

Dynamic Cyber-Incident Response

A thesis submitted for the degree of Doctor of Philosophy



By

Eur Ing Kevin Mepham

Defence and Cyber-Security Research Group

Department of Computer Science

Brunel University

July 2018

ACKNOWLEDGEMENTS

Pursuing a PhD, whilst ensuring that the daily demands of a busy full-time cyber-security position are met, is not a task without challenges, especially when based in a different country to the University. When this position requires travel, often at short notice, to areas that do not always have the best infrastructure for remote connections to the University and adding an occasional major mountain-biking accident, these challenges are exacerbated significantly. Invariably, this leads to more time than would be hoped being taken away when back with the family to ensure that the research progresses. For this I would like to thank Julie, Kieran, Tierney and Lewis who have understood and supported in my endeavours for the six years that this research has taken.

I would also like to thank Prof Panos Louvieris for his flexibility in providing support and mentoring, mostly during weekends via sometimes difficult video communication. He has persevered in trying to turn my concise military style of writing into something suitable for the academic community. He has also ensured that I have supported assertions in my research which I initially perceived as “common sense” with suitable academic references and solid statistical grounding.

I am also grateful to Dr George Ghinea and Dr Natalie Clewley for their support, particularly in the early stages of the research, as I was getting to grips with the concepts of writing papers and statistical analysis to support (or otherwise) my initial suppositions. I also wish to express my gratitude to my fellow Brunel University students for acting as sounding boards for some of my presentations and providing advice from their own experiences of conducting research.

Finally, I would like to thank the Information Security, CIS, Intelligence and Operational communities from many different nations and organisations who have participated in the research as well as providing the expert advice and feedback relating to the problems, solutions and model concepts investigated during this research.

Declaration

I, Kevin Douglas Mephram, declare that this thesis is the result of my own independent work and research, except where otherwise explicitly stated and referenced. The views expressed are my own and do not necessarily reflect those of Brunel University nor my current or previous employers. This work has not been submitted for any other degree or award at this or any other university nor is it being submitted concurrently for any other degree or award.

Abstract

Cyber-Incident Response (or, as it was initially called, Computer Incident response) has traditionally followed cyclic models such as the SEI Incident Response Cycle and SANS models, which aim to detect and identify incidents, stop, contain and eradicate them. Using the knowledge gained from the incidents, these models then advocate improving the capabilities to defend against subsequent attacks of the same nature. Although some later versions of these models, including the NIST model proposed in 2012, have nested the cycles to provide a more reactive response, they are neither demonstrably empirically founded nor do they represent the interests of all stakeholders within an organisation.

This research addresses cyber-incident response from a broader perspective, looking from the viewpoint of a cross-functional set of stakeholders and ensures that incident response decisions are sensitive to temporal priorities, taken from an organisation-wide perspective and provide a range of responses rather than only containing and eradicating an incident. During this research, principal component analysis and structural equation modelling were used to develop the Dynamic Cyber Incident Response Model (DCIRM) which resulted in the development of a fielded prototype tool, the Cyber Operations Support Tool (COST). COST was then subjected to both controlled experimentation and operational validation. Empirical analysis of both of these activities confirmed the utility and effectiveness of the COST and the underlying DCIRM. The COST has since been used to train military cyber operational planners.

The novel areas of this research are the dynamic nature of DCIRM which takes account of the changing asset values based on the point in the business/mission cycle, the trade-off between risk to the organisation and gathering intelligence during an incident, the flexibility in response options within organisational constraints and the abstraction of the information to allow a non-cyber specialist to make an appropriate incident response decision.

Publications Relating to this Research

Dynamic Cyber Incident Response, K D Mepham, P Louvieris, G Ghinea, N Clewley, 6th International Conference on Cyber Conflict, (CYCON 2014), 121 - 136, (3-6 June 2014),

Impact-Focused Incident Response, K D Mepham, P Louvieris, G Ghinea, 20th International Command and Control Research and Technology Symposium (ICCRTS), Paper 057, (2015)

Integration of Cyber Impact Assessment into Operational Decision-Making, K D Mepham, P Louvieris, G Ghinea, Natalie Clewley, 21st International Command and Control Research and Technology Symposium (ICCRTS), Paper 009. (6-8 September 2016).

Table of Contents

Abstract.....	4
Publications Relating to this Research.....	5
List of Abbreviations	9
1 Introduction	11
1.1 Background	11
1.2 Research Context and Problem Statement.....	11
1.3 Research Question, Aim and Objectives.....	12
1.3.1 Research Question	12
1.3.2 Aim	12
1.3.3 Objectives:.....	13
1.4 Intended Research Significance and Impact	13
1.5 Thesis Structure	14
2 Literature Review and Related Research.....	15
2.1 Overview	15
2.2 Cyber Environment, Doctrine, and Cyber Incident Response Evolution.	15
2.2.1 Cyber Environment	15
2.2.2 General Warfare Doctrine.....	16
2.2.3 C ² , C ³ I and Intelligence	18
2.2.4 Intelligence and Related Models	22
2.2.5 Incident Response Evolution.....	26
2.2.6 Cyber-Defence Model Taxonomy	35
2.3 Other Research Relevant to Cyber-Incident Response.....	37
2.3.1 Cyber Intelligence	37
2.3.2 Legal Perspective and Attribution.....	40
2.3.3 Situational Awareness and Information Fusion	43
2.3.4 Collaboration.....	49
2.3.5 Risk, Stakeholders and Decision-Making	52
2.3.6 Academic Integrity	55
2.3.7 Areas of Concern and Shortfalls in Current Theory and Models	57
2.3.8 Additional Notes on Gaps	59
2.3.9 Hypothesised Model	62
3 Research Methodology.....	64

3.1	Methodological Review	64
3.2	Applicable Research Methods	69
3.3	Survey.....	71
3.4	Statistical Evaluation.....	73
3.5	Operational Validation.....	73
3.6	Experimental Methodology	77
3.7	Experiment Method and Vignettes.....	79
4	Data Analysis.....	83
4.1	Introduction	83
4.2	Survey Development.....	83
4.3	Sample Frame and Procedure.....	84
4.4	Data Preparation.....	86
4.5	Survey Analysis and Results	87
4.6	Contrast with Current Models	101
4.7	Practical Implications	102
5	Operational Validation Results and Analysis	103
5.1	Background	103
5.2	Cyber Operations Support Tool	103
5.3	Evaluation	105
5.4	Analysis	105
5.5	Feedback	107
6	Experimental Results and Analysis.....	108
6.1	Experimental Aim.....	108
6.2	Experimental Objectives:	108
6.3	Experimental Results and Analysis.....	109
7	Discussion and Conclusions	113
7.1	Model Comparison and Evolution	113
7.2	Key Findings	115
7.3	Evaluation of Analysis Outcomes compared to Research Objectives.....	117
7.4	Contribution to the Field.....	120
7.5	Research Constraints, Limitations and Complications.....	123
7.6	Future Work	124
7.7	Final Remarks.....	125
8	Bibliography	126
	Appendix 1 – Survey Questionnaire.....	133

Appendix 2 - Cyber Security Variables	144
Appendix 3 – Principal Component Analysis	146
Appendix 4 – Structural Equation Modelling: Fit Indices.....	147
Appendix 5 – COST Feedback.....	148
Appendix 6 – Experiment Scenario and Vignettes.....	151
Appendix 7 – Equipment and Software Used for Experiment.....	154
Appendix 8 – Evaluation Questionnaire	156
Appendix 9 – Situational Awareness and Decision Support Results.....	158

List of Abbreviations

ACL	Access Control List
ARNC	Attack, Repair, Neutralise and Containment
AV	Antivirus
BST	Battle-Staff Training
C ²	Command and Control
C ³ I	Command, Control, Communications and Intelligence
CAPEC	Common Attack Pattern Enumeration and Classification
CCDCOE	(NATO) Cooperative Cyber Defence Centre of Excellence
CDWG	Cyber Defence Working Group
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CERT/CC	CERT Coordination Centre
CIO	Chief Information Officer
CIPB	Cyber-Intelligence Preparation of the Battlespace
CIS	Communication and Information Systems
CISO	Chief Information Security Officer
CM	Configuration Management
COA	Course of Action
COST	Cyber Operations Support Tool
CSIRT	Computer Security Incident Response Team
CVE	Common Vulnerabilities and Exposures
DCIRM	Dynamic Cyber-Incident Response Model
DEP	Data Execution Prevention
DSR	Design Science Research
FBI	Federal Bureau of Investigation
FIRST	Forum of Incident Response and Security Teams

GDPR	(European Union) General Data Protection Regulation
HIDS	Host Intrusion Detection System
IA	Information Assurance
IDP	Intrusion Detection and Prevention
IDS	Intrusion Detection System
INFOSEC	Information Security
IRC	Internet Relay Chat
IT	Information Technology
JFCBS	Joint Force Command Headquarters Brunssum
LCD	Likely Compromised Devices
MCDC-CICOA	Multinational Capability Development Campaign - Cyber Implications for Combined Operational Access
MISP	Malware Information Sharing Platform
MNE7	Multi-National Experiment 7
NATO	North Atlantic Treaty Organisation
NC3A	NATO Consultation, Command and Control Agency
NIDS	Network Intrusion Detection System
NIPS	Network Intrusion Prevention System
NIST	National Institute of Standards and Technology (USA)
OODA	Observe, Orient(ate), Decide, Act
PCI-DSS	Payment Card Industry Data Security Standard
URL	Uniform Resource Locator
SA	Situational Awareness
SANS	Sysadmin, Audit, Network and Security (SANS Institute)
SEI	Software Engineering Institute
TTPs	Tactics, Techniques and Procedures
USAF	United States Air Force

1 Introduction

1.1 Background

In recent decades technology has changed rapidly, especially in the Information Technology (IT) area. In a drive for efficiency and cost-saving organisations and governments have become increasingly-dependent upon IT and its supporting infrastructure. This transformation has also led to an increasing dependence upon the Internet by critical and important infrastructure as remote support and centralised control mechanisms often use the Internet as a core communication medium. However, the other side of the coin is that this evolution has led to an increased exposure to exploitation or compromise by those with hostile intent as traditionally closed networks or systems have become more accessible, exposing a larger potential attack surface to hostile entities. To exacerbate the problem, the cyber domain can in military terms be considered as constituting asymmetric warfare as an attacker (or attackers) with relatively few resources can achieve a catastrophic effect on a well-resourced defending organisation. To counter these cyber-attacks, many organisations have cyber-incident response processes based on one of the industry-standard computer incident response models. These models were initially developed by computer specialists prior to the advent of the Internet in its current form and before the computer became so ubiquitous in its use and so available to such a large proportion of the worldwide population (along with mobile devices such as mobile phones, tablets and laptops).

1.2 Research Context and Problem Statement

Despite the rapidly-evolving environment described in the previous section, with all associated risks, standard computer security incident response models have remained largely unchanged since the 1990s; these tend to be linear models which are fashioned into a circle with very little evidence of feedback between the components within the cycle. Moreover, the models that are currently used to take little account of related or contributing disciplines such as Intelligence (in the military or government context), Command and Control (C²) and Human Factors research with little regard for stakeholders outside of the IT and security domains. The primary focus of current cyber-incident response remains containing or neutralising incidents as quickly as possible (for example by

isolating systems and network segments or by denying the attacker access at the boundaries of the defended infrastructure). This approach ignores the potential advantages of actively utilising live incidents to provide a better understanding of attackers, their techniques and their capabilities. Whilst both of these disparate approaches would have their supporters, typically the Intelligence professionals on one side and the Communication and Information Systems (CIS) support staff on the other, the optimal solution could also be a balanced decision taken between the two paths (which could arguably be considered to be the best operational or strategic approach). However, at the time of commencing the research, (October 2011) there was no Cyber-community accepted standard or procedure for achieving this. The relevant literature was again reviewed in the later stages of the research (July 2017) and whilst at this point many nations had known or were believed to be developing cyber operational capabilities covering the range of activities from defensive to offensive operations (Clapper, Lettre, & Rogers, 2017) there were no new published methods or standards that were found to be applicable in achieving this balance.

1.3 Research Question, Aim and Objectives

As a consequence of the situation described in the previous paragraphs, this research is intended to investigate the effectiveness of the current standard cyber-incident response models and to see if there is a better way to serve organisational interests.

1.3.1 Research Question

Is it possible to create a more tailored (i.e. customisable to an organisation's specific requirements and values) and dynamic way of implementing Cyber Security Incident Response than by enforcing linear processes based on traditional static Security Incident Response Models which aim to contain or neutralise incidents immediately?

1.3.2 Aim

To provide a dynamic and relevant model for Cyber Security Incident Response to be used as a reference by Information Assurance (IA) management staff in constructing cyber-incident response plans and procedures which will continue to evolve with the rapidly-changing threats, culture, business/mission priorities and technology and, in doing so, to provide relevant situational awareness (SA) for the operational risk owner and decision makers.

1.3.3 Objectives:

The objectives of this research are to:

- a. Analyse the problem space by investigating the key variables that define its dimensions, specifically this should include all variables deemed to be influential in providing the decision maker in the cyber incident response process with the best information to decide upon a response.
- b. Develop a model to represent the defined problem space and potential solutions whilst addressing perceived gaps within the prevalent cyber incident response models.
- c. Evaluate the developed model against the prevalent incident response models and the perceived deficiencies in those models.
- d. Assess the implications of practical instantiations of the employed model against the problem space.

1.4 Intended Research Significance and Impact

This research has determined that there is a discernible gap in the effectiveness of the traditional cyber-incident response models with respect to supporting long-term organisational goals. The research addresses this shortfall by providing a dynamic cyber-incident response model which allows key decision-makers to take all stakeholders and organisational goals into account when making decisions about possible response options to cyber incidents. The model caters for the changing values of assets, information and intelligence over time and also considers impact on the mission during the evaluation of response options.

This research develops a conceptual model which:

- a. Provides a theoretical framework for Cyber-Security professionals to create organisation-tailored Cyber-Incident Response procedures. This model allows procedures to be organisation specific and therefore tailored to resources, regulatory constraints and risk appetite of the subject organisation.
- b. Provides Cyber-Security professionals a model encompassing the different phases of Cyber-Incident Response in a way that will enable communication of

Cyber-Security concepts to non-cyber audiences including the operational risk owners and key decision-makers.

1.5 Thesis Structure

In Chapter 2, Literature Review and Related Research, researched literature identified as having relevance to cyber incident-response is investigated; this covers not only core cyber-security areas but also Intelligence (in the military context), military doctrine and philosophy, C² and SA. Although this section primarily addresses the literature review, the rapidly changing nature of cybersecurity results in a noticeable lag between published literature and the “state of the art” in the domain. Consequently, concepts discussed in expert working groups and other relevant meetings which the author attended are also considered within this chapter as supporting information for the literature review.

Chapter 3, Research Methodology, provides a description of different research methodologies and their relevance to this research. It then leads onto an outline of the resulting survey and experiment and operational validation.

Chapter 4, Data Analysis, describes the survey development in more detail. It then provides a detailed analysis of the results through all stages up to the development of the structural equation model. This chapter then concludes with a comparison between the structural equation model and the traditional models.

Chapter 5, Operational Validation, describes the development and use of a prototype tool based on the Dynamic Cyber Incident Response Model which was used to support NATO training and exercises.

Chapter 6, Experiment, describes the academic experiment in detail. It describes the environment, the tools and the interaction within the environment. It then investigates the results and explores implications for refinement of the structural equation model developed from the survey.

Chapter 7, Discussion and Conclusions, discusses the main points from Chapters 2 through to 6 and evaluates whether or not the research has met its aims and objectives as well as conclusions that can be drawn from the research.

2 Literature Review and Related Research

2.1 Overview

This literature review develops a theoretical grounding to investigate potential improvements to the standard security/cyber incident response processes and models which have been traditionally employed. In order to do this, it will also investigate doctrines and fields which may have influence on incident response processes such as (Military) Intelligence, C² and Human Factors research.

However, due to the different approaches taken by the current practical implementation of cyber-incident response together with experience in this field and the contrast with the academic work that has been done in this field, the literature review has been split into two main sections, these are:

- a. Cyber Environment, doctrine and Cyber-Incident response evolution from a practitioner's and industry perspective.
- b. Published academic research relevant to Cyber-Incident Response.

Finally, these two disparate areas are brought together to identify synergies, contradictions and any gaps that remain.

2.2 Cyber Environment, Doctrine, and Cyber Incident Response Evolution.

This section of Chapter 2 concentrates on literature associated with historical and current practices in both the core Cyber Security field and those fields which are closely related such as military doctrine, military intelligence and C².

2.2.1 Cyber Environment

In British military doctrine (Ministry of Defence (UK), 2016), "Cyberspace" is defined as "*An operating environment consisting of the interdependent network of digital technology infrastructures (including platforms, the Internet, telecommunications networks, computer systems, as well as embedded processors and controllers), and the data therein spanning*

the physical, virtual and cognitive domains". UK doctrine further classifies this from a military perspective as:

- a. "Near": infrastructure under the control of and protected by the commander or their Defence collaboration partners (where infrastructure comprises networks and systems).
- b. "Mid": infrastructure critical to the campaign or mission but not under direct control or protection of the commander; they may, however, be controlled or protected by a third party on the commander's behalf.
- c. "Far": infrastructure which, if manipulated, will have critical impact on the operation or campaign. This infrastructure will to a large extent be outside the protection or ownership of "friendly forces".

