scenarios, effectiveness of a CR and its core capability elements through its evolution over time.

2. **Measurement of Performance (MoP)**: The sub-categories measured are speed, throughput, fidelity, switching ability between cyber events, quick configuration, traffic generation, storage and retrieval, security assessment, and instrumentation connectivity focused on the core capability elements of a CR.

3. **Measurement of Threat (MoT)**: The sub-categories are the ability of the CR to generate cyber threats for cyber scenarios, capacity of security threat tools, and the ability of the core capability elements to maintain threats internally within the CR.

4.5.2 Measurement of Maturity (MoM)

Measuring maturity is a complex and often difficult measure, most maturity models are incremental in nature, using the achievement of milestones to determine a level. The maturity of a CR is measured in accordance with the identified CR core capability element within the elements for the MoM.

1. **People Maturity**: The sub-categories measured are developing individual capability to perform in a CR with the necessary knowledge and skills; building work groups and culture based on communication and coordination in a CR; motivating and managing performance of individuals, including managing unacceptable performance and rewarding exceptional performance; shaping the workforce of the CR to ensure that people have the necessary skills to operate in a CR according to the CR's' purpose, and core capability elements of a CR.

2. **Processes Maturity**: The sub-categories measured are process management, which covers the whole range of developing and improving CR processes; project management, which covers the CR project management activities; engineering processes, which cover the CR technical development and maintenance; and support processes, which cover the CR activities that support the evaluation of a CR. All of these processes are focused on the core capability elements of a CR.

3. **Technology Maturity:** The sub-categories measured are the ability and upgrade of the technology used in a CR through its life-cycle management; the technology drivers and maturity thereof; managing the technology as a capability in a CR, and the maturity of computational devices and SW. All of these processes are focused on the core capability elements of a CR.

4.5.3 Measurement Conceptual Model

The measurement conceptual model for the MoC and MoM for a CR are based around the core capability elements of a CR. The MoC is based on its elements, in which the CR MoE is fed by the CR's MoP and MoT. Achievement of the MoE is based on obtaining the desired end state of what is to be achieved in a certain cyber event in a CR. The MoP allows for the CR to enable the methods and the means to achieve the MoE in a CR. The MoT enables the CR to maintain threats on different levels to ensure

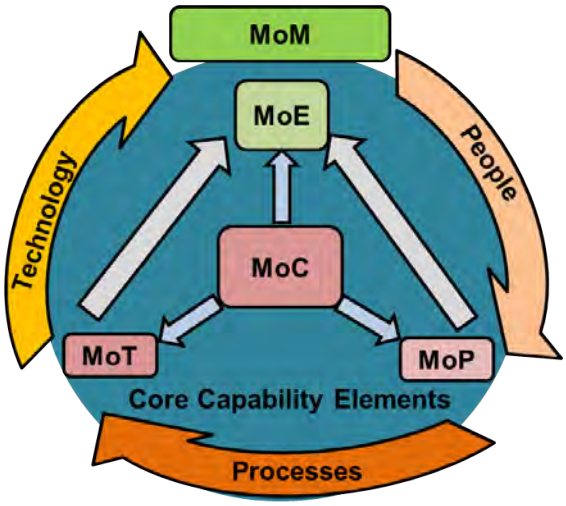


Figure 4.1: Measurement Conceptual Model for a Cyber Range

that the threats generated in the CR achieve the effect necessary for the end-state cyber event. The MoM in a CR is based on the elements of its people, its processes and its technology implementation, and allows for the CR to be measured according to each element's maturity at different levels, forming a baseline from which to incrementally improve from one level to the next.

The relationship between the two measures is best described as follows. Measurement of Capability measures the capability that the CR has for its purpose and use, including its ability to deliver a quality of service with high fidelity, simulation and emulation, using quality specification HW and/or cloud infrastructure that is reliable and cost-effective. The Measurement of Maturity measures the maturity of the CR as it evolves, reaching certain standardised incremental levels. The maturity is determined by the CR's ability to provide a service to the users where they have access to a quality system that is user-friendly, interactive and seamless. The two measurement categories when merged together provide an accurate evaluation of the current state of a CR. The concept model of the MoC and MoM for a CR is depicted in Figure 4.1.

The quality of computational technology products used in a CR, be they HW, SW or FW, is vital for a CR. This in turn needs a balance of analytical skill of a human nature, with ICT skills being critical to manage, support, maintain and execute activities and tasks as and when required. Employing all the latest technology in a CR does not equate to a mature CR due to other elements that can impact on the capability maturity thereof, namely cost, outsourcing competencies, national requirements for cyber threats, and so forth. A quality scoring metric needs to be defined to ensure that there is a fair and accurate measurement of the capability maturity of a CR.

4.6 Evaluating a Cyber Range

An increase in regulations, standards, governance, management and legislation of ICT globally has become law in many countries, hence evaluation has become essen-

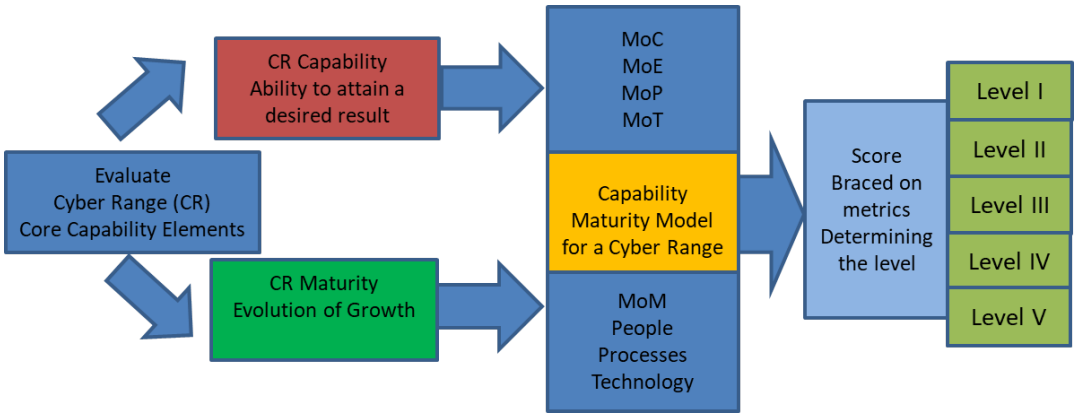


Figure 4.2: Evaluating a Cyber Range Capability Maturity

tial. This raises the applicability for a CR to be evaluated. Pridmore *et al.* (2010) states that to evaluate a CR is to meet the operational requirements the CR is intended to fulfil. In order to evaluate a CR, planning is fundamental in terms of the evaluation criteria for the CR and the implementation of measurements. The purpose of the CR evaluation is to address the following areas: Verification: has the CR met the design specifications? Validation: is the CR purpose fulfilled? Exploitation: is the CR exploitable? Mitigation: is the CR defensible and certified, and against what standards (Hwang and Bush, 2015)? Such evaluation data would ensure compliance with a certain criteria or standards, and will also determine the CR level of capability maturity to ensure that the CR purpose is fulfilled, namely providing cyber resilience training and cyber products testing to deliver accurate results.

Evaluation is viewed as the process of observing and measuring an object for the purpose of judging it and determining its value, either by comparison to similar objects, or to a standard (Surbhi, 2017). Thalheim (2010) agues that evaluation is the passing of judgement against a certain set of standards, however judgement is not in this case objective, as people judge differently. In laymans terms, evaluation is the judgement of the quantitative information over a specific period of time. Evaluation can be performed if a CR is implemented in accordance with the specific criteria, standards and metrics against which it is measured.

A suggested guideline for the evaluation of a CR is a two-pronged approach, focusing on capability and maturity. Capability is evaluated against the CR's ability to attain a desired set of result according to the core capability elements, which are measured according to the MoC with its elements MoE, MoP and MoT. Maturity is evaluated against the MoM of people, processes and technology, using the CMM for a CR. This is based on a set of metrics for each level, which are used to determine the CR level of capability maturity. Figure 4.2 depicts a generic process when evaluating a CR capability and maturity. The evaluation of a CR is out of scope of this thesis.

A CR testing strategy should be compiled to give guidelines on evaluation, especially when CR's are federated and share capabilities, with the focus on achieving a common standard for CR operation and cyber events exchange. Hwang and Bush

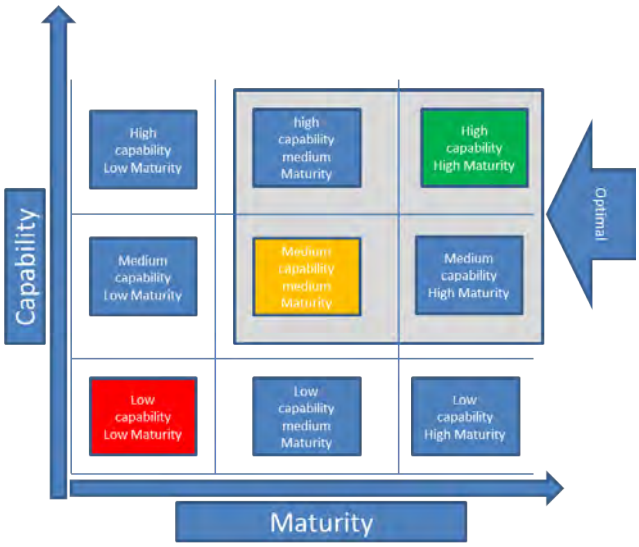


Figure 4.3: Capability Maturity Comparison Table

(2015) describes the benefit of having guidelines as allowing for the CR evaluation to have the appropriate defined set of objectives; scenarios are developed in accordance with metrics and measures to align to the end-state of the evaluation. When evaluating a CR two evaluation objectives are to be defined, of which the objectives are to be specific with reference to the characteristics and purpose of the CR (Hwang and Bush, 2015). A cyber evaluation begins with defining the components of the traditional computational stack or cloud components used by a service provider, followed by the evaluation of the cyber event itself and finalised by how effectively the outcome of the cyber event was reached.

Another consideration to take into account when starting a cyber evaluation focuses on the lessons learn" in the cyber security domain, which ensures that both failures and wins are addressed. The cyber evaluation objective can vary due to a number of factors, including the network topology being physical or virtual, cyber methodologies used by attackers to penetrate computer systems, cyber countermeasures that are activated, and the evaluation of computer systems that are not monitored. Capability maturity can be evaluated simply by low, medium and high scores depending on where the CR fits in after an evaluation has taken place, as shown in the capability maturity comparison table for evaluating a CR (Figure 4.3).

4.7 Summary

In Chapter 4 a baseline selection criteria was established for a CR to give guidance for the successful development of a CR, or for an organisation to benchmark against when procuring CR services. NICE have provided additional criteria, which are similar to the selection criteria proposed. These criteria discussed in the chapter allow for the capability maturity of a CR to be measured qualitatively. The proposed baseline criteria for CR capability maturity levels was defined, and a proposed set of CR levels

was established. Suggested standards were discussed, which mostly focused on cyber terminology and technical and security training guidelines; these were presented as guidelines for a CR, and it was noted the standards discussed are not limited.

The introduction of the Measurement of Capability and Measurement of Maturity, with the establishment of the "measurement conceptual model for a CR", creates the building blocks for measuring a CR's capability maturity according to predetermined identified CR levels. These measures will form the basis for a novel proposed CMM for a CR. A proposed process to evaluate a CR was highlighted for an organisation to use to identify gaps in a CR capability maturity and improve the CR as it evolves. In Chapter 5, the development of a synthesised MoC and MoM is discussed, which forms the baseline for the development of the proposed novel CMM for a CR.

5

Proposed Capability Maturity Model for a Cyber Range

In Chapter 4 the selection criteria for a CR were established and the criteria and classified CR levels were determined. This chapter also introduced measurements, namely MoC and the MoM with their elements, and a measurement conceptual model for a CR. In Chapter 5 a conceptual model type approach has been utilised to provide a level of abstraction for the development of a CMM for a CR. The outcome of this chapter is a proposed novel conceptual CMM for a CR, which has been developed and synthesised according to identified CMM in the literature study as discussed in Section 2.6. In Section 5.1 an overview of the CMM for a CR is introduced. This is followed by Section 5.2, which provides a high level view of the MoC elements discussed, and Section 5.3 which discusses the MoM to give a conceptual picture of the different levels for each element. This is followed by Section 5.4, which provides an initial proposed CMM for a CR. Section 5.5 presents a summary of the chapter.

5.1 Overview of a Proposed Capability Maturity Model

An overview of the CMM for a CR is introduced to give context, for understanding the proposed CMM for a CR. The CMM for a CR is formed from the following three areas, the core capability elements, the MoC and the MoM. Utilising these three areas, this forms the baseline for the CMM for a CR. The core capability elements of a CR were defined in Section 3.3, and the measurement criteria were discussed in Section 4.5, in which the MoC and MoM were introduced with their different elements. A high level view of the elements is discussed in Section 5.2 and 5.3, which does not go into the granular detail of the measurement itself.

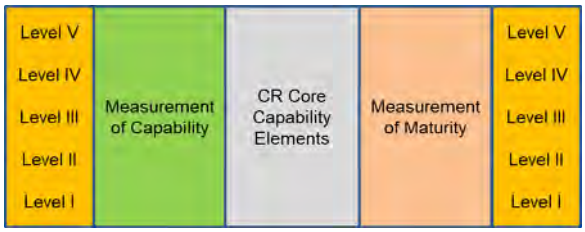


Figure 5.1: High Level Capability Maturity Model for a Cyber Range

The model indicates the levels for capability maturity, as discussed in Section 4.2. For understanding the proposed criteria levels for a CR are utilised for the measurements for a CR, namely the MoC and MoM levels, which allows for the level of a CR to be determined. The measurement of the capability maturity levels in a CR in theory are similar to the proposed criteria levels for a CR. The results of this is not perfect but gives a baseline conceptual theory against which a CR level is determined. An understanding of the defined elements is taken from certain characteristics of CMMs, as in Section 2.6, of which the elements of measurement are not in proportion to each other due to different areas of measurement. A high-level CMM for a CR is depicted in Figure 5.1 for understanding, and the following sections will define the measures in more detail and provide a proposed CMM for a CR.

5.2 Measurement of Capability for a Cyber Range

A capability is a long term commitment which is budgeted, supported and maintained throughout its life-cycle. The capability of a CR is an integrated system that requires not only computational elements, but also the human component, with processes and related technology. A CR capability is measured according to the MoC, based on its linked elements MoE, MoP and MoT, as in the conceptual model for measurement of a CR in Figure 4.1. The elements of measurement are not in proportion to each other due to different metrics of measurement. The MoC are determined based on the proposed baseline CR capability levels: Limited, Low, Medium, High and Ultimate. A matrix of MoC for CR levels is shown in Figure 5.2, which also indicates the levels of the elements. The core capability elements, as defined in Section 3.3, will form the bases for determining the capability of a CR.

5.2.1 Measurement of Effect

Effectiveness is defined as how well something does something; it is considered a top-down approach, and is mainly a qualitative measurement (Hwang and Bush, 2015). Hence, effectiveness in the context of this project can only be measured against the accomplishment of a sets of cyber events, missions or a systems-intended purpose (Sproles, 2001). By contrast, a MoE is more of a statement that is measured, due to the MoE being independent of a specific solution, namely the CR. To minimise risks through T&E a set of MoE are developed to provide a guide as to what is to be tested

to ensure systems do the job required. MoE is an essential part of systems engineering standards, and a powerful tool for judging whether a system that is developed to solve a problem performs its functional requirements. Hence an MoE is able to identify whether a CR that is developed fulfils its target purpose.

MoE is a measure that is viewed from the stakeholder perspective, which is an external view (Sproles, 2000). Developing MoE is a cognitive process, using functional requirements considered critical for the stakeholder to accept the system; if these requirements, or Critical Operational Issues (COI), are not met then the system will not be accepted (Sproles, 2001). In the context of a CR, the COIs will determine whether the CR can be accepted to fulfil its intended purpose. To test the CR as a system, the MoE needs to be given to ensure that the tests can verify if the desired effect that the stakeholder requires is met. It is important to note that this process does not work the other way around, where the test determines the effect for the stakeholder.

The data used to measure the effect of a mission accomplishment comes from the use of the system in its expected environment (Whiting School of Engineering, 2013). This data can be generated by observing how effectively a user stops an attack in a given operational cyber scenario, how a user performs under pressure in a given cyber scenario, or the responses the user executed during the cyber scenario.

Chandra and Mishra (2019) describe MoE from an attack and defensive view. The former considers the number of computers affected, data losses in terms of time and volume, target identification, number of targets engaged, number of attempts or mechanisms used to breach, targets missed, DOS induced in terms of time frame, number of routers attacked or compromised, number of antivirus defeated, number of OS breached, number of websites attacked, and the number of applications breached. The latter focuses on time delay in detection of attack, value of asset before and after attack, data losses in terms of time and volume. Donovan *et al.* (2015) view of MoE focuses on the effectiveness and performance of the Tools, Tactics, Techniques and Procedures (TTTP's) that were utilised to defend an ICT network against an adversary. Hence, the three main themes that are the main outcomes for the MoE for a CR are:

- The effectiveness of the CR as a system - the provision for a cyber event and the CR core elements to its functional requirement and ability to integrate with other core elements.
- The effectiveness of the CR to provide cyber training and content by cyber events, injects ability, tools, security attacks, monitoring ability and scoring, and ease of use.
- The effectiveness of the user in a CR - having the ability to operate under pressure, the time to complete a cyber event, and the user's ability to solve a cyber problem (this theme is focused on the human behaviour).

Other aspects that are applicable to all levels include operators cyber skills, CR ability to maintain a single or multiple cyber operational tasks, CR ability to adapt to

different cyber environment scenarios, CR ability to manage cyber activities, the effectiveness of the CR with different levels of cyber scenarios, and the effectiveness of the CR through its evolution over time. A description of the levels follow:

1. **Level I**: Very Low Level; the metrics provided by the stakeholder are haphazard and there is no clear understanding of what the CR needs to accomplish. CDX and CFT exercises and the defensive and attack effects are not achieving the desired result.

2. **Level II**: Low Level; the metrics are defined to a level of understanding of what is required for the CR to achieve its purpose.

3. **Level III**: Medium Level; the metrics are managed both technically and according to a set of predetermined goals for cyber events which identify the effect that needs to be achieved.

4. **Level IV**: High Level; the metrics provided by the stakeholder are clear and the functional requirements are understood.

5. **Level V**: Very High Level; the metrics are optimised for quality to ensure that the CR fulfils its purpose.

5.2.2 Measurement of Performance

Measurement of Performance (MoP) is viewed from a developer's perspective, and is thus an internal view Sproles (2000). The MoP is also a subset of MoE in that it supplies data to help evaluate the MoE. Together MoE and MoP determine the operations for the CR as a system (Whiting School of Engineering, 2013). Performance is considered a bottom-up approach, and is mainly a quantitative measurement (Hwang and Bush, 2015), hence the measurement of the performance and efficiency of component elements. Donovan *et al.* (2015) summarises the MoP very simply as the computing power and performance (memory, processor speed, storage speed). The MoP view focuses on how well the system does what it must do relative to the system's effectiveness, efficiency, accuracy and precision, all of which defines and measures the characteristics of the CR system capability.

Other aspects that are applicable to all levels include speed and throughput, fidelity high or low, switching ability between cyber events, quick configuration, traffic generation, storage and retrieval, security assessment, instrumentation connectivity, up-time, quality of links, geographical size, IP count (IPV4 or IPV6), latency, complexity, packet flow, hosts, services, availability, bandwidth, scalability, compression ratios, channel capability, manual or automated, and measuring how well the CR accomplishes a task that it must execute. A description of the levels follow:

1. **Level I**: Very Low Level; CR as a system does not perform effectively, multiple errors are encountered.

2. **Level II**: Low Level; CR system is slow to provision the cyber event.

3. **Level III**: Medium Level; CR system is performing at an acceptable manner according to the system specifications.
4. **Level IV**: High Level; CR system operates according and has no down time.
5. **Level V**: Very High Level; CR system operates at a high level of optimal performance,according to the system specifications.

5.2.3 Measurement of Threat

Models for measuring cyber threat levels have been published in a variety of literature. For the measurement of threat in this thesis, the threat tiers as in Section 2.2 and Table 2.1. are utilised as a baseline to allow for an incremental view on what cyber threats a CR is able to maintain. The MoT will measure the ability of the CR to generate cyber threats for cyber events, security threat tools, and the ability to maintain threats internally within the CR. A description of the levels follow:

1. **Level I**: Simple Level; CR has the ability to maintain simple code that has been developed and can deliver know exploits.
2. **Level II**: Defined Level; CR can maintain and develop code and tools from known vulnerabilities.
3. **Level III**: Developed Level; Ability to maintain unknown and undiscovered malicious code.
4. **Level IV**: Advanced Level; Ability to maintain highly sophisticated cyber threats developed by teams to discover vulnerabilities and develop exploits and threats with the ability to design, develop or manufacture products to enable the exploitation of networks and systems of interest.
5. **Level V**: Highly Advanced Level; CR ability to execute the full spectrum of cyber threat capabilities in combination with military and intelligence to achieve a specific outcome

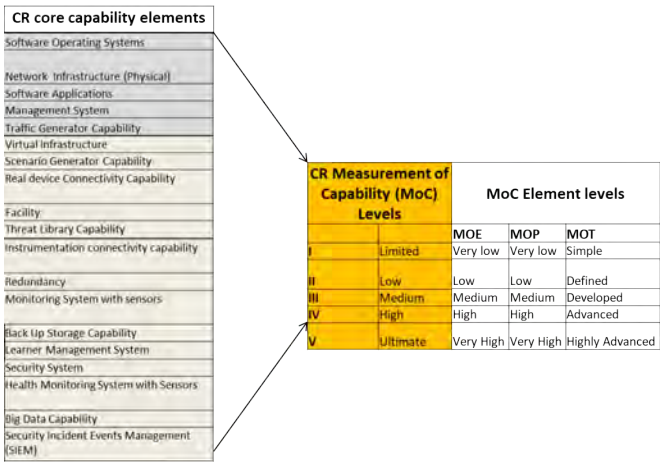


Figure 5.2: Matrix of MoC for Cyber Range levels

Understanding the measurement of capability with its elements is based on a theoretical view as given in this example: *MoE = Low, MoP = High, MoT = Highly Advanced*. This then will give a level of *Capability = Low* due to the effectiveness of a CR. Hence the level of capability will consider the level of effect as the level of capability, due to the MoP and MoT that feed into the MoE for a CR as per the measurement concept model as discussed in Section 4.5.3. However the determined level according to the elements gives a baseline for improvement of the capability to be implemented in a CR.

5.3 Measurement of Maturity of a Cyber Range

When increasing a CR capability through its maturity there are three main areas that are integrated and focused on: the people, the processes and the technology (Valdez *et al.*, 2008). A maturity level is not recommended to be skipped as it is a building block to attain the next level - this is a ground rule that must be applied, as it will ensure that there is less risk in the long term Wiegers (1996), and is a key factor in establishing the maturity level for a CR through its evolutionary process. CRs are complex systems and a holistic approach to improve on maturity is needed in a CR due to the rapid changes in the cyber realm. A matrix of MoM for CR levels is shown in Figure 5.3 illustrating the different MoM elements levels. Growth in maturity can be attributed to multiple areas within the CR, especially in the building of skills capacity in people, the processes for development and training, and the adoption of technologies. Different maturity models give a structured approached to incremental improvement in an organisation and, in this context, a CR (Chapman *et al.*, 2018).

When determining the maturity of a CR the three elements (people, processes and technology) are viewed from a high level. The elements of measurement are not in proportion to each other due to different metrics of measurement. Almuhammadi and Alsaleh (2017) describe maturity models as qualitatively measured and divided into five levels. The proposed baseline for CR maturity levels are: Basic, Intermediate, Fully Functional, Advanced and Highly Advanced. The core capability elements - the MoM elements and sub categories, as defined in Section 3.3 - will form the bases for determining the maturity of a CR.

5.3.1 Cyber Range People Maturity

The maturity of people focuses on four process trend areas, namely developing individual capability, building work groups and culture, motivating by rewarding and managing performance and shaping the workforce (Valdez *et al.*, 2008, pg 39). Cyber skills, as in Section 2.4.4, are a huge concern globally due to the shortage thereof. The maturity in developing individuals cyber skills and capacity of a CR workforce are synthesised according to the People CMM in Section 2.6.5. Some of the focus areas that are to be considered for a CR, both when training participants and resources in a CR, include determining the level of cyber skills, cognitive abilities, handling of

cyber-related challenges and cyber endurance. Managing and developing the workforce of a CR and their cyber skill levels allows them to form a firm basis from which to mature over time in developing cyber skills according to the threat tiers discussed in Table 2.1, and enhances their ability to operate and utilise the core capability elements. A synthesised adoption of these People CMM levels (Curtis *et al.*, 2009) are utilised to define CR people maturity levels, which are:

1. **Level I**: Initial level; there is inconsistent management, and managers need to take responsibility to develop people's cyber skills to build capacity and to retain the desired skills, talent and repeatable practices within a CR. In level I cyber skills are not retained and there is a skills shortage within a CR. In this level, skills are not certified, training is more up to the individual, and skills performance is not quality driven.