Using this encompassing context, cyber warfare and cyber-incident response should be considered. For the purposes of this research, the considered cyber-incidents are those within "Near Cyberspace" as defined above and further restricted to those owned/controlled directly by defending forces i.e. not those under the control of collaboration partners although information exchange is expected to take place with them.

2.2.2 General Warfare Doctrine

One of the earliest popular military doctrinal guides is *The Art of War*, reportedly written in 5th century BC by Sun Tzu (Tzu, 1963) this provides guidance on not only military tactics in battle, but also includes the philosophy and psychology of warfare in general. This advice, which is independent of technology, politic or nation, underpins much of the military strategy (and business strategy) still employed today. As will be seen, the ideas from *The Art of War* are repeated in current doctrine; they are not only limited to the physical battlefield but are also relevant to the cutting-edge environment of the cyber battle-space.

In the UK, current Defence Doctrine (Ministry of Defence (UK), 2014) states that doctrine "is a guide to commanders and subordinates on how to think and not what to think" it is "a guide to anyone who wants to learn about war from books; it will light his way, ease his progress, train his judgement and help him to avoid pitfalls. Doctrine is meant to educate the mind of the future commander... not to accompany them to the battlefields". In this context when looking at Cyber Defence and, in particular at Cyber Incident Response, it is

useful to look at the related doctrines and models in Defence and the associated areas. Some key concepts and definitions can be drawn directly from the UK Defence Doctrine which are pertinent to the Cyber environment: the first and most important from a Cyber perspective is “Security” which is defined as “the provision and maintenance of an operating environment that affords the necessary freedom of action, when and where required, to achieve objectives”. This is further amplified to explain that security is always a risk management exercise which balances the protection of high-value assets against the operational objectives and available resources. From Sun Tzu we are told to “assess the advantages in taking advice, then structure your forces accordingly” which again echoes this risk-management perspective. One of the other key concepts from the UK doctrine is “Flexibility” which is defined as “the ability to change readily to meet new circumstances; it comprises agility, responsiveness, resilience, acuity and adaptability”. These components of flexibility are reinforced with several examples in the teachings of Sun Tzu. Within any response model this would reinforce the requirement to use dynamic information rather than relying on static information which does not change with the circumstances.

SA is also identified as a key concept in UK Doctrine, named as “Inform” under the UK MoD’s Defence Conceptual Framework (Ministry of Defence (UK), 2014). It is defined as “the ability to collect, analyse, manage and exploit information and intelligence to enable information and decision superiority”. This is also echoed by Sun Tzu, who is reputed to have stated “know the enemy and know yourself, in a hundred battles you will never be in peril” (Tzu, 1963). In other words, make sure you understand your own infrastructure and capabilities, your strengths and weaknesses and also those of your opponent in order to be victorious in battle. This is one of the driving forces behind the field of Military Intelligence; to know what your enemy is doing and is capable of doing will help a commander to make the best decisions when trying to achieve operational and strategic goals. This would lead to comprehensive situational awareness being a key component of any model dealing with response to any form of incident.

Consequently, if it is accepted that the Cyber is just another domain of modern warfare, from both the ancient seminal work of Sun Tzu and current military doctrine it could be anticipated that some key aspects would be reflected in the defence of the Cyber domain. Therefore, by including Cyber as a domain of modern warfare, security, flexibility and SA should be key components of any Cyber strategy and the employment of Cyber Defence and Cyber Incident Response.

To assess the applicability of each of these key concepts in relation to Cyber Defence, the C² area will be reviewed to see how flexibility is achieved in military C² models, then by incorporating the communication and intelligence aspects i.e. Command, Control, Communication and Intelligence (C³I) and Intelligence as a separate discipline, the creation of SA will be investigated. Finally, security will be examined in relation to current cyber-incident response processes and how the models and processes have evolved.

2.2.3 C², C³I and Intelligence

In a paper primarily concerned with Combat Operations and C³I (Orr, 1983) some issues and models are discussed which are relevant to both Intelligence doctrine and Cyber-security. Specifically, the evolution of a C² model to a C³I model and the foundation of both models in the air combat OODA loop model (discussed in a subsequent paragraph) provide relevant parallels in responding to cyber-security incidents. The paper was produced in order to address a perceived gap between C³I concepts and military strategy; a similar case can be made for the gap between Intelligence, C³I and cyber-incident response techniques and procedures as, to date, no published literature has been discovered which comprehensively investigates the balance of equities between Intelligence requirements, Mission requirements and the requirements espoused by traditional cyber-incident response.

Colonel John Boyd USAF proposed a model of Observe (monitor the enemy's actions), Orient (work out possible actions and consequences based on the observations of the enemy and knowledge of your own capabilities), Decide (choose a course of action), Act (carry it out), this was otherwise known as the OODA loop. In Figure 1, this is shown as not only a single unidirectional loop but also a series of inner feedback loops which influence the observation and consequently orientation, decision-making and subsequent action. This was originally intended to reflect air combat, however, it has since been recognised that this has wider application for military strategy as well as SA and C² in other domains.

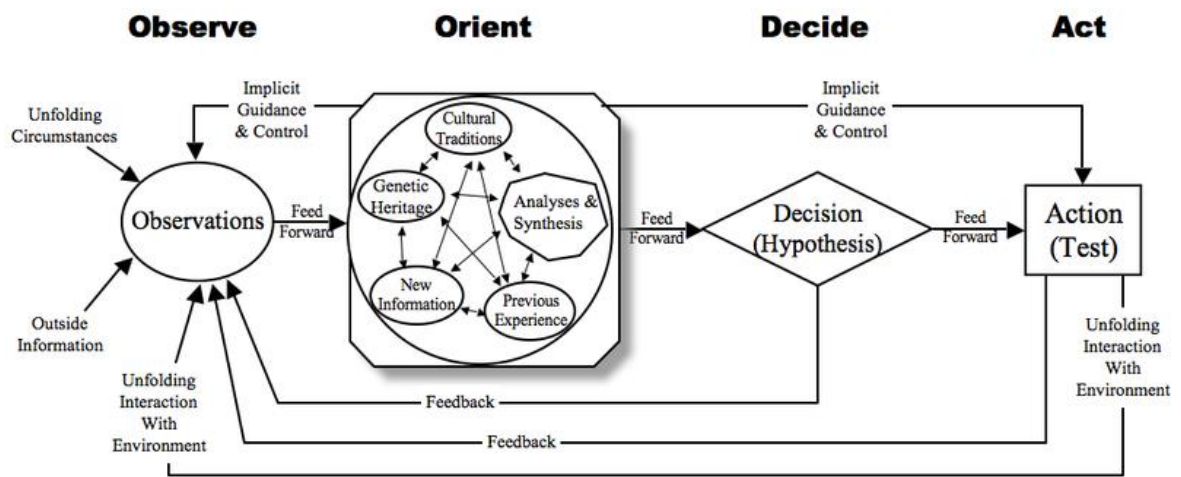


FIGURE 1 - COLONEL JOHN BOYD'S (USAF) OODA LOOP

The general thrust of the model was that if an OODA loop could be completed inside that of an enemy then superiority could be achieved. This is also relevant for cyber warfare and cyber defence as being able to react to an attack before an adversary has a chance to achieve their goals or change tack will provide the defender with an advantage. From a doctrine perspective, the ability to react rapidly to an enemy's actions or changes to them could be considered as "flexibility", i.e. the ability to respond to a changing threat with a suitable countermeasure or action. In order to do this the changing impact on a mission and cost (in terms of asset value) will also need to be understood as the focus of an attack potentially shifts as a result of defensive actions.

Within the same paper the OODA loop is also reflected in a C³I model (Figure 2) developed from the C² models proposed by the US Naval Postgraduate School (Lawson, 1980).

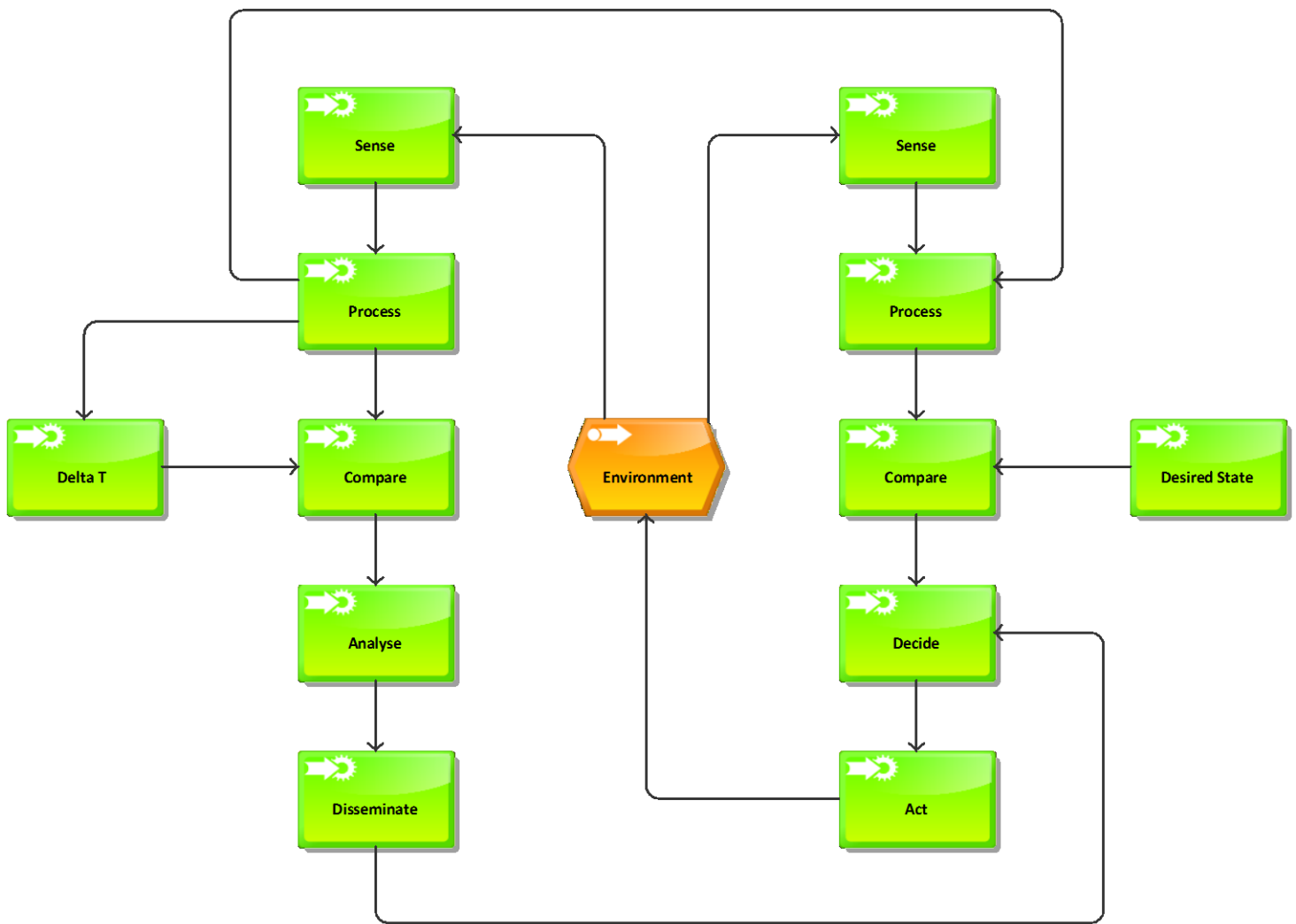


FIGURE 2 - C³I PROCESS MODEL

In this model, the Intelligence aspect can be seen on the left-hand side of the model (with Delta T representing a time difference) and the C² aspect on the right (the communication would be in the sensing and dissemination). Effectively, this creates two unidirectional OODA loops, one for Intelligence and one for C². In the right-hand side, 'sense' equates to 'observe'; 'process' and 'compare' equate to 'orient(ate)' the current situation compared to the desired situation; 'decide' and 'act' then influence the environment which is then reassessed. In the left-hand loop which feeds into the decision-making process of the right-hand loop, analysis is carried out with respect to time which allows some prediction of the direction of the environment; this is then fed into the decision-making to allow more informed actions to be taken rather than relying upon a static snapshot of the environment.

However, in the context of cyber-incident response, the “Desired State” could be replaced with “normal” state to reflect normal infrastructure operation whilst the left-hand side assesses whether the environment is moving away from or towards this state over time. This is a good demonstration of SA; if used in a military decision-making process, the sensors would provide Intelligence information which is then used with expert knowledge or systems to provide a prediction of the future infrastructure state based on monitored behaviour over time. This model immediately draws out several relevant variables: sampling interval, i.e. how often do sensors have to be polled and analysis to take place in order not to miss a change in direction but not so frequently that redundant data is collected pointlessly; granularity of information, i.e. what level of data is relevant to inform the SA, for example, is there any point in collecting an entire packet of data when the tools only analyse headers?

An important issue discussed in the paper relates to the difficulties in prediction of outcomes, particularly when trying to predict past a single decision point. It identifies a probability-based prediction process based on input from domain experts. It also infers a numerical value for the number of decision points which would give an indication of the complexity of the prediction of outcomes. In the context of cyber, the manner of the discussion points to a risk-assessment based decision-making process founded on best available intelligence. An example of how this could be achieved using the Power Distribution Model is then demonstrated in the paper using a scenario of red and blue forces which are tasked with attacking and defending three towns connected by roads which are equidistant from each other in terms of travelling time; weightings are applied in terms of likelihood of successful defence and attack and force sizes are constrained. Even for the initial simple single-decision example for choosing deployment of personnel between these three towns, this is shown to be a complex process which is exacerbated by creating additional decision points beyond the first in order to respond to adversary action. Due to the identified complexities in prediction, it can also be inferred that for better prediction, up to a point, an increasing number of sensors will be required. Beyond saturation information overload will undoubtedly reduce the effectiveness of the prediction or due to the increased requirement for processing and analysis slow the process down.

2.2.4 Intelligence and Related Models

Intelligence and how it is provided as an input to SA will now be examined as this also follows its own models and processes. Since the time of Sun Tzu the aim of Intelligence has generally remained the same (“know the enemy and know yourself”) but the representation of the process has evolved; this now follows the generally accepted cyclic model (Figure 3) of Planning and Direction, Collection, Analysis and Dissemination (Boni & Kovacich, 2000) in some environments e.g. US FBI, the cycle is broken down further to include additional steps such as Requirements and Processing and in the UK current doctrine (Ministry of Defence UK, 2011) this is summarised as Direction, Collection, Processing and Dissemination (i.e. it is accepted that analysis is part of the processing function). This could also be seen to have a parallel with the detection stage of an incident response cycle where the data is collected from the sensors, analysed to detect the incidents and then reported for further action and then sensors will be tuned according to the results. If applied to an incident-response model this would appear to identify an inner loop of incident detection which rotates continuously inside a larger incident response cycle.

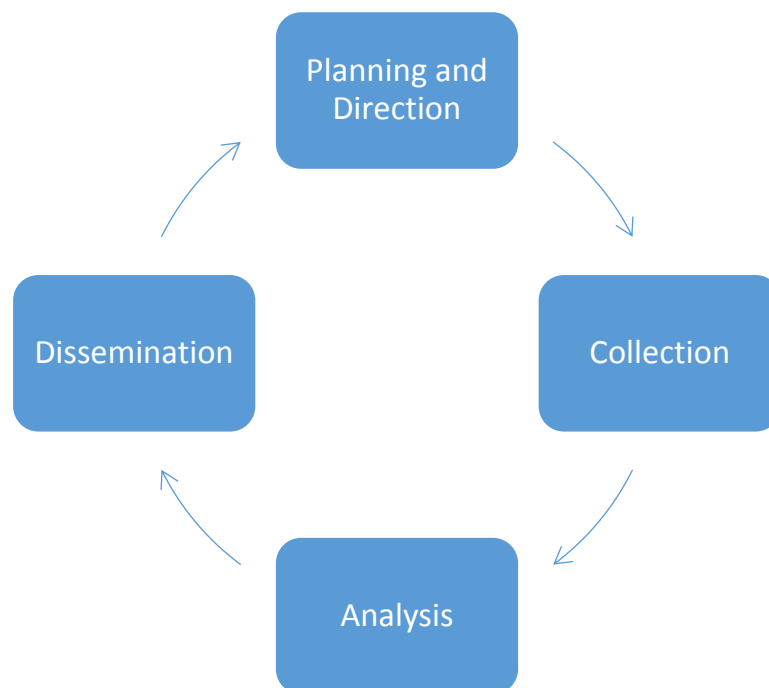


FIGURE 3 - INTELLIGENCE CYCLE

Cyber warfare is an extension of conventional warfare, i.e. originally conventional warfare was land-based, which then extended to include maritime, progressed to include air (and

potentially space) and cyber has now become one of the newest domains. With this in mind, intelligence relating to cyber-warfare is equally valid in the cyber-domain as it is in the conventional warfare domains. This is discussed in detail (Boni & Kovacich, 2000) using the concept of “Netspionage”; a term used to describe network-enabled espionage. The concept describes the changing face of warfare where the conventional goals have been replaced by competitive edge and industrial espionage has become a driving factor. Three realms are discussed where “netspionage” takes place: the ethical and legal, the unethical but legal and finally the unethical and illegal which are named the White Zone, Gray Zone and Black Zone respectively. This infers a variable which describes the propensity of an organisation to cross the boundaries of legal behaviour which will be known as legal tolerance. Within an incident response model this would be seen as a constraint on the response options as undoubtedly all organisations have legal/regulatory constraints on the actions that they are allowed to take in the event of a cyber incident.

Recently, information and intelligence sharing with regards to cyber incidents and attacks has become a higher priority to many nations as was demonstrated by the passing of the “Cyber Intelligence Sharing and Protection Act” (Congress, 2015) where the US Federal Government was tasked to “provide shared situational awareness that enables integrated operational actions to protect, prevent, mitigate respond to, and recover from cyber incidents”. This interest has also been mirrored in international communities where collaborative work has been conducted to improve the information-sharing between disparate entities. One example is Multi-National Experiment 7 (Multinational Experiment 7 Contributing Nations, 2013), an international experiment with the involvement of the UK Ministry of Defence’s Development, Concepts and Doctrine Centre, which investigated maintaining access to the “Global Commons”. In this experiment one of the sub-outcomes relating to the Cyber Domain looked specifically at the issues surrounding Cyber Situational Awareness which culminated in a limited objective experiment with 60 participants from 11 nations where information-sharing between a government hub and four sector nodes was simulated. By throttling or opening information-sharing channels between the nodes and the hub, the effects of changes to incident response were observed. Despite some conclusive results, the experiment did not provide formatted information sharing with communication only being provided in an ad-hoc manner between the various entities. Whilst conclusions could be drawn from this experiment, providing formatted information sharing could have made the information less subjective and would have made it more

digestible for those receiving the information (as if the information is always exchanged in the same format, the processing of the information can be more procedural and consequently repeatable and likely to be more consistent in interpretation). However, the results did indicate that collaboration should be an essential component of any incident response mechanism.

An international collaboration led by MITRE Corporation (sponsored by the United States Department of Homeland Security) addresses the issue of exchanging cyber information through standard formats by the production of a standard to exchange cyber intelligence information (Barnum, 2012). The standard, Structured Threat Information eXpression (STIX) allows collaboration between entities to exchange cyber intelligence including information concerning cyber incidents, attackers and techniques. An overview of the architecture is illustrated in Figure 4. In this architecture, an attack is correlated against known attacks, campaigns, incidents, targets and attackers which are then used to provide a more informed course of action for a decision-maker. In the current version of STIX (OASIS Cyber Threat Intelligence Technical Committee, 2017), 12 domain objects are defined comprising: attack pattern, campaign, course of action, identity, indicator, intrusion set, malware, observed data, report, threat actor, tool and vulnerability. Within these objects, their properties define or infer several variables of interest including: Common Attack Patterns and Enumeration Classification, Vulnerabilities, Course of Action (response). The framework itself also implies both inbound and outbound collaboration.

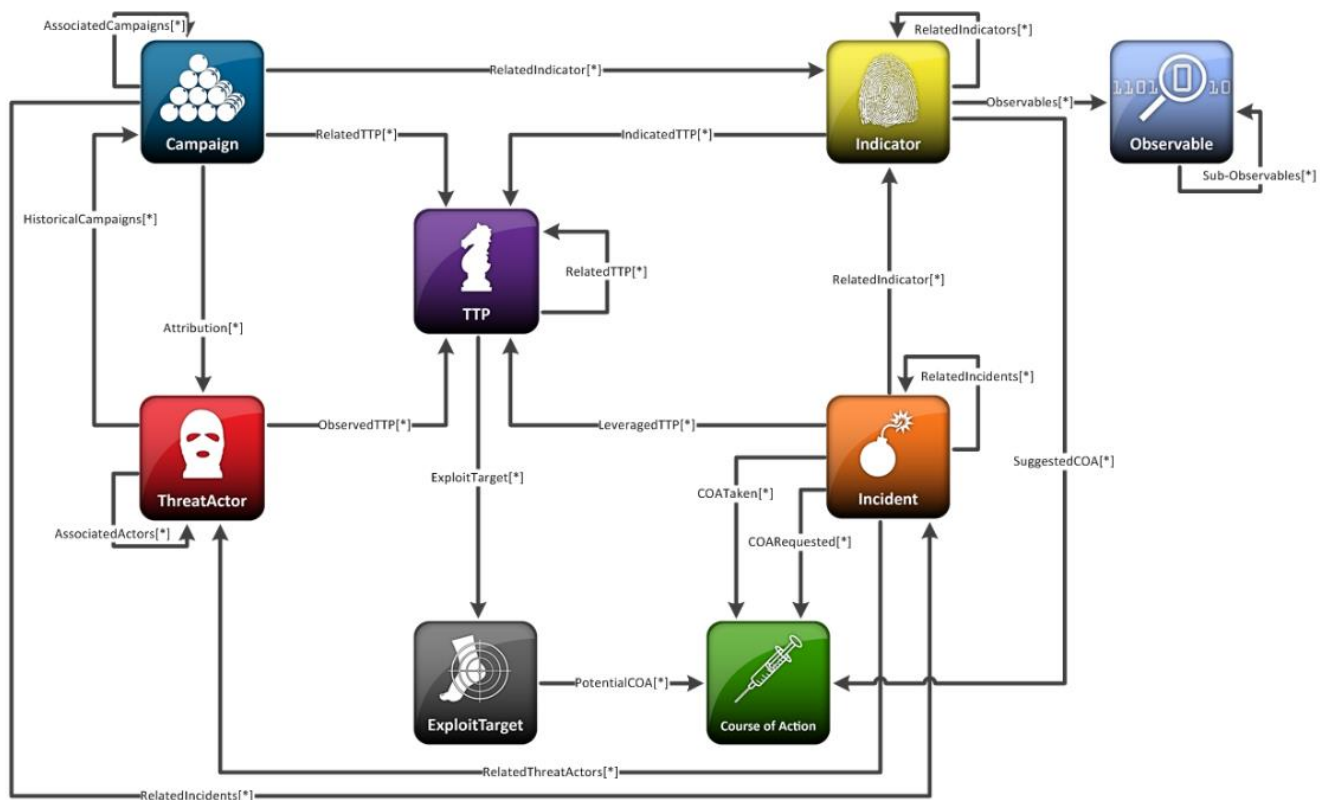


FIGURE 4 - MITRE CORPORATION STRUCTURED THREAT INFORMATION EXPRESSION (STIX) v1.0 (DRAFT) ARCHITECTURE

The paper relating to this standard (Barnum, 2012) discusses the requirement for intelligence relating to attackers and their known methods in order to provide a projection of subsequent action and therefore more effective defence. It also recognises the lack of structured information sharing as being an obstacle to automated analysis but accepts that human analysis will also be required in this complex field. The existence of the STIX standard provided several potential variables (Appendix 2 - Cyber Security Variables) relating to cyber-incident response which were included for evaluation in this research. In terms of a model, this reinforces the requirement for collaboration but also recognises the value of automated tools; it also identifies the requirement for trained and experienced analysts. A European Union-backed development of the information-sharing concept is the Malware Information Sharing Platform (MISP), this open-standard platform allows real-time or controlled exchange of information between collaborating partners in an automated manner (Wagner, Dulaunoy, Wagener, & Iklody, 2016). Although compatible with STIX and many other structured information-sharing formats, this implementation also

expands on information-sharing capabilities by allowing for the granularity requirements of information exchange agreements to be met. It achieves this by controlling distribution of populated information based on community participation or local policy requirements.

2.2.5 Incident Response Evolution

To develop a perspective on the current incident response ethos and processes it is useful to look at how computer/cyber incident response has evolved from its infancy. The first widely-publicised Computer Security Incident Response Team (CSIRT) or Computer Security Incident Response Capability (CSIRC) was announced in 1988 (Schleris, 1988), established as the renowned Computer Emergency Response Team Coordination Centre (CERT/CC) at Carnegie Mellon University with the aim to support the research, commercial and defence industry communities. Members of this CERT and the US Department of Energy Computer Incident Advisory Capability (formed a year later) provided input into one of the first definitive documents to produce a general framework for such a capability (Wack, 1991). Key concepts in this early document include a centralised capability for dealing with computer security incidents, providing security advice, liaison with vendors to address security issues and liaison with security and investigation authorities; but even at this early stage this was envisaged as a capability that could range from supporting a few users to multiple organisations. Additionally, in this document, it was recognised that the CSIRC should not just have a reactive role but also an awareness and prevention role; utilising the experience gained from incidents to influence infrastructure, maintenance and policies. However, although establishing the framework for a CSIRC, this document did not provide a lower-level process description for how incidents would be handled, with the majority of detail provided in the area of legal issues such as how to log and gather evidence for legal purposes, how to store information securely and how to produce disclaimer statements. The derived variables from this document can be found in Appendix 2 - Cyber Security Variables. The leading role of the Carnegie Mellon CERT was reinforced in these early years when it published a paper (Pethia & van Wyk, 1990) emphasising the requirement for collaboration between CERTs/CSIRTS and similar organisations across different communities and international boundaries to achieve the best response to cyber incidents. In 1992 a Dutch CSIRT was established (CERT-NL) followed by a German CSIRT in 1993 (DFN-CERT) and an Australian CSIRT in the same year (SERT, later AusCERT), all comprising members from university research networks. In 1994 more detail about the establishment of a CSIRT was added in a paper (Smith, 1994) presented to the global Forum for Incident

Response and Security Teams (FIRST), using the experience gained from setting up the Australian SERT. This identified many of the same issues highlighted in the 1991 report but also identified in more detail some of the constraints of a CSIRT such as limiting the scope of hardware, software, type of incident and depth of analysis to a level supportable by the resources available. This was one of the early strong advocates for what would now be termed asset management with the commensurate detailed configuration control. Again, the proactive/preventative role of the CSIRT was reinforced.

However, the first comprehensive mainstream document (183 pages) to provide detailed information was produced by Carnegie Mellon University Software Engineering Institute (SEI) in 1998 (West-Brown, Stikvoort, & Kossakowski, Handbook for Computer Security Incident Response Teams (CSIRTs), 1998) the founders of CERT/CC. This described a CSIRT being part of a wider security team within an organization and described a peering relationship between CSIRTs and a breakdown of mandatory and optional CSIRT services. The detail in this document started to point to the CSIRT response not only being the decision of the “security staff” but also other stakeholders in the organization. This could be seen in the “Optional Services” named by this document which included “Risk Analysis” and “Coordination” (with internal and external parties); also the requirement of the incident to be prioritized by the impact on the organization (and not only the type of incident) was introduced. These considerations started to indicate a more intelligent risk-based approach to response but stopped short of involving the senior decision-makers in the organization in the response process for serious incidents. However, in this document a simplistic model for incident response services was illustrated comprising four functions (Figure 5): Triage, the initial evaluation of the alert (be it a report or a request) and a priority allocation; Incident, the confirmation or otherwise of the incident and the identification of appropriate responses; Feedback, by request (e.g. from press/media) or routinely such as annual summaries; Announcement, for example, providing updates on specific incidents and appropriate countermeasures that can be taken by the constituency.

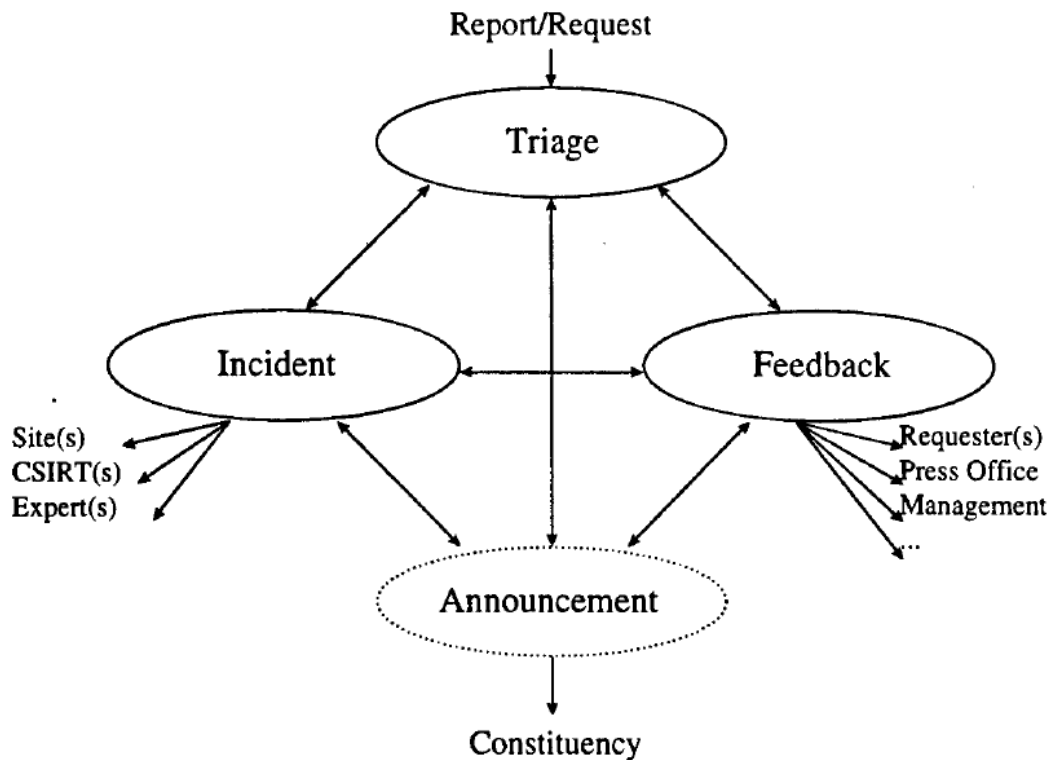


FIGURE 5 - IR SERVICE FUNCTIONS (FROM HANDBOOK FOR CSIRTS, 1998)

This document also identified 3 examples of CSIRT to explain the widely differing aims of different types of CSIRT, these types were: International Coordination Centre, Corporation and Technical. Although not dealing specifically with security incidents at low-level, variables could be derived from the text which are listed and described in Appendix 2 - Cyber Security Variables. However, even at this early stage in a formal process the impact of an incident on an organisation was seen as being an important contributor to an incident-response process and should therefore be included in any model.

In the same year in a collaborative effort between CERT/CC and Sandia Laboratories (a division of Lockheed Martin) taxonomy for Computer Security Incidents was produced (Howard & Longstaff, 1998) which was sponsored by the US Government. This report took several best-practice reference documents from that period which identified individual components of an incident, combined these with the database of incidents reported to the CERT/CC and adjusted them to produce an overall taxonomy. The aim was to produce standard categories that would allow incident information and statistics to be exchanged between CSIRCs and other interested parties. This result was a breakdown of a computer security incident into 3 levels; the incident, the attack and the event which occurred during the attack. The levels were then further broken down (Figure 6) into subcomponents, each

with associated properties. Although not directly affecting the incident response processes and models, these classifications provide a common language; this undoubtedly provides a more formal way to describe and consequently categorise a computer security incident. However, if trying to create an Intelligence perspective some important factors are missing such as individual identification of the attackers (by for example, organisation, team and nation), resources available to them e.g. how many zombie machines are they utilising, how much bandwidth can they access, how many networks do they have access from; complexity of the attack i.e. multistage, zero-day, COTS or developed in-house.