2. **Level II**: Managed level focuses on the managing of CR Resources and stabilising the CR work environment by implementing basic practices and addressing relationship building as a work group. The Process Areas (PAs) that are addressed in this level include:

   (a) Staffing, the formal process to select the correct CR resource needed to operate and maintain the CR.

   (b) Communication and coordination, to establish and maintain a physical CR working environment for CR resources to perform their tasks efficiently and share information to coordinate activities in a process manner.

   (c) Performance management measures are set for CR resources to perform to a set standard and to continuously enhance performance.

   (d) Training and development of all CR resources to have the required cyber skills to perform tasks.

   (e) Compensation for CR resources based on remuneration and benefits of skills obtained or attained, this is linked back to the discussion on incentive balance in Section 2.3.

3. **Level III**: Defined level focuses on competencies in CR. Resources are managed and measured according to a framework and the overall strategic intent of the CR in an organisation. The CR workforce develops accordingly and improves on their competencies. The PAs that are addressed include the following:

   (a) Competency analysis, which identifies competencies needed in the CR.

   (b) Workforce planning, which coordinates activities to reach the CR's end state, hence a plan for CR skilling on the core capability elements and other cyber competency areas. This is to enhance the competency development of the CR resources for career development, which helps to develop the CR workforce competencies to build on or towards a new career in the ICT environment.

(c) CR work group development to enhance specific competencies within a CR, specific to cyber events or newer core capability elements.

(d) Developing a participatory culture, which allows CR resources to share CR information and knowledge to be incorporated in the decision-making processes in a CR.

4. **Level IV**: Predictable level focuses on CR resources and improves on their capability and capacity, which are managed qualitatively. This is achieved by performing data collection that allows for predictions to be made to better augment competencies and performance in a CR for the future. The PA that are addressed include the following:

   (a) Competency integration, which encourages CR resources to be multi-skilled. By implementing this it empowers the CR work groups to use initiative to enhance the CR abilities and application.

   (b) Quantitative performance management is utilised to predict and measure the performance of CR resources. This is also related to the capability management of a CR to manage the capability of the CR workforce by providing mentoring, transferring experience and knowledge to people in the organisation.

5. **Level V**: Optimizing level focuses on change management and the continuous optimising of CR resource capability and competence to strive for excellence. The PA that are addressed include the following:

   (a) Continuous capability improvement of CR resources capability to perform optimally, by continuous aligning performance abilities.

   (b) Continuous CR workforce innovations to identify positive cyber competencies and methods to implement throughout the CR community.

Synthesising the People CMM gives a clear indication of the levels of maturity needed with regard to CR resource's cyber skills competencies. In a CR it is important to have the necessary cyber skills to understand and utilise the core capability elements of a CR, as well as the skills to train users and test and evaluate computational devices or a SUT. One of the drawbacks of people generally is the time and effort needed for adopting the processes and learning the technology, especially the core capability elements of a CR - this is also a key factor in ensuring that the necessary adoption of processes and technology is managed, and people are exposed and trained accordingly. CR resources with the wrong cyber skills competency will often misunderstand, misinterpret and miscommunicate the cyber event or utilisation of the CR core capability elements, which can cause a definite complication for the desired outcome (Haron *et al.*, 2013).

5.3.2 Cyber Range Processes Maturity

Buttles-Valdez *et al.* (2008, pg 9) describes processes as "addressing the business needs, the workforce and competencies required to meet them". From a CR view, processes allow for a CR to improve and increase its effectiveness and performance over time to ensure a quality CR outcome (cyber event). The CR PAs are adopted and synthesised from the Capability Maturity Model Integration (CMMI-DEV) model. A process maturity model for the development of a CR has been synthesised and developed, and is presented in Appendix D. However the process maturity is more focused on the development of a CR and the processes needed to develop a CR, thus allowing for a more mature CR as a system focused on the core capability elements for a CR. However CR training and testing of SUT processes is important and can be implemented in the process management and support process PA.

CMMI Team (2010) discusses the categories which are key in developing mature processes for CR development, namely Process Management, which covers the whole range of building processes in improving CR processes; Project Management, which covers the CR project management activities; Engineering, which covers the CR development and maintenance; and Support Process, which covers the CR activities that support a CR. A description of the levels follows:

1. **Level I**: Initial start-up focuses on the CR development process: CR development on this level is where processes are omitted, not documented, a CR is built and working, but is over-budgeted for and success cannot be replicated, therefore the CR is not maintained. CR processes are not structured and the processes need to start. At this level, the following PA can be initiated:

   (a) Analysis of CR Processes - A process in understanding the needs, requirements, specifications and operation of a CR as a capability is initiated.

   (b) Deciding on what processes - A thought process to determine what processes to implement for developing the CR and application thereof utilising the core capability elements and processes for the implementation of cyber events.

   (c) Initializing processes - Getting the necessary processes in place to develop a CR through its developmental maturity process.

2. **Level II**: Managed focuses on CR processes that are implemented as a project in which the processes are more reactive in nature (able to act whenever something happens). The CR is more controlled by the project in its development of the core capability elements. Products and processes are the focus of Level II, ensuring that CR processes are maintained and executed as documented to achieve the outcome of the specified CR. The following PA forms the focus of Level II maturity of a CR:

   (a) Project Management Process: This typically begins with the project plan, which highlights what to build and identifies the, size, type, and capability

required for a CR, including what components and products are needed for the development of a CR, what to do, and measurements and standard for compliance. CR Project Monitoring and Control is a process of controls that are put in place to monitor the progress of the project plan, for example the frequency of reporting and ensuring the plan is implemented correctly. CR Requirements include management processes for tractability to ensure that changes to requirements are implemented in project plans, activities, and work products. Changes in the requirements will have an impact on the complete process in the development of a CR. CR Supplier Agreement Management is a process to ensure the suppliers deliver a specific work product, with the specified quality and timeline.

(b) Support Process: CR Configuration Management is a repository in which all related work products are recorded with reference to the development of the CR and are captured for tractability and future revision or use. These can include, for example, requirements, specifications, designs, codes and so forth, applicable for all process areas. CR Measurement and Analysis provides the measurement guides and analyses of the CR processes for improving the performance of process in the CR , applicable for all process areas. CR Process and Product Quality Assurance covers the evaluation and quality of CR processes and CR work products, delivered or provided, which is to compile the ISO/TS 9000 standard family on quality assurance which is applicable for all process areas.

3. **Level III**: Defined focuses on the CR, has standardized its processes and controls, and is more proactive in its implementation. The CR's standards, procedures, tools and methods are understood and well-defined to ensure consistency in the CR development. The organisation-specific set of standard processes are linked for standardization; this is important due to the dynamics of different nations and organisations globally. The CR processes clearly state its purpose, inputs, entry criteria, activities, roles, measures, verification steps, outputs, and exit criteria. The following PA are focused on for level III maturity of a CR:

   (a) Process Management Process: CR Process Definition - To define, establish, and maintain the CR set of standard processes and work environment standards that benefit the complete processes of the CR, for example, the life cycle process for the CR. CR Process Focus assists to focus on the current strong and weak points of CR processes to help plan, implement, and deploy improved processes. The CR Training process identifies common strategic and tactical training needs for a CR. The training process is developed or obtained to develop the skills required to perform the CR set of standard processes.

   (b) Project Management Process: CR Integrated Project Management (at the advanced level) - Integration of all project processes with other relevant

parties who are involved with the CR according to the CR Standard set of processes. CR Risk Management Process to manage risks in the CR, identifying risk parameters, risk assessments, and risk mitigation.

(c) Support Process: CR Decision Analysis and Resolution: This is a formal evaluation process used in the Technical Solution process area to select a technical solution for the CR.

(d) Engineering Process, which is linked to Capability Development Process for a CR, as discussed in Section 3.6: CR requirement development identifies CR needs and converts them to requirements for CR products, whether it be to procure or develop a set of requirements. These are processed to ensure the requirement is properly implemented. CR Technical Solution is the process in which the components that are envisaged for the CR are selected per a criteria in which they are examined, these are specifications with reference to performance, the type of product procured or developed, its operational effectiveness and cost projected for its life-cycle. The selection of the products is done through the Decision Analysis and Resolution PA. The CR Product Integration process ensures that the requirements are met with the integration of the technical solution products. CR Verification verifies the products or developed products of a CR against a specific set of requirements in which this is an incremental process from initial component to fully integrated CR. CR Validation is focused on whether the CR meets the needs to which it is to perform operationally. The coordination with the operational environment of a CR is vital in the validation of the CR.

4. **Level IV**: Quantitatively Managed focuses on the CR processes that are measured for performance and quality; the outcome is used as a criteria in managing the CR maturity further. Quality and process performance is well-defined to reach a certain quality quantitative process, using statistical and other quantitative techniques in analysing the results of the processes to better them accordingly. The following PA are focused on for level IV maturity of a CR:

   (a) Process Management using the CR Process Performance process, which uses quantitative techniques to analyse the quality of the performance of the processes used throughout the development of a CR.

   (b) Project Management by implementing the CR Quantitative project management, the process used is to take the basic performance baselines and models of the CR to understand if it meets the requirements from a project view point and then proactively select and deploy incremental and innovative improvements that measurably improve the CR's performance.

5. **Levels V**: Optimising focuses on the continuous CR improvement and process performance through incremental and innovative process and technological improvements. This is important, especially in the evolution of cyber threats and

technology improvements with reference to cyber defence. The following PA is focused on for level V maturity of a CR

(a) Process Management by implementing CR Performance Management which focuses on improving a specific area in which CR processes are augmented to ensure a level of excellence is achieved.

(b) Support process using the causal analysis and resolution process which focuses on changes that add value to the processes of the CR are to be implemented.

Utilising the synthesised CMMI-DEV model for the processes for the development of a CR focusing on the core capability elements will give a clear indication of what level of process maturity a CR has attained. When viewing the processes on the specific level, the interpretation of the process areas can accommodate other processes that are needed in a CR itself. The processes of operating and provisioning cyber events and the configuration thereof are inclusive and accommodated in the process management PA and the support PA. The support processes for a CR will ensure that processes are augmented and change with the growing trends in the cyber environment. The loop-back approach for processes are good practice at any level, as this allows for improvement to be continuous, as described in level V (Optimizing).

5.3.3 Cyber Range Technology Maturity

Technology maturity is influenced by a variety of different elements, including certain hub cycles that exist in industry, the life-cycle of technology which has a specific life span, or a midlife upgrade or newer technology that is developed (whether smaller, faster, smarter or more intelligent). Time is relative within the technology world in that multiple technologies can rapidly evolve within a predetermined hub cycle, but are not mature technologies at a specific time. Gartner (2018) notes that the technology hype-cycle includes five steps for the maturity of technology, namely an initial trigger for technology, a hype of expectation of the technology, then a technology dip, an understanding of the technology is then formed, and then an acceptance and utilisation of the technology globally. MITRE (2018) describes the maturity of technology as follows: new technology improves as the technology develops, the technology then matures and then reaches a performance limit. In reaching this limit the technology starts to age. (Hurley, 2018) suggest the maturity of technology is also often misunderstood because the technology not been actually mature. This is due to technology evolving over time and in many cases developed according to a standard that changes over time. However Kaminski (2011)states that mature technology will give a better accuracy. The most universally-accepted methodology for technology maturity is the Technology Readiness Level (TRL) scale (Mai, 2012). TRL measures the maturity of evolving technologies before they are incorporated in a system. There are 9 stages in the TRL, where the lowest level of maturity is TRL 1 and the highest TRL 9 (Mitchell, 2007). The TRL 1 to 9 is listed in Table 5.1.

Table 5.1: Technology Readiness Levels (Mitchell, 2007)

TRL Stages	Technology Readiness Levels
1	Basic principles observed and reported
2	Concept and application formulated
3	Concepts demonstrated analytically or experimentally
4	Key elements demonstrated in laboratory environment
5	Key elements demonstrated in relevant environments
6	Representative of the deliverable demonstrated in relevant environments
7	Final development version of the deliverable demonstrated in operational environment
8	Actual deliverable qualified through test and demonstration
9	Operational use of deliverable

The Roger's Bell Curve is based on the adoption of technology in which he explains the ratio between innovators 2.5% early adopters 13.5%, early majority 34%, late majority 34%, and laggards 16%. These percentages give a clear view on where most of the adoption takes place, however in a CR the technology needs to be viewed as cutting edge technology due to the dynamic at which technology changes in the cyber environment. Accurate technology is also vital to ensure validity of the CR output.

Gove and Uzdzinski (2013) describe the lack of systems maturity that is implemented. By implementing technology in a CR, there is a clear engineering process that must happen in order to ensure that the technology functions within the CR system. The upgrades that do occur during a technology life cycle can have a massive impact on the CR, as there can be core capability elements that are not comparable in the configuration and the weighing up of performance verses quality will come into play. Upgrading or implementing different technologies at different stages of their life cycle is a key gap that will need to be managed accordingly in a CR.

To reach a certain technology maturity level in a CR five levels are identified, of which the TRL scale are synthesised and adopted with other sub-categories to give a clear indication of what level of maturity the CR's technology is. Only the first three levels are adapted to the TRL, due to level 9 TRL being the operational use of the technology as it has evolved. The mature technology has evolved to its level of performance, and the optimisation of technology augments the current technology used in the TRL stage. These sub-categories include the ability and upgrade of the technology used in a CR through life-cycle management, the technology drivers and maturity thereof, managing the technology as a capability in a CR, and the maturity of computational devices and SW, focused on the core capability elements of a CR. A description of the levels follows:

1. **Level I**: Initial, which is new technology based on a proof of concept, is not

mature or is not supported. TLR stage 1 to 3 is applied in the initial level of a CR in that the basic principles of the technology are observed and reported on and the concept and application is formulated with the concepts demonstrated analytically or experimentally.

2. **Level II**: Developed technology, where the technology is still in a development phase and is being tested against standards. TLR stage 4 to 7 is applied in which the key elements are demonstrated in a laboratory and relevant laboratory environment, which is then deliverable and demonstrated in the relevant environments with the final development version of the deliverable demonstrated in an operational environment.

3. **Level III**: Improving technology allows for the technology to be modified to allow for improvement. TLR stage 8 and 9 is applied in that the actual deliverable of technology has qualified through tests and demonstration and is now ready for operational use.

4. **Level IV**: Defined technology reaches a performance limit and all known faults and errors are solved and it is accepted in the broader CR community.

5. **Level V**: Optimised technology allows for the technology to be customised and integrated to augment its current mature performance to suit a specific functionality or purpose within a CR.

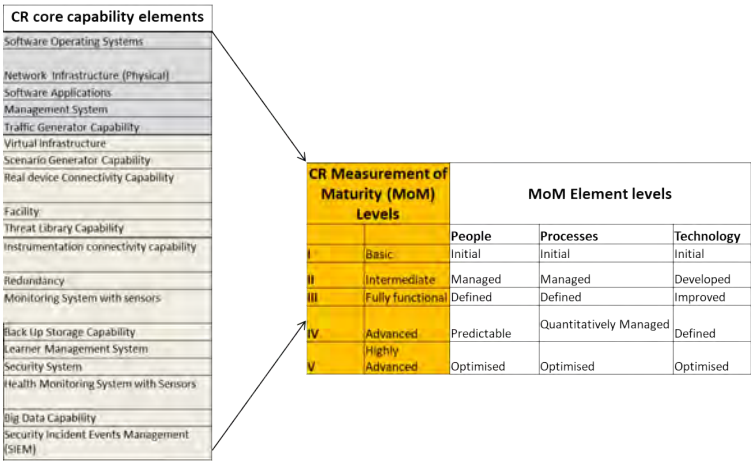


Figure 5.3: Matrix of MoM for Cyber Range levels

Understanding the measurement of maturity with its elements is based on a theoretical view as given in this maturity example; *People* = *Managed, Processes* = *Defined, Technology* = *Defined*, this then will give a level of *Maturity* = *Intermediate* based on the people maturity. Hence the level of maturity will consider the level of processes and technology. However, people need to understand and operate the CR with the necessary skills. Furthermore, the determined level according to the elements gives a baseline for improvement of maturity to be implemented in a CR.

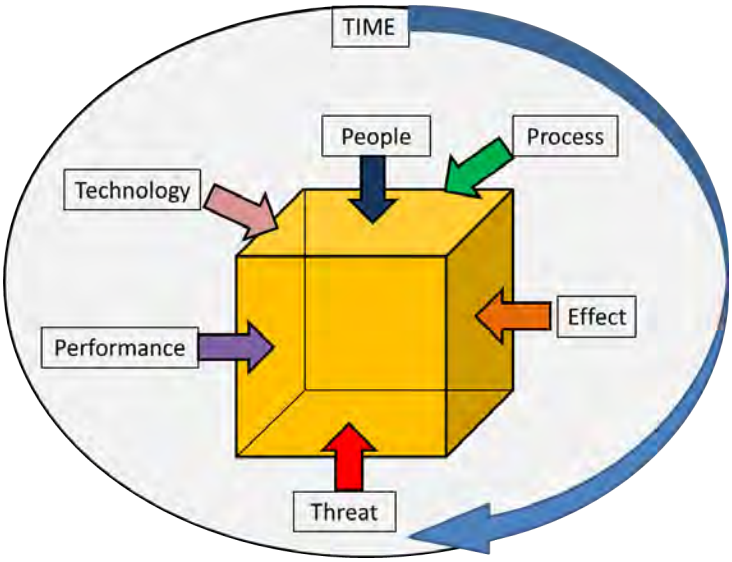


Figure 5.4: Cyber Range Measurement Cube

5.4 Proposed Capability Maturity Model for a Cyber Range

In developing the proposed CMM for a CR, a conceptual model type was utilised which provides a level of abstraction, as discussed in Section 2.6. The CMM for a CR is based on the modelling properties, namely the purpose of the model provides a graphical representation to determine a CR level of capability maturity where the elements are based on the MoC and MoM. The development is based on an understanding of the core capability elements and the CMM that currently exist in the literature. Due to the novel nature of the development of the CMM for a CR, a CR measuring cube is introduced and forms the basis for measuring capability maturity of a CR. The proposed model utilises the measuring cube and the core capability elements to determine different levels of capability maturity. From defining a CR in understanding its core capability elements, to establishing a suggested selection criteria and determining levels for MoC and MoM, the integration of this understanding has aided the formulation of a proposed CMM for a CR. The modelling construct of the CMM for a CR tries to create a baseline to determine the level of a CR capability maturity.

In Figure 5.4 a CR measurement cube is represented. This cube represents the high-level elements that are to be measured in the complex environment of a CR. The cube approach, consisting of six sides, is used to illustrate the complexity of measuring a CR capability maturity. Using this cube as a concept forms part of the implementation in the CMM of a CR. The cube includes six elements in two different categories: MoC and MoM. For MoC these elements include effect, performance, and threat, and for MoM these are people, processes and technology, with the common factor for all elements being time as the CR evolves. The cube is used to measure these core capability elements to determine the level of capability maturity in a CR, providing a benchmark to evaluate and to improve on the gaps identified in the CR.

The significance of the cube is linked to the MoC and MoM, with their core capability elements used to determine the CR level. The proposed CMM for a CR indicated in Figure 5.5 is the first iteration. Representing the capability maturity of a CR is complex and difficult, however Figure 5.5 gives a proposed interpretation to determine CR levels (note that the x's are used to provide an example model).

The CMM for a CR provides a simple three-dimensional view. First, the CR capability level using the MoC score is allocated to the core capability elements of a CR. This is to indicate its capability on a scale of limited to ultimate level. Secondly, the maturity level using the MoM score is allocated to the core capability elements on their level of maturity, from basic to highly advanced. Finally time capability is assessed - this is the amount of time the CR takes to reach a certain capability maturity level.

For more clarity, a slice of the proposed CMM for a CR is explained to give a clearer understanding. Note that this is the same generic explanation for all CR core capability elements as in Figure 5.6. The slice describes the core capability element, a traffic generator, where the CR capability levels indicate what level a traffic generator has according to the MoC elements. This includes the effectiveness of the traffic generator at accomplishing its function, its performance thereof and its ability to generate traffic and security threats in the CR. Its maturity, according to the MoM and its elements, includes people's skills capacity and workforce maturity, and overall ability to configure, develop and utilise the traffic generator. The processes that are implemented to operate and maintain the traffic generator, and the level of technology currently in operation in the traffic generator at a specific time in its lifecycle. This approach in scoring a traffic generator determines its level of capability maturity within a CR. This approach is then completed for all the CR core capability elements, enabling a specific score for each. The scores are then consolidated to determine an overall score of the CR capability maturity.

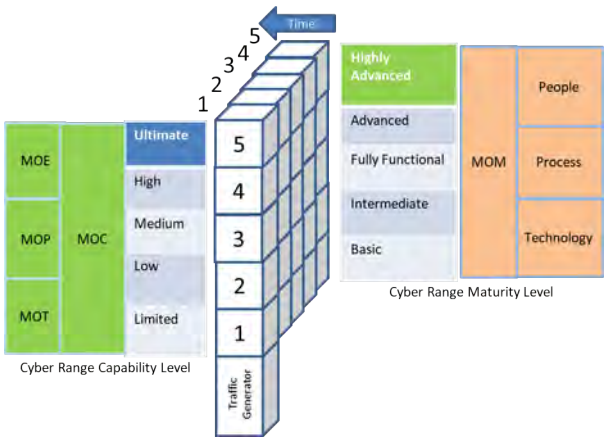


Figure 5.6: Slice of the Capability Maturity Model for a CR

The difficulty of representing the capability maturity of a CR is complex, in that a mixed measuring method both qualitative and quantitative would be best suited, which in itself is difficult to achieve as discussed in Section 4.5. The CMM for a

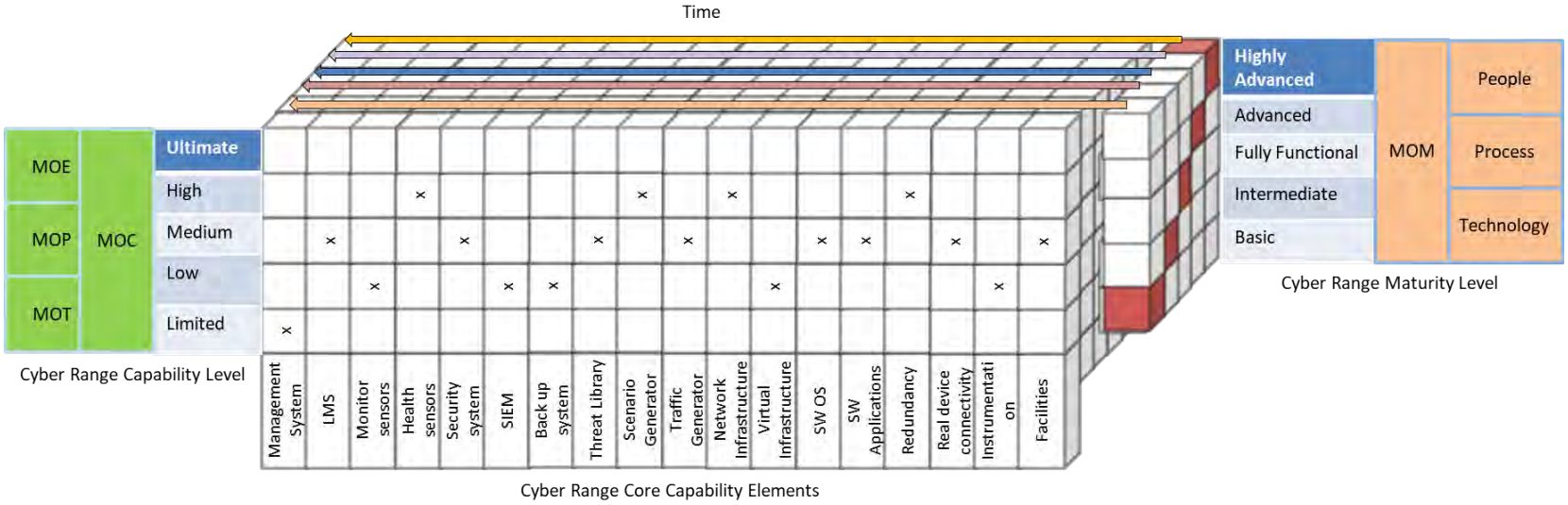


Figure 5.5: Proposed Capability Maturity Model for a Cyber Range (First Iteration)

CR gives a proposed interpretation of capability maturity to determine CR levels. A outcome of a CR score for example, which indicates a low capability and an advanced maturity, would therefore indicate a Level II capability and Level IV maturity. This score allows for gaps to be identified in a CR to be improved upon according to an identified level of capability maturity. An integrated matrix view of the utilisation of the CR measuring cube in the CMM for a CR is linked to the core capability elements, as in Figure 5.7.