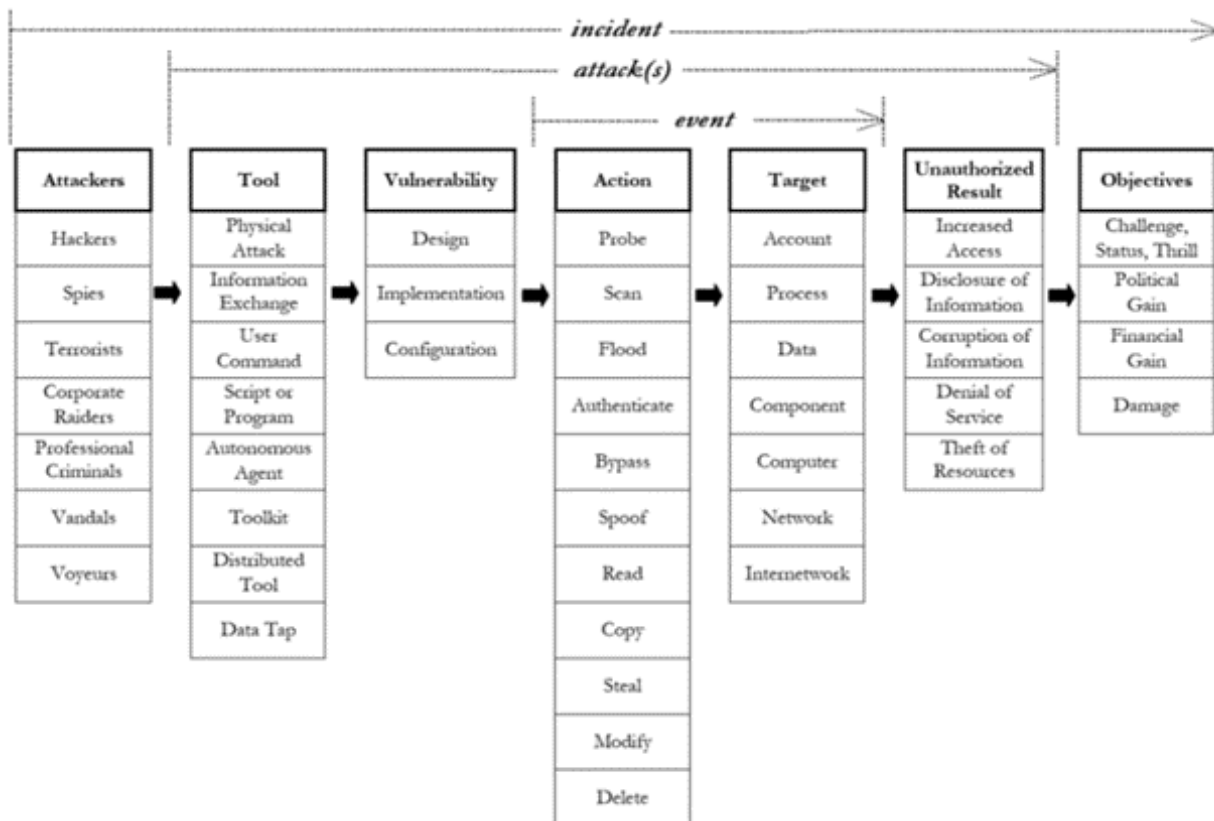


FIGURE 6 - COMPUTER SECURITY INCIDENT TAXONOMY

Later, in 2003, another document produced by SEI (Killcrece, Kossakowski, Ruefle, & Zajicek, 2003) used the results of surveys of 29 CSIRTs across 12 countries to attempt to establish the “state of the art” at that time for CSIRTs (at that time a global total of 151 CSIRTs were registered with FIRST). Although as SEI admitted the sample was not large enough to be statistically significant, it was the most comprehensive study at the time (analysing just under 20% of the registered CSIRTs) and produced results that allowed SEI to come to some interesting conclusions. In 2003, it could be seen that the organizational

placement of the CSIRT varied widely between organizations and sectors; however, in the banking and finance sector the CSIRT was placed consistently under the direction of the CIO which is significant when looking at incident escalation and the values which influence the decision-making process. This report discussed the ability of the CSIRT to make autonomous decisions (also mentioned in the 1998 paper) identifying three types of CSIRT authority ranging from full authority (i.e. no requirement to liaise with higher level authorities or constituents when taking action) to no authority (i.e. liaison and external permission required to take any active response measures). From the review of the surveys and other literature at the time SEI produced a synopsis of the Incident Response Cycle at the time (Figure 7).

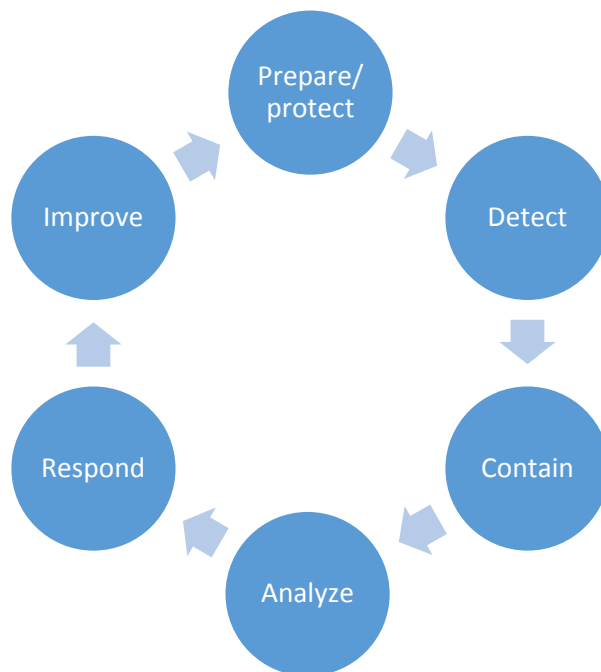


FIGURE 7 - INCIDENT RESPONSE CYCLE - STATE OF THE PRACTICE, 2003

Furthermore, Killcrece also referred to the revised CSIRT Handbook produced by SEI in the same year (West-Brown, et al., 2003) where a more detailed process model of the incident-handling process was illustrated (Figure 8) which combined elements of the IR Service Functions and the 2003 Incident Response Cycle. Although not shown in this model, the importance of retaining statistics relating to incidents to inform the “bigger picture” was stressed in this document, effectively stating the requirement for building intelligence relating to attacks and an evolving knowledge-base. The concept of an asymmetric threat

was also discussed in this document i.e. one skilled attacker only needs to find one weakness in a huge infrastructure protected by a multitude of IA personnel to achieve a compromise. However, this process does not address the improve and planning stages, instead only dealing with the stages “detect” up to the “respond” stages using the parlance of the incident response cycle.

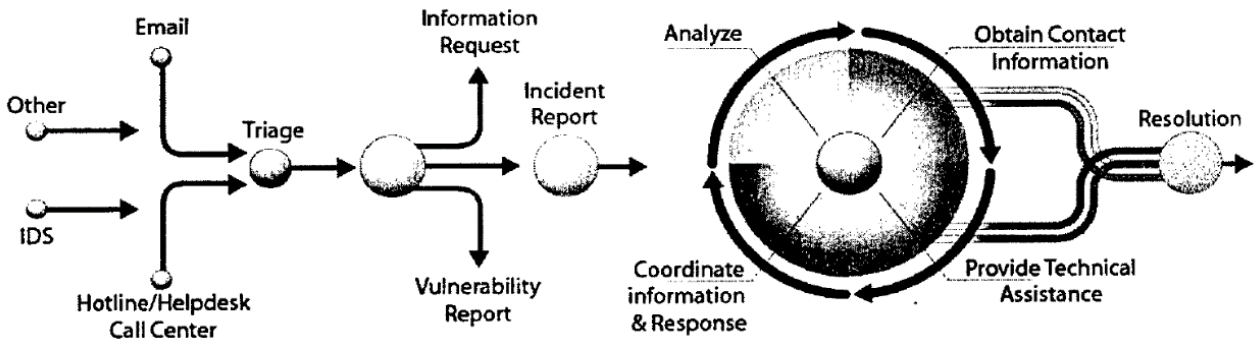


FIGURE 8 - CERT/CC INCIDENT HANDLING LIFE-CYCLE, 2003

One of the other organisations coming to the fore in the field of computer security during this era was the SANS Institute (a private US company specialised in security training and hosting its own CSIRT, the Internet Storm Centre). This also contributed to the modelling of best-practice Incident Response process in the document it produced in the same year (Northcutt, 2003) describing a cycle illustrated in Figure 9 . Although there are some differences when compared to the current models, the supporting text effectively describes a similar cyclic process which still broadly reflects the processes used today.

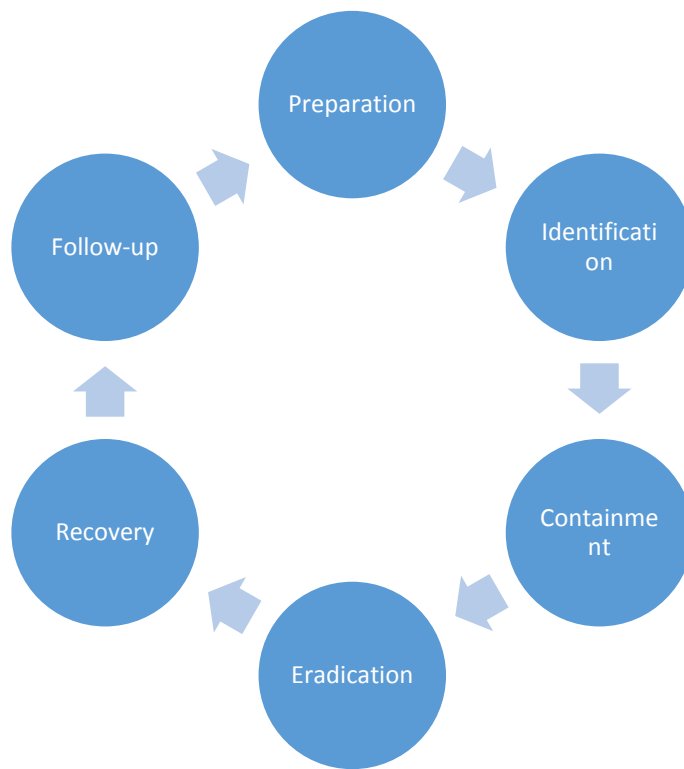


FIGURE 9 - SANS INSTITUTE INCIDENT RESPONSE CYCLE, 2003

Since the incident response cycle models from SANS and SEI CERT in 2003, the most widely-used interpretations of the Incident Response cycle have largely remained the same, however, the current version of the NIST Computer Security Incident Handling Guide (Cichonski, Millar, Grance, & Scarfone, 2012) illustrates this as an inner circle of incident-handling with preparation and post-incident activity (or follow-up) outside of the core incident-handling process (Figure 10). This perspective identifies a longer incident-response process which utilises post-incident analysis to influence the infrastructure and processes in the longer-term i.e. outside of the immediate incident. From the Intelligence Cycle theory described earlier in this chapter it could also be argued that an additional cycle exists inside the NIST model just for detection and analysis.

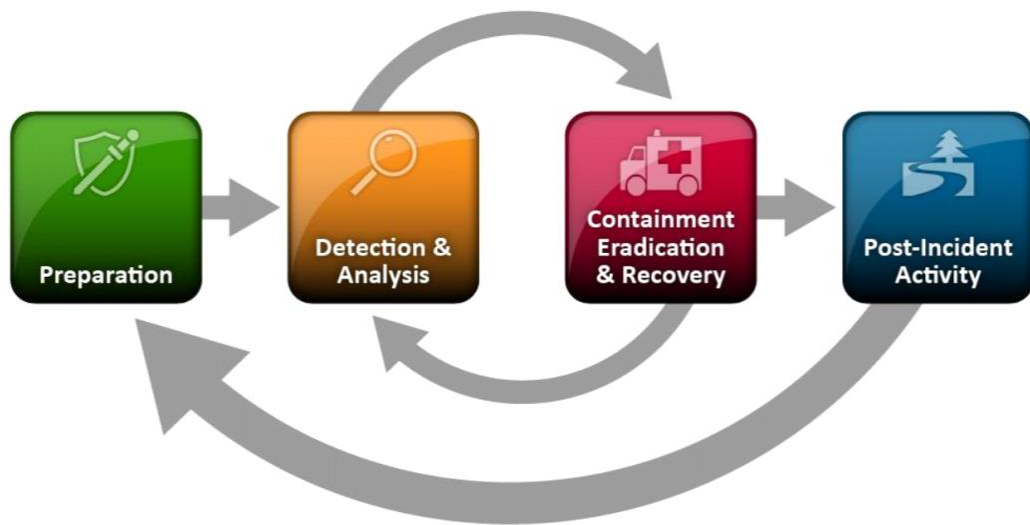


FIGURE 10 - NIST SPECIAL PUBLICATION 800-61 INCIDENT-HANDLING PROCESS, 2012

This very comprehensive and detailed document describes the CSIRC organisational responsibilities, communication strategies, incident-handling processes and records that should be kept during an incident. However, although collecting intelligence during an attack and during the post-incident activity are important areas covered by this document, one significant limitation is that it still advocates containment, eradication and recovery as the prime aims of the CSIRC. In common with its predecessors, even this current model does not envisage monitoring of an attack without actively responding to it as a valid response mechanism i.e. the “do nothing” and observe option to enhance intelligence is not explored. In order to provide optimal protection against subsequent attacks, intelligence about characteristics of attacks and attackers (such as those defined in STIX) must be considered an essential component in preparing an environment to defend against subsequent attacks, consequently, this limitation will be explored in this research.

However, in a more recent paper (Grispos, Glisson, & Storer, 2014) the shortcomings of a linear approach are outlined and an “agile” response advocated. One of the persuasive arguments outlined in this paper is that the incident response should not only cater for the importance of the attacked assets in its approach but also consider the information relating to the attack during the incident itself and when the asset should be handed back to the owner from an investigative perspective. Extending the “agile” theme (He & Janicke, 2015), recent research identifies the lack of effective incident response models for industrial control systems and proposes to address this by making use of agile software

principles in incident response. In using this approach, collaboration between stakeholders is advocated as is providing the flexibility to adapt a response from documented plans by having trained and experienced personnel. However, whilst training and experience are crucial in getting the best result during an incident, standard procedures and documentation are bed rocks to fall back upon during a crisis situation such as a major cyber incident, as advocated in international information security management standards such as ISO27001:2013.

In 2011, a NATO agency (with cooperation from several NATO member nations participating in a NATO-led research task group) produced a document looking at the wider CIS security framework (Hallingstad & Dandurand, 2011) including the incident-response processes (Figure 11). The general theme of incident response in this framework can be seen under the “Operate CIS Security” branch; however, in keeping with the NIST concepts of post-incident activity and preparation, many of the other branches are also relevant outside of the inner cycle (Figure 10). This document also described the importance of dynamically managing risk during an incident and dynamically modifying response to meet the assessed risk (for example, relocating priority assets to sections of the network not being attacked). However, it also introduces a concept under a sub-component of “Assess Damage and Attacks” of allowing an attack to continue (under close supervision) to gain additional intelligence relating to the attack.

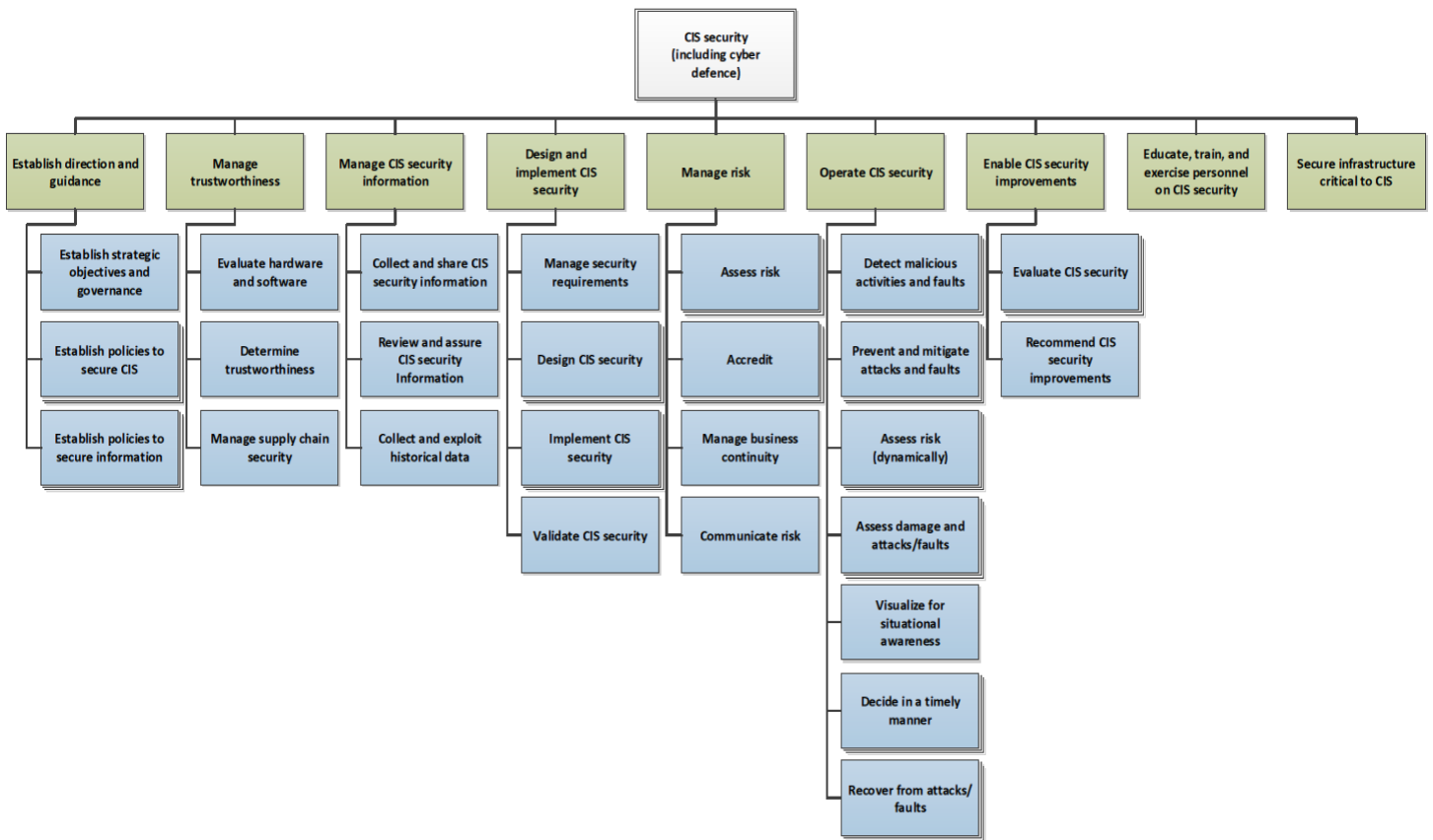


FIGURE 11 - NC3A CIS SECURITY (INCLUDING CYBER DEFENCE) CAPABILITY BREAKDOWN, 2011

Using this concept, a CSIRC traditionally follows a response cycle that only lasts for the duration of the incident (with follow-up action taking place whilst preparing for the next attack). However, if it is recognised that gaining additional intelligence will allow better preparation (by allowing more focused targeting of sensors, protection and resources) it could be argued that allowing an incident to continue could form part of a longer incident response cycle i.e. the incident could continue unimpeded until it is judged that the impact is no longer tolerable to the organisation. This will be dependent upon the mission and consequently risk appetite of each organisation.

2.2.6 Cyber-Defence Model Taxonomy

A general principle applied to the general provision of Information Security according to the early iterations of the Information Security Management standard ISO 27001 (up to ISO27001:2005), (Calder & Watkins, 2008), was the Deming Cycle of Plan, Do, Check, Act. In this interpretation policy, processes and procedures related to managing risk and

delivering and improving information security are planned. The “Do” relates to the implementation of the planned framework including the provision of the necessary infrastructure and resources, “Check” ensures that the implemented system meets the objectives and “Act” is the refinement for the areas where it falls short of the objectives or further potential improvements are identified. Although the explicit reference to the Deming Cycle has been removed from the current version of the ISO 27001 standard (ISO27001:2013) it can still be seen in the layout of the standard, i.e. Section 6 -Planning, Section 8 - Operations (Do), Section 9 – Performance Evaluation (Check) and Section 10 – Improvement (Act). This echoes the NC3A position shown in Figure 11 that Cyber Defence and Incident Response are only a small part of the CIS Security picture.

Drilling down into the incident handling/incident response the latest internationally-recognised standard is provided by NIST (as illustrated in Figure 10). This identifies a preparation phase outside of the incident response loop and a post-incident activity (also outside of the loop) which equate to elements of the Plan, Check and Act of the Deming Cycle but the core processes (i.e. the “Do”, but also elements of “Check” and “Act”) are identified as “Detection and Analysis” and “Containment, Eradication and Recovery” which reflect the “Do” of incident response. Effectively, in this model, elements of the “Do, Check and Act” become a sub-loop of the Plan, Do, Check, Act.

This is in contrast to the earlier SANS (Figure 9) and CERT/CC (Figure 7) models where all processes, which largely follow the same pattern, form a continuous loop.

To summarise, the general thrust of current incident response models in use by the practicing security community is the goal of immediate incident containment or eradication; in these models all intelligence building is carried out in a post-incident analysis phase by which time valuable information may have been lost or new techniques prevented from being exploited. In short, this is an approach that deprives the Cyber Intelligence community of valuable real-time insight into the attacker, their techniques and their available resources. This approach, whilst minimising immediate risk to a defending organisation may harm their longer-term strategic objectives by preventing better, longer-term protection to their and their partners’ infrastructure and information. However, recent academic work (Grispos, Glisson, & Storer, 2014), (He & Janicke, 2015), has highlighted some of the shortcomings of the current incident response methods but has stopped short of providing a new model to deal with them.

2.3 Other Research Relevant to Cyber-Incident Response

In this section, other research will be evaluated for its contribution in supporting or decrying the existing models used by the security community or for its utility in filling existing shortfalls identified in the models so far. The areas related to Cyber Intelligence, Situational Awareness and Collaboration are of particular interest as they appear to be areas of interest for many governmental and international organisations (for example these areas were of significant importance in the recent Multi-National Experiment 7 (MNE7), an experiment looking at the maintenance of access to the “global commons” of Air, Maritime, Space and Cyber); however, they are not addressed comprehensively in any of the reviewed models so far with respect to Incident Response.

2.3.1 Cyber Intelligence

As early as 2000, the importance of usable intelligence in a cyber-environment was recognised (Yuill, et al., 2000). In their research Yuill et al looked at using a military intelligence type process to enhance the effectiveness of intrusion detection and the subsequent incident response. At that time (prior to the introduction of the SEI State of the Practice process (Killcrece, Kossakowski, Ruefle, & Zajicek, 2003), Yuill considered standard incident-response process to be attack repair, neutralization and containment (ARNC). However, by providing a positive identification of the attacker (using part of a proposed technique referred to as Cyber-Intelligence Preparation of the Battlespace (C-IPB)), likely compromised devices (LCDs) could also be identified based on models of the attacker and the infrastructure. This information could then be used to produce two types of estimate for Courses of Action (COA) by the attacker: possible and likely. From these estimates, further monitoring could be more targeted and incident-response measures more relevant. As an example, Yuill uses an example of a “script kiddie” targeting Linux machines in order to run IRC bots; when the sort of machine that he was trying to compromise and his objective had been determined the incident response measures could be scaled appropriately. The C-IPB process is summarised in four steps: define the battlespace (define the boundaries of the infrastructure), describe the battlespace effects (evaluate the infrastructure and its influence on attack and defence), evaluate the threat (assess attacker capabilities and intent) and determine the threat’s COA and infrastructure LCDs. In this process the first three steps all feed into the final step whilst all four steps continue to loop in a continuous unidirectional process. Within the intelligence to be gathered (Yuill, et al., 2000) takes step three (evaluate the threat) and breaks it down into

areas of intelligence to be gathered: what the attacker has done (executed action), capabilities, personal traits, intentions and then dealing with multiple attackers (syndicates or groups). Despite the age of the research, the detail provided in this paper would provide a good base for a cyber-intelligence database; however, as in subsequent research the stated aim of incident response at the time was to negate or mitigate an attack rather than actively allowing it to continue in order to gain better intelligence.

Although cyber-warfare missions may attempt to achieve the same aims as traditional warfare such as disabling critical infrastructure, communications networks and disruption of logistics support (Goel, 2011), the intelligence gathering is not quite as straightforward as deception is much easier to accomplish in a cyber-environment and conclusive attribution much harder to establish. In an examination of the trends in cyber-warfare since 1999 and some prediction of future trends, Professor Goel examines the sponsors, motivation and goals of cyber-warfare and the challenges for intelligence-gathering including the often-overlooked area of unstructured data which can be gathered from blogs, forums and websites prior to an attack. An ontology of unstructured data was mentioned in the article which could contribute to a larger intelligence database; this included attributes such as hacker alias, URLs, post content and dates and times (to allow a relationship to be built between posts and actual attacks). This led on to a discussion of the development of behavioural profiles of actors based on content analysis of open-source data and the proposal to combine this with network data in order to provide better analysis of cyber incidents. A project which examined 120 attacks on the US power grid from around the world over a 10-year period using open-source intelligence (OSINT) and the information recorded from the attacks was used by Professor Goel to illustrate some of the challenges in cyber intelligence-gathering. Some of the issues highlighted included the difficulties in attribution, difficulties in establishing the link between governments and patriotic hacking groups, differing cyber-laws from nation to nation and conflicting political and national interests in providing relevant information to assist investigations. Furthermore, it was suggested that centralised intelligence databases containing information about active hacker groups with information about their political and national affiliations should be created in order to correlate this information with political events and cyber-attacks. Logically it could be inferred that a shared intelligence database between several collaborating partners would provide an even more valuable resource than a central database produced by a single organisation. Due to the speed with which new

attacks propagate (e.g. WannaCry¹), currency of information is also highly important, consequently, both shared intelligence and currency will be investigated as part of this research. The discussion concluded with a recommendation that human intelligence analysis should be supported with tools and techniques to combat cyber-warfare; it also stated that technical analysis (for example, network data, malware analysis and digital forensics) should be supported by the analysis of unstructured data such as websites, blogs and forums in order to complete a more comprehensive cyber-intelligence picture and that techniques should be drawn from computer science, forensics, psychology and linguistics.

For the cyber environment, traditionally one of the key tools for intelligence gathering has been (and remains) the honeypot or honeynet (a single decoy system or a network of decoy systems intended to simulate a real system or network); these are also discussed by Professor Goel (Goel, 2011). These are intended to gather intelligence about hackers, their methods, their resources and their capabilities. However, due to the prevalence of counter-deception tools and methods it is becoming increasingly difficult to produce a convincing honeypot or honeynet. This has been borne out by mathematical analysis of the elements required to produce a convincing honeypot (statistical analysis of file-systems of real and honeypot systems) by comparing popular implementations with metrics taken from real-world systems (Rowe, 2006). This paper concentrates on difficulties in emulating static file-systems of real-world systems and supports this with extensive mathematical analysis of both deception and live file systems. However, when also taking the emulation of running processes, network connections and network traffic into account, the problem becomes even more complex. The increasing effectiveness of counter-deception tools in identifying honeypot/honeynet and other monitoring environments is also discussed. This limitation in gathering relevant and current intelligence information naturally leads to the question “where can the best intelligence information be obtained?” This discussion is not only relevant for variables relating to cyber-intelligence but also those relating to possible response options.

The problems relating to honeynet use are reinforced by a paper (Wang, Wu, Cunningham, & Zou, 2010) which demonstrates that the use of a popular honeynet tool would routinely alter worm propagation and characteristics through a network in such a way that it would be detectable to a person controlling a botnet created by the worm. The research

¹ <https://www.ft.com/content/82b01aca-38b7-11e7-821a-6027b8a20f23>

conducted to support the paper uses a specific worm implementation to create a functioning botnet in an experimental environment and demonstrates how a honeynet would be detected. It also models the worm propagation if a honeynet detection procedure were to be embedded in the worm, demonstrating that this sort of counter-deception technique would not significantly influence worm propagation i.e. the worm would detect and signal the presence of a honeynet and take appropriate action but the operator of the honeynet would not realise that the worm had this capability as the performance of the worm would not be detectably affected. This again adds weight to the argument that traditional honeynets and honeypots are not necessarily effective methods of gaining intelligence about advanced attackers and their techniques. This research will therefore investigate other methods of obtaining intelligence.

Another issue in the production of usable intelligence information, rather than unprocessed intelligence data, is that the language used must be unambiguous to all recipients of the information; this would logically lead to the requirement for a common language to describe the observed cyber activities or phenomena. This issue was investigated in the context of military cyber-simulation (Chapman, Leblanc, & Partington, 2011) where an unspecified number of cyber-attack model and simulation implementations were examined. Despite the military context and the lack of direct supporting data (although references were provided), the paper provides a logical language to describe an attack which would also be usable outside of the military domain. However, it constrains itself to general cyber-attacks i.e. not those government-supported attacks against specific targets using techniques which are not widely-available. It categorises the attack into levels of privilege required to execute an attack and then subtypes of each these to describe the attack. It then discusses delivery methods for the cyber-attacks. The last section of the body of the paper then describes how the characteristics of the attacks can be simulated. However, by limiting the paper to attacks not executed by government-sponsored entities using advanced techniques, the description of an attack is unlikely to meet the requirements of all incident response facilities. Despite this, with some expansion on some of the main categories, this could provide the basis for a usable cyber-intelligence database (again reiterating the requirements for frameworks such as STIX).

2.3.2 Legal Perspective and Attribution

When examining the potential response to a cyber-attack, it is wise to examine the current (December 2017) international legal norms and constraints. In this respect, this section

discusses some of the relevant legal issues, discussions and consequently the constraints and difficulties in responding to attacks. In general, a cyber-attack can be considered to be a “wrongful act” defined as *“The breach of an international obligation by a State through a series of actions or omissions defined in aggregate as wrongful occurs when the action or omission occurs which, taken with the other actions or omissions, is sufficient to constitute the wrongful act.”* (United Nations, 2001). A response to a “wrongful act” is legitimate as *“the wrongfulness of an act of a State is precluded if the act constitutes a lawful measure of self-defence taken in conformity with the Charter of the United Nations”*². The Charter of the United Nations (Article 51) states *“Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security”* (United Nations, 1945).

However, when responding to a “wrongful act” it is the responsibility of the “wronged state” to establish attribution beyond reasonable doubt before responding (United Nations, 2001); this concept is also deemed to be applicable to the Cyber domain (Shackleford, 2010). The discussion relating to the requirement for establishing attribution beyond reasonable doubt and the thresholds required to necessitate a response has recently been a point of discussion in the cyber warfare legal community (Lucas Jr, 2014). Unlike the physical warfare domain this is not a straightforward task as those launching the attacks may be hidden behind several layers of intermediate proxies, often located in countries which have no formal agreement with those being attacked (Geers, 2011). Even the code used in tools such as malware may be manipulated in “false flag” operations to shift the blame to others (Rid & Buchanan, 2014). However, the Tallinn Manual (NATO Cooperative Cyber Defence Centre of Excellence, 2016) does not absolve those whose infrastructure is inadvertently used for cyber-attacks of responsibility (Rule 6 – Due Diligence) as there is a requirement for due diligence on their part.

² Article 21 - (United Nations, 2001)

When considering different responses to cyber-attacks, the following aspects are understood to be the appropriate legal statuses per international norms at this point (December 2017):

- a. Traditional response: this is the response where the attack is stopped or negated as quickly as possible using only resources under agreed control of (or in cooperation with) the defending organisation and influence is only applied internally. There is no known legal controversy surrounding this approach as there is no subterfuge involved and the only resources directly affected or are those of the organisation or partners collaborating with the organisation. This is reinforced by the Tallinn Manual where Rule 2 (Internal Sovereignty) where it is stated that “*A State enjoys sovereign authority with regard to the cyber infrastructure, persons, and cyber activities located within its territory, subject to its international obligations*” For this response, no attribution is required (although, undoubtedly, the defending organisation will attempt to establish attribution when the attack has been neutralised during the post-incident follow-up).
- b. Passive response: in this response although subterfuge is used, with the intention of appearing that the attack hasn’t been noticed, no physical influence is applied upon the attacking infrastructure (or intermediate infrastructure being used as proxies by the attacker). This method of response and intelligence gathering is not known to contradict any relevant legislation as Rule 2 of the Tallinn Manual (Internal Sovereignty) remains applicable.
- c. Active Reconnaissance/Intelligence Gathering: this is an offensive act which could be used in response to a damaging attack to establish attribution or additional intent. Rule 32 of the Tallinn Manual (Peacetime Cyber Espionage) states that this activity is not per se a violation of international law when carried out in peacetime but the method by which it is carried out could be a violation. Rule 89 (Spies), states that “*Cyber Espionage and other forms of information gathering do not per se violate the Law of Armed Conflict*”. This rule applies to members of the armed forces when carrying out cyber espionage during armed conflict; however, it also mentions that cyber

espionage conducted by civilians could be seen as “direct participation in hostilities” which would also make them a valid target for an opposing state.

- d. Kinetic Response: when an attack has been adjudged an “armed attack”, the nature of the attack is irrelevant as one of many similar interpretations states that *“a cyber-attack need only penetrate a critical system to justify a conventional military response that could start a physical, kinetic war.”* (Hathaway, et al., 2012).

- e. Cyber Offensive Operations: these have a number of issues, the first is that the nature of the operations need to be almost surgical in nature as Rule 111 of the Tallinn Manual (Indiscriminate Attacks) states that *“Cyber Attacks that are not directed at a lawful target, and consequently are of a nature to strike lawful targets and civilians or civilian objects without distinction, are prohibited.”*. This is also echoed in Rule 113 (Proportionality) where an attack which is deemed to cause incidental death or injury to civilians and is judged to be excessive with respect to an anticipated and justified military advantage is prohibited. Rule 114 (Collective Punishment) also iterates the nature of precise targeting and attacks as it prohibits the punishment of those not involved in the conflict, the example provided is depriving an area of Internet activity to punish its inhabitants for actions carried out by some individuals.

However, Rule 123 (Ruses) does permit cyber deception along the lines of Information Operations and deployment of honeypots/honeynets.

2.3.3 Situational Awareness and Information Fusion

Although important, Cyber Intelligence alone (with regard to information regarding an adversary’s actions, capabilities and resources) cannot provide enough information for decision-making as the mission, defending infrastructure and capabilities are equally important. To this end, cyber-intelligence forms only one component part of SA, which in aptly simplistic words can be summarised as “knowing what is going on so you can figure out what to do” (Adam, 1993).

With its origins in the Air environment, a paper discussing SA proposed a model based on human factors (Endsley, 1995). Extensive analysis of human factors research discussed in the paper resulted in a model (Figure 12) which distilled SA into 3 key stages: perception, comprehension and projection. However, as can also be seen in this model, the environmental constraints (e.g. automation, interface design, complexity) and human factors (e.g. ability, training and experience) have also been recognised as important contributors in providing the situational awareness, taking decisions and in carrying out the response. Parallels can be drawn from Endsley's SA elements with Lawson's C³I process model where the sense, process, compare and analyse functions could be interpreted as equivalent to the perception, comprehension and projection, especially as the dissemination from the analysis feeds into the decision-making (Moore, Friedman, & Procaccia, 2010) in the same way that SA feeds into decision-making in Endsley's model.