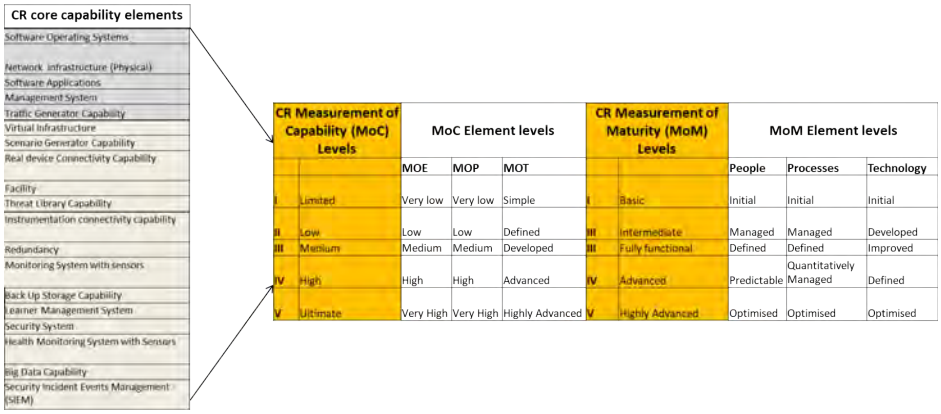


Figure 5.7: Matrix of MoM and MoM for Cyber Range levels

5.5 Summary

Chapter 5 established a baseline for the development of a synthesised Measurement of Capability and Measurement of Maturity for a CR, which formed the baseline for the development of a proposed novel CMM for a CR. The Measurement of Capability and its elements of effect, performance and threat were defined. The MoC covered the measures of effect, which focused on the management of metrics for a CR according to the three main themes: the effect of the system, the training, and the human behaviour. Performance was focused on measures of functionality for the core capability elements of a CR against levels of performance. Threat was focused on the different threat tier levels a CR is able to maintain and generate. This established a clear distinction for measuring the CR capability utilising a combination of these elements.

The Measurement of Maturity with it elements - people, processes and technology - was defined and synthesised utilising capability maturity models in literature. The MoM focused on the following measures: People, which focused on developing CR resource's cyber skills competencies to understand and utilise the core capability elements of a CR capability, and the management and development the workforce of a CR. Processes, which focused on the processes to develop a CR from the categories of Process, Project, Engineering and Support areas in a CR to support the development of the core capability elements of a CR. Finally, technology, which focused on the technology levels for a CR, using the Technology Readiness levels, the life cycle management, and technology drivers.

Using the measures of capability maturity elements with their levels against the CMM for a CR enables a qualitative measure of a CR capability maturity. The metrics for the different measures of capability maturity were not defined for this thesis. The establishment of a proposed novel CMM for a CR was developed using the core capability elements as a baseline to measure against predetermined CR levels of capability maturity. The CMM for a CR is the first iteration to enable discussion and allow for inputs to be given from CR experts utilising a questionnaire. Chapter 6 addresses the analysis and results of the CR questionnaire that was sent out to CR experts and provides a discussion of the key areas of agreement and disagreement that were captured.

6
Results and Discussion

In the previous chapter, the development of a novel, proposed CMM for a CR was presented to demonstrate the complexities in determining capability maturity levels. In Chapter 6 the discussion is focused on the results captured from expert responses to the distributed CR questionnaire. The results captured give a clear view from the experts on CR capability maturity. While most of the experts do agree with what is proposed for a CR CMM, there are differences, and these are discussed and consolidated in this chapter to come to a conclusive understanding of a CMM for a CR.

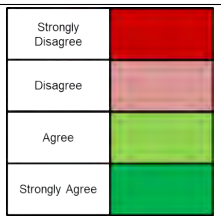
This chapter will present and describe the results in a systematic and detailed method. The results that are reported are qualitative, in that the author has highlighted and commented on the key agreements and disagreements that emerge from the analysis. These comments are illustrated with extracts from the data received. Section 6.1 discusses how the analysis was completed based on the CR capability maturity questionnaire. Section 6.2 addresses the core capability elements, Section 6.3 the relevance ratings for a CR, and Section 6.4 the proposed capability levels. Section 6.5 outlines the proposed CR classified capability levels, Section 6.6 the proposed maturity levels with the findings of people, processes and technology, and Section 6.7 describes the CMM methodology for a CR. Section 6.8 provides a summary of the chapter, highlighting the results of the broad themes across the previous sections.

6.1 Analysis of Expert Review

The ethics committee of Rhodes University approved the context document and the CR capability maturity questionnaire, this is included in both paper form and electronic form (see Appendix F). The ethics trace-key number provided by Rhodes University Ethics Board for these documents is CIS18-09, approved on 16 November

Table 6.1: Range of Numerical Values and Likert Score Legend

Strongly Disagree	Disagree	Agree	Strongly Agree
1	2	3	4



2018. Participant data with regard to the questionnaire includes the following: thirty initial requests to take part in the questionnaire were sent to identified CR experts, resulting in seventeen replies. Seventeen questionnaires were then sent out, with fourteen questionnaires received back. Participants included five international experts and nine South African experts, of which five are from the same organisation that have successfully implemented a CR. Job roles that were reported by the fourteen experts was a reasonable comprehensive spectrum, including a Security Advisor, CR Scenario developer, Computer Science lecturer, Security Penetration (Pen) Tester, CR SW Developer, CR Operator, CR Evaluator, CR Computer Systems Engineer, CR Analyst, Malware Analyst, an Executive Director, a Cyber Security Manager, a Cyber Security Threat Analyst and previous and current Research Scientist. Although the current study was based on a small group of participants the feedback was completed in detail. The questionnaire was mainly a Likert scale approach with comments captured from expert participants. The analysis was conducted using a data coding score method, with the range of numerical values indicated in Table 6. 1. The range of numerical values was then calculated according to the values indicated on the Likert scale, dividing the result by the number of experts to determine the outcome of the themes for this research thesis. The results of the analysis were rounded off to a higher Likert score when the result was 0.5 and higher. All responses were viewed as relatively equal, and no additional weights were added. The following analysis presents a synthesis of the views of these experts, which is further reflected in the project undertaken in this thesis. Going forward, the focus is on the key agreement and disagreement areas that were captured from the questionnaire. From initial analysis, seven broad themes emerged:

- Defining a Cyber Range: Definitions as generated from experts in their own opinion are analysed to determine key words used.
- Core capability elements: Determines which core capabilities are agreed on.
- Relevance ratings: The relevance of the core capability elements to determining the main elements for a CR.
- Proposed capability levels: The view of the experts on the proposed capability levels.

- Proposed classified CR capability levels: To determine a consensus for a baseline to classify a CR on different levels.
- Proposed maturity levels: The view of the experts on the proposed maturity levels.
- CMM methodology for a CR: To determine which CMMs to use to synthesize a CMM for a CR.

6.2 Defining a Cyber Range

The definitions provided below were reported by CR experts in the field as per the questionnaire. The definition, from the relevant literature, for a CR was provided in Section 2. 4. A word cloud, generated from the definitions provided by CR experts, is presented in Figure 6.1; this visualisation highlights the dominant words used, with cyber, environment, training, range, security, network, test, evaluation, scenarios and simulation representing the top word usage across all the definitions provided, as listed below:

- “A CR is a simulated or real segregated environment that allows personnel to learn, exploit and defend assets connected to networks or the Internet”.
- “The CR is defined as a scalable, flexible and configurable modelling and simulation environment allowing realistic and customisable scenarios to be created and deployed in a cost-effective, timely and repeatable manner within a secure and isolated environment”.
- “A CR is a training and education program. It is the sum of the educational content and the delivery platform”.
- “A simulated cyber environment that provide the ability to test people, processes and technology with regards to information technology”.
- “Safe environment to simulate cyber threats, "build" counter measures as well as testing new remediation methods”.
- “Visualized test bed environment containing data collection sensors with the objective to validate performance metrics pertaining to people, processes and technologies”.
- “A sandbox environment or test bed composed of physical or virtual infrastructure, providing high fidelity simulation and emulation of network, hardware and software ecosystems to support cyber training, cyber exercises, modelling, testing, and evaluation related to network and security operations or events, with minimal interference with existing organisational, national, private or public infrastructure, and providing high fault tolerance or recovery and extensive event logging to support experimentation, evaluation, training, and other network and security related research, development and testing”.

- “Training facility (sandbox) for gaining cyber security experience, conducting training and running simulations”.
- “A virtual environment capable of simulations, a cyber warfare training zone”.
- “It is a capability that provides functionality to enable training for, simulation and execution of cyber operations”.
- “A CR is a sandboxed environment in which cyber security professionals can: monitor the behaviour of malicious software; train personnel in defensive and offensive cyber security; and test network protocol implementations in “real-world” scenarios.
- “A configurable environment wherein a cyber operator could test and perform certain tasks or scenarios for training or evaluation purposes”.
- “CR is a both a physical and virtual environment that closely resembles a realistic operational environment, but is meticulously monitored and controlled to facilitate the training of cyber capabilities to ultimately strengthen cyber security defences and skills”.
- “A CR is a simulated environment used for the emulation or simulation of real life activities on a network. It can be used to test new products and network topographies, but is essential for practical training for a cybersecurity workforce”.

Based on the definition given initially in this thesis, along with the definitions in relevant literature as in Section 2.4, the dominant words are cyber, environment, capabilities, development, research, experimentation, hands on training, security and simulated (see Figure 6.1). Common vocabulary for defining a CR across experts' definitions, definitions found in the literature review, and for this thesis include cyber, environment, training, security, network, testing, simulated, and capabilities. From this comparison, a CR can be holistically defined as a simulated cyber environment for security training and network testing as a capability.

6.3 Core Capability Elements for a Cyber Range

The core capability elements for a CR are agreed upon by experts, and these results are presented in Figure 6.1. The general view of the experts was captured by asking participants to rate the core capability elements as follows: “strongly agree” for essential components; “agree” for components that are desired but not essential, “disagree” for components which are optional, and “strongly disagree” for those not needed. However, it is important to remember that CRs are only as useful as the content that they provide - their specific purpose and capabilities - from this the CR core capabilities are determined . This makes sense with respect to only utilising the core component necessary for the purpose of a given CR.

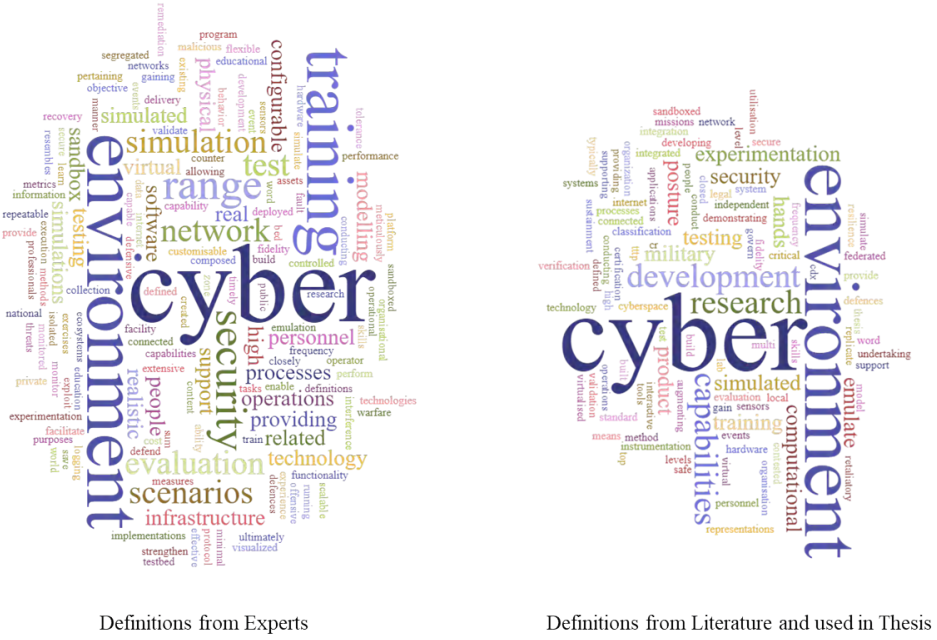


Figure 6.1: Cyber Range Definitions Word Cloud

The two main areas of disagreement with regard to core capability elements were Redundancy and Big Data. Big Data is generally regarded as merely a storage and processing methodology, and forms part of a backup storage capability as required. Redundancy for a CR is not regarded as an operational environment, and more as a training and virtual environment that can be provisioned on demand and not needed if the CR goes cold. However, the focus for redundancy was on data loss, errors or a system failure from a stack or cloud implementation. Redundancy will form part of the backup of a CR to allow for instances to be captured and replicated when needed. The health monitoring system with sensors is inclusive of the monitoring system for a CR, due to the monitoring system being the hub for viewing and collecting data.

From an infrastructure view, it was discussed that a commercial, low cost cloud service provider - as a solution for a CR - is better than buying and maintaining physical stack type infrastructure. There are advantages and disadvantages when provisioning a CR using a cloud service provider, and visa versa from a stack implementation, however this will depend entirely on the purpose and type of CR that is required, with determining factors including Internet speed, cost and access ability of users. The security system plays a major role, especially for real devices' connectivity. Cyber incident recording should take place within a CR to monitor its networks, where a SIEM as a core capability element was regarded as extreme within a CR. Security of the CR is important due to the nature of its purpose, in that malicious code is to be contained on all levels - monitoring this is essential in the management system of the CR.

Other core capability elements that were suggested included a reporting capability that allows for customisation and control of the reports that are generated from the CR event, allowing users of the CR to have control and capture information that is

relevant for them to use as a learning reference to improve their skills. This functionality is an added benefit in the LMS capability for a CR. Similarly, a scoring engine for lab exercises and competitive exercises was suggested, in that a scoreboard tells CR users how far they have progressed during the exercises, or how they are positioned against other students in a CDX or CTF. This capability will form part of the monitoring system, utilising multiple different sensors that fit the purpose of a CR. Data collection was also mentioned as a core capability, as a way to accurately indicate the impact of a cyber event. Data collection as a collective is viewed as part of the monitoring system, with the sensors of a CR considered a core capability element. From a spatial and temporal consideration this should form part of a CR, the rationale being that in many cases, attacking an asset requires proximity to the location where the asset is used. Most current CRs focus on only remotely attacking a target and not on the asset's proximity. The ability for a CR to attack an asset in a specific proximity, for example via wireless or Bluetooth, should be considered when planning the cyber event, ensuring the CR has the ability to provide such a cyber event.

Consensus core capability elements for a CR are presented below in Figure 6.2. Overall the conclusion to be drawn is that the respondents agreed with the core capability elements, with Big Data not regarded as a core capability element. The main core capability elements for a CR, by priority, can be concluded as follows: management system, virtual infrastructure, SW applications, scenario generator, traffic generator, monitoring system with sensors, SW operating systems and threat library.

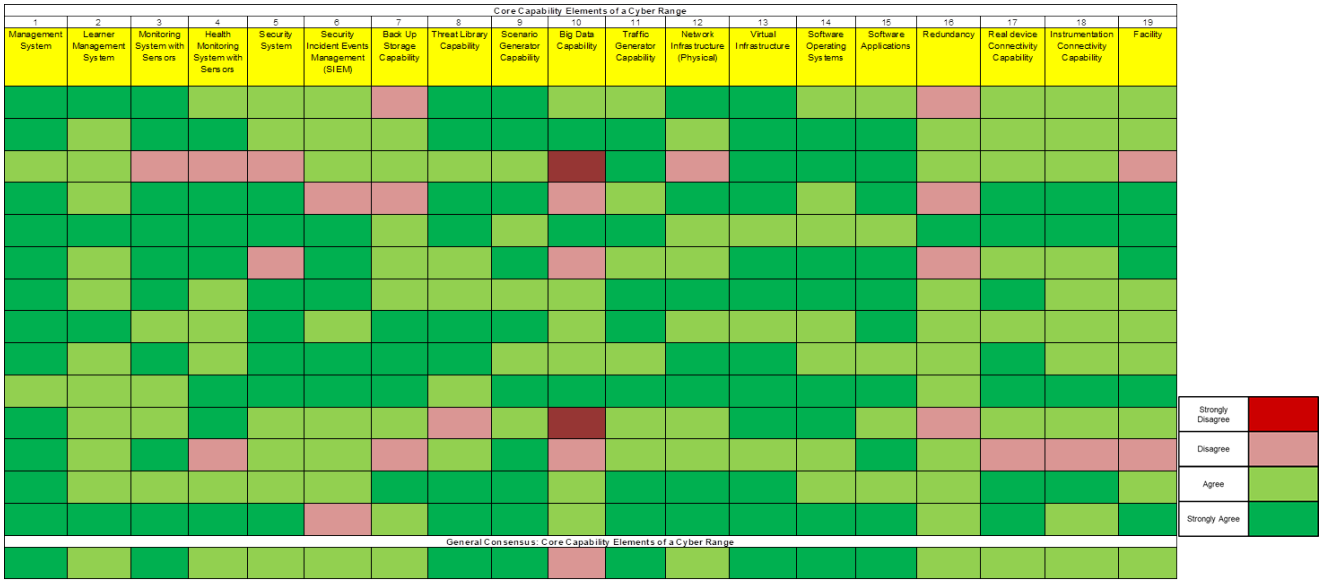


Figure 6.2: Consensus Core Capability Elements for a Cyber Range

6.4 Relevance Rating for a Cyber Range

This Section presents the feedback from experts pertaining to the Pairwise Comparison Analyses that was conducted in Section 3.5. The relevance rating for a CR was generally agreed upon, with the main disagreements as follows:

- Physical Network Infrastructure. This disagreement centred on a discussion of cloud vs. stack, in that a more mature CR organisation would utilise a cloud service provider to provision a CR, utilising mature content and developed cyber events. However Physical Network Infrastructure is important for a CR in a developing organisation, especially when there is low Internet availability and a cost constraint utilising a cloud service provider.

- Real device connectivity. This disagreement was due to a CR operating in a virtual environment, with no specific interface to allow for the connection of a real device.

- Facility disagreement was due to the ability to utilise a cloud service provider and to reduce costs.

- Redundancy and Big data was due to the discussion presented in Section 6.1.

The main relevance rating factors for a CR, as analysed, were prioritised as: management system, scenario generator and monitoring system (strongly agreed upon with the virtual infrastructure), physical network infrastructure, operating systems, traffic generator, SW applications, threat library, learner management system, security system, health monitoring system, instrument connectivity, SIEM, real device connectivity, backup storage, facility, big data and redundancy. The management system, scenario generator and monitoring system were indicated as the three main relevance rating factors for the core capability element for a CR.

Comparing the relevance rating from the Pairwise Comparison analysis and the expert review reveals that the main relevance rating of the core capability elements for a CR focuses on: the management system, scenario generator capability, monitoring system with sensors, virtual infrastructure, SW applications and traffic generator capability. From the analysis the utilisation of the relevance rating for developing levels for a CR is to be reconsidered due to the content the CR is to provide and its purpose. However when observing the results of the main core capability elements and their relevance rating, the generic fundamental elements are essential for a CR to function. Below is the consensus for the relevance rating of the core capability elements for a CR. The results of the analysis are presented in Figure 6.3.

6.5 Proposed Capability Cyber Range Levels

The proposed capability CR levels are generally agreed upon. The results of the analysis are presented in Figure 6.4, however there is disagreement in terms of level IV and V, due to the statement “virtual, instantaneous, and on demand” as set out in the questionnaire. The argument raised focused on where one draws the boundaries between CRs, as it is possible for them to be one distributed CR. Hence the CRs at different levels of capability can be distributed geographically, depending on their purpose. In creating a distributed CR environment, there needs to be a centralised

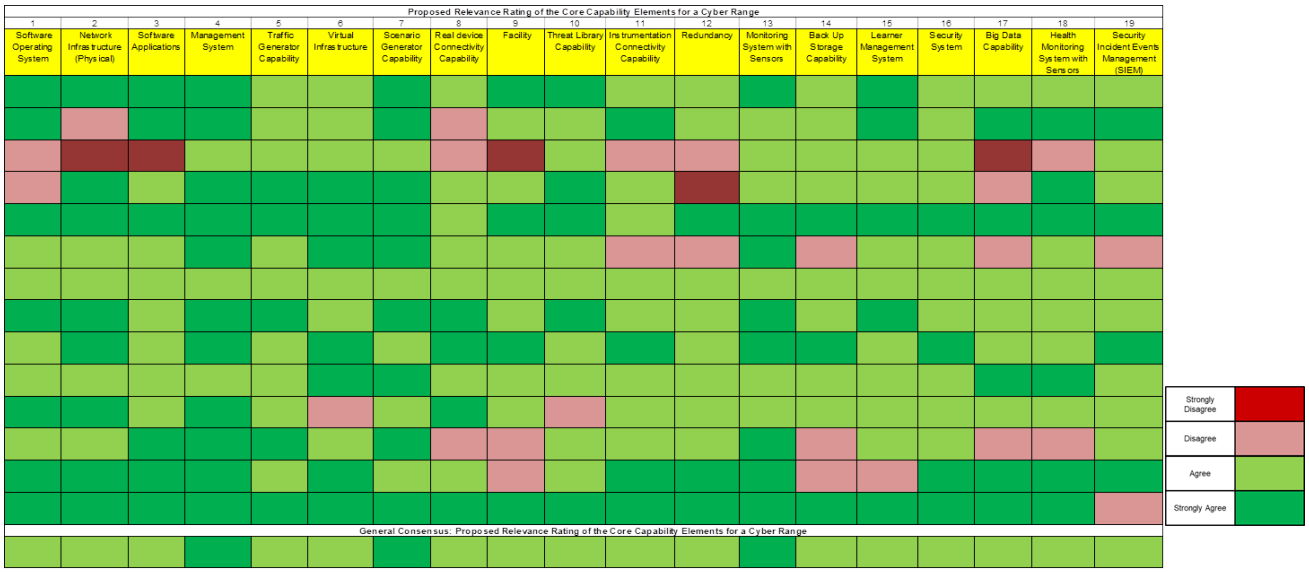


Figure 6.3: Consensus Relevance Rating for a Cyber Range

CR authority that will distribute the latest cyber threats, training content, CDX and CTF exercises and other CR operational matters to other CRs that are under its control. However, in the authors opinion, the boundary between levels for a distributed CR is viewed as the capabilities the distributed CR environment is able to provide to users and other CRs, if federated with other CRs, to share and utilise their capabilities. Another opinion is that the distributed CR can be measured individually within a distributed environment.

Another disagreement is that of hyperconvergence for a CR, in which the argument raised suggested that hyperconvergence is highly integrated and not as flexible, and a CR must be highly adaptable and flexible to accommodate the high rate of demand and services on a specific level of capability. Hyperconvergence brings to a CR a platform to run infrastructure clouds in isolation due to the integration of computational networking, storage and virtualisation. This enables multiple cyber events to be isolated in different virtual containers. Certainly hyper-convergence is complex in nature, however once configured it has the ability to rapidly configure cyber events in a short space of time for multiple users.

The integration into the real world as a critical capability was also proposed, to ensure that a CR can cater for a hyper-real environment and allow for a real user experience. This subject is also discussed in Section 2.5.5. The fidelity of the CR is fundamentally important for a CR capability, more so than up-sizing the functional scales for the CR capability levels. The experts agreed that fidelity in a CR is a key consideration, as is also discussed in Section 2.5.4. Comments regarding the human element, from a development viewpoint, emphasised the importance of enhancing the CR capability incrementally to ensure that the user understands and is able to utilise the CR. In conclusion, levels I and III were accepted as a basic baseline, while levels IV to V were agreed upon from a more distributed and fidelity capability perspective, rather than an up-sizing incremental approach to the functional capability of a CR.

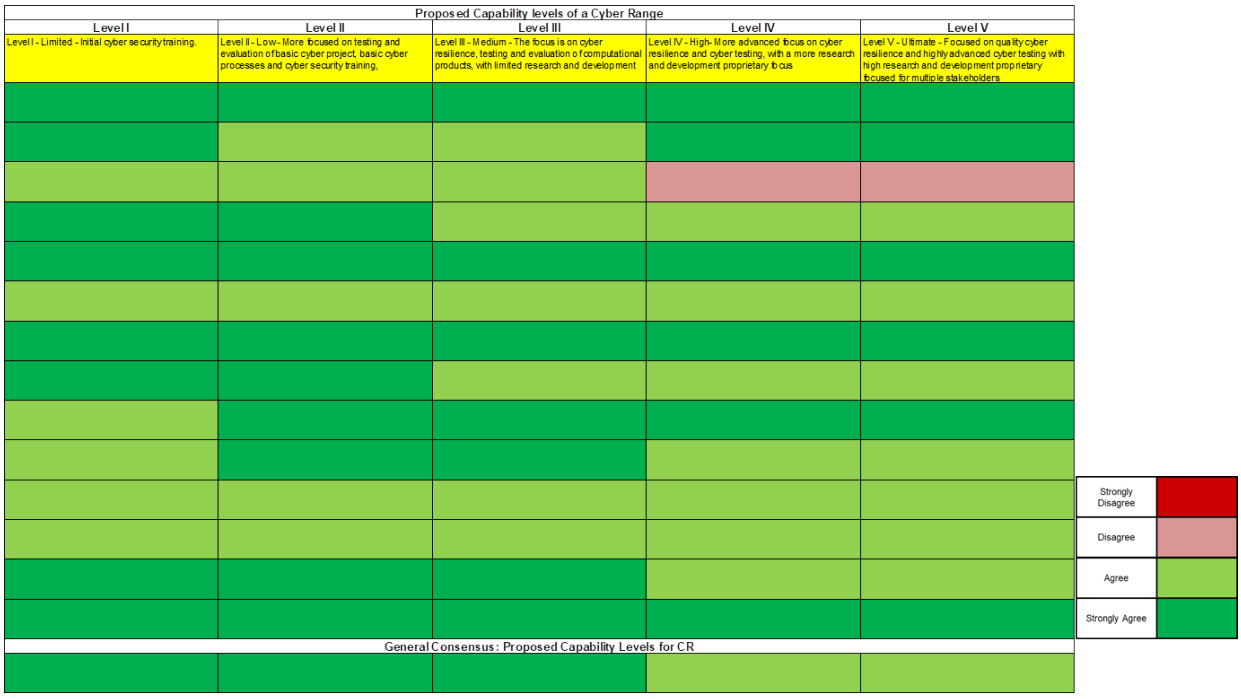


Figure 6.4: Consensus Proposed Capability Cyber Range levels

6.5.1 Measurement of Effect

One disagreement raised concerns about measuring the effect of personnel and infrastructure separately. This is to get a better view of how effectively the user accomplishes the cyber event and how effectively the CR maintains a cyber event. Of chief importance was the effectiveness of instrumentation to capture data from a CR event, which can be used to gain more detailed information on aspects of the scenario that are most relevant to them. This is also applicable to the CR system, where it is important to analyse the data generated in the CR to ensure optimal effectiveness. This is a core capability of a CR collecting data to indicate the effect and impact of a cyber event (see Section 6.3). The MoE is also used to measure the availability and stability when conducting tests, addressing whether the CR achieved the desired outcome of a cyber event.