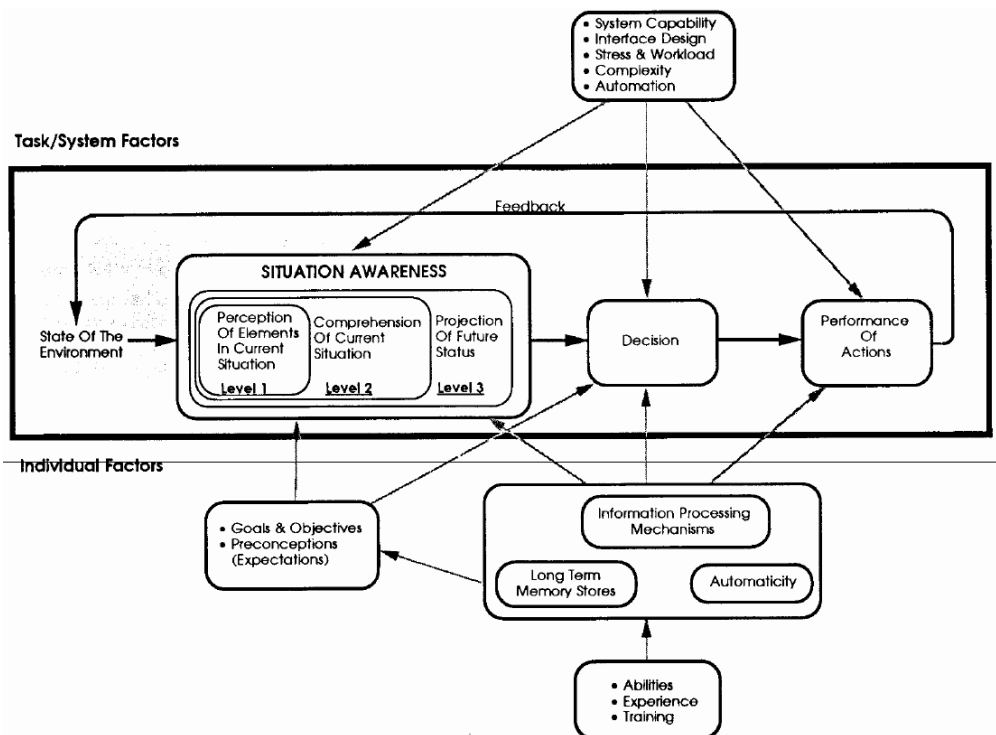


FIGURE 12 - ENDSLEY'S SA MODEL IN DYNAMIC DECISION MAKING

Adding more detail and expanding on the process to include a 4th level of SA, a newer model (Figure 13) was developed from by extending and combining Endsley's SA model and the Joint Directors of Laboratories (JDL) Data Fusion Model; this model was created specifically to represent the Cyber SA domain (Tadda & Salerno, 2010). One important concept within this model, which also addresses Intelligence processes, is that it requires

the sensors/data collection requirements be reviewed and refined with each iteration of the SA cycle. In the description of this model importance is placed on not only “Knowledge of Them” i.e. understanding the strengths, weaknesses and capabilities of the adversary, but also “Knowledge of Us” i.e. knowing the vulnerabilities within your own environment and the impact that the adversary may cause by their actions.

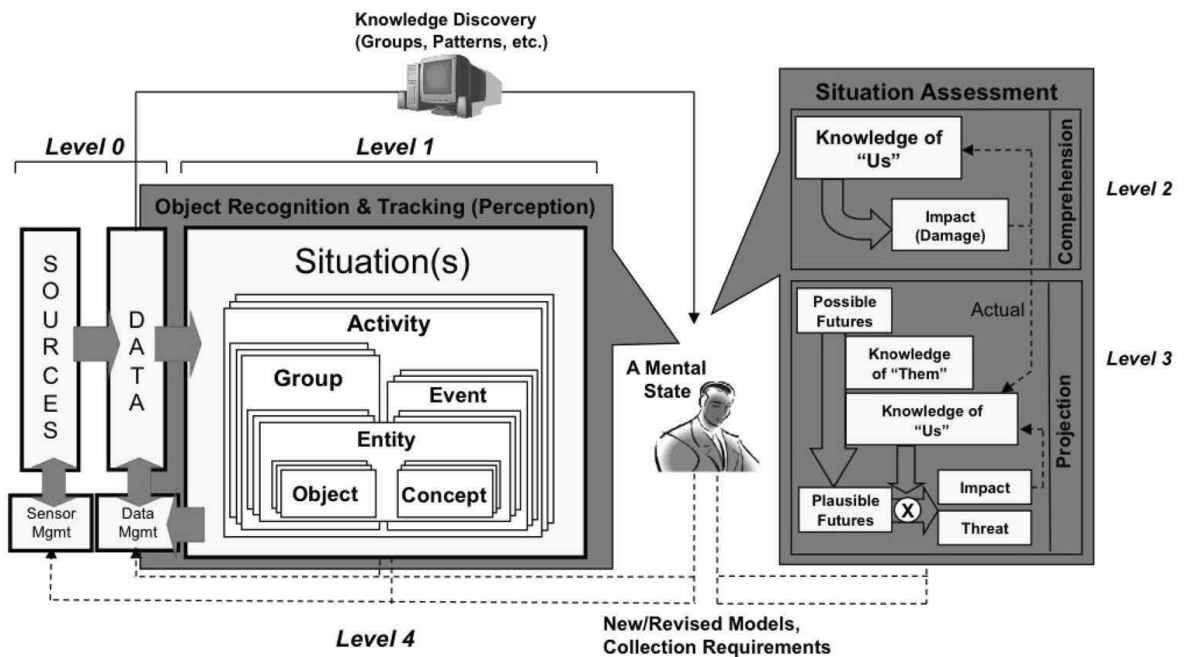


FIGURE 13- TADDA AND SALERNO'S CYBER SA REFERENCE MODEL

Looking in more detail at some of these practical issues related to SA and referring back to Sun Tzu’s tenet of “know the enemy and know yourself”, it is as important to know your capabilities, infrastructure and weaknesses as those of your adversaries. This issue is discussed in a paper discussing the dual-hatted nature of vulnerabilities (Moore, Friedman, & Procaccia, 2010). In this paper vulnerabilities are discussed from both an attacker’s and defender’s perspective. The initial discussion concentrates on the discovery of a new vulnerability and the quandary for the entity discovering it relating to whether they should announce it to the producer (in order to receive a patch and better secure their own infrastructure) or to “stockpile” the vulnerability in order to develop an exploit which could be utilised later on against an adversary (provided that they haven’t already discovered the vulnerability first and stockpiled it whilst mitigating in other areas).

The second discussion (assuming that vulnerabilities haven't been disclosed) relates to whether knowledge of the vulnerabilities will be utilised aggressively (i.e. to actively develop and employ exploits against an adversary) or defensively (i.e. develop mitigation strategies to negate the effect of an attack exploiting the vulnerability). Two separate gaming models are proposed in the paper to represent these decisions and analysed (albeit from a US-focused perspective). As the US has a declared cyber-offensive capability, the gaming models proposed are valid for this environment; however, other nations (and many organisations) are neither resourced to conduct nor are legally allowed to conduct any offensive action (Clapper, Lettre, & Rogers, 2017). Despite this, the conclusions of the paper are still interesting from an incident-response perspective, one of the key findings was that cyber-warfare exchanges are likely to lead to escalating cyber-offensive behaviour (even if a defensive posture is the preferred *modus operandi*). Despite the political nature of the high-level decision-making inferred by this paper one of the underlying concepts required to support these models is comprehensive asset management, otherwise a defender will not know where their vulnerable infrastructure is and what it is vulnerable to; this is one of the key requirements in national risk management (Federal Emergency Management Agency, 2017) and is also mandated in international Information Security standards e.g. ISO 27001:2013. Expanding upon the asset management issue, the relative values of the assets at the time of the attack should also influence the prioritisation of effort and resources which should be an integral part of the decision-making during a cyber-incident.

Taking asset management in a slightly different direction, research was conducted into correlating scanned and known vulnerabilities in an organisation's infrastructure with known exploits to indicate potential attack paths (Patsos, Mitropoulos, & Douligeris, 2010). In this research, a map was created of infrastructure and known vulnerabilities by using vulnerability assessment tools and public vulnerability databases (such as CVE from Mitre Corporation). A tool called the Incident Response Intelligence System (IRIS) was developed to take this information with IDP signatures (at the time of the research totalling 33,000 vulnerabilities and 16,000 IDP signatures) and create a topological vulnerability analysis (TVA), effectively mapping out the vulnerabilities and attack paths (as well as response paths) through the infrastructure and indicating a schedule of exploitation in order to accomplish a compromise. The vulnerabilities were also scored according to base (relating to the fundamental characteristics of the vulnerability), temporal (time dependant

characteristics of the vulnerability) and environmental (impact on local infrastructure) metrics. This information was then correlated and used to create a set of tuned signatures. When used in experimental networks and the real-world network of a private bank, it was discovered that not only did the correlation provided by this tool reduce the number of signatures required, but also reduced the number of false positives (therefore improving SA by reducing clutter). The research also included evaluation of the tool by 20 professionals from the Greek Information Security community; although a small sample size, it is reported that the tool received very favourable feedback.

Leading on from the asset management discussion, one field that generally has good control of assets within its infrastructure is the safety-critical/critical national infrastructure domain. Despite the comprehensive asset management, this is also susceptible to cyber-attacks like any other directly or indirectly connected infrastructure e.g. Stuxnet. However, much of the infrastructure tends to be specialised e.g. the associated equipment and network components may be of the SCADA variety; consequently, research into cyber protection of this infrastructure tends to be fairly specialised. Nevertheless, some of this research has wider applicability in terms of general concepts. A paper in 2016 investigated automated identification of cyber-attacks in cyber-physical systems, (Ntalampiras, 2016), this concentrated on attacks against integrity i.e. corruption of critical information. Of particular note, is that this paper proposed using detected incidents as an input to an automatic identification engine utilising machine learning which would then identify the type of attack in order to allow a responder to counter the attack more efficiently. This paper reinforces two important points highlighted in other papers discussed in this chapter; automated detection is essential in order to cope with the quantity of information being received by the sensors and a trained human should always make the final decision about the response to be taken.

One of the difficulties with responding to an incident is assessing the potential damage that may be caused if an incident is not contained effectively; this is exacerbated by the ever-evolving nature of complex multi-stage attacks. To address this issue, research was conducted into information fusion (Yang, Stotz, Holsopple, Sudit, & Kuhl, 2009) which mapped cyber-defence into Endsley's model (and a related model from the US Joint Directors of Laboratories relating to Information Fusion). The stages identified were "malicious activity detection", "alert correlation and tracking" and "threat projection and impact assessment". To accomplish this, work carried out by the research team in the

Information Fusion Engine for Real-Time Decision-Making (INFERD) and Threat Assessment for Network Data and Information (TANDI) was combined and utilised. The first tool tracks an attack (using IDS alerts) and combines this with a template for standard attacks (independent of actual infrastructure configuration) and then overlays this onto basic IP configuration of the infrastructure to map the progress of the attack. Using a 4-step process this then establishes context for the attack in order to provide new attack tracks. TANDI then uses a database which maps machines, privileges and databases to work out the next vulnerable assets, based on those which have already been compromised. Threat levels are also assessed based on the assessment of hacker intention, target value, hacker skill level and exposed vulnerabilities. From the perspective of Endsley's model, INFERD is heavily focused on the "projection" phase.

Making more use of the available Cyber Intelligence, research was conducted (Hutchins, Cloppert, & Amin, 2011) into the use of kill chains to target Advanced Persistent Threats (APTs). In the paper discussing this research it was identified that cyber security methods currently concentrate on reacting to incidents post-compromise rather than using existing intelligence and targeted detection to uncover persistent attacks. A core component of Intelligence is described in this paper as an indicator which can be atomic (indicators which maintain their identity during an intrusion such as an IP address, email address or CVE number), computed (those which are calculated or derived such as hash values or regular expressions) and behavioural (descriptive but potentially also using a combination of both atomic and computed indicators to describe the pattern of an attack). The attacks were assessed as being spilt into seven disparate phases, starting with "Reconnaissance" and culminating in "Actions on Objectives". An example matrix (Figure 14) was used to demonstrate how courses of action (COAs) could be taken to detect, mitigate and stop the various phases, it should be noted that this example does not cover all possibilities as, for example, a honeypot could be used in multiple phases described by the example.

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	“chroot” jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

FIGURE 14 - COURSES OF ACTION MATRIX [HUTCHINS, E. 2011]

By tracking the attacks (and changes to the attacks) over time as well as the effectiveness of the employed response measures in each element of the potential kill-chain it is asserted that the defenders gain an advantage as the attackers will invariably reuse components in their attacks. This is then illustrated by utilising three separate but related incidents where an intelligence picture was constructed highlighting the common areas behind the attacks.

Whilst recognising that being able to block an attack earlier in the kill-chain may deprive a defender of intelligence relating to novel methods later in the attack Hutchins recommends analysing the blocked attack for evidence of new directions in the later stages. However, no proposals not to counter an attack are suggested (which could gather more comprehensive and accurate intelligence).

2.3.4 Collaboration

Looking at incidents in isolation (i.e. per site or per organisation) will logically provide only a very small cross-section of information for Cyber-Intelligence or SA purposes. Whilst this can be supplemented with open-source information from public vulnerability and other databases such as those at cve.mitre.org or nvd.nist.gov, sharing of information in near real-time with those in a similar geographical location, sector or culture may provide relevant information which helps “complete the picture” during a cyber-attack.

In 2009, as a result of a large-scale distributed attack on infrastructure in 2004, the University of Illinois tried to produce a framework to provide a multi-site collaborative incident response framework known as Palantir (Khurana, et al., 2009). In this research, the challenges of collaboration were discussed including the establishment of trust between collaborating organisations, coordination of processes between organisations and the coordination of incident response across organisations. The paper utilised the “lessons learned” from the attack which, due to the complex nature of the attack, cost more than 3000 hours of investigation effort by a variety of parties including the FBI. Although only using one complex security incident to evaluate the framework against, the generic descriptions defined in the “Roles and Responsibilities” within the framework would be applicable for a wide range of incidents, however, these only address the incident from the incident-handling perspective; it could be imagined that there might be a higher-level process (at a more political/command decision-making level) where decision-making and communication with collaboration partners would be carried out at a more political level (e.g. between CEOs of rival telecommunications companies addressing a common threat but where proprietary information would be of utmost importance).

Within the framework, the Process Model (Figure 15) describes several components of a collaborative process, which are split into those of a site participant and those of an “Independent Centre for Incident Management” (ICIM). Examination of the “Detection and Strategy Development” and “Local Investigation and Recovery” elements within the “Site” process components reveal that they largely reflect the steps used in standard incident response cycles with the analysis being conducted by the ICIM. The ICIM then coordinates the investigation, if deemed necessary and formulates a collaborative response. However, unless the ICIM is also aware of individual organisational priorities the suggested collaborative response may not be appropriate for the sites; equally the suggested “collect and preserve evidence in a forensically sound manner” for the sites may not always be possible due to operational imperative. Ultimately, the final decision for a response should be approved by an appropriately-informed individual at a site with the authority to make that decision with full knowledge of the impact on the organisational priorities. Despite these minor issues, the framework addresses some important issues such as “trust”, “anonymization of data” and collaborative workspaces, furthermore the creation of a functioning prototype collaborative web application complete with incident templates was certainly a step forward at that time.