When measuring effect in a CR from a capability view, the measurement will indicate the CR's ability to execute its intended purpose; when users are performing a cyber event, the effect of the event that the CR is performing gives an indication of the effectiveness of the users. This allows for the identification of gaps and focus areas that users need to be trained in, and whether there are any content changes that might allow for improvement. The main comments for the MoE for a CR were as follows:

- The MoE is separate from the user and the capability of a CR, hence measuring both the user and CR itself provides an indication of the CR's combined effectiveness.
- The effectiveness of a CR's ability to adapt to different cyber environment scen-

arios, and its ability to manage cyber activities, were strongly agreed upon as the main areas for measuring effectiveness in a CR.

- Finally, the CR's ability to capacitate and handle a single or multiple cyber operational tasks, operators' cyber skills, and the effectiveness of the CR at maintaining different levels of cyber events throughout its evolution over time were agreed on for measuring effectiveness.

6.5.2 Measurement of Performance

Comments that were raised included the fact that the MoP is important for a CR and is a key metric to measure. This enables the development and implementation of an effective CR. Overall, performance measures were agreed upon, with the measurement of fidelity, traffic generation, switching ability between cyber events and security in a CR strongly agreed upon as the main MoP. Likewise speed, throughput, quick configuration on demand, instrumentation connectivity and the measuring of a CR as a system based on how well the CR accomplishes a task were also agreed upon.

6.5.3 Instrumentation

The security and performance instrumentation with NetFlow for a CR was strongly agreed on, which augments the CR. The key areas of disagreement were the honeypot or honey net, which are based on the cyber event and not necessarily an additional function of a CR, in which the inclusion thereof will augment the reality of the threat landscape. Network telescope, honeypot or honey net and NetFlow are more focused functions, especially geared towards network traffic, which will also depend on the cyber event. However honeypot or honey net and network telescope are functions that can be utilised to test effectiveness, and can also be deployed in a CR. The use of additional instrumentation is dependent on the owners of the CR and cyber event selection that allows for a detailed analysis of traffic flow in the CR. Other instrumentation that can be utilised in a CR includes specific instrumentation for advanced analysis, prediction of user behaviour, identification of gaps in training, or monitoring for developing cyber resilience content. The main conclusions for the instrumentation for a CR are that security and performance instrumentation with NetFlow are strongly agreed upon as adding to the CR functionality, whereas a network telescope and honeypots or honey net are more focused functions, especially on network traffic and specific cyber events.

6.6 Proposed Classified Cyber Range Capability Levels

The general consensus supported the classified CR capability levels. The results of the analysis are presented in Figure 6.5, however a qualitative approach is needed to address some of the main points of disagreement raised. The difficulty of reaching

a consensus on the number of nodes and concurrent sessions for different CR levels is difficult. The main argument for classifying the capability levels for a CR is the difficulty of separating CR levels with the number of hosts, services, throughput and IP ranges against a quantitative number. In general, the number of IP addresses is not desirable due to the capability of infrastructure needed. Hence the focus on content and capability of a CR when classifying CR levels, rather than on the infrastructure details (nodes and services) and storage capacity of a CR. It was suggested that the mixing of infrastructure details with application capabilities for a CR is to be avoided, and to measure the capability of the CR rather than the capacity; examples given were the PlanetLab[1] and DETERlab[2] projects.

An incremental approach was used for the CR levels, as in Appendix B. However the key point of disagreement focused on a consideration for limiting the scaling of network size metrics, due to the nodes amounts indicated, which are excessive. For example, a network size of over 10 000 unique nodes seems excessive for a test, especially if they are of high fidelity. By contrast, there are large and multi-national organisations which have less than 100 000 nodes. Hence, a CR that provisions a small network with exceptional capability and high fidelity is worth more than a CR that can do almost nothing with 10 million hosts.

In today's world of elastic cloud computing, a level I CR making use of a cloud service provider is considered not difficult, hence the same implementation for a level V CR in a super computing centre. The drive for scales of economy and scalability is dependent on the CR's purpose and cyber events provisioned, hence the amount of hosts, IP ranges, concurrent services and throughput will differ. The disagreements raised are very complex, with a focus on the need to determine and classify CR levels as a baseline.

Making use of cloud service providers for a CR as a quick, effective and efficient solution to virtual infrastructure provides great flexibility, provisioning the resources needed for each host with limited effort, and having the ability to operate a cyber event remotely. However, the cost of data connections, the connection footprint, and the speed of the Internet differ geographically, due to many factors in a given country's ICT networks. Hence the argument for a stack approach for a CR. The choice from these two options - cloud or stack - will depend on the CR's purpose, whether it is an open or closed CR, Internet capability, accessibility, failure, lag or latency of the CR, resources and skills needed, funding available, and CR size.

The debate over AI in a CR suggests that it is to be defined and utilised to enhance a CR, but not to develop a CR. Hence, ML and AI is not a CR capability, but rather an enhancement for the automation of a CR. The analysis returned various views on the different levels pertaining to the CR classified capability, for example:

- **Level V**: Should be more focused on the evaluation of technology and processes, fully integrated with the real environment.

[1] https://www.planet-lab.org/
[2] https://deter-project.org/

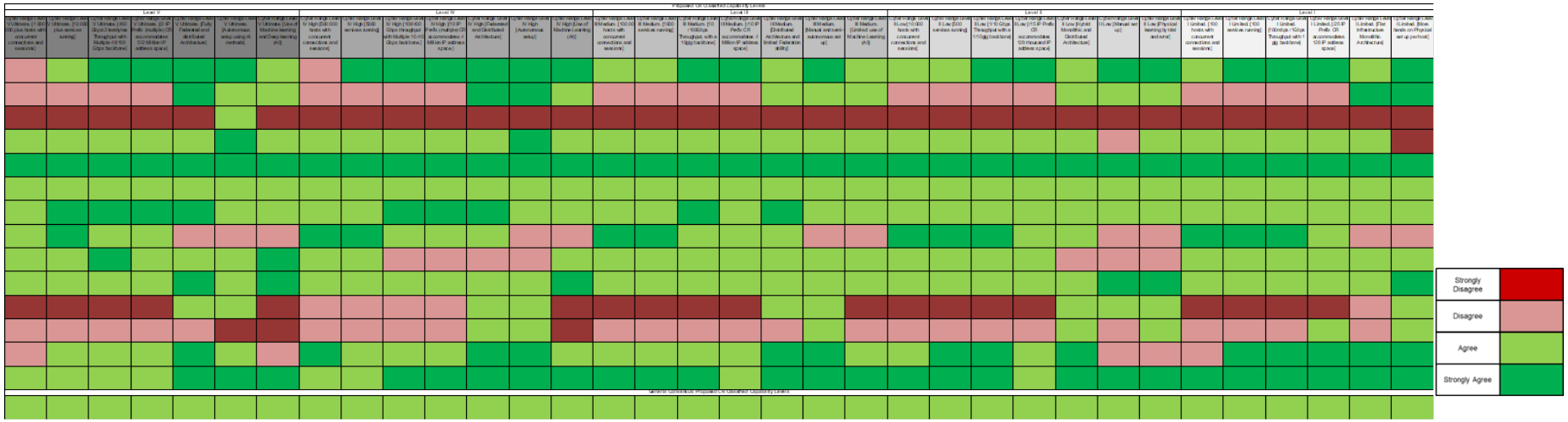


Figure 6.5: Consensus Proposed Classified Cyber Range Capability levels

- **Level IV**: The automated and federated system is a benefit.
- **Level III and Level II**: Should be more focused on the evaluation of peoples' behaviour in a cyber event, and the setup of 10 hosts or 500 services manually is challenging. The manual set up and physical learning by trial and error should form part of Level I.
- **Level I:** Sufficient for initial cyber security training, and will provide a realistic "feel" to the impact and complexity of threats, and should be more focused on training using 100 or fewer hosts.

The main conclusions for the classified CR capability levels are as follows: a more qualitative approach for the CR classified capability levels is to be established, with metrics being determined for different CR purposes. Therefore, a modified CR classified capability level was developed, as in Section 7.1, and the amount of hosts, IP addresses, services, and throughput should not be the determining metric for CR levels. Instead the content and capability, especially the provisioning of high fidelity nodes, that a CR can provide are to be used as metrics.

6.7 Proposed Maturity Levels of a Cyber Range

The proposed maturity levels and maturity elements, namely PPT for a CR were agreed upon. The results of the analysis are presented in Figure 6. 6. However, the view generally given by respondents was that the maturity levels are optimistic. The key disagreement centred on mixing staff credentials with operational processes, meaning staff credentials are people skills and operational processes are the operation of the CR and the process it uses to operate. However, one disagreement raised was with the inclusion of people in the maturity of a CR. This argument is based on a focus on CR maturity, and not the people who operate or use the CR.

This view can, however, be considered a first-world perspective, one that already has a mature CR, is using cloud-based services with high bandwidth and speed that are low in cost, and has highly skilled developers to provision the CR on demand. The generic PPT is based on the initial CR maturity level, which focuses on lower skill capacity; as the CR progresses, people are less important, and the maturity of a CR increases due to automation and provisioning of networks, either in the cloud or by federating with other CRs as a collective. The maturity of people also differentiates among the users and technical support teams for their different maturity levels, taking into account relevant cyber skills. Other maturity elements that were commented on included the following:

- Realism in a CR, or how close to a “real” feel does the CR give to the user during a cyber event.
- Federation for a CR, or how CRs are able to share CR content cyber events.

- Scalability and fidelity of nodes that allows the CR to replicate and size up cyber resources quickly with low inference.
- Integration of systems, how integrated is a CR system against a mature level.

More generally, from a technology maturity perspective, although a CR may utilise advanced technology, if the technology is not used adequately to drive capabilities, the CR will lack maturity. The main conclusion for the proposed maturity levels and its maturity elements - People, Processes and Technology - for a CR can be concluded as largely agreed upon, with the main disagreement being that skills of individuals matter less as a CR evolves due to the CR maturity and automation, as depicted in Table 6. 6.

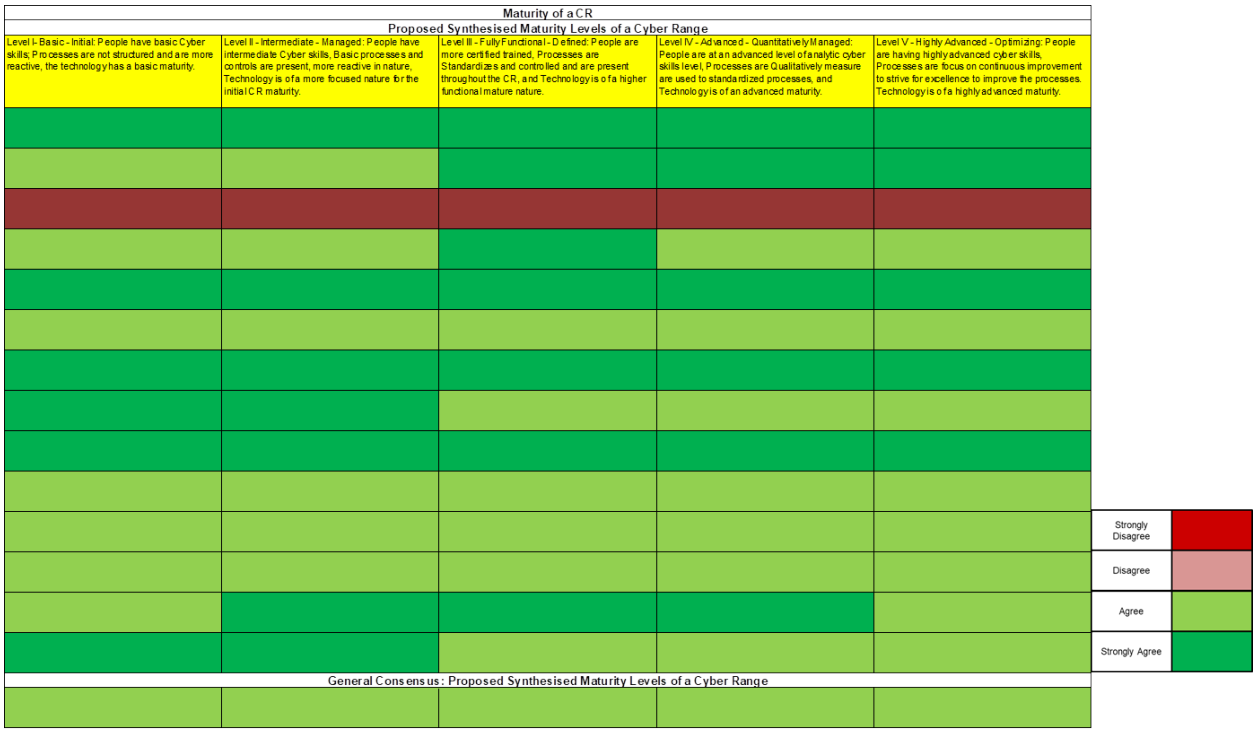


Figure 6.6: Consensus on Synthesised Maturity Levels of a Cyber Range

6.7.1 People Maturity

People maturity was divided into two sections. First, people maturity pertaining to cyber skills and cognitive ability to cope under pressure, with the main question being how this might be evaluated. Second, how would the maturity of people's cyber skills be evaluated, and against what measurement? People maturity, which includes an evaluation of cyber skills, cognitive ability and ability to cope under pressure, was suggested to be measured based on the metrics captured when the user is participating in a cyber event. An examples of this is the duration of time before a user takes action after being notified of a cyber event which occurred on a network. This can include the duration of time a user took to resolve an issue and complete the incident management process, the duration of time a user took to diagnose or identify the root

cause of an incident, and the capturing and analysing the steps that a user took when the event took place.

The use of a grading curve to visually display the number of respondents that have completed various scenarios as part of a cyber event can be utilised as a tool to evaluation respondents progression. By implementing the grading curve, the utilisation of external and internal sensors are needed to correlate telemetry data with the actions conducted by the user. By measuring the time taken to complete the cyber exercise, the processes followed and the attack or defence vectors used, the outcomes equals the speed at which the user completed the cyber exercise. This is measured against a specific cyber training standard as determined by an organisation or international training standard body. With regard to the ability of a user to cope under pressure, an evaluation would depend on the cyber event generated and not on a specific task that is completed. Linking this to the turn around time makes it possible to gauge operational and temporal efficiency, measuring the output from a real operational environment. Another way was to consider the cyber activities and tasks executed that are orthogonal or unrelated to the desired outcome; an example of this would be attempts to access or modify unrelated services. However this would be heavily dependent on activity logging, and require a solid baseline on a per task basis. One suggested approach was to simulate pressure, utilising a Red and Blue team scenario against a script or simple AI application that generated cyber injects and changes to the cyber event based on time, with negative marking for extraneous actions. This would evaluate how well the operator could prioritise threats and think quickly.

The main conclusion for people maturity on how to evaluate cyber skills, including the cognitive ability of the user and the ability of the user to cope under pressure in a CR, is the implementation and utilising of internal and external sensors to correlate the telemetry data to visually display the user's ability when solving a cyber event. This is determined however according to predetermined metrics that are measured against a training standard. The implementation of time metrics based on real operational cyber events, using scripts that generate cyber injects, is a valuable way to measure users' ability to cope under pressure.

The evaluation measurement for the maturity of people cyber skills was identified as the user's ability to function and contribute in a team scenario (Red, Blue, Purple, White), be less inclined to rely on hints and tips that are available in the cyber events, and accomplish objectives is a certain time. The user is also measured according to their ability to reasonably assess the situation and resolve the problem under pressure with unknowns or modified knowns, the quality of the solution they provide during a cyber event, and their ability to effectively utilize technology and apply the correct processes. The use of best practices and the alignment of a developed measurement for cyber skills processes, as a baseline was suggested to be utilised when evaluating people's cyber skills.

The main comments for the evaluation measurement for the maturity of people cyber skills for a CR can be concluded as a combination of best practices and in-

dividual skill at functioning and adapting in a cyber event in a certain time while using technology and not being reliant on assistance sources.

6.7.2 Process Maturity

There was a general consensus regarding the maturity process areas pertaining to a CR, however there was disagreement in the project management area. The disagreement raised was that research areas are responsible for investigating new technology and trends for how to integrate with a CR, and this should not be left in the project area. However, research can be considered a part of the project process area. An additional comment suggested that including security-specific areas would be useful, however this area would be better suited in the management or engineering areas due to similarities to other processes. Training process was suggested to be incorporated to ensure that the processes of the content provided in the CR are completed. In conclusion management, engineering and support process areas are strongly agreed upon, training processes are to be incorporated, and the project management area was disagreed upon.

6.7.3 Technology Maturity

In measuring the maturity of technology in a CR it was mainly commented on that the CR technology should be evaluated against the purpose the CR is to deliver. Similarly, the technology is to aid the cyber event so as to match the operational environment in the CR, hence the ability to mimic and incorporate real world cyber events and adapt to new technology trends on demand. In general, evaluating and measuring the maturity of technology in a CR was agreed upon in principle, with some specific points of consideration mentioned in Table 6.2 as commented on from the expert review. A disagreement on the measures for technology maturity was that the measures proposed in the questionnaire were all the normal processes that have to be in place to manage technology, and not necessarily to measure the maturity. Hence a comparison with standards may be a better approach, thus if there are no standards available, they should be developed. Similarly, implementing the latest technology in a CR does not guarantee that it will be utilised to its fullest capacity, especially if the training content of the CR is out of date. The main conclusion for the measurement and maturity of technology for a CR focused on a combination of standards, investigation and observation of the technology performance in a CR to fulfil operational effectiveness fit for the CR's purpose.

6.8 Capability and Maturity Models Methodology for a Cyber Range

The consensus opinion from the expert reviews of the CMM methodologies proposed was general agreement. The results of the analysis are presented in Figure 6.7 (note

Table 6.2: Technology Maturity Considerations for a CR

Evaluating the maturity of technology	**Measuring the maturity of technology**
Is the technology supported and established.	Maturity of licensing, certifying and processes used.
The popularity and adoption of the technology in CRs.	Upgrades, any limitations when expanding or enhancing the CR itself, and the number of bugs reported when utilising the technology.
Licences or open-source considerations.	By measuring the ability to integrate technology in a CR.
Flexible to support new cyber events.	Its machine learning capability, and interoperability with other systems and technologies in use.
The technologies adaptation to the latest speed and security risks.	The current adoption of the technology that is being used in a CRs, and how widely is the technology being used.
Life expectancy of the technologies and behaviour when integrating or utilising in a CR	
Benchmarking and comparing similar technology and its effectiveness in a CR.	
The technology of cloud services versus facility stack-based implementation, to automate scenario generation and the deployment of cyber events.	

the yellow indicates “not commented on”). The major disagreement argued that models that are developed for evaluating the maturity of services that a CR provides would be better suited. This is a valid comment for future work that is to be explored. Another disagreement was that each of the models suggested can evaluate a sub-component of a CR, but not a CR as a whole, hence an integrated approach to the model is to be utilised. The CMM was rated by an expert as agreed and the other models were to be negated, this was due to the view of the SW applications that are in a CR and the development there of due to a virtual environment. This is a valid point, as the maturity of the CR SW applications is to ensure that it has the ability to maintain the content and purpose of a CR, especially in a virtual environment. The rating of the models during the analysis was prioritised as CMMI, CMM, CSCMM and then the LISI Model. The main conclusion for an appropriate CMM for a CR is as follows: the CMMI was rated higher in the analysis calculation than that of the other models in priority, namely CMM, CSCMM and LISI. However, a combination of the models would allow for a more comprehensive approach to determine a CR capability maturity on different levels.

6.9 Other Analysis Consolidated

A discussion was held with an expert after data was acquired, in which the expert highlighted the rationale behind the disagreements holistically: when observing a CR capability maturity, the purpose of the CR must take into account the fact that a CR

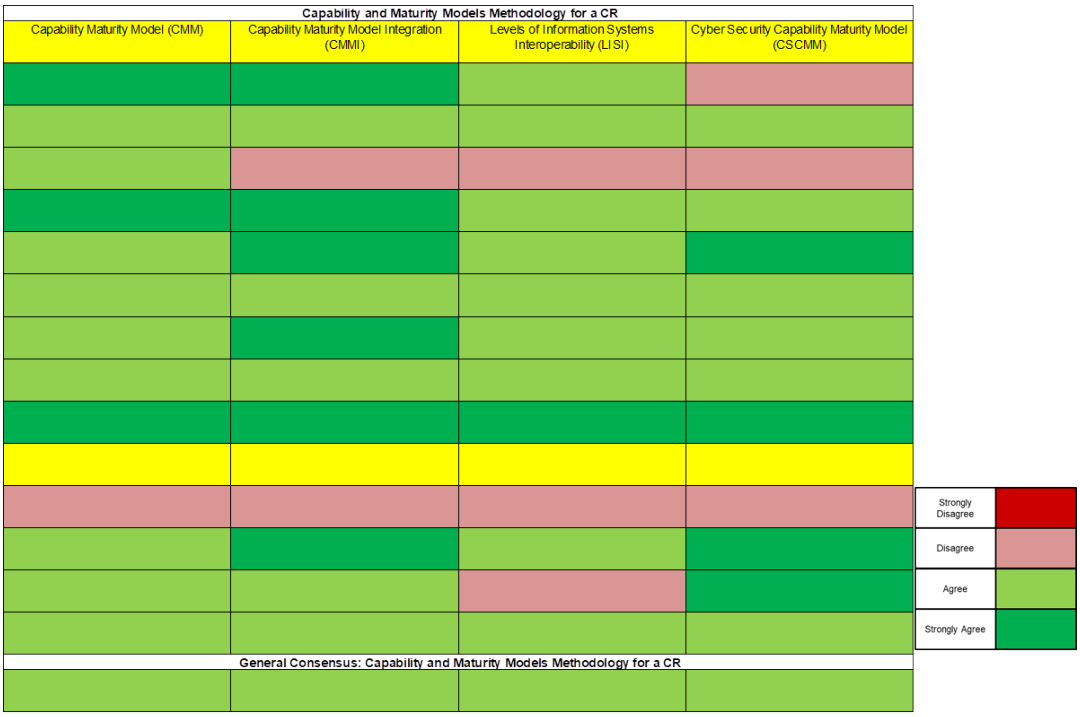


Figure 6.7: Consensus Capability and Maturity Models Methodology for a Cyber Range

can have different focus areas. These can include, for example, cyber education and training, Critical Information Infrastructure Protection training (CIIP) for SCADA networks, and cyber security training for military and the public. When measuring the capability of the CR, it is important to consider what the CR can achieve based on its operational ability and how current the CR is with reference to cyber threat generation and its ability to maintain or detect threats in a cyber event.

The measuring of infrastructure for a CR is misleading, due to the size, amount and load the infrastructure can maintain. Rather, one should serve the user's demand and not develop CR content without understanding its purpose. Some CRs have moved to using cloud service providers to provision a CR to host its scenarios for a cyber event. The trade-off is the cost of the cloud service provider and the cost of Internet connectivity over time.

The upkeep of a closed CR with its own infrastructure and staff is costly, however this is also dependent on the CR's purpose. Some ranges are closed, such as military or CIIP CR, while CRs for cyber resilience in businesses can be open. This is typically a cloud versus stack trade-off for a CR when looking at cost benefits in the long term, with the major points of consideration being frequency of use, operation and maintenance, and resource support. A part of maturity should be focused on the user's subjective opinion and experience: are there lag or latency issues experienced during the utilisation of the CR? Is there enough access to tools and other services? Finally, was the use of the CR a positive experience? One of the key maturity areas is the processes, for example the process for self-provisioning, either manually or autonomously, and utilising chat bots for user interaction as part of an LMS. Size

of a CR can be misleading, especially from a vendor viewpoint; a CR can be a small setup but have the ability to provision high fidelity, allowing for a more real world experience, where as a larger CR will have the capacity to host low fidelity nodes and will not deliver an accurate, real-world cyber experience. Therefore, the size of a CR is to be considered and measured based on its content and application.

6.10 Summary

Chapter 6 establishes the qualitative view from CR experts in the field on the proposed CMM for a CR. The data analysis from the questionnaire has given a clear indication of areas of agreement and disagreement. Table 6.3 presents a summary of the findings, showing the main results that were captured. Chapter 7 establishes a reworked and modified CMM for a CR, factoring in the feedback of the key agreements and disagreements from the expert review. A discussion of the CMM for a CR is put in perspective to give an understanding of the model as a concept.

Table 6.3: Summary of Expert Review Findings

Broad Themes	**Main Findings**
Defining a Cyber Range	There is a definite common understanding for a CR, however defining a CR is dependent on the intended purpose thereof. In comparing the expert review, literature review and thesis definitions, the most common words used were cyber, environment, training security, network, testing, simulated, and capabilities. The agreed-upon holistic CR definition was as a simulated cyber environment for security training and network testing as a capability.
Core capability elements	The main core capability elements for a CR include the following priorities:: management system;, virtual infrastructure, SW applications, scenario generator, traffic generator, monitoring system with sensors, SW operating systems and threat library. The other elements are viewed as optional. Big Data, SIEM and redundancy were not agreed on as core capability elements.
Relevance ratings	The main relevance rating for a CR in order of priority are the management system, scenario generator capability, monitoring system with sensors, virtual infrastructure, SW applications and traffic generator capability.
Proposed capability levels	Levels I to III are accepted as a basic baseline, whereas level IV to V are agreed upon from a more distributed and fidelity capability perspective rather than to up-sizing incremental the functional capability of a CR. The key areas to measure effect are highlighted as the effectiveness of a CR's ability to adapt to different cyber events and its ability to manage cyber events. The key areas identified to measure performance were fidelity, traffic generation, switching ability between cyber events and security assessment.
Proposed CR classified capability levels	The number of hosts, IP addresses, services, and throughput should not be the determining metrics for CR levels, rather the focus is on the content and capability, especially the provisioning of high fidelity nodes, that a CR can provide. A qualitative approach for the CR classified capability levels is more appropriate and metrics are determined for different CR purposes.
Proposed maturity levels	People as a collective (skills and workforce) become less important as the maturity of a CR evolves and increases due to automation in a CR. That the maturity of the management, engineering, support and operational processes areas for a CR are important to support and maintain the content that the CR is to deliver is agreed upon. Project process areas were not agreed on. A training process area is to be incorporated to ensure the content of the CR is captured accordingly. Technology that is not used adequately to drive capabilities results in a lack of maturity. When measuring technology maturity, a combination of standards, investigation and observation of the technology performance in a CR is needed to fulfil operational effectiveness with respect to the CR's intended purpose.
CMM methodology for a CR.	The CMMI was more accepted than the other models, followed by CMM, CSCMM and LISI, which was agreed upon.

7

Modified Capability and Maturity Model for a Cyber Range

The findings from Chapter 6 were analysed and captured accordingly from the expert reviews gathered via questionnaire. The findings have indicated the gaps that need to be factored into the modified CMM for a CR. In Chapter 7 the results are factored in to form a newly modified CMM for a CR. In Section 7.1, the influencing factors for a CMM for a CR are discussed, including how they impact on the modified CMM for a CR. In Section 7.2, the modified CMM for a CR is described and discussed, including how the model can be utilised, and Section 7.3 provides a summary.

7.1 Influencing Factors for a CMM for a Cyber Range

The factors that indicated necessary changes to the initial CMM for a CR are used to develop a modified CMM for a CR. These factors have allowed for improvements to the baseline model for the capability maturity of a CR. The factors discussed are the main factors that have an influence on the development of the proposed CMM for a CR from a capability maturity perspective.

7.1.1 Cyber Range Capability

There are three core capability elements that have been extracted due to the expert review. Noticeably, there is no significant influence on extracting the three core capability elements, as this was discussed in Section 6.3, which included the following points:

- Big data, due to this being more a methodology used in storage if required.

- Redundancy, because a CR is not regarded as an operational environment, but rather as a training and virtual environment that can provisioned on demand. Thus no redundancy is needed as a backup image can be utilised.

- SIEM was seen to be a bit excessive in a CR, as logs are captured using sensors and controlled within the management system.

Date collection was suggested to be added as a core capability for a CR, however this function is inherent in the monitoring system, with sensors, for a CR, which itself is inclusive of the health monitoring of the CR system and thus has no impact on the CMM for a CR. Health monitoring systems with sensors are inclusive of the monitoring system for a CR. The MoE is qualitatively measured to determine the level of effectiveness the CR can maintain; the three main themes identified with regard to MoE were the effectiveness of the CR as a system, the training content, and the human behaviour (Section 5.1.1). The MoP is measured quantitatively, hence these measures will stay the same as in the literature. However, a mixed method approach is best suited, as stated in Section 4.5, when measuring effect and performance. The instrumentation not agreed on included the network telescope, honeypot or honey net, and partially the NetFlow, as these are more focused on network traffic. The security and performance instrumentation was however agreed upon, thus instrumentation is included in the core CR elements. The impact of the instrumentation not agreed on will only be for the utilisation of specific network tests within a CR. Machine learning was suggested as not being a CR capability, however it can be utilised to augment the CR, leaving no impact on the CMM for a CR.

The general consensus regarding the CR classified capability levels was that the host size is quantitative and needs to be defined. Hosts are to be derived via higher fidelity rather than from the number of hosts. Thus the more hosts with high fidelity the higher the maturity. The suggested focus was on the content and capability of the CR for the CR classified capability levels, and not on the infrastructure details and storage capacity of a CR.

The influence of this factor will allow for a more qualitative approach to the CR classified capability levels, by not delineating the levels but rather factorising in the areas that are to be considered and developing metrics from a capability maturity view for a CR. The proposed modified classified CR levels focus on the level of capability by addressing the following: the content a CR provides, the application of the CR as synthesised from Section 4.1, and the core capability elements of the CR. Similarly, the level of maturity addresses the People, Processes and Technology. Table 7.1 presents the proposed modified classified CR levels based on the analysis of the expert reviews and the relevant importance of the CR core capability elements, which have been changed as in Chapter 6. The proposed classified CR levels are modified qualitatively as per the analysis of the expert reviews given in Section 6.6.

Table 7.1: Modified Proposed Qualitative Classified CR Levels

	CR Capability			**CR Maturity**		
CR Levels	CR Content	CR Core Capability Elements	CR Application	People	Processes	Technology
V Ultimate and Highly Advanced IV High and Advanced III Medium and Fully Functional II Low and Intermediate I Limited and Basic	The realism of the delivery of content on different CR levels are dependent on objectives and workforce development frameworks of an organization and the purpose of the CR. The content the CR is to provide. • Cyber Learning Material • Lab Exercises • Group Exercises, CDX and CTF	Eight main core capability elements: • Management Systems • Virtual Infrastructure (cloud vs. stack infrastructure) and the size of infrastructure dependent on the demand, purpose and type of the CR. • SW Applications and Operating Systems • Scenario Generator • Traffic Generator • Monitoring System with Sensors • Threat Library Other Core Capability Elements • SIEM • Health Monitor • LMS • Backup (Various Sizes) • Redundancy • Instrumentation • Facility • Real Device Connectivity	• Quality of Service • Apply high fidelity nodes, demonstrating realism compared to the operating environment • Federated • Distributed used according to CR capability • Replay ability of exercise and tests. • AI enhancing CR capability • Repeatable tests with low administration costs (resources and licenses) • Scalability of CR, its delivery scale (on premises or in the cloud) • Class room and resource capability (manual set up vs. self-provisioning) • Exercise results vs. processes used (scoring) • Users accessibility to CR remotely or networked (collocated system or VPN) • Customization of content provided; security threats generated; scenario development (automation vs. manual) • The effectiveness of the CR according to the deliverable.	• People become less important as the level of maturity increases due to automation • The uses maturity level of cyber skills • The technical support maturity level of cyber skills.	Maturity of processes areas implemented on different CR levels. • Engineering • Support • Management • Operational • Training	Technology that is not used adequately the maturity level lowers. A combination of • Standards • Investigation • Observation of the Technology Performance, to fulfil operational effectiveness through its life cycle.

7.1.2 Cyber Range Maturity

The people maturity was generally accepted, however a point is to be made that people are less important as the maturity of a CR increases due to automation and provisioning of networks through a cloud or CR service provider. For this reason, skills of individuals matter less as one evolves to a higher level of capability maturity. The influence of this factor, however, is both determined by and dependent on whether one takes a first or third world view - the skills of individuals, access to high speed internet services, and cost can vary greatly globally.

Process areas that were determined important were the management, engineering, support, training, and operational processes areas, all of which are factored in the CMM for a CR. The impact of this is that the training and operational process areas are to be defined to determine the different levels to measure against. The maturity of technology was suggested to be measured by using standards which are objective, rather than using processes to measure the maturity of technology, which can be subjective. This will influence the fact that the standards are agreed upon and alleviate conflicting views of the maturity of technology. The adoption of the CMMI model and CMM was more suited to measuring the capability maturity of a CR. However, a combination of the models would allow for a more comprehensive approach to determine a CR capability maturity on different levels.

In comparison with the previous CMM for a CR (see Section 5.3), it is clear that the impact on the original model is substantial. This major change was a result of factoring in all findings that impact the understanding of capability maturity for a CR. The previous model showed a more six dimensional approach to measuring capability maturity; this did not take into account the activities in the model (as discussed in Section 2.6) to measure the capability maturity for a CR. The MoC and MoM has been modified accordingly with the categories that are to be evaluated to measure a CR capability maturity.

7.2 Modified Capability Maturity Model for a Cyber Range

The CMM for a CR has been modified by factoring in the results of the expert reviews. The categories for measurement and their elements are inherent in the model and are factored in accordingly. The identified categories under each element to be developed further into process areas are highlighted in the model. Their attributes are to be utilised when measuring the CR, however a more detailed examination of these process areas is outside the scope of this thesis. This modified CMM for a CR is a suggested generic model that can be utilised for any type or purpose that a CR might evaluated against.

The modified CMM for a CR describes the different levels, from I to V, that a CR will achieve; these levels are built from the levels of the MoC and MoM with their corresponding elements. The levels are shown in a triangular form to illustrate the increments of capability maturity. The level of MoC, which includes the threat,

performance and effect, is captured in the model. Threat is derived from the MoT in Section 5.2.3 and Table 2.1 according to the threat tier levels. Performance is derived from the MoP, as in Section 5.2.2, and from the results analysed in Section 6.5.2 in which a quantitative measure is to be developed with respect to the metric for speed, fidelity of nodes, CR switching ability, traffic generation, CR configuration on demand and CR security, focusing on the performance of the CR core capability elements. Effect is derived from the MoE in Section 5.2.1 and the results in Section 6.5.1, which considered the effectiveness of the core capability elements and their performance from a system view, focusing on the maturity of people, processes and technology in a CR, the training content of a CR, and the behaviour of the user during training. The CR application of the CR capability focuses on the CR ability to apply certain abilities and functions which are inherent in measuring the CR effectiveness as a system. The core elements are derived from Section 3.3 and the results in Section 6.3; of nineteen core elements initially determined, the end result was fifteen, with four core elements excluded as in 7.1.1.

The level of the MoM, which includes the people, processes and technology, is captured in the model. People maturity is measured as in Section 5.3.1 and Section 6.7.1, with the main focus on skills, cognitive ability and speed to solve problems and injects from cyber events. Process maturity is measured accordingly from a deployment view, as in Section 5.3.2 and results from Section 6.7.2, in which the key areas are management, engineering, support, and training and operational processes. Process maturity focuses on the processes utilised within the core capability elements, people, technology and content the CR provides. Technology maturity is measured as in Section 5.3.3 and the results from Section 6.7.3, and focuses on a combination of standards, investigation, and observation of the technology performance to fulfil operational effectiveness through its life cycle, capturing its effectiveness as a measure against the CR requirements, as in Section 6.7.3.

As discussed in Section 4.5, a mixed method for measuring a CR to determine its level of capability maturity will allow the strengths of both a qualitative and quantitative approach to augment each other, giving a more complete and comprehensive result. Time in context to the model is the measure of time that it will take a CR to reach a certain determined level of capability maturity. The modified CMM for a CR is presented in Figure 7.1.

The following questions, which arose during the course of this research, are relevant to the broader field of work related to this thesis and are enumerated and answered here in order to add value to the wider understanding of CRs in general. These questions and answers allow for debate in the CR community, and gives a sense of reasoning to the questions collected during the research. The answers to these questions are reasoned according to the authors view.

- Why evaluate a CR? Assessing a CR is to incrementally solve the gaps in the CR and to evolve its capability maturity. When evaluating a CR, it can be measured against CR criteria and standards for analysis to identify the gaps in the CR's

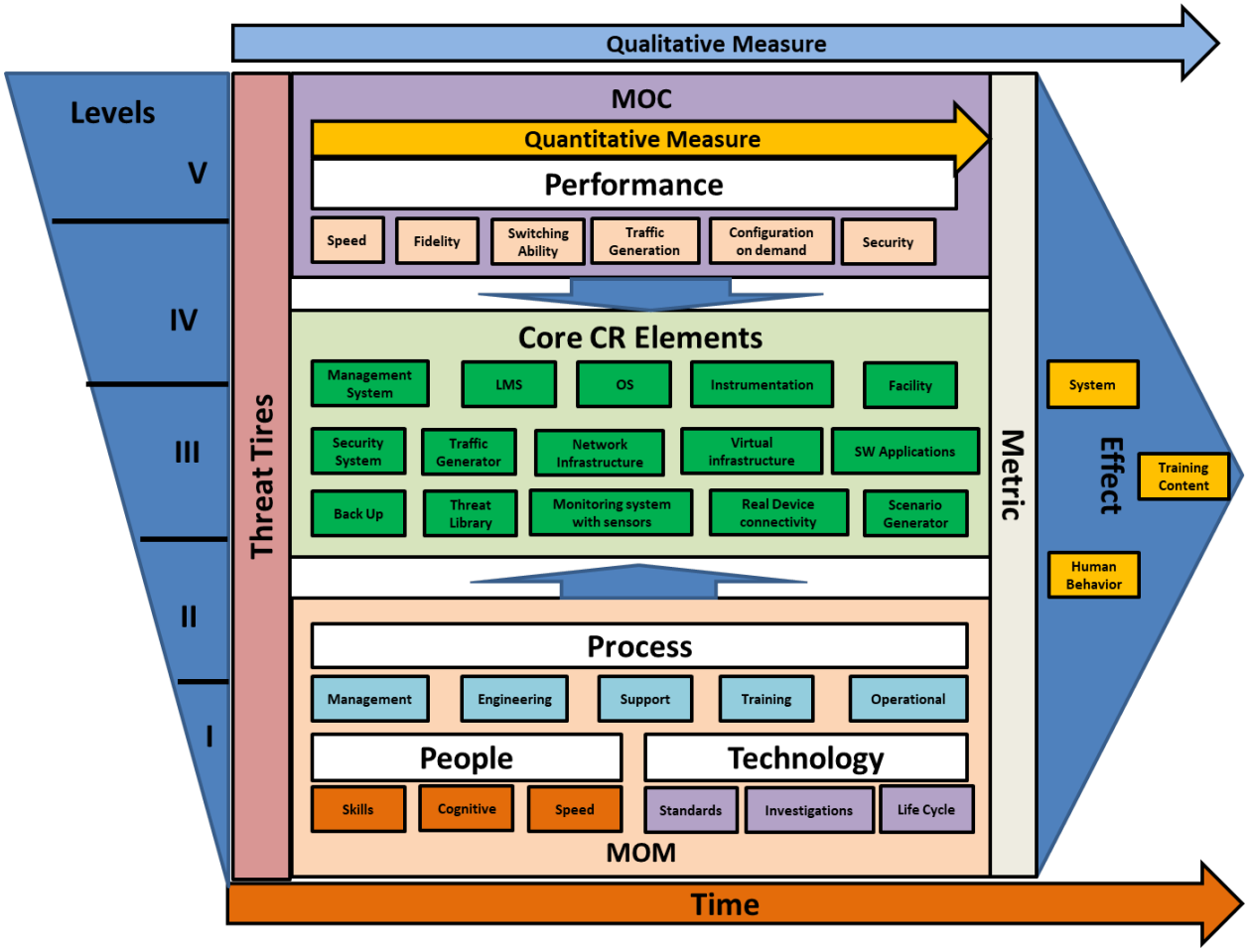


Figure 7.1: Modified Capability Maturity Model for a Cyber Range

capability maturity and to draw up a plan to close the gaps accordingly.

- Why measure a CR? To categorise the CR against a baseline CR level of capability maturity to allow for improvement, identifying gaps that would not be typically made visible in a CR evolution.

- What would motivate an organisation or nation to develop a CR capability? In many cases, an organisation will have a need that must be satisfied in order to achieve its organisational objectives. Organisational motivation in this case is the willingness to achieve organisational objectives, for example resilience against a cyber threat or establishing a capability for attribution. Thus in developing a CR, a hands-on approach (need) against a cyber threat (motive) to ensure cyber security (behaviour) will limit cyber transgressions (consequences) and the cyber threats in the organisation (satisfaction).

- Where to prioritize effort for developing a CR capability? This is dependent on the organisation's or nation's cyber threat, and their posture on cyber security as whole. One of the main priorities would be to ensure that there is a real-time, up-to-date threat and scenario generator to develop cyber scenarios in order to train people for cyber resilience. For an organisation to invest in its people and

remain vigilant against cyber attacks will allow for more focused and mature organisational security as a whole. Another priority is the ability to guarantee that T&E of products before deployment in an organisation's computational network is undertaken, ensuring that there are no known default vulnerabilities so that simple security configurations can be implemented.

- What to focus financial commitment on for a CR and why? A national CR is a CAPEX commitment on a national level; building a cyber capability in a nation would be appropriate for a nation that has developed and is committed to its cyber strategy. The focus on this level is firstly the ultimate level of capability to ensure that they are ready to defend the cyber sovereignty of their nation's cyber space. Related focus areas include: high processing computational power to ensure that cyber scenarios are emulated at high fidelity, research and development to consistently enhance the CR capability, and the maintenance and support of ensuring CR cyber skill levels for the future. Within all these focus areas, cost is exponential and will need to be budgeted for on a national level. However, for an organisation to focus their cost on developing or augmenting a CR will depend on both the size of the organisation's computational network and their current threat tier. These two factors will largely determine the level of CR to invest in. Fundamentally, it is the people in an organisation that are its greatest asset, and training people to be more cyber resilient by using a CR on different levels will augment the cyber defensive posture of that organisation. Thus, with cyber security training, organisations are able to securely maintain their data in a secure environment, ensuring that the laws pertaining to information confidentiality are followed

- Why are CRs being invested in? Cyber threats have become so sophisticated and highly technical that a system had to be developed to test, train and keep current with cyber threats. Developing skilled personnel to defend against a cyber attack is one of the reasons for the cyber security revolution, which has as a result generated masses of revenue in its ongoing effort to protect digital information and computational assets and adhere to legislation.

7.3 Summary

In Chapter 7, the data analysis and the results gathered, together with the findings from Chapter 6, have allowed for the proposal of a revised version of the CR levels and modified CMM for CR. This chapter established the second iteration of a CMM for a CR, as per the results from the expert review. A set of key questions that were raised during the research were addressed by the author. Chapter 8 will provide concluding remarks on the research undertaken during the course of this project, providing an overall view on the work described in this thesis and the outcomes thereof.

8 Conclusion

At the start of this thesis the focus was on a proposed CMM for a CR. Chapter 8 revisits the problem statement and the research questions to evaluate to what extent this was accomplished. Section 8.1 provides a summary of work completed, Section 8.2 addresses research goals, Section 8.3 describes contribution and research outputs, Section 8.4 suggests future work on the subject and Section 8.5 gives a conclusion.

8.1 Research Summary

The development of a CMM for a CR is challenging, with the difficulty lying in determining the capability maturity of a CR due to the diversity of approaches to measuring different aspects of a CR. The core capability elements that compose a CR as a system were determined through an examination of the relevant literature and via expert review. This allowed for an understanding of how a CR operates. Using the core capability elements as a focus area, the relevance importance of the elements was determined, allowing for the development of CR levels, which form guidelines for the development of a baseline for categorising capability maturity. The measurement of these levels lead to the development of the MoC and MoM, where the MoC is specifically focused on the measurement of effect, performance and threat that a CR is able to provide, and the MoM is based on the people, processes and technology that are applied. It was established that there needs to be a balance in ensuring that the elements in both capability and maturity are taken into account to determine the overall capability maturity of a CR. Using these two categories allowed for the development of a CMM for a CR.

A questionnaire was sent out to determine if the CR community agrees with the core capability elements, the CR levels, and the maturity approach for a CR. Analysis

was conducted and results were captured, which were then factored in to formulate a baseline CMM for a CR. The CMM for a CR can be utilised to measure the status of a CR or it can assist in the development of the CR's capability in its evolution through the different levels for which it is intended and towards the purpose it should fulfil. The following overview provides a research review of the chapters, indicating what research was completed:

1. Introduction (Chapter 1): An overview of the research, including the problem statement, research question and scope of the thesis was presented.

2. Literature Review (Chapter 2): The key concepts of the thesis are identified, which include an understanding of the cyber domain, cyber ranges, and capability maturity models. This chapter provided a background both in context and on the current research landscape relating to CRs and discussed the need for a CR. The chapter also elaborated on other related work pertaining to the detailed operation and functioning of a CR.

3. Defining a CR (Chapter 3): An interpretative overview of the literature on CRs was addressed, with a particular focus on the CR design, system, and core capability elements on a high level. A paired comparison was completed to determine a baseline for CR levels.

4. Criteria for a CR Capability and Maturity Model (Chapter 4): This chapter identified measurement criteria for a CR and introduced the Measurement of Capability (MoC) and Maturity (MoM), as well as the proposed baseline criteria for CR levels, and described a process to evaluate a CR.

5. Proposed Capability Maturity Model for a CR (Chapter 5): This chapter defined the Measurement of Capability (MoC) and Maturity (MoM), and established the theory and concepts used to develop the first iteration of a CMM for a CR, which was then established as a baseline for further development.

6. Results and Discussion (Chapter 6): This chapter provided the results of the data captured from the questionnaire that was distributed to CR experts, with the findings analysed and discussed.

7. Modified Capability and Maturity Model for a CR (Chapter 7): This chapter described the development of a modified CMM for a CR, as achieved by factoring in results obtained from the expert review. The second iteration of a modified classified capability CR levels and a CMM for a CR was established and presented.

8. Conclusions (Chapter 8): This chapter summarises the project undertaken, addressing the initial research questions and how they were met, commenting on the significance of the research and findings, and outlining potential future work.

8.2 Research Goals

The research objectives that have been attained are associated with the research questions, as initially presented in Chapter 1. The research goals are evaluated to the degree to which they have been met. The primary research goal - defining the measures of capability maturity with their different elements as in Section 5.2 and 5.3 - has been met to a certain level of understanding. The focus was on defining the core capability elements for a CR, as in Section 3.3 and 6.3, and providing a modified CMM for a CR, as in Section 7.2. This was determined by factoring in results gained from the expert review, as in Chapter 6 and Section 7.1, towards the proposed CMM for a CR. However, the research for a CMM for a CR is novel and has stimulated an approach that can be further developed. The current findings presented in this thesis add to the areas and attributes that are to be measures for further development of metrics, which would in turn enable a more standardised measure of a CR capability maturity.

The secondary research goals aided in reaching an understanding of the primary research goal; core capabilities were determined as in Section 3.3, and by utilising the Pairwise Comparative analysis to determine the relative importance thereof, as in Section 3.4. The higher the relative importance, the more critical the core capability element, which informs the level of capability for a CR. The relative importance was then reviewed in Section 6.4 to determine the agreed-upon core capability elements for a CR and their relevance. This was synthesised into the proposed classified capability CR levels as in Section 4.3 and Appendix B, which utilised a real network topology as an inspiration, as in Section 3.5. This then enabled the establishment of a baseline criteria for CR levels, as in Section 4.2. The expert review aided in determining a consensus for the core capability elements and synthesised capability levels for a CR, as in Sections 6.3-6.6 . The maturity levels were synthesised by utilising defined CMM models identified in the literature review, as in Section 2.6, and synthesising the models, as in Section 5.3.

The maturity levels for a CR were then analysed from the expert review, as in Section 6.7, and factored into a modified CMM for a CR, as in Section 7.1.2. The results of the expert review were analysed to aid in qualitatively determining a consensus for a baseline modified CMM for a CR, as in Section 7.2. One of the main challenges in fully understanding the measuring of a CR capability maturity using the CMM for a CR was to incrementally reach a certain standardised level that is agreed upon in the CR community as a whole, in that the complexities to measure a CR are dependent on its purpose.

8.3 Contributions and Research Output

The significance of this research lies in its novel approach and focus on establishing a baseline to understand and develop a CMM for a CR, as measured against its MoC and MoM within certain determined levels. The proposed model is generic in nature

and can be adopted for different CR types and purposes, to be classified according to a certain level of capability maturity.