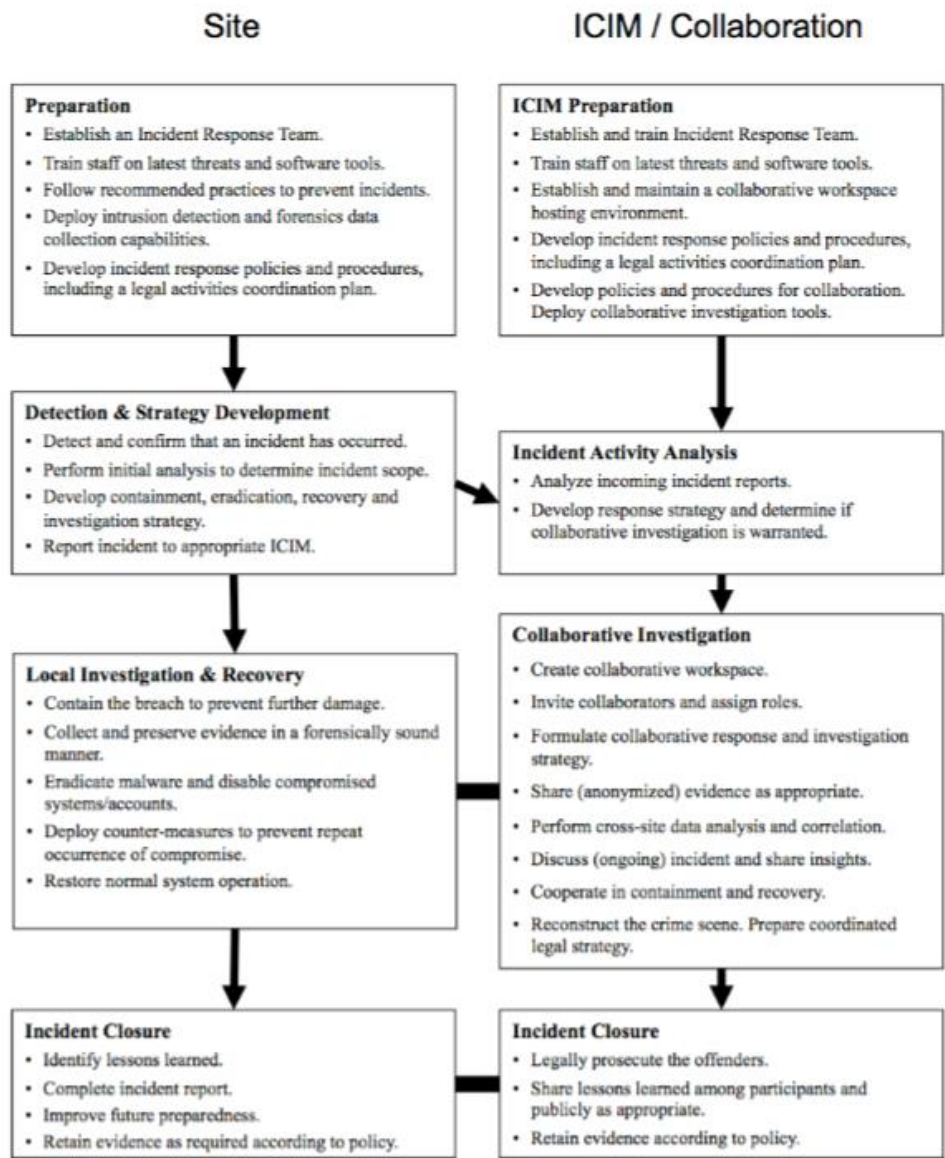


FIGURE 15 - PALANTIR FRAMEWORK PROCESS MODEL

The following year more research was published in this area (Takahashi, Fujiwara, & Kadobayashi, 2010); by dividing cyber-security into 3 operational domains (Incident Handling, IT Asset Management, and Knowledge Accumulation) interfaces are defined between the domains with a function named “registrar” inside the Knowledge Accumulation domain that is responsible for organising and maintaining relevant information so that it can be used by other organisations. This also identifies the requirement to have comprehensive asset management where known vulnerabilities can be mapped against known attacks for organisational infrastructure to produce a risk knowledge base.

It refers to some existing non-aligned standards for some of the information required by these domains such as Common Event Expression (CEE), Common Vulnerabilities and Exposures (CVE) and Common Attack Pattern Enumeration and Classification (CAPEC) from MITRE Corporation, Incident Object Description Exchange Format (IODEF) also known as RFC 5070 from the Internet Engineering Task Force (IETF) and Common Vulnerability Scoring System (CVSS) from FIRST; these and several others are candidates for sharing but even the multitude of existing standards also have gaps (including a standard to describe an attack unambiguously). Although this paper only touches on collaboration, concentrating instead on the formal registration of cyber infrastructure, posture and incidents in databases, the provision of common standards such as STIX for sharing incident information must be an essential component of any collaborative incident response process. However, due to organisational and national sensitivities, there must also be some mechanism to censor or anonymise data which could be regarded as damaging to the organisation when collaborating (as also discussed in the Palantir Framework).

2.3.5 Risk, Stakeholders and Decision-Making

To realise effective cyber-incident response, a decision maker requires the support of effective risk-assessment tools and risk-management strategies, taking account of all affected stakeholders and organisational goals.

Looking at the risk issue, one of the significant problems with cyber incidents is a lack of historical data with sufficiently accurate information to be able to assign meaningful values to the constituent components required for risk assessments. This issue was one of those encountered by the Italian Ricerca Sistema Energetico (RSE) Laboratory (Dondossola, Garrone, & Szanto, 2011) although targeted at investigating the effects of cyber-attacks on power control and distribution networks this research has much wider applicability. One of the objectives of the research was to mitigate the lack of historical data to produce meaningful values for plausibility and severity associated with vulnerability existence, threat occurrence and attack successfulness. The intent of this research was to produce a methodology for producing a power-specific risk index variable (i.e. an assessment of risk specific to this industry) to support the cyber-response decision-making process. To accomplish this, the research used experimentation on a special-to-type network configured in accordance with international standards for power networks. The experimental network was designed to represent a multi-site and multi-component network used to control and distribute power. A number of attacks (comprising 5

identified stages) using multiple attack paths were used to attempt compromises of the infrastructure, however, these were all looking from the perspective of a network based attack (i.e. Internet inwards).

Some of the results from the research were to be expected such as: risk is highly dependent on security policies and employed security measures; an intrusion is successful if access controls and authentication measures can be bypassed; the robustness of the communications protocols at application and transport layers influences the complexity of an effective malware mechanism. However, some of the conclusions were less obvious and may not be true for other infrastructures including: sneaky intrusions are those in which the malware tasks are executed for a brief period of time; a lot of first-hand information is needed for an attacker to be able to interfere with the communication of devices in the process networks, this decreases the probability of successful intrusions during critical functions. This last conclusion in particular is not necessarily true for other networks and, as Stuxnet has proved, “security by obscurity” is no guarantee of protection; in fact this was already alluded to as far back as 1883 in a paper discussing cryptographic principles (Kerckhoffs, 1883).

Overall, this paper from a national laboratory whose responsibilities include research into the protection of critical national infrastructure provided an excellent insight into the cyber issues experienced by the power sector and utilised an experimental approach supported by extensive mathematics to address a gap in the existing literature. However, the concerns of the power industry are seen as primarily availability and integrity whereas for other sectors confidentiality would be equally if not more important. Additionally, this research concentrated on attacks from outside the local network whereas “insider threat” (both intentional and unintentional) are also equally legitimate threats.

One of the issues within risk management is that a standard calculation for risk is given by $\text{Risk} = \text{Asset Value} \times \text{Threat Rating} \times \text{Vulnerability Rating}$ or similar wording (Federal Emergency Management Agency, 2017). However, asset value can be very subjective as can threats and vulnerabilities depending on the perspective of the person carrying out the assessment. In the previous paragraphs risk was reviewed from the standpoint of the operational power provider. Consequently, when considering the Information Security tenets of Confidentiality, Integrity and Availability, confidentiality was treated as a lower priority than integrity or availability which would potentially lead to a higher threshold for acceptable risk for confidentiality, however, a bank would undoubtedly view confidentiality

differently. To address this issue, research was conducted (Aissa, Abercrombie, Sheldon, & Mili, 2011) into building a tool to calculate failure cost (i.e. cost of a compromise) from different user perspectives. This utilised matrices to model stakeholders and their willingness to implement security measures based on their interpretation of asset value. Additional matrices used in the calculation catered for impact of a compromise and dependencies within the architecture.

The paper demonstrated the use of a tool to automate the calculations and also discussed several interesting concepts such as classes of stakeholder, allocating a financial value to all assets (but not as a reflection of literal financial value). However, a statement was made in the paper that only security measures should be implemented which provide a positive return on investment (ROI) for all stakeholders but I strongly disagree with this assertion; even in a corporate environment it is often the case that positive ROI may not be achieved by all parties but a measure is still worth implementing when the overall picture is taken into account (for example if failure would result in fines from legislative bodies or significant reputation loss). Some other interesting observations which were mentioned in the paper were that satisfying a particular security requirement may have different priorities for different stakeholders; additionally, although stakeholders may have different priorities and risk tolerances; these were not necessarily orthogonal. This identification of different perspectives is interesting from a cyber response perspective as the perception of the appropriateness of the response measure may differ depending on the stakeholder consulted (which may also not be aligned with strategic objectives). This is also a worthwhile investigation area for this research.

Another scientific approach to decision-making was investigated (Roy, 2010), where the use of attack countermeasure trees (a similar concept to fault tree analysis used in the safety-critical engineering domain) was proposed to assist the decision-maker in choosing optimal cyber defence infrastructure and countermeasures. The proposed model takes into account not only the risk and impact of an attack, but also return-on-investment (ROI) for the defender and what it terms the "return-on-attack" (ROA) for the attacker. The model uses three classes of event to represent an attack and defensive measures; these are an attack event, a detection event and a mitigation event. The model allows for both qualitative and probabilistic analysis which was implemented using software packages to calculate ROA and ROI. The algorithm was also modelled using a software package but this was to calculate the minimum defence infrastructure to cover the widest range of attacks

and, to demonstrate this, an attack on SCADA infrastructure was used as a case study. The calculation for the SCADA attack claimed that an optimal solution was obtained in less than 16 seconds for 5000 leaf nodes (i.e. lowest level nodes in the tree). However, neither processing power required to achieve this result or verification by any other method that this was indeed an optimal result was discussed.

At a higher level, research was conducted into the inherent biases involved in strategic security decision-making (Workman, 2012). Although not directly related to incident-response, which tends to be operational decision-making, the impact of the discussed biases has some relevance. The paper made 4 propositions which essentially boiled down to people with higher risk acceptance, who are optimists, are overconfident and/or rely on tools to support decision-making are more likely to continue with strategic security initiatives. To evaluate this, a study of a large multinational corporation was conducted over a period of 3 years, specifically looking at the way that their Research and Development (R&D) committee responsible for strategic security initiatives functioned. This R&D committee comprised membership from a broad cross-section of the departments and levels of seniority across the company. Utilising a survey to analyse the decisions that were made and Structured Equation Modelling (SEM) to analyse the results, 3 out of the 4 propositions were supported and the other (relating to high behavioural anchors or what I have classed as optimism) confirmed.

One of the findings of the paper was that when making long-term strategic security decisions, decision-makers tend to rely on “gut-feel, heuristics and naïve theories but as timescales were shortened decision-makers were more willing to be supported by tools in their deliberations. This is of interest for incident-response as decision timelines tend to be very short and this research (although targeted at a different decision-making level) would indicate tools are likely to be utilised by decision-makers for selecting optimal incident-response actions.

2.3.6 Academic Integrity

An analysis of security models, metrics and frameworks was carried out in 2009 (Verendel, 2009); this document demonstrated that at least up until 2008 very few security concepts and models had a scientifically quantifiable grounding. The 90 papers examined were subdivided into 4 perspectives used to create the paper; these were “confidentiality, integrity and availability”, “economic”, “reliability” and “other”. In total, only 11 of the

papers were assessed as being created from the traditional perspectives and of these only one was validated using empirical data and 4 by theoretical arguments. The paper also asserts that many of the common assumptions used in some of these papers have some evidence disputing them and that probabilistic independence assumed by some of the models is contradicted by statistical testing. From a logical perspective, this makes sense, as the state of a component in a system is not completely independent of the components around it, for example, a compromise of an internal system would first require a compromise of some form of perimeter defence; equally from an attack perspective, the execution of an exploit for an advanced attack would first require some form of reconnaissance. Even considering all of the evaluated papers together, only a minority of the papers attempted to support hypotheses with empirical evidence. However, even where empirical evidence has been used much of this has been based on expert judgement or superficial testing (e.g. small sample sizes and unrepeated tests). One of the major criticisms of the research investigated by this paper was that the testing environments did not accurately reflect the “real-world” operational security environment in that the normal interaction between attacker and defender could not be simulated, for example, the attacker changing tack when the defender employs a countermeasure. Therefore, this research should evaluate the practical implementation of any developed models in an environment where “real-world” employment is validated.

The challenges related to producing verifiable theory and models relating to Cyber Security were expanded upon in a later paper (Carroll, Manz, Edgar, & Greitzer, 2012). This research identified some issues which were common to all areas of science and then some which were particular problems for evaluating the cyber-security domain specifically. It was asserted that a falsifiable theory, where a hypothesis is disproved by observation, is not easy to confirm as the decision-making processes and motivation of attackers are by their nature difficult to confirm as real-world attackers do not usually make themselves available to the scientific or academic communities. The difficulties in ensuring that reproducibility of experiments was ensured was also described, although it was accepted that the hardware environment could be “imaged” virtually, the reluctance of the researchers in releasing the software which formed the instantiations of algorithms or models was seen as an issue as was the release of any data that was used. This led on to the control of variables, where cyber variables were divided into two categories: environmental and social. It was stated that whilst environmental variables were

controllable as for other natural sciences (as, for example, computers, networks and other systems could be controlled) the social variables could be more problematic but could be overcome by the use of experimental and control groups.

However, leading on from the social aspects, bias was perceived to be a problem both from the perspective of bias on the part of the researcher and due to perception of the experiment participants. Biased experimentation design by the researcher i.e. trying to prove a hypothesis rather than looking for flaws in it is logical and well understood but the paper describes a phenomenon where subject groups naturally try to fulfil the expectations of a researcher rather than acting as they would when unobserved. A proposed solution for this was to use a double-blind experiment where neither the participant nor experimenter knows which conditions are control or treatment. In practice, this may prove difficult to achieve for a cyber-incident response model as knowledgeable participants will be able to identify what “normal practice” is for cyber response.

2.3.7 Areas of Concern and Shortfalls in Current Theory and Models

From the reviewed literature, up until 2017 from both the practical and academic perspectives, there are several areas of concern and shortfalls in the reviewed research, documentation and the consequent models and concepts. These could be summarised as narrow perspectives and lack of credible supporting evidence. The following paragraphs describe these areas in more detail.

The majority of the Computer/Cyber Incident Response models and concepts appear to address the incident response process from a security practitioner or a CIS manager’s short-term perspective, i.e. the intention is to eliminate, mitigate or contain an incident and recover full functionality as quickly as possible. However, if an incident is viewed from an intelligence-gathering or command and control (C²) perspective the standard incident response process may be counter-productive as not observing the incident for a longer period may deprive the defender of additional information which could be used to protect and monitor the infrastructure better in the longer-term. This is addressed in the NC3A framework document which, whilst not describing a model or process (instead describing an organisational and capability framework), accepts that observing an incident without countering it (within constraints) is a valid incident response option.

Furthermore, when reviewing intelligence and C³I models, there is significant scope for integration of some processes and harmonizing of others between the models, including feeding observed incident behaviours into intelligence SA tools to provide enhanced SA to the intelligence community. Endsley's model recognises that Goals and Objectives should be one of the driving factors for obtaining SA. Therefore it could be argued that obtaining an Intelligence advantage could be an SA objective and, if comprehension and projection were deemed to be insufficiently grounded, the decision-making process could be used to influence the information gathering process (although in this model there is no feedback to loop to the sensors or environment feeding the SA).

Lawson's C³I model could address this shortcoming as the SA, if modelled by the left-hand side influences the decision-making process (on the right-hand side) which then results in an action which influences the environment. However, to be effective the whole process of this evaluation, the modified information gathering, and the reaction would still need to be inside the adversary's OODA loop, otherwise the information gained will be too late to be of use i.e. the adversary will change tactic before the intelligence advantage can be used effectively; this would require a more active approach to Cyber Defence. Ultimately, the use of SA gained from the incident response process will allow the intelligence community to provide better-founded advice to commanders. The draft STIX standard and the supporting research, the US Cyber Intelligence Sharing and Protection Act and the work carried out during MNE7 are also helping the movement towards more collaborative SA which will invariably feed a better Cyber Intelligence knowledgebase.

Some of the models discuss criticality of incidents and infrastructure but the practical literature reviewed rarely describes risk-based approaches to incident response (and never describes dynamic risk as a function of the organisational business cycles) although the academic work in this field is starting to support this approach (although not directly in the incident-response area). At the level of an operational or strategic commander/CEO a risk-based approach to incident response could provide a more efficient (and cost-effective) method of reacting to incidents whilst still taking account of organisational missions and goals.

The models and concepts, although largely based on the experience of very knowledgeable and experienced security professionals, are not often shown to be based on incontrovertible empirical evidence. Furthermore, some analysis of some of these models

and the supporting research has asserted that there is evidence directly contradicting some of the assumptions that are made.

2.3.8 Additional Notes on Gaps

If instead of current incident response models, the protection of CIS infrastructure is viewed in the longer-term, it may be beneficial to place more importance on learning about the attackers, their methods and their resources; this could allow more efficient use of resources in configuring the protective infrastructure. In the past, this was possible with honeynets or honeypots but the resource requirements (in terms of manpower and training/experience) to establish a credible honeynet/honeypot (i.e. indistinguishable from a live system or network) have become significant and are certainly beyond the reach of many organisations. From an Intelligence perspective, the indicators of an incident (or reporting of an incident) could be viewed as part of the collection process. If the analysis, dissemination and planning/directing processes occur quickly enough (i.e. inside the enemy's OODA loop) they could be used to inform the next stages of the incident response process. Although mainstream Incident Response cycles do not currently allow for events to continue unimpeded, the documentation supporting NC3A's CIS Security Capability Framework recognises that this could be a valid response within some constraints.