The research also contributes in giving a high-level view of the core capability elements for a CR which are to be considered. This has enabled the development of a baseline to classify the level of a CR. The CMM for a CR suggests a guide to develop metrics to measure a CR on different levels of capability maturity. During the research the following themes emerged that were unfortunately outside the scope of the thesis: The analysis of CRs from a quantitative view, using a CR evaluation tool, to evaluate a CR capability maturity against metrics. The legal application of a CR, due to the challenging nature of different interpretations and opinions of cyber domain laws and rules of engagement. No specific recommendation is given on the application of a CR, as this is dependent on user or client requirements. In consolidating the contribution of the research, the main research output was a focus on a novel CMM for a CR. The lessons learnt during this research include the complexities involved in developing a CMM for a CR, including how to effectively map the attributes determined to the model, and the need to get a common consensus from experts in the CR field.

8.4 Future Work

Previous chapters outline the discussions and results that have been analysed, and which have contributed to this research. However, it is the author's opinion that there is not a complete consensus on the MoC and MoM levels, the classified CR levels, or the CMM for a CR. This is due to difficulty of developing levels of capability maturity for a CR; this suggests several future areas of work that can be explored, with the following list not by any means exhaustive:

1. The standardisation of CR capability maturity measurement: to develop a standard to determine the measurement of a CR capability maturity, which will allow for a common metric to to be established for defined CR levels.

2. The establishment of a centralised CR web-based application to evaluate and measure the capability maturity of a CR according to cyber-security environmental trends, events and responses linked to industrial technological developments and standards in the area of cyber security.

3. To develop a CR evaluation tool according to standardisation of capability maturity measurements.

4. Further develop the CMM for a CR, and review maturity by evaluating the maturity of services if this would be best suited for a CMM of a CR.

5. An overview of the best approach for CR in countries: whether to adopt cloud or stack implementations for a national CR in developing countries.

6. The development of standard CR Artificial Intelligence (AI) algorithms for specific functionality for automation to augment the Next Generation CRs.

8.5 Conclusion

Drawing to the end, the proposed CMM for a CR is a conceptual model, which is utilised to measure a CR capability maturity incrementally according to defined levels. The model defines certain critical elements that are to be focused on to determine the CR's effectiveness, performance, ability to maintain cyber threats, people, processes and technology. Measuring these identified elements will aid an organisation to evaluate a CR capability maturity. Cost will always be a factor in deciding on the best approach to host a CR, whether in the cloud or in a traditional stack setup. The content and application of a CR will depend on its purpose, and according to the CR capability. Maturity of a CR through its people with cyber skills, process areas and technology allows for a more conducive environment for a CR to operate in. The qualitative value of a CR is not a clear and defined measurement, there are many factors that need to be considered and appreciated, all of which have an impact on the levels of capacity maturity of a CR. Future work will aid in clarifying a defined quantitative value for the formal evaluation of a CR against the CR MoC and MoM, using the CMM for a CR as a baseline.

References

Abbadi, Z. Security Metrics What Can We Measure. Technical report, Open Web Application Security Project (OWASP), October 2006. Accessed 17 January 2018.
URL https://www.owasp.org/images/b/b2/Security_Metics-_What_can_we_measure-_Zed_Abbadi.pdf

Adams, W. J. Minutes of the National Initiative for Cybersecurity Education (NICE) Cyber Range Sub-Working Group for Criteria of a Cyber Range. Technical report, National Initiative for Cybersecurity Education (NICE), January 2019. Accessed 25 January 2019, Submitted by the Author.

Almuhammadi, S. and Alsaleh, M. Information Security Maturity Model for NIST Cyber Security Framework. *Computer Science and Information Technology*, 51:51–62, 2017.

Alpaydin, E. Introduction to Machine Learning (Adaptive Computation and Machine Learning). The MIT Press Cambridge, Massachusetts London, England, Second edition, 2010. ISBN 978-0-262-01243-0.

Antonio, R., Douglas, S., and Hannon, D. J. Assessing the Cognitive Complexity of Cyber Range Environments. *The Journal of Defense Modeling and Simulation*, January 2019. Special Issue.
URL https://doi.org/10.1177/1548512918820654

Arsham, H. Topics in Descriptive Simulation Modeling. Electronic, 2015. Accessed 03 April 2016.
URL http://home.ubalt.edu/ntsbarsh/Business-stat/simulation/sim.htm

Astrom, K. J. and Murray, R. M. Feedback Systems: An Introduction for Scientists and Engineers. Princeton University Press, Third edition, October 2010. ISBN 978-0-691-13576-2. Version 2.10c.

Baham, C. and Kisekka, V. Applying Cyber Range Concepts of Operation to Disaster Recovery Testing. A Case Study. In *21st Americas Conference on Information Systems (AMCIS) Puerto Rico*, pages 1–5. August 2015.

Baldor, L. C. Air, Land, Sea, Cyber: North Atlantic Treaty Organization (NATO) adds Cyber to Operation Areas. Electronic, June 2016. Accessed 14 March 2019.
URL https://phys.org/news/2016-06-air-sea-cyber-nato-areas.html

Banafa, A. The Internet of Everything (IoE). Electronic, August 2016. Accessed 02 June 2018.
URL https://www.bbvaopenmind.com/en/the-internet-of-everything-ioe/

Baudrillard, J. The Hyper Realism of Simulation. Stanford University Press, 1988. ISBN 9780804714785, 143–147 pages.

Bell, T. E. Final Technical Report Project Boeing Standard Global Services (SGS). Technical report, Boeing, 2014. Accessed 29 March 2017.
URL https://www.smartgrid.gov/files/BoeingSGS_FinalTechnicalReport_10Dec2014.pdf

Bentley, L. D. and Whitten, J. L. Systems Analysis and Design for the Global Enterprise, volume 417. McGraw-Hill/Irwin, 2007. ISBN 9780071107662.

Benzel, T., Braden, R., Kim, D., Joseph, A. D., Neuman, B. C., Ostrenga, R., Stephen, S., and Sklower, K. Design, Deployment, and Use of the DETER Testbed. In *DETER Community Workshop on Cyber-Security and Test*, pages 1–8. 2007.

Beuran, R., Pham, C., Tang, D., Chinen, K.-i., Tan, Y., and Shinoda, Y. Cytrone: An integrated cybersecurity training framework, pages 157–166. SCITEPRESS Science and Technology Publications, 2017. ISBN 978-989-758-209-7.

Biscoe, C. Sophisticated Cyber Attacks are Biggest Technology Concern in 2018. Electronic, January 2018. Accessed 05 April 2019.
URL https://www.itgovernance.co.uk/blog/sophisticated_cyber_attacks_are_biggest_technology_concern_in_2018

Bishop, C. M. Pattern Recognition and Feed-Forward Networks. In *The MIT encyclopedia of the cognitive sciences*, volume 13, pages 629–632. MIT Press, 1999.

Black, P. E., Scarfone, K., and Souppaya, M. Cyber Security Metrics and Measures. In **Voeller, J. G.**, editor, *Handbook of Science and Technology for Homeland Security*, pages 1061–1067. John Wiley & Sons, Inc., July 2008. ISBN 978-0-471-76130-3.

Bodeau, D. and Graubart, R. Cyber Resilience Metrics Key Observations. Technical Report 16-0779, The MITRE Corporation, 2016. Accessed 27 November 2017.
URL https://www.mitre.org/sites/default/files/publications/pr-16-0779-cyberresilience-metrics-key-observations.pdf

Bonanni, L. Living with Hyper-Reality. Springer, 2006. ISBN 978-3-540-37788-7, 130–141 pages.

Botha, J. and De Vries, M. Towards a Capability Planning and Design Methodology for Enterprises Handling Anthropogenic Hazards. In *Computers and Industrial Engineering*, pages 229–238. July 2012.

Braje, T. M. Advanced Tools for Cyber Range. *Lincoln Laboratory*, 22(1):24–33, 2016.
URL https://www.ll.mit.edu/publications/journal/pdf/vol22_no1/22_1_2_Braje.pdf

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B. *et al.* The Malicious use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. *arXiv preprint arXiv:1802.07228*, 2018.

Buttles-Valdez, P., Svolou, A., and Valdez, F. A Holistic Approach to Process Improvement using the People CMM and the CMMI-DEV: Technology, Process, People, & Culture, the Holistic Quadripartite. In *Software Engineering Process Group (SEPG) Conference*, pages 1–84. Software Engineering Institute, 2008.
URL https://resources.sei.cmu.edu/asset_files/Presentation/2008_017_001_24459.pdf

Buyya, R., Abramson, D., and Giddy, J. An Economy Driven Resource Management Architecture for Global Computational Power Grids. In *Parallel and Distributed Processing Techniques and Applications (PDPTA) Las Vegas*, pages 26–29. June 2000.

Calheiros, R. N., Netto, M. A., Rose, C. A. D., and Buyya, R. Emusim: An Integrated Emulation and Simulation Environment for Modeling, Evaluation, and Validation of Performance of Cloud Computing Applications. *Software: Practice and Experience*, 43(5):595–612, 2013.

Caralli, R., Knight, M., and Montgomery, A. Maturity Models 101 A Primer for Applying Maturity Models to Smart Grid Security Resilience and Interoperability. Technical report, Software Engineering Institute, November 2012.
URL https://resources.sei.cmu.edu/asset_files/WhitePaper/2012_019_001_58920.pdf

Chandra, Y. and Mishra, P. K. Design of Cyber Warfare Testbed. In *Software Engineering*, pages 249–256. Springer, 2019. doi:10.1007/978-981-10-8848-3_24.

Chapaev, N. K., Akimova, O. B., Selivanov, A. V., and Shaforostova, T. V. The Activity-Based Approach to Achieving Theoretical and Practical Consensus in Pedagogy of NF Talyzina. *International Journal of Environmental and Science Education*, 11(16):8821–8833, 2016.

Chapman, J., Chinnaswamy, A., and Garcia-Perez, A. The Severity of Cyber Attacks on Education and Research Institutions: A Function of Their Security Posture. In *ICCWS 2018 13th International Conference on Cyber Warfare and Security*, pages 111–116. Academic Conferences and Publishing Limited, 2018.

Chie, S. Can Level of Information Systems Interoperability (LISI) Improve DOD C4i Systems Interoperability? Master's thesis, Naval Postgraduate School. Monterey, California, 2001.

Cisco. Cisco IOS NetFlow. Electronic, 2019. Accessed 07 May 2019.
URL https://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-netflow/index.html

Claise, B. Cisco Systems Netflow Services Export Version 9. Technical Report RFC 3954, Internet Engineering Task Force (IETF), 2004.
URL https://tools.ietf.org/html/rfc3954

Cloppert, M. Security Intelligence: Attacking the Cyber Kill Chain. *SANS Computer Forensics*, October 2009.
URL https://digital-forensics.sans.org/blog/2009/10/14/security-intelligence-attacking-the-kill-chain

CMMI Team. CMMI for Development Version 1.3. Technical Report CMU/SEI-2010-TR-034, Carnigie Mellon Software Engineering Process Management Program, November 2010.
URL https://resources.sei.cmu.edu/asset_files/TechnicalReport/2010_005_001_15287.pdf

Coetzee, D. Visualisation of PF Firewall Logs Using Open Source. Master's thesis, Rhodes University, 2015.

Compute Scotland. Cyber Threat Landscape Protection. Electronic, September 2015. Accessed 21 September 2018.
URL https://www.computescotland.com/cyber-threat-landscape-protection-8200.php

Conklin, W. A. and Kohnke, A. Cyber Resilience: An Essential new Paradigm for Ensuring National Survival. In *ICCWS 2018 13th International Conference on Cyber Warfare and Security*, pages 126–130. Academic Conferences and Publishing Limited, 2018.

Constantinescu, R. and Iacob, I. M. Capability Maturity Model Integration CMMi. *Journal of Applied Quantitative Methods*, 2(1):31–37, 2007.

Conway, G. Technical Infrastructure Management: Insights in the Digital Context. Technical report, Innovation Value Institute, 2018.
URL http://mural.maynoothuniversity.ie/9389/

Cooper, H. How Systems Security Engineering (SSE) Addresses Cyber Seucrity Risk Management Framework (Cyber-RMF) For Test & Evaluation (T&E) Project Management. Electronic, May 2018. Accessed 10 May 2019.
URL https://www.itea.org/wp-content/uploads/2018/05/SSE-Addresses-Cyber-RMF-for-TE-Project-Mgmt.pdf

Curtis, B., Hefley, B., and Miller, S. People Capability Maturity Model (P-CMM) version 2.0. Technical Report Second Edition, Carnegie Mellon University Pittsburgh, Pennsylvania Software Engineering Institute, 2009.
URL https://resources.sei.cmu.edu/asset_files/TechnicalReport/2009_005_001_15095.pdf

Damodaran, S. and Smith, K. CRIS Cyber Range Lexicon, Version 1.0. Technical report, Massachusetts Institute of Technology (MIT) Lexington Lincoln Laboratory, 2015.
URL https://apps.dtic.mil/dtic/tr/fulltext/u2/a627477.pdf

Damodaran, S. K. and Couretas, J. M. Cyber Modeling and Simulation for Cyber Range Events. In *Proceedings of the Conference on Summer Computer Simulation*, SummerSim 2015, pages 1–8. Society for Computer Simulation International, San Diego, CA, USA, 2015. ISBN 978-1-5108-1059-4.

DARPA. The National Cyber Range: A National Testbed for Critical Security Research. Technical report, Defence Advanced Research Project Agency (DARPA), 2008. Accessed 03 July 2017.
URL https://obamawhitehouse.archives.gov/files/documents/cyber/DARPA-NationalCyberRange_FactSheet.pdf

Davis, J. and Magrath, S. A Survey of Cyber Ranges and Testbeds. Technical report, Defence Science and Technology Organisation Australia, 2013.
URL https://apps.dtic.mil/dtic/tr/fulltext/u2/a594524.pdf

Defence Science Board Task Force. Resilient Military Systems and the Advanced Cyber Threat. Electronic, January 2013. Accessed 21 September 2018.
URL https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-081.pdf

Defense Acquisition University. DOTmLPF-P Analysis. Electronic, June 2005. Accessed 11 January 2017.
URL https://www.dau.mil/acquipedia/Pages/ArticleDetails.aspx?aid=d11b6afa-a16e-43cc-b3bb-ff8c9eb3e6f2

Deloitte. Responding to Cyber Threats in the New Reality a Shift in Paradigm is Vital. Electronic, 2015. Accessed 05 April 2019.
URL https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-thought-leadership-noexp.pdf

Denning, D. E. Rethinking the Cyber Domain and Deterrence. *Joint Force Quarterly (JFQ)*, 77(2nd Quarter):8–15, 2015.

DOD Republic of Korea. South Korea Defense White Paper. Electronic, 2012. Accessed 21 September 2018.

URL https://www.scribd.com/document/269491725/South-Korea-Defense-White-Paper-2012

Donovan, P. J., McLamb, J. W., Okhravi, H., Riordan, J., and Wright, C. V. Quantitative Evaluation Of Moving Target Technology. In *2015 IEEE International Symposium on Technologies for Homeland Security (HST)*, pages 1–7. IEEE, 2015. doi:10.1109/THS.2015.7225289.

Eborn, K. Pentagon Plans more Anti-Hacker Cyber Ranges. Electronic, March 2017. Accessed 21 October 2017.
URL https://about.bgov.com/blog/pentagon-plans-anti-hacker-cyber-ranges/

Edgar, T. W. and Manz, D. O. Research Methods for Cyber Security. Syngress, 2017. ISBN 978-0-12-805349-2.

Edwards, D. What is DevOps? Electronic, February 2010. Accessed 20 August 2019.
URL http://dev2ops.org/2010/02/what-is-devops/

Elite, O. Learning Management Systems. Electronic, 2019. Accessed 07 May 2019.
URL https://elite.co.za/lms-design-development/

ENISA. ENISA Threat Landscape Report 2018. Technical report, European Union Agency for Network and Information Security (ENISA), 2018. Accessed 16 July 2019.
URL https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018/at_download/fullReport

Ericsson, A. Deliberate Practice And Acquisition Of Expert Performance: A General Overview. *Academic Emergency Medicine*, 15(11):988–994, 2008.

Estonian Ministry of Defence. Cyber Range Digital Library Study. Technical report, Estonian Ministry of Defence, 2017. Accessed 03 September 2018.
URL http://www.etag.ee/wp-content/uploads/2018/04/CR-Digital-Library-Study_aruanne_KaM.pdf

European Cyber Security. European Cyber Security Strategic Research and Innovation Agenda for a Contractual Public, Private, Partnership. Technical report, European Cyber Security, June 2016. Accessed 18 September 2018.
URL https://ecs-org.eu/documents/ecs-cppp-sria.pdf

European Defence Agency. Cyber Ranges EDA's First Ever Cyber Defence Pooling and Sharing Project Launched By 11 Member States. Electronic, May 2017. Accessed 10 April 2017.
URL https://www.eda.europa.eu/info-hub/press-centre/latest-news/2017/05/12/cyber-ranges-eda-s-first-ever-cyber-defence-pooling-sharing-project-launched-by-11-member-states

Ferguson, B., Tall, A., and Olsen, D. National Cyber Range Overview. In *Military Communications Conference (MILCOM)*, pages 123–128. IEEE, 2014. doi:10.1109/MILCOM.2014.27.

FoodRisc. Mixed Method Research. Electronic, 2016. Accessed 18 March 2019.
URL http://resourcecentre.foodrisc.org/mixed-methods-research_185.html

Fowler, M. Maturity Model. Electronic, August 2014. Accessed 07 May 18.
URL https://martinfowler.com/bliki/MaturityModel.html

Fox, D., McCollum, C., Arnoth, E., and Mak, D. Cyber Wargaming: Framework for Enhancing Cyber Wargaming with Realistic Business Context. Technical report, Homeland Security Systems Engineering and Development Institute (HSSEDI), The MITRE Corporation, August 2018.
URL https://www.mitre.org/sites/default/files/publications/pr_18-1636-ngci-cyber-wargaming.pdf

Franke, U. and Brynielsson, J. Cyber Situational Awareness - A Systematic Review of the Literature. *Computers and Security*, 46:18–31, 2014.

Frost, B. Measuring Performance: Using the New Metrics to Deploy Strategy and Improve Performance. Measurement International, Second edition, 2000. ISBN 978-0970247117.

Fulp, J. Training the Cyber Warrior. In *IFIP World Conference on Information Security Education*, pages 261–273. Springer, June 2003.

Garrido, J. Introduction to Elementary Computational Modeling: Essential Concepts, Principles, and Problem Solving. CRC Press, 2011. ISBN 978-1439867396.

Gartner. Gartner Hype Cycle. Electronic, 2018. Accessed 14 March 2019.
URL https://www.gartner.com/en/research/methodologies/gartner-hype-cycle

Godwin, J., Kulpin, A., Rauscher, K. F., and Yaschenko, V. Critical Terminology Foundations 2: Russia and US Bilateral on Cybersecurity. Technical report, East-West Institute, 2014.
URL https://www.files.ethz.ch/isn/178418/terminology2.pdf

Gove, R. and Uzdzinski, J. A Performance Based System Maturity Assessment Framework. *Procedia Computer Science*, 16:688–697, 2013.

Goverment of Austria. Austrian Cyber Security Strategy (2013). Technical report, Goverment of Austria, 2013. Accesed 20 September 2018.
URL https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/austrian-cyber-security-strategy

Goverment of Canada. Canada Cyber Security Strategy: For a stronger and more prosperous Canada. Technical report, Goverment of Canada, 2010.
URL http://publications.gc.ca/collections/collection_2010/sp-ps/PS4-102-2010-eng.pdf

Goverment of Finland. Finland Cyber Security Strategy. Technical Report Government Resolution 24.1.2013, Finland Secretariat of the Security Committee, 2013. Accessed 20 September 2018.
URL https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf

Goverment of Montenegro. National Cyber Security Strategy for Montenegro 2013-2017. Technical report, Goverment of Montenegro, 2013. Accessed 21 September 2018.
URL http://www.mid.gov.me/ResourceManager/FileDownload.aspx?rid=165416&rType=2&file=Cyber+Security+Strategy+for+Montenegro.pdf

Goverment of Quatar. Qatar National Cyber Security Strategy. Technical report, Goverment of Quatar, May 2014. Accessed 21 September 2018.
URL http://www.motc.gov.qa/sites/default/files/national_cyber_security_strategy.pdf

Gregg, M. CISSP Exam Cram 2. Que Corporation, First edition, 2005. ISBN 9780789738066.

Grobelnik, M. Big Data Tutorial. Technical report, Jozef Stefan Institute, 2012.
URL http://www.planet-data.eu/sites/default/files/presentations/Big_Data_Tutorial_part4.pdf

Guardtime. Guardtime Awarded Contract for Next Generation NATO Cyber Range. Electronic, February 2017. Accessed 14 March 2019.
URL https://guardtime.com/blog/guardtime-awarded-contract-for-nato-cyber-range

Guzman, G. Security Implications of National Development of Strategic, Ideational Cyberpower. In *ICCWS 2018 13th International Conference on Cyber Warfare and Security*, pages 530–532. Academic Conferences and Publishing Limited, 2018.

Haron, A., Sahibuddin, S., Harun, M., Zakaria, N., and Mahrin, M. The Important Role of People, Process and Technology during Software Project Requirement. *International Journal of Machine Learning and Computing*, 3(1):24, 2013.

Heller, B. Reproducible Network Research with High-Fidelity Emulation. Ph.D. thesis, Stanford University, 2013.

Henninger, A. E., Dannie, C., Margaret, L., Robert, L., Robert, R., Randy, S., and Steve, S. Live Virtual Constructive Architecture Roadmap (LVCAR) Final Report. Technical report, Institute for Defense Analysis, September 2008.

Herbert, A. Bolvedere: A Scalable Network Flow Threat Analysis System. Ph.D. thesis, Rhodes University, 2018. doi:10.13140/RG.2.2.13934.66888.

Hurley, J. S. Beyond the Struggle: Artificial Intelligence in the Department of Defense (DoD). In *ICCWS 2018 13th International Conference on Cyber Warfare and Security*, pages 297–303. Academic Conferences and Publishing Limited, 2018.

Hutchins, E. M., Cloppert, M. J., and Amin, R. M. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. *Leading Issues in Information Warfare & Security Research*, 1(1):80, 2011.

Hwang, N. J. and Bush, K. B. Operational Exercise Integration Recommendations for DoD Cyber Ranges. Technical Report 1187, Massachusetts Instiute of Technology Lexington Lincoln Lab, 2015.
URL `https://www.ll.mit.edu/sites/default/files/publication/doc/2018-04/2015-Hwang-TR-1187.pdf`

IEEE Institute. IEEE Standard for Local and Metropolitan area Networks: Port-Based Network Access Control. Electronic, February 2010.

Irwin, B. V. W. A Framework for the Application of Network Telescope Sensors in a Global IP Network. Ph.D. thesis, Rhodes University, 2011.
URL `http://nrfnexus.nrf.ac.za/handle/20.500.11892/21351`

Irwin, B. V. W. Standing Your Ground: Current and Future Challenges in Cyber Defense, chapter 6, pages 100–108. Information Security in Diverse Computing Environments, IGI Global, June 2014. ISBN 9781466661585.
URL `https://www.igi-global.com/chapter/standing-your-ground/114372`

ISO Institute. Information Technology Security Techniques Evaluation Criteria for IT security Part 1: Introduction and General Model. Electronic, 2009a.

ISO Institute. Information Technology Security Techniques Information Security Management Systems: Overview and Vocabulary. Electronic, 2009b.

ISO Institute. Systems and Software Engineering: Architecture Description. Electronic, December 2011a.

ISO Institute. Systems and Software Engineering Systems and Software Quality Requirements and Evaluation: System and Software Quality Models. Electronic, March 2011b.

ISO Institute. Information Technology Security Techniques Guidelines for Cyber Security. Electronic, July 2012a.

ISO Institute. Information Technology Security Techniques Guidelines for Cybersecurity. Electronic, April 2012b. Accessed 23 July 2018.

ISO Institute. Selection and use of the ISO 9000 family of standards. Electronic, 2016. Accessed 08 August 2018.
URL https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100208.pdf

ITU Institute. Overview of Cybersecurity. Electronic, April 2008.
URL https://www.itu.int/rec/dologin_pub.asp?lang=f&id=T-REC-X.1205-200804-I!!PDF-E&type=items

Jansen van Vuuren, J. C. and Leenen, L. A Model for Measuring Perceived Cyberpower. In *ICCWS 2018 13th International Conference on Cyber Warfare and Security*, pages 320–327. Academic Conferences and Publishing Limited, 2018.

Johnson, J. and Henderson, A. Conceptual Models: Begin by Designing what to Design. *Interactions*, 9(1):25–32, 2002.

Jones, A., Angelopoulou, O., Vidalis, S., and Janicke, H. The 2016 Hard Disk Study on Information Vailable on the Second Hand Market in the UK. In *European Conference on Cyber Warfare and Security*, pages 193–199. Academic Conferences International Limited, 2017.

Kaminski, J. Diffusion of Innovation Theory. *Canadian Journal of Nursing Informatics*, 6(2):1–6, 2011.

Karlzén, H. An Analysis of Security Information and Event Management Systems. Master's thesis, University of Gothenburg, 2009.

Kasunic, M. Measuring Systems Interoperability Challenges and Opportunities. Technical report, Software Engineering Institute, 2001.
URL http://www.dtic.mil/get-tr-doc/pdf?AD=ADA400176

Kick, J. Cyber Exercise Playbook. Technical Report MP140714, The Massachusetts Institute of Technology Research & Engineering (MITRE), November 2014. Accessed 08 February 2017.
URL http://www.mitre.org/sites/default/files/publications/pr_14-3929-cyber-exercise-playbook.pdf

Kiemele, M. J., Schmidt, S. R., and Berdine, R. J. Basic statistics: Tools for Continuous Improvement. Air Academy Press, Fourth edition, 1997. ISBN 978-1880156063.

Knowww. Can "Cyber Security" and "Information Security" be used Interchangeably? Electronic, 2017. Accessed 20 November 2018.
URL https://knowww.eu/nodes/5bd5c2e5e5403a7b2da1009d

Kulpa, M. K. and Johnson, K. A. Interpreting the CMMI (R): A Process Improvement Approach. Auerbach Publications, Second edition, March 2008. ISBN 9780429151392.

Labuschagne, W. A. and Grobler, M. Developing a Capability to Classify Technical Skill levels within a Cyber Range. In *ECCWS 2017 16th European Conference on Cyber Warfare and Security*, pages 224–234. Academic Conferences and Publishing Limited, 2017.

Labuschagne, W. A. and Veerasamy, N. Metrics for Smart Security Awareness. In *ECCWS 2017 16th European Conference on Cyber Warfare and Security*, pages 235–242. Academic Conferences and Publications Limited, 2017.

Langer, R. Cyber Power: An Emerging Factor in National and International Security. *Journal of International Relations and sustainable development. HORIZONS: Global Security Challenges, Autumn*, 8, 2016.

Le, N. T. and Hoang, D. B. Can Maturity Models Support Cyber Security? In *2016 IEEE 35th International Performance Computing and Communications Conference (IPCCC)*, pages 1–7. IEEE, 2016.

Levison, D. Open vs. Closed Archutecture Technology Systems. Electronic, February 2019. Accessed 13 May 2019.
URL https://commissiontrac.com/the-difference-in-open-architecture-vs-closed-architecture-technology-systems/

Lewis, R., Strachan, A., and Smith, M. M. Is High Fidelity Simulation the Most Effective Method for the Development of Non-Technical Skills in Nursing? A Review of the Current Evidence. *The Open Nursing Journal*, 6:82–89, 2012. doi: 10.2174/1874434601206010082.

Lockheed Martin. Gaining the Advantage Applying Cyber Kill Chain Methodology to Network Defence. Technical report, Lockheed Martin, 2015. Accessed 16 April 2019.
URL https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf

Mai, T. Technology Readiness Level. Electronic, October 2012. Accessed 20 September 2018.
URL https://www.nasa.gov/directorates/heo/scan/engineering/technology/txt_accordion1.html

Mammadov, S. High Fidelity Adaptive Cyber Emulation. Ph.D. thesis, Florida Institute of Technology, 2017.

Mateski, M., Trevino, C. M., Veitch, C. K., Michalski, J., Harris, J. M., Maruoka, S., and Frye, J. Cyber Threat Metrics. Technical Report SAND2012-2427, Sandia National Laboratories, March 2012.
URL https://fas.org/irp/eprint/metrics.pdf

Maurer, T. and Morgus, R. Compilation of Existing Cybersecurity and Information Security Related Definitions. Technical report, New America Open Technology

Institute, October 2014. Accessed 18 September 2018.
URL https://www.giplatform.org/sites/default/files/Compilation%20of%20Existing%20Cybersecurity%20and%20Information%20Security%20RelatedDefinition.pdf

Mavroeidis, V. and Bromander, S. Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards and Ontologies within Cyber Threat Intelligence. In *European Intelligence and Security Informatics Conference (EISIC)*, pages 91–98. IEEE, 2017. doi:10.1109/EISIC.2017.20.

Mead, N. The Common Criteria. US CERT, July 2013. Accessed 20 June 2017.
URL https://www.us-cert.gov/bsi/articles/best-practices/requirements-engineering/the-common-criteria

Merriam Webster. Metric. Electrionic, 2018. Accessed 10 April 2018.
URL http://www.merriam-webster.com/dictionary/metric

Mindtools. Paired Comparision Analysis: Working Out Relative Importance. Electronic, 2018. Acessed 02 May 2018.
URL https://www.mindtools.com/pages/article/newTED_02.htm

Mitchell, J. A. Measuring the Maturity of a Technology: Guidance on assigning a TRL. Technical report, Sandia National Laboratories, October 2007.
URL https://cfwebprod.sandia.gov/cfdocs/CompResearch/docs/TRL-Guidance-final.pdf

MITRE. Assessing Technical Maturity Systems Engineering Guide. Electronic, 2018. Accessed 13 March 2018.
URL https://www.mitre.org/publications/systems-engineering-guide/acquisition-systems-engineering/acquisition-program-planning/assessing-technical-maturity

Moore, D., Shannon, C., Voelker, G., Savage, S. *et al.* Network Telescopes: Technical Report. Technical report, Cooperative Association for Internet Data Analysis (CAIDA), 2004.
URL http://www.caida.org/publications/papers/2004/tr-2004-04/tr-2004-04.pdf

Moore, T., Friedman, A., and Procaccia, A. D. Would a 'Cyber Warrior' Protect Us: Exploring Trade-offs Between Attack and Defense of Information Systems. In *Proceedings of the 2010 New Security Paradigms Workshop*, NSPW '10, pages 85–94. ACM, New York, NY, USA, 2010. ISBN 978-1-4503-0415-3. doi:10.1145/1900546.1900559.

Mosleh, M., Dalili, K., and Heydari, B. Distributed or Monolithic? A Computational Architecture Decision Framework. *IEEE Systems Journal*, 12(1):125–136, 2016. doi:10.1109/JSYST.2016.2594290.

Murphy, K. P. Machine Learning: A Probabilistic Perspective. MIT Press, 2012. ISBN 9780262018029.

Newhouse, B., Keith, S., Scribner, B., and Witte, G. National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NCWF). Electronic, November 2016.

NICT. Next Generation Testbed JGN-X. Electronic, 2016. Accessed 09 February 2017.
URL http://www.jgn.nict.go.jp/jgn-x_archive/english/info/what-is-jgn-x.html

NIST. Security and Privacy Controls for Federal Information Systems and Organizations. Technical Report NIST SP 800-53, CNISS, April 2013. Accessed 20 September 2018.
URL https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final

NIST. The Cyber Range: Guide. Electronic, 2015. Accessed 14 August 2018.
URL https://www.nist.gov/document/cyber-range-guide

NIST. Cyber Ranges. Electronic, 2017. Accessed 02 April 2019.
URL https://www.nist.gov/sites/default/files/documents/2018/02/13/cyber_ranges.pdf

NIST Institute. Technical Guide to Information Security Testing and Assessment. Electronic, September 2008.
URL https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

NIST Institute. Computer Security Incident Handling Guide. Electronic, August 2012.
URL https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

NIST Institute. Glossary of Key Information Security Terms. Electronic, May 2013.
URL https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

Oltsik, J. Research Suggests Cyber Security Skills Shortage is Getting Worse. Cybersecurity Snippets, January 2018. Accessed 17 October 2018.
URL https://www.esg-global.com/blog/esg-research-suggests-cybersecurity-skills-shortage-is-getting-worse

Oltsik, J., Cahill, D., and Lundell, B. Cyber security Skills Shortage: A State of Emergency. Electronic briefing, February 2016. Accessed 03 September 2018.
URL http://www.esg-global.com/hubfs/ESG-Brief-Cybersecurity-Skills-Shortage-Feb-2016.pdf

Ošlejšek, R., Toth, D., Eichler, Z., and Burská, K. Towards a Unified Data Storage and Generic Visualizations in Cyber Ranges. In *16th European Conference on Cyber Warfare and Security (ECCWS)*, pages 298–306. Academic Conferences and Publishing Limited, 2017.

Ošlejšek, R., Vykopal, J., Burská, K., and Rusňák, V. Evaluation of Cyber Defense Exercises Using Visual Analytics Process. In *48th Frontiers in Education (FIE) Conference*. IEEE, 2018. doi:10.1109/FIE.2018.8659299.

Oxford University. Cyber Security Capability Maturity Model (CMM) Version 1.2. Technical report, Global Cyber Security Capacity Centre, December 2014. Accessed 08 July 2017.
URL `https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20Version%201_2_0.pdf`

Page, L. Blighty to get own Cyber Range. Electronic, December 2009. Accessed 08 February 2017.
URL `http://www.theregister.co.uk/2009/12/18/uk_cyber_range/`

Pahi, T., Leitner, M., and Skopik, F. Data exploitation at large: Your way to adequate cyber common operating pictures. In *Proceedings of the 16th European Conference on Cyber Warfare and Security*, pages 307–315. 2017.

Paulk, M. C., Curtis, B., Chrissis, M. B., and Weber, C. V. Capability Maturity Model for Software, Version 1.1. Technical Report CMU/SEI-93-TR-24, Software Engineering Institute (SEI), February 1993.
URL `https://resources.sei.cmu.edu/asset_files/TechnicalReport/1993_005_001_16211.pdf`

Pridmore, L., Lardieri, P., and Hollister, R. National Cyber Range (NCR) Automated Test Tools: Implications and Application to Network-Centric Support Tools. In *2010 IEEE Autotestcon*, pages 1–4. Sept 2010. ISSN 1088-7725. doi: 10.1109/AUTEST.2010.5613581.

Priyadarshini, I. Features and Architecture of the Modern Cyber Range: A Qualitative Analysis and Survey. Ph.D. thesis, University of Delaware, 2018.

Protect, E. External vs. Internal Cybersecurity Risks: Know the Difference. Electronically, April 2019. Accessed 16 April 2019.
URL `https://ermprotect.com/blog/external-vs-internal-cybersecurity-risks-know-difference/`

Rabinovich, D., Genah, M., and Gartsbein, A. Reducing Input/Output (I/O) Operations for Centralized Backup and Storage. Electronic, July 2018. US Patent App. 10/037,252.

Rege, A., Obradovic, Z., Asadi, N., Parker, E., Pandit, R., Masceri, N., and Singer, B. Predicting adversarial cyber-intrusion stages using autoregressive

neural networks. *IEEE Intelligent Systems*, 33(2):29–39, Mar 2018. ISSN 1541-1672. doi:10.1109/MIS.2018.111145153.

Reith, M., Trias, E., Dacus, C., Martin, S., and Tomcho, L. Rethinking USAF Cyber Education and Training. In *ICCWS 2018 13th International Conference on Cyber Warfare and Security*, pages 439–447. Academic Conferences and Publishing Limited, 2018.

Robinson, M., Jones, K., Janicke, H., and Maglaras, L. An Introduction to Cyber Peacekeeping. *Journal of Network and Computer Applications*, 114:70–87, 2018. ISSN 1084-8045. doi:10.1016/j.jnca.2018.04.010.

Salah, D., Paige, R., and Cairns, P. An Evaluation Template For Expert Review Of Maturity Models. In *International Conference on Product Focused Software Process Improvement*, pages 318–321. Springer, 2014. doi:10.1007/978-3-319-13835-0_31.

SANReN. South African National Research Network (SANRen) Backbone Map: Geographical. Electronic, 2018. Accesssed 26 February 2018.
URL `https://www.sanren.ac.za/backbone`

Schiess, C. Emulation: Debug it in the lab not on the floor. In *Proceedings of the 33nd conference on Winter Simulation*, pages 1463–1465. IEEE Computer Society, 2001. doi:10.1109/WSC.2001.977471.

Schmidt, K. Cyber Kill Chain: Hope or Hype? Electronic, August 2013. Accessed 14 March 2019.
URL `http://www.onthenetgang.com/2013/08/cyber-kill-chain-hope-or-hype.html`

Schmitt, M. N. Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press, Reprint edition, April 2013. ISBN 978-1107613775. doi:10.1017/CBO9781139169288.

Schreuders, Z. C., Shaw, T., Shan-A-Khuda, M., Ravichandran, G., Keighley, J., and Ordean, M. Security Scenario Generator (SecGen): A Framework for Generating Randomly Vulnerable Rich-scenario VMs for Learning Computer Security and Hosting (CTF) Events. In *Workshop on Advances in Security Education (ASE)*, pages 1–10. USENIX Association, August 2017.

Security. Cybersecurity Skills Crisis Causing Rapidly Widening Business Problem. Electronic, November 2017. Accessed 21 September 2018.
URL `https://www.securitymagazine.com/articles/88480-cybersecurity-skills-crisis-causing-rapidly-widening-business-problem`

Shamsi, J. A., Zeadally, S., Sheikh, F., and Flowers, A. Attribution in Cyberspace: Techniques and Legal Implications. *Security and Communication Networks*, 9(15):2886–2900, April 2016. ISSN 1939-0122. doi:10.1002/sec.1485.

Simon, P. and Graham, S. Potential Privacy Ramifications of Modern Vehicle Software and Firmware. In *16th European Conference on Cyber Warfare and Security (ECCWS)*, pages 452–458. Academic Conferences and Publishing Limited, 2017.

Smith, C. and Oosthuizen, R. Applying Systems Engineering Principles Towards Developing Defence Capabilities. *ISEM 2011 Proceedings. Stellenbosch, South Africa*, September 2011. doi:10.1002j.2334-5837.2012.

Spacey, J. What is Affective Computing? Electronic, 2016. Accessed 19 April 2019.
URL https://simplicable.com/new/affective-computing

Spacey, J. Architecture vs Design: The Difference Explained. Electronic, 2017. Accessed 19 April 2019.
URL https://simplicable.com/new/architecture-vs-design

Spirent. Operational Impact of Cyber Range Elements Simulations and Realism. Technical report, Spirent, 2017.
URL https://www.spirent.com/~/media/White%20Papers/Broadband/PAB/Cyber_Range_WhitePaper

Spirkin, A. Philosophy As A World-View And A Methodology. Progress Publishers, 1983. Accessed 07 October 2018.
URL https://www.marxists.org/reference/archive/spirkin/works/dialectical-materialism/ch01.html

Sproles, N. Coming to Grips with Measures of Effectiveness. *Systems Engineering*, 3(1):50–58, 2000.

Sproles, N. The Difficult Problem Of Establishing Measures Of Effectiveness For Command and Control: A Systems Engineering Perspective. *Systems Engineering*, 4(2):145–155, 2001.

Sreenivasamurthy, K. Software Defined Storage or Hyperconverged Infrastructure. May 2018. Accessed 18 September 2018.
URL https://thenewstack.io/software-defined-storage-or-hyperconverged-infrastructure/

Stefan, D., Walter, B., William, Y., and Massimo, R. Cybersecurity Meets IT Risk Management. Electronically, September 2014. Accessed 16 April 2019.
URL https://www.bcg.com/publications/2014/technology-strategy-organization-cybersecurity-meets-it-risk-management.aspx

Stevens, M. Cybersecurity verses Information Security Is there a Difference? Electronic, March 2016. Accessed 29 March 2017.
URL https://www.bitsighttech.com/blog/cybersecurity-vs-information-security

Stillions, R. The Detection Maturity Level Model (DML) Model. Electronic, April 2014. Accessed 17 May 2018.
URL http://ryanstillions.blogspot.com/2014/04/the-dml-model_21.html

Strickland, J. How Hackers Work. Electronic, 2017. Accessed 31 March 2017.
URL https://computer.howstuffworks.com/hacker.htm

Su, X. Introduction to Big Data. Technical Report IINI3012, Norwegian University of Science and Technology, 2012.
URL https://www.ntnu.no/iie/fag/big/lessons/lesson2.pdf

Subhalakshmi, G. The Absolute Guide to SIEM. Electronic, 2018. Accessed 02 July 2019.
URL https://www.manageengine.com/log-management/the-absolute-guide-to-siem.pdf

Summers, J. Black Swan Events Popular Misconseptions. Institute of Risk management Northe West England, January 2012. Accessed 07 May 2019.
URL https://www.theirm.org/media/1120524/Popular-misconceptions-about-blackswan-events-JohnSummers.pdf

Surbhi, S. Difference between Assessment and Evaluation? Electronic, October 2017. Accessed 27 March 2017.
URL https://keydifferences.com/difference-between-assessment-and-evaluation.html

TechGenix. Must have Cybersecurity Skills that Make You an in Demand Expert. Electronic, October 2018. Accessed 20 November 2018.
URL http://techgenix.com/cybersecurity-skills/

Thaba, J. M. Technology Support for Military Capability Based Acquisition. In *2017 International Association for Management of Technology (IAMOT) Conference Proceedings*, pages 1–10. 2017.
URL https://researchspace.csir.co.za/dspace/bitstream/handle/10204/9450/Thaba_19264_2017.pdf?sequence=1

Thalheim, B. Towards a Theory of Conceptual Modelling. *Journal of Universal Computer Science*, 16(20):3102–3137, 2010. doi:10.1007/978-3-642-04947-7_7.

Thalheim, B. The Science And Art Of Conceptual Modelling. In *Transactions on Large Scale Data and Knowledge Centered Systems VI*, pages 76–105. Springer, 2012. doi:10.1007/978-3-642-34179-3_3.

Thalheim, B. The Conception of the Model. In **Abramowicz, W.**, editor, *Business Information Systems*, pages 113–124. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013. ISBN 978-3-642-38366-3. doi:10.1007/978-3-642-38366-3_10.

Thalheim, B. and Dahanayake, A. A Conceptual Model For Services. In *International Conference on Conceptual Modeling*, pages 51–61. Springer, 2015.

Thalheim, B. and Tropmann-Frick, M. Enhancing Entity-relationship Schemata For Conceptual Database Structure Models. In *International Conference on Conceptual Modeling*, pages 603–611. Springer, 2015. doi:10.1007/978-3-319-25264-3_47.

Thalheim, B. and Tropmann-Frick, M. Models and their Capability Computational Models of Rationality. *College Publications Series*, 29:34–56, 2016.

Threat Analysis Group. Threat, Vulnerability, Risk Commonly Mixed up Terms. Electronic, May 2010. Accessed 18 September 2018.
URL https://www.threatanalysis.com/2010/05/03/threat-vulnerability-risk-commonly-mixed-up-terms/

TMRC. National Cyber Range Overview. Technical report, Test Management Research Centre (TMRC), February 2015. Accessed 02 July 2017.
URL https://www.acq.osd.mil/dte-trmc/docs/20150224_NCR%20Overview_DistA.pdf

TRAK-Community. Defence Line of Development. 2010. Accessed 13 October 2017.
URL http://trak-community.org/index.php/wiki/Defence_Line_of_Development

Tsukida, K. and Gupta, M. R. How to Analyze Paired Comparison Data. Technical report, Washington University Seattle Department of Electrical Engineering, 2011.
URL https://apps.dtic.mil/dtic/tr/fulltext/u2/a543806.pdf

UK Goverment. Defence Minister Opens UK Cyber Security Test Range. Electronically, October 2010. Accessed 06 May 2018.
URL https://www.gov.uk/government/news/defence-minister-opens-uk-cyber-security-test-range

USDOD. Cybersecurity Test and Evaluation Guidebook. Electronic, July 2015. Accessed 13 September 2018.
URL http://www.dote.osd.mil/docs/tempguide3/cybersecurity_te_guidebook_july1_2015_v1_0.pdf

USDOD. Cybersecurity Test and Evaluation Guidebook. Electronic, July 2018. Accessed 14 October 2018.
URL https://www.acq.osd.mil/dte-trmc/docs/CSTE%20Guidebook%202.0_FINAL%20(25APR2018).pdf

Valdez, B., Svolou, A., and Valdez, F. A Holistic Approach to Process Improvement Using the People CMM and the CMMi-DEV: Technology Process, People and

Culture, The Holistic Quadripartite. Techreport, Software Engineering Institute, 2008.
URL https://resources.sei.cmu.edu/asset_files/Presentation/2008_017_001_24459.pdf

van Haaster, J. Assessing Cyber Power. North Atlantic Treaty Organization (NATO) Cooperative Cyber Defence Centre (CCDCOE) Publications, Eighth edition, 2016. ISBN 978-9949-9544-9-0, 7–21 pages.

Verizon. 2018 Data Breach Investigations Report. Investigation report, 2018. Accessed 16 July 2019.
URL https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf

Vill, M. Guardtime Awarded Contract for Next Generation NATO Cyber Range. Electronic, February 2018. Accessed 13 March 2018.
URL https://guardtime.com/blog/guardtime-awarded-contract-for-nato-cyber-range

Wehner, S., Elkouss, D., and Hanson, R. Quantum Internet: A Vision for the Road Ahead. *Science*, 362(6412):1–10, 2018. doi:10.1126/science.aam9288.

Wheeler, D. A. and Larsen, G. N. Techniques for Cyber Attack Attribution. Technical report, Institute for Defense Analyses Alexandria Virginia, 2003.
URL http://www.dtic.mil/docs/citations/ADA468859

Whiting School of Engineering. Explaining KPPs, KSAs, MOEs, and MOPs. Electronic, November 2013. Accessed 06 June 2018.
URL https://ep.jhu.edu/about-us/news-and-media/explaining-kpps-ksas-moes-and-mops

Wiegers, K. E. Misconceptions of The Capability Maturity Model. *Software Development Magazine*, 4(11):57–64, 1996.

Zeltser, L. What is an Information Security Expert? Electronic, 2017. Accessed 29 March 2018.
URL https://zeltser.com/what-is-an-infosec-expert/

A

Cyber Ranges Globally

The table below indicates the types of CR globally, this is by no means and the entire list of CR globally, for further views on CRs read Davis and Magrath (2013), Priyadarshini (2018).

Types of Cyber Range	Date Build	Location	Developed By	Type of CR (Public, Military, Other)	Remarks
National CR (NCR) TMRC (2015)	2009	USA	DOD (DARPA) (TCMC)	Military	Emulation of 40 000 nodes with high fidelity. Consistent upgrades implemented
United Kingdom(UK) Cyber Range (UK Goverment, 2010) SATURN (Self-organising Adaptive Technology Under Resilient Networks). 2009 (Page, 2009)	2010	Northrop Grumman Corporation's Fareham facility	Northrop Grumman	Military and Public	UK range is federated with the existing US Cyber Range in Northrop Grumman's Cyber Space Solutions Centre (CSSC) in Maryland

Types of Cyber Range	Date Build	Location	Developed By	Type of CR (Public, Military, Other)	Remarks
Arizona Cyber Warfare Range Arizona Cyber Warfare Range (AZCWR)[1]	Feb 2012 Aug 2017	East side range , East valley in Mesa and West side range Grand Canyon University campus	Group of Volunteers non profit organisation in Arizona	Private	Live fire Exercises operated by Volunteers
The Michigan CR[2]	Nov 2012	Michigan University	Michigan University	Public	Cyber Exercise Powered by Merit Network
Estonia - (NATO Cyber Range) - CCDCOE Guardtime (2017)	2012	Tallinn Estonia	NATO use in June 2014 for cyber defence exercise	Military	Estonia is Building a Next Generation CR 2018 developed by Gaurdtime
Boeing[3]	2014	France	Boeing	Private	Cyber Range in a Box
IXIA CR[4]	2014	California USA	IXIA	Private	Delivering cyber security training to Organisations
CISCO CR, the platform is integrated with IXIA[5]	2015	USA	CISCO (Company in USA)	Private	Implementation as a product in an organisation
SimSpace[6]	2015	Boston USA	SimSpace	Private	Delivering cyber security training to Organisations
IBM CR (X force Command centre)[7]	2015	USA	IBM	Private	Delivering cyber security training to Organisations
Australia cyber security Centre (ACSC)[8]	2015	Australia	Australian	Public	Delivering cyber security training to Organisations

[1]https://www.azcwr.org/
[2]https://www.merit.edu/cyberrange/
[3]https://www.boeing.com/defense/cybersecurity-information-management/
[4]https://www.ixiacom.com/solutions/cyber-range
[5]https://www.cisco.com/c/dam/global/en_au/solutions/security/pdfs/cyber_range_aag_v2.pdf
[6]https://www.simspace.com/
[7]https://www.ibm.com/security/services/managed-security-services/security-operations-centers
[8]https://www.acsc.gov.au/

Types of Cyber Range	Date Build	Location	Developed By	Type of CR (Public, Military, Other)	Remarks
Raytheon (Defence Company USA) CR [9]	2016	USA	Raytheon	Private	Delivering cyber security training to Organisations
Elbit Systems (Israeli Company)[10]	2016	Israeli	CYBERBIT Range training centres	Private	Delivering cyber security training to Organisations

[9]https://www.raytheon.com/cyber/capabilities/range
[10]http://elbitsystems.com/

B

Proposed Classified Cyber Range Levels

First proposed classified CR level baseline criteria based on the Pairwise Comparison analysis methodology and the relevant importance of the CR core capability elements which have been defined in Chapter 4.

Capability Levels CR (High Level Description)	Core Capability Elements (Critical Capabilities)	Capabilities (CR Effect and Performance)	Maturity (People, Process, Technology)	Threat Tire Level (CR Ability to Maintain Levels of Threat)
Level V. Ultimate Focused on quality cyber resilience and highly advanced cyber testing with high research and development closed source focus	Multiple Level V CR.	1 000 000 plus hosts with concurrent connections and sessions. 10 000 plus services running 400 Gbps/2 terabytes Throughput with multiple 40/100 Gbps backbone /3 IP Prefix (multiple) CR accommodates 512 Million IP address space. Fully Federated and distributed architecture. Autonomous setup using AI methods. Use of Machine learning and Deep learning (AI) .	Optimizing: People are having highly advanced cyber skills, processes are focus on continuous improvement to strive for excellence to improve the processes. technology is of a highly advanced maturity.	Threat Tire Level 6 and 5. To maintain the ability to execute the full spectrum of cyber threat capabilities in combination with military and intelligence to achieve a specific outcome.

Capability Levels CR (High Level Description)	Core Capability Elements (Critical Capabilities)	Capabilities (CR Effect and Performance)	Maturity (People, Process, Technology)	Threat Tire Level (CR Ability to Maintain Levels of Threat)
Level IV. High More advanced focus on cyber resilience and cyber testing, with a more research and development closed source focus.	Security System. Health Monitoring. System with Sensors. Data Capability. Security Information. Events Management (SIEM).	500 000 hosts with concurrent connections and sessions. 5000 services running. 100/400 Gbps throughput with multiple 10 /40 Gbps backbone. /10 IP Prefix (multiple) CR accommodates 4 Million IP address space. Distributed architecture and Federated. Autonomous setup. Use of Machine Learning (AI).	Quantitatively Managed: People are at an advanced level of analytic cyber skills level, processes are qualitatively measure are used to standardized processes, and technology is of an advanced maturity.	Threat tire level 5 and 4. To maintain the ability to execute highly sophisticated cyber threats developed by teams to discover vulnerabilities and develop exploits and threats with the ability to design, development or the manufacturing of products to enable exploitation of networks and systems of interest.
Level III. Medium The focus is on cyber resilience, testing and evaluation of computational products, with limited research and development.	Instrumentation connectivity capability. Redundancy. Monitoring System with sensors. Back Up Storage Capability. Learner Management System.	100 000 hosts with concurrent connections and sessions 1000 services running 10 /100 Gbps Throughput, with a 10 Gbps backbone /10 IP Prefix CR accommodates 4 Million IP address space. Distributed Architecture and limited Federation ability. Manual and semi-autonomous set up. Limited use of Machine Learning (AI).	Defined: People are more certified trained, processes are standardizes and controlled and are present throughout the CR, and technology is of a higher functional mature nature.	Threat tire level 3 and 4. To maintain the ability to execute unknown and undiscovered malicious code.

Capability Levels CR (High Level Description)	Core Capability Elements (Critical Capabilities)	Capabilities (CR Effect and Performance)	Maturity (People, Process, Technology)	Threat Tire Level (CR Ability to Maintain Levels of Threat)
Level II. Low More focused on testing and evaluation of basic cyber project, cyber processes and cyber security training.	Virtual Infrastructure. Scenario Generator. Capability. Real device Connectivity Capability. Facility. Threat Library Capability.	10 000 hosts with concurrent connections and sessions. 500 services running 1/10 Gbps Throughput with a 1/10 Gbps backbone /15 IP Prefix CR accommodates 128 thousand IP address space Hybrid Monolithic and Distributed architecture. Manual set up Physical learning by trial and error.	Managed: People have intermediate Cyber skills, Basic processes and controls are present, more reactive in nature, technology is of a more focused nature for the initial CR capability maturity.	Threat tire level 2 and 3. To maintain the ability to execute develop code and tools from known vulnerabilities.
Level I. Limited Initial cyber security training on an isolated simulated network.	Software Operating Systems. Network Infrastructure (Physical and Virtual). Software Applications. Management System. Traffic Generator Capability.	100 hosts with concurrent connections and sessions. 100 services running. 100mbps/1Gbps throughput with a 1 Gbps backbone. /25 IP Prefix CR accommodates 128 IP address space Flat Infrastructure. Monolithic Architecture. More hands on manual set up per host.	Initial: People have basic Cyber skills; processes are not structured and are more reactive, the technology has a basic maturity.	Threat tire level 1. To maintain the ability to execute simple code that has been developed and can deliver know exploits.

C

Cyber Range Pairwise Comparison

Pairwise Comparison analysis results to determine the CR capability levels using the core capability elements for a CR as discussed in Section 3.4.

Table C.1: Cyber Range level I Pairwise Comparison

CYBER RANGE CORE ELEMENTS		Management System	Learner Management System	Monitoring System with sensors	Health Monitoring System with Sensors	Security System	Security Incident Events Management (SIEM)	Back Up Storage Capability	Threat Library Capability	Senarion Generator Capability	Big Data Capability	Traffic Generator Capability	Network Infastructure (Physical)	Virtual Infastructure	Software Operating Systems	Software Applications	Redundancy	Real device Connectivity Capability	Instrumentation connectivity capability	Facility
		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
Management System	A	X	A2	A1	A1	A1	A1	A2	A2	A2	A2	A2	L2	A2	N2	A2	A1	A2	A2	A1
Learner Management System	B		X	C2	D1	E1	B1	G2	H1	I1	B2	K1	L2	M2	N2	O2	P1	Q2	R1	S1
Monitoring System with sensors	C			X	D1	E2	C1	G1	H1	I1	C1	K2	L2	M1	N2	O2	C1	Q1	R1	S1
Health Monitoring System with Sensors	D				X	E1	D1	G1	H1	I2	D1	K2	L2	M1	N2	O2	P1	Q1	R2	S2
Security System	E					X	E1	E1	H1	E1	E1	K1	L2	E1	N2	O2	P1	E1	E1	E1
Security Incident Events Management (SIEM)	F						X	G1	H1	I2	F1	K1	L2	M1	N2	O2	P1	Q1	R1	S1
Back Up Storage Capability	G							X	G1	I2	G2	K1	L2	M1	N2	O2	G1	G1	G1	G1
Threat Library Capability	H								X	I1	H1	K1	L2	M1	N2	O2	H1	H1	H1	H1
Scenario Generator Capability	I									X	I2	K2	L2	M2	N2	O1	P1	I1	I1	S1
Big Data Capability	J										X	K1	L2	M1	N2	O1	P1	Q1	R1	S1
Traffic Generator Capability	K											X	L2	M1	N2	O1	K1	K1	K1	K1
Network Infastructure (Physical)	L												X	L2	N2	L2	L2	L2	L2	L2
Virtual Infastructure	M													X	N2	O2	M1	M1	M1	T1
Software Operating Systems	N														X	N2	N2	N2	N2	N2
Software Applications	O															X	O2	O2	O2	S1
Redundancy	P																X	Q1	R1	S1
Real device Connectivity Capability	Q																	X	Q1	S1
Instrumentation connectivity capability	R																		X	S1
Facility	S																			X

Table C.2: Cyber Range level II Pairwise Comparison

CYBER RANGE CORE ELEMENTS		Learner Management System	Monitoring System with sensors	Health Monitoring System with Sensors	Security System	Security Incident Events Management (SIEM)	Back Up Storage Capability	Threat Library Capability	Senarion Generator Capability	Big Data Capability	Virtual Infastructure	Redundancy	Real device Connectivity Capability	Instrumentation connectivity capability	Facility
		A	B	C	D	E	F	G	H	I	J	K	L	M	N
Learner Management System	A	X	B2	A2	D1	A1	F2	G2	H2	A2	J2	K1	L2	M2	N1
Monitoring System with sensors	B		X	B2	DI	B2	F2	G1	H2	B2	J2	K1	B1	M1	N1
Health Monitoring System with Sensors	C			X	D1	C1	F2	G1	H2	C1	J2	K1	L2	M1	N1
Security System	D				X	D1	F1	G1	H2	D2	J2	K1	L1	M1	N1
Security Incident Events Management (SIEM)	E					X	F1	G1	H2	E1	J2	K1	L2	M1	N1
Back Up Storage Capability	F						X	G1	H2	F1	J2	F1	L1	F1	N1
Threat Library Capability	G							X	G2	G2	J2	G1	L2	M1	N1
Senarion Generator Capability	H								X	H2	J2	H1	L1	M1	N1
Big Data Capability	I									X	J2	K1	L1	M1	N1
Virtual Infastructure	J										X	J2	J2	J2	N1
Redundancy	K											X	L1	K1	N1
Real device Connectivity Capability	L												X	L1	N1
Instrumentation connectivity capability	M													X	N1
Facility	N														X

Table C.3: Cyber Range level III Pairwise Comparison

CYBER RANGE CORE ELEMENTS		Learner Management System	Monitoring System with sensors	Health Monitoring System with Sensors	Security System	Security Incident Events Management (SIEM)	Back Up Storage capability	Big Data Capability	Redundancy	Instrumentation connectivity capability
		A	B	C	D	E	F	G	H	I
Learner Management System	A	X	B3	A2	A2	A2	F3	A2	H2	I2
Monitoring System with sensors	B		X	B2	B1	B2	F1	B2	H2	I2
Health Monitoring System with Sensors	C			X	C2	C2	F1	C2	H2	I2
Security System	D				X	D3	D2	D2	H2	I2
Security Incident Events Management (SIEM)	E					X	F2	G2	H2	I2
Back Up Storage Capability	F						X	F2	H2	I2
Big Data Capability	G							X	H2	I2
Redundancy	H								X	I2
Instrumentation connectivity capability	I									X

Table C.4: Cyber Range level IV Pairwise Comparison

CYBER RANGE CORE ELEMENTS		Health Monitoring System with Sensors	Security System	Security Incident Events Management (SIEM)	Big Data Capability
		A	B	C	D
Health Monitoring System with Sensors	A	X	B2	A2	D1
Security System	B		X	B2	D1
Security Incident Events Management (SIEM)	C			X	D1
Big Data Capability	D				X

D

Cyber Range Process Maturity Model

This proposed model represents the process areas suggested to develop a CR as synthesised using the CMMI Dev model.

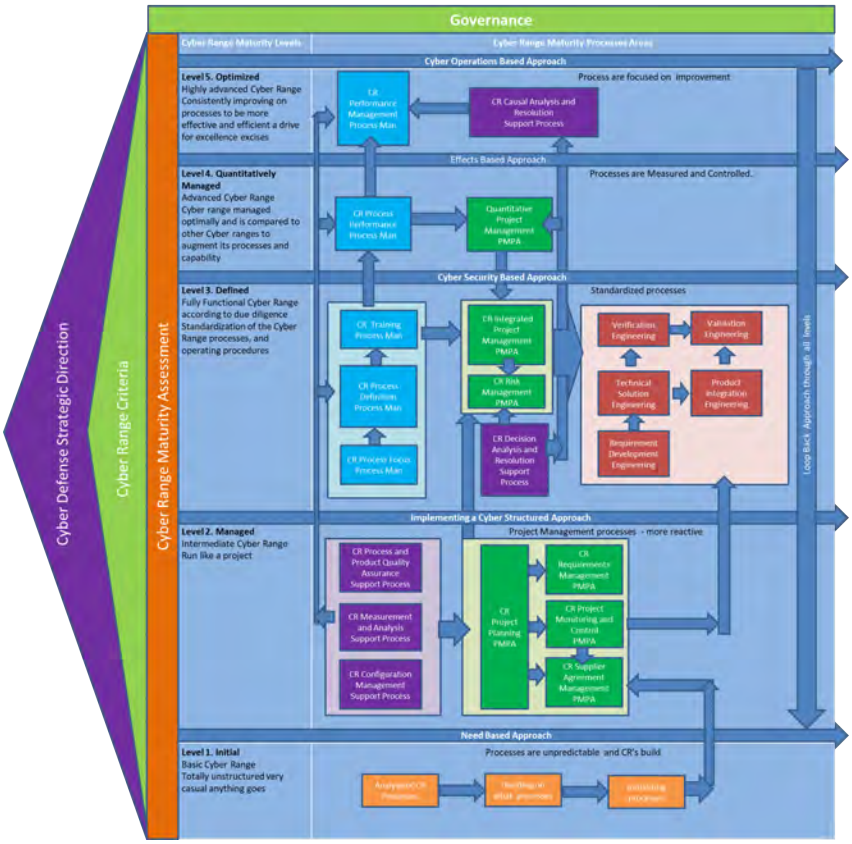


Figure D.1: Proposed Process Maturity Model for a Cyber Range as Synthesised from the CMMI Dev Model

E

Cyber Range Questionnaire

The cyber range questionnaire capability and maturity evaluation questionnaire was distributed in an electronic form, which was completed by identified cyber range experts in the field. The questionnaire aided in aquiering viewpoints from cyber range experts in the field. The results were analysed and are reported in Chapter 6 of this thesis.

Cyber Range Capability and Maturity Evaluation Questionnaire

Michael J. Aschmann
Rhodes University Grahamstown South Africa

1. Introduction

Thank you for participating in the questionnaire. This questionnaire seeks to gain insight into the evaluation of both the Capability and Maturity of a Cyber Range (CR). The value of this is to establish a baseline by which Cyber Ranges can be measured and classified according to their functional capability and degree of process maturity.

As an identified expert, with experience in a Cyber Range environment, your assistance is appreciated in collecting data, based on your expert opinions. The results of this research instrument, together with other research will be analyzed and reported in a Master's thesis tentatively titled - *Toward a Capability and Maturity Model for a Cyber Range.* This work will propose a framework for the evaluation, mapping, and comparative analysis of Cyber Range platforms and environments.

The evaluation questionnaire following should be answered in the context of the accompanying document, **Cyber Range Capability and Maturity Evaluation Context Document** with which you were provided. Please familiarise yourself with this document before commencing with the questionnaire. Pre-reading time will be approximately 20 minutes

The questionnaire time allocation is approximately 40 min if done start to finish. Participants are encouraged to try and complete this in one sitting.

2. Background Data

The preferred level of skills requested to complete this evaluation is preferably Cyber Range personnel who have knowledge in the operation and development of a Cyber Range from a computer science viewpoint, with preferably 5 to 7 years' experience. Please cross the appropriate block with the years of experience in a Cyber Range or in the computer science environment.

Years' Experience in Cyber Range	Less than 5	5-7	7-10	10 and more

Tick the box(es) appropriate to your (Respondent) job role; Please provide alternative job role if necessary.

Recipients Job Role	Tick	Recipients Job Role	Tick	Recipients Job Role	Tick
Cyber Range Operator		Cyber Range Computer Systems Engineer		Enterprise Architect	
Cyber Range SW Developer		Cyber Range Analyst		Business Analyst	
Cyber Range Evaluator		Cyber Range Scenario developer		Computer Engineer	
Cyber Range Events Manager		Cyber Range Coordinator		Computer lecturer	
Cyber Range Security Staff		Malware Analyst		Security Advisor	
Security Pen Tester		Other type of job role please state			

3. Guidelines

The guidelines of the questionnaire are;

1. Be honest in your assessment; if you do not agree or would like to provide guidance, please make use of the feedback space provided.
2. Do not disclose any information that will be to the determent of your integrity;
3. Be as discreet and direct as possible, your opinion will be kept confidential and will not be disclosed in public and will be used strictly for the purpose of this specific research only. Only the aggregated results will be reported on.
4. This questionnaire is of a purely voluntary nature and anonymous participation will be accepted.
5. Should you wish to withdraw your participation please submit a request.
6. A consolidated report will be written on receipt of questionnaires and participating parties will be notified of the results.
7. The handling of data collected will be processed by the researcher and research supervisor only. Data will be archived accordingly.
8. While completed responses are preferable, if you feel you cannot answer, questions can be omitted.

4. Structure

The structure of the questionnaire will evaluate two criteria of Cyber ranges. The first is the Capabilities of a Cyber Range and the second, the, maturity of a Cyber Range.

5. Questions

5.1 Capability of a Cyber Range

1. Would you agree that the following listed core capability elements are part of a Cyber Range?

Cyber Range Core Capability Elements	Strongly Agree	Agree	Disagree	Strongly Disagree
Management System				
Learner Management System				
Monitoring System with sensors				
Health Monitoring System with Sensors				
Security System				
Security Incident Events Management (SIEM)				
Back Up Storage Capability				
Threat Library Capability				
Scenario Generator Capability				
Big Data Capability				
Traffic Generator Capability				
Network Infrastructure (Physical)				
Virtual Infrastructure				
Software Operating Systems				
Software Applications				
Redundancy				
Real device Connectivity Capability				
Instrumentation connectivity capability				
Facility				

If you disagree please motivate your reason or suggest other core capability elements?

2. In your expert opinion what is your definition of a Cyber Range?

3. In your expert opinion are there any other core capability elements that can be added to a Cyber Range, and if so why?

4. To what degree do you agree with the proposed relevance rating of the core capability elements for a Cyber Range in which the different Cyber Range levels are proposed? (See attached Cyber Range Capability and Maturity Evaluation Context Document for Questionnaire; Paired Compression) from page 5.

Core Capability Elements	Relevant Importance	Strongly Agree	Agree	Disagree	Strongly Disagree
Software Operating Systems	1				
Network Infrastructure (Physical)	2				
Software Applications	3				
Management System	4				
Traffic Generator Capability	5				
Virtual Infrastructure	6				
Scenario Generator Capability	7				
Real device Connectivity Capability	8				
Facility	9				
Threat Library Capability	10				
Instrumentation connectivity capability	11				
Redundancy	12				
Monitoring System with sensors	13				
Back Up Storage Capability	14				
Learner Management System	15				
Security System	16				
Health Monitoring System with Sensors	17				
Big Data Capability	18				
Security Incident Events Management (SIEM)	19				

5. Proposed suggested capability levels of a Cyber Range.

CR levels	Capability	Purpose	Strongly Agree	Agree	Disagree	Strongly Disagree
I	Limited	Initial cyber security training on an isolated simulated network with limited hosts and limited cyber scenarios, limited legacy stack infrastructure.				
II	Low	More focused on testing and evaluation of basic cyber project, basic cyber processes and cyber security training, with a modeling, simulating and emulating capability for medium cyber scenarios with a legacy stack infrastructure and limited hyper convergence infrastructure.				
III	Medium	The focus is on cyber resilience, testing and evaluation of computational products, with limited research and development, with a modeling, simulating and emulating capability, for advanced cyber scenarios, with limited federation capability which is virtual, instantaneous and on demand for limited stakeholders, with a legacy stack and hyper convergence infrastructure and a limited SW defined converged infrastructure.				
IV	High	More advanced focus on cyber resilience and cyber testing, with a more research and development proprietary focused, with a modeling, simulating and emulating capability, for highly advanced cyber scenarios and wider federation access capability which is virtual, instantaneous and on demand for limited stakeholders on a national level with a hyper convergence and advanced SW defined converged infrastructure.				
V	Ultimate	Focused on quality cyber resilience and highly advanced cyber testing with high research and development proprietary focused for multiple stakeholders with a modeling, simulating and emulating capability, for Ultra highly advanced cyber scenarios which is virtual, instantaneous and on demand, testing cyber capabilities with sophisticated instrumentation, with national and global federation, with a hyper convergence and highly advanced SW defined converged infrastructure.				

Comments

6. Proposed Cyber Range levels (holistically) with different capability; to classify a Cyber Range level.

Cyber Range levels	Capability (Holistically)	Strongly Agree	Agree	Disagree	Strongly Disagree
Level V. Ultimate	• 1 000 000 plus hosts with concurrent connections and sessions				
	• 10 000 plus services running				
	• 400 Gbps/2 terabytes Throughput with **Multiple 40/100 Gbps backbone**				
	• /3 IP Prefix (multiple) CR accommodates 512 Million IP address space				
	• Fully Federated and distributed Architecture				
	• Autonomous setup using AI methods				
	• Use of Machine learning and Deep learning (AI)				
Level IV. High	• 500 000 hosts with concurrent connections and sessions				
	• 5000 services running				
	• 100/400 Gbps throughput with **Multiple 10 /40 Gbps backbone.**				
	• /10 IP Prefix (multiple) CR accommodates 4 Million IP address space.				
	• Federated and Distributed Architecture				
	• Autonomous setup				
	• Use of Machine Learning (AI)				
Level III. Medium	• 100 000 hosts with concurrent connections and sessions				
	• 1000 services running				
	• 10 /100Gbps Throughput, with a 10gig backbone				

	• /10 IP Prefix CR accommodates 4 Million IP address space				
	• Distributed Architecture and limited Federation ability				
	• Manual and semi-autonomous set up				
	• Limited use of Machine Learning (AI)				
Level II. Low	• 10 000 hosts with concurrent connections and sessions				
	• 500 services running				
	• 1/10 Gbps Throughput with a 1/10gig backbone				
	• /15 IP Prefix CR accommodates 128 thousand IP address space				
	• Hybrid Monolithic and Distributed Architecture				
	• Manual set up				
	• Physical learning by trial and error				
Level I. Limited	• 100 hosts with concurrent connections and sessions				
	• 100 services running				
	• 100mbps /1Gbps Throughput with a 1gig backbone				
	• /25 IP Prefix CR accommodates 128 IP address space				
	• Flat Infrastructure Monolithic Architecture				
	• More hands on manual set up per host				

Comments

7. What instrumentation as an additional function to a Cyber Range is recommended holistically?

Instrumentation	Strongly Agree	Agree	Disagree	Strongly Disagree
Network Telescope				
Honey Net or Honeypot				
Netflow				
Security Instrumentation				
Performance Instrumentation				

Comments or additional instrumentation? Please motivate your reason why?

8. Should a Cyber-Range be measured against the Measurement of Effect (MOE)?

MOE (Observing the use of the CR by the measurement of)	Strongly Agree	Agree	Disagree	Strongly Disagree
Operators Cyber skills				
CR ability to capacitate / handle a single or multiple cyber operational task/s				
CR ability to adapt to different cyber environment scenarios				
CR ability to managed Cyber activities				
How effective is the CR with different levels of Cyber scenarios				
How effective is the CR through its evolution over time.				

Comments or suggest other Measurement of Effect? Please motivate your reason why?

9. Should a Cyber Range be measured against the Measurement of Performance (MOP)?

MOP (Measuring ICT Performance and efficiency of the CR by its:)	Strongly Agree	Agree	Disagree	Strongly Disagree
Speed				
Throughput				
High Fidelity				
Switching ability between Cyber Events				
Quick Configuration				
Traffic Generation				
Storage and retrieval				
Security assessment				
Instrumentation Connectivity				
Measuring as a system, how well the CR accomplishes a task that it must execute.				

Comments or suggest other Measurement of Performance? Please motivate your reason why?

5.2 Maturity of a Cyber Range

10. Proposed synthesized maturity levels of a Cyber Range as adopted from the CMMi Dev model.

Cyber Range levels	Maturity	Purpose	Strongly Agree	Agree	Disagree	Strongly Disagree
I	Basic	Initial: People have basic Cyber skills; Processes are not structured and are more reactive, the technology has a basic maturity.				
II	Intermediate	Managed: People have intermediate Cyber skills, Basic processes and controls are present, more reactive in nature, Technology is of a more focused nature for the initial CR capability maturity.				
II	Fully Functional	Defined: People are more certified trained, Processes are Standardizes and controlled and are present throughout the CR, and Technology is of a higher functional mature nature.				
IV	Advanced	Quantitatively Managed: People are at an advanced level of analytic cyber skills level, Processes are Qualitatively measure are used to standardized processes, and Technology is of an advanced maturity.				
V	Highly Advanced	Optimizing: People are having highly advanced cyber skills, Processes are focus on continuous improvement to strive for excellence to improve the processes. Technology is of a highly advanced maturity.				

Comments on the proposed synthesized maturity levels of a Cyber Range

11. When looking at maturity of a Cyber Range, would these be the elements to evaluate?

Maturity Core Elements	Strongly Agree	Agree	Disagree	Strongly Disagree
People				
Process				
Technology				

12. Other Maturity elements? Please motivate your reason why?

13. People maturity pertaining to Cyber Skills and cognitive ability to cope under pressure, how would this be evaluated?

14. How would the maturity of the people cyber skills be evaluated, against what measurement?

15. What general processes areas pertaining to a Cyber Range should be in place?

CR Processes Areas	Strongly Agree	Agree	Disagree	Strongly Disagree
Management Process				
Project Management Process				
Engineering (Technical) Process				
Support Process				

16. In your expert opinion are there any other general processes pertaining to a Cyber Range?

17. Looking at the maturity of technology what would be a **good approach**, to evaluating technology in a Cyber Range?

18. Against what measurement would the maturity of the technology be evaluated?

Technology Maturity	Strongly Agree	Agree	Disagree	Strongly Disagree
Ability to be maintained and supported in a CR				
Life Cycle management				
Technology drivers				
Managing the technology as a capability				

Comments.

19. There are multiple Capability and Maturity Models (CMM) that have been developed, which methodology stands out as a standard model that can be used in a Cyber Range context when evaluating its capability and maturity?

Capability and Maturity Models	Strongly Agree	Agree	Disagree	Strongly Disagree
Capability Maturity Model (for software) (CMM)				
Capability Maturity Model Integration (CMMi)				
Levels of Information Systems Interoperability (LISI)				
Cyber Security Capability Maturity Model (CSCMM)				

20. Other capability and maturity models that will be applicable for a Cyber Range?

6 Summary

The results of the questionnaire will be added to my thesis "*Toward a Capability and Maturity Model for a Cyber Range*". Are you available for a Skype session or further email correspondence please indicating, "yes or no" in the block provided.

Yes	No

Thank you for your participation it is appreciated.