Although risk assessment is frequently mentioned in the initial configuration of the security infrastructure and periodically reviewed, little mention is made of using this dynamically in response to specific incidents in real-time/near-real-time. This is undoubtedly a shortcoming in most environments as the priority and sensitivity of information and systems changes with time and mission e.g. the sensitivity and priority of a mission plan (or marketing strategy in a corporate environment) is undoubtedly higher prior to execution than it is after execution/implementation.

To be able to credibly establish the effectiveness of differing incident response models and processes, a formal testing environment would need to be established. However, in order to do this, a key set of variables and a method of grading the achieved results would need to be produced to allow a valid comparison between the models and their processes.

Additionally, SA considerations would need to be taken into account which can also be deduced from the literature including: the reliability of the sources, the optimum level of abstraction required to track incidents, the best method to present the information, the timeliness of the information and the quantity of the information.

In **Error! Reference source not found.**, the relevant areas covered by the reviewed literature are summarised, this highlights some additional areas of concern from a practical point of view. Although several good databases are available which describe known vulnerabilities and the corresponding exploits, none of the reviewed literature has a comprehensive tool for creating a cyber-intelligence knowledgebase (although some of the components are described which would be included in such a database). In particular, trying to identify an attacker (be it an individual attacker, a group or an organisation) from the attack characteristics (e.g. attack methods, objectives, complexity, employed resources etc.) is a complex problem. The complexity comprises several factors such as: the time and resources required to dissect an attack and any malware that is employed, and the possibility of “false flag “operations where an attacker tries to mislead a defender by employing a third party’s tactics, techniques and procedures (TTP)s.

Such a resource which allows reasonable confidence in identifying an attacker could prove invaluable in the decision-making associated with cyber-security incident response as it could contribute to the projection/prediction process.

TABLE 1: AREAS OF INTEREST DISCUSSED IN REVIEWED LITERATURE

	Collaboration	Infrastructure/ Environment	Intelligence	Modelling	Priorities	Dynamic Risk/Value Assessment	Enhanced SA	Response
AISSA (2011)	X	X	X	X	X	X		
BARNUM (2012)	X	X	X				X	X
DONDOSSOLA (2012)	X	X		X				
ENDSLEY (1995)	X	X	X	X			X	X
GOEL (2011)			X			X	X	X
HALLINGSTAD (2011)	X	X	X	X	X	X	X	X
HOWARD (1998)	X	X	X	X				
HUTCHINS (2011)			X	X		X	X	X
KHURANA (2009)	X	X	X				X	X
KOVACICH (2000)			X		X			
MOORE (2010)		X	X	X				X
ORR (1983)	X		X	X			X	X
PATSOS (2010)		X	X	X		X	X	
ROWE (2006)			X					
ROY (2010)		X	X	X	X	X	X	X
TADDA (2010)		X	X	X	X	X	X	
TAKAHASHI (2010)	X	X	X					X
VERENDEL (2009)		X				X		
WANG (2010)			X	X				
YANG (2009)	X	X	X	X			X	
YUILL (2000)		X	X	X			X	

2.3.9 Hypothesised Model

Based on the areas identified in the literature review which were covered in the previous sections, general groupings of contributing elements are hypothesised in **Error! Reference source not found.**. These groupings comprise a number of variables, identified in the researched papers as deeming to contribute to robust Cyber Security in general and effective incident response in particular. These variables and their references in the documents are described at Appendix 2 - Cyber Security Variables.

Using these variables, an initial model was hypothesised to explain the potential interaction between the associated processes. This resulted in the model shown at Figure 16; this model describes several peripheral processes (fed by sensors, local and partner intelligence sources and interacting with local resources and capabilities). These peripheral processes drive the core processes of situational awareness and dynamic risk/value assessment which in turn drive enhanced situational awareness to provide optimal decision-making. Based on the capabilities and constraints of the defending organisation an appropriate response is then chosen.

The groupings in the hypothesised model can be interpreted as follows:

- a. Collaboration Partner: this grouping receives both outbound information from incidents and provides information relating to incidents in partner networks.
- b. Infrastructure and Environment: this is the locally controlled environment determined by policy, resources, budget and other constraints (such as legal).
- c. Intelligence: this is the intelligence information contained in a knowledge base, built from history, live incidents and collaboration information.
- d. Priorities: these are the organisational priorities based on owner valuation, mission information and stage in the mission/business cycle.

- e. Response: these are the response options expanded from the traditional contain and eradicate response to include more intelligence driven and offensive options.
- f. The modelling is required to determine the effect of the known situation (both in the defended infrastructure and with respect to the nature of the attack) and provide a projection of the future. The situational awareness and dynamic assessment then provide enhanced situational awareness to better inform a response decision.

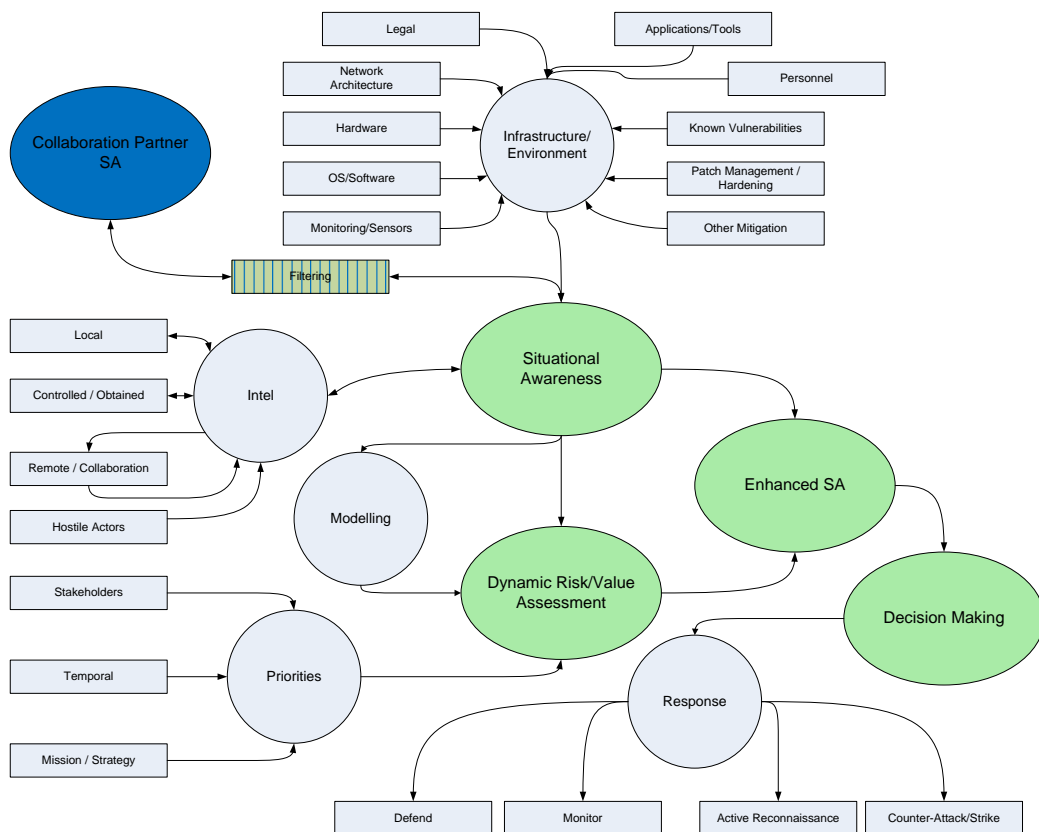


FIGURE 16 - INITIAL HYPOTHESISED MODEL

3 Research Methodology

This chapter describes the research methodology approaches employed in this research and the reasoning behind the choices. The initial section provides an overview of some of the epistemologies used in researching in general, this is then investigated in more detail for the methods used in this work. Finally, the relevance of the employed methods is demonstrated by explaining how these are implemented in practice in this research.

3.1 Methodological Review

This section investigates research strategies, philosophies and their strengths and weaknesses. The applicability of the strategies and philosophies to different types of research is also discussed in this section. This is dependent upon the paradigm, i.e. the lens or perspective through which the environment is viewed, and the approach of the researcher. One example is the researcher that is experienced in the domain and already has ideas about the problem and solution, they may wish to prove or disprove their preconceptions. The other end of the scale is the researcher who approaches the problem from a position of domain naivety; they may be unaware of the scale of the problem and any potential solutions or direction towards them. However, ultimately, the chosen philosophy must support the achievement of the aims and objectives which, for this research, are summarised below.

- a. Aim: to provide a dynamic and relevant model for Cyber Security Incident Response.
- b. Objective 1: analyse the problem space by investigating the key variables that define its dimensions, specifically this should include all variables deemed to be influential in providing the decision maker in the cyber incident response process with the best information to decide upon a response.
- c. Objective 2: develop a model to represent the defined problem space and potential solutions whilst addressing perceived gaps within the prevalent cyber incident response models.

- d. Objective 3: evaluate the developed model against the prevalent incident response models and the perceived deficiencies in those models.
- e. Objective 3: assess the implications of practical instantiations of the employed model against the problem space.

3.1.1 Research Strategies

In general, research strategies can be described as qualitative, quantitative or a combination of the two, often described as mixed methods and sometimes as triangulation (Dawson, 2009), these are summarised in Table 2. Quantitative methods lend themselves to the numerical analysis of survey research data and experimental data where well-defined measurements can be taken. Qualitative methods are more complicated as the approach may be more subjective (due to conditioning of the researcher). For example, Ethnography includes observation and interview, which relies upon unbiased collection of and interpretation of relevant data over a long period of time (Creswell, 2009). Grounded theory, another qualitative approach, is a strategy where the researcher interprets the views of participants in order to create abstract theory which explains the research subject, however, this itself will be undoubtedly be influenced by the inherent cultural norms and biases of the researcher. Whilst it may appear that this would lead to quantitative research being the preferred method for credible research, not all research topics are capable of providing data which can be measured or quantified objectively. Consequently, to try and achieve the optimum result from research a combination of these strategies is often used, known as mixed methods. Mixed method strategies strike a balance between the measurable, where the area of research lends itself to the collection of well-defined data, and the interpretable, where no acceptable measurable variables exist or can be established. Mixed method strategies are then further divided into sequential (where one method is used after another), concurrent (where methods are used at the same time) and transformative, which is described as choosing the appropriate combination of methods determined by the perspective of a theoretical lens (Creswell, 2009).

TABLE 2 - COMPARISON OF RESEARCH STRATEGIES

Quantitative Methods	Qualitative Methods	Mixed Methods
<ul style="list-style-type: none"> • Pre-determined metrics • Measurable data • Statistical analysis and statistical interpretation (Hevner, Ram, March, & Park, 2004) 	<ul style="list-style-type: none"> • Open-ended questions • Interview and observation data • Interpretation of patterns and themes 	<ul style="list-style-type: none"> • Closed and open questions • Mixed data (measurable and subjective interpretable) • Statistical and interpretative analysis

This PhD research is conducted from the perspective that a gap exists in current cyber-incident response processes; to evaluate the gap a literature review was conducted, from this a number of variables were identified (qualitative) and then the importance of the variables evaluated by professionals potentially impacted by cyber incidents. The format of the evaluation was based on Likert scale responses (again qualitative). This was reinforced by the subsequent statistical analysis of these qualitative responses including the structural equation modelling. However, during the experimentation, measurements were taken of response times and deviation compared with expected responses which could be considered to be quantitative. Therefore, the chosen research strategy is Mixed Methods and more specifically Transformative Mixed Methods (Creswell, 2009) as the qualitative approaches and quantitative strategies are determined by the goals and stages of the research.

3.1.2 Research Philosophies and Methodologies

With the research strategy in mind, within each strategy there are several different perspectives, often referred to as world views, paradigms or epistemologies and ontologies

(Creswell, 2009). The way that these perspectives are differentiated is summarised quite succinctly by a set of three questions extracted from (Guba & Lincoln, (1994)):

- a. *The ontological question.* What is the form and nature of reality and what is known about it?
- b. *The epistemological question.* What is the nature of the relationship between the knower and the would-be knower and what can be known?
- c. *The methodological question.* How can the inquirer (would-be knower) go about finding out whatever he or she believes can be known?

Using this framework, some of the relevant philosophies are described below.

Positivism and Post Positivism

One of the best-known philosophies is positivism (usually associated with quantitative research although also relevant for some qualitative research), which maintains that there is an attainable absolute truth which can be established from objective unassailable facts and measurements. However, this has now fallen out of fashion to be replaced by post-positivist (essentially a revised more realistic form of positivism) which maintains that absolute truth cannot be established but if the methods of enquiry are competent that “authorised conviction” or “warranted belief” can be achieved (Phillips & Burbules, 2000). This philosophy is deterministic, believing that causes are likely to lead to certain effects or results. It is assumed that the researcher and the subject are completely independent with no influence being exerted by the researcher upon the research results. The approach for post-positivism is to start with a theory, make objective empirical observations and take appropriate objective measurements; these will either support or refute the theory. The theory is then revised appropriately before subsequent tests are carried out. Positivist approaches aim to predict through understanding of absolute truths (Hudson & Ozanne, 1988).

Critical Theory

Critical Theory is also relevant for this research; in this philosophy it is assumed that once relevant “realities” have been shaped by external influences over time. Although historically these realities may have been relevant, changes in the environment or understanding may have rendered the historical reality unsuitable for the present. In this

philosophy the researcher and the research subject are linked (i.e. the outcome is likely to be subjective). The nature of this philosophy requires extensive dialogue between the researcher and those impacted by the research. The outcome is likely to challenge traditional thinking and will undoubtedly require community acceptance in order to achieve its goals.

Interpretive

The interpretive approach takes this one step further, it has the view that reality is a perception; it is wholly dependent upon the person viewing it and is only reality because it helps the viewer make sense of their world i.e. several realities exist dependent upon the individual or groups interpreting the information (Hudson & Ozanne, 1988). The goal of the interpretivist approach is to understand behaviour, with understanding being a continually refined process rather than a result. This approach therefore sits at the other end of the philosophy spectrum from positivism.

Constructivism

Constructivism is therefore an interpretive approach, it relies upon individuals and communities for its reality; it is dependent upon the experiences of those impacted by the research and the interpretation of those carrying out the research. It encourages the researcher to continually reshape their findings during the research based on interaction with the subjects or those impacted by the research. This philosophy requires extensive interaction between the researcher and respondents in order to elicit opinions and feedback.

Design Science Research

However, the social science origins of these philosophies do not necessarily meet all requirements of research in the technical arena. In order to conduct research in a technical field it was necessary to utilise a method with clearly defined stages and outputs. To make optimal use of the mature behavioural science research methods, whilst incorporating best practices from the problem-solving design science approach Design Science Research (DSR) has been proposed as a more relevant research method for the Information Systems Research field than traditional research philosophies (Hevner, Ram, March, & Park, 2004). In this respect, DSR cannot be evaluated directly against the same 3 questions, as it relies upon the traditional behavioural science research methods to establish the initial business needs thus identifying the problem. However, when the problem has been identified in

enough detail to allow the development of a prototype artefact, a combination of rigorous scientific methods and empirical methods may be used to establish the nature of reality. By the nature of DSR, the spiral iterations of build and evaluate require an intimate relationship between the researcher, those affected by the research and the evaluation of the artefact. In general, this method captures the more practical design, build and evaluate model, similar to the spiral prototyping model commonly used in software development (Boehm, 1988). The DSR process comprises awareness of a problem, a suggestion to address the problem, development of a solution, evaluation of the solution and then conclusions which are used to refine the awareness of the problem. It utilises a combination of establishment of truth from the behavioural science research methods and creation of utility from Design Science.

In summary, the overall approach for the research is Design Science Research (DSR) as this accommodates different approaches at different stages of the research. The spiral-development approach for the artefacts produced by DSR also suits this research as a mix of objective measurement (aligned with positivist approaches) and subjective opinions and observations (aligned with interpretive and constructivist approaches) can be used to refine the artefacts in order to produce the optimal solution for those impacted by the research.

3.2 Applicable Research Methods

Overall, the research methodology is mixed methods as many of the philosophies and strategies were best suited for different stages of the research. However, this mixing of approaches is catered for within the DSR paradigm, which is the main thrust of the research methodology throughout this research. To elaborate, the early stages of the research would utilise the traditional philosophies from the critical theory and positivist philosophies in identifying the variables that were thought to be influential in Cyber-Incident Response; this would be followed by the development of the hypothesised model which could be considered the first artefact in the DSR cycle. This stage would be followed by the more objective post-positivist evaluation of the relative importance of those variables. In the DSR framework, these initial stages establish the business need and relevance of the research whilst reinforcing and providing refinement to the awareness of the problem. This would then lead to the production of a principal component model to address the problem which would then be subjected to Structural Equation Modelling (SEM), which is also a positivist approach (during the second DSR cycle). After refinement of the model

based on the results of the SEM, the model would then be subjected to operational validation, experimentation and further analysis utilising the fielded prototype (COST), the final artefact following the DSR approach. The reflection of the overall use of Design Science Research advocated by Hevner utilising 4 phases i.e. Problem Awareness, Suggestion, Artefact and Evaluation is illustrated in Figure 17-Research Philosophy Use.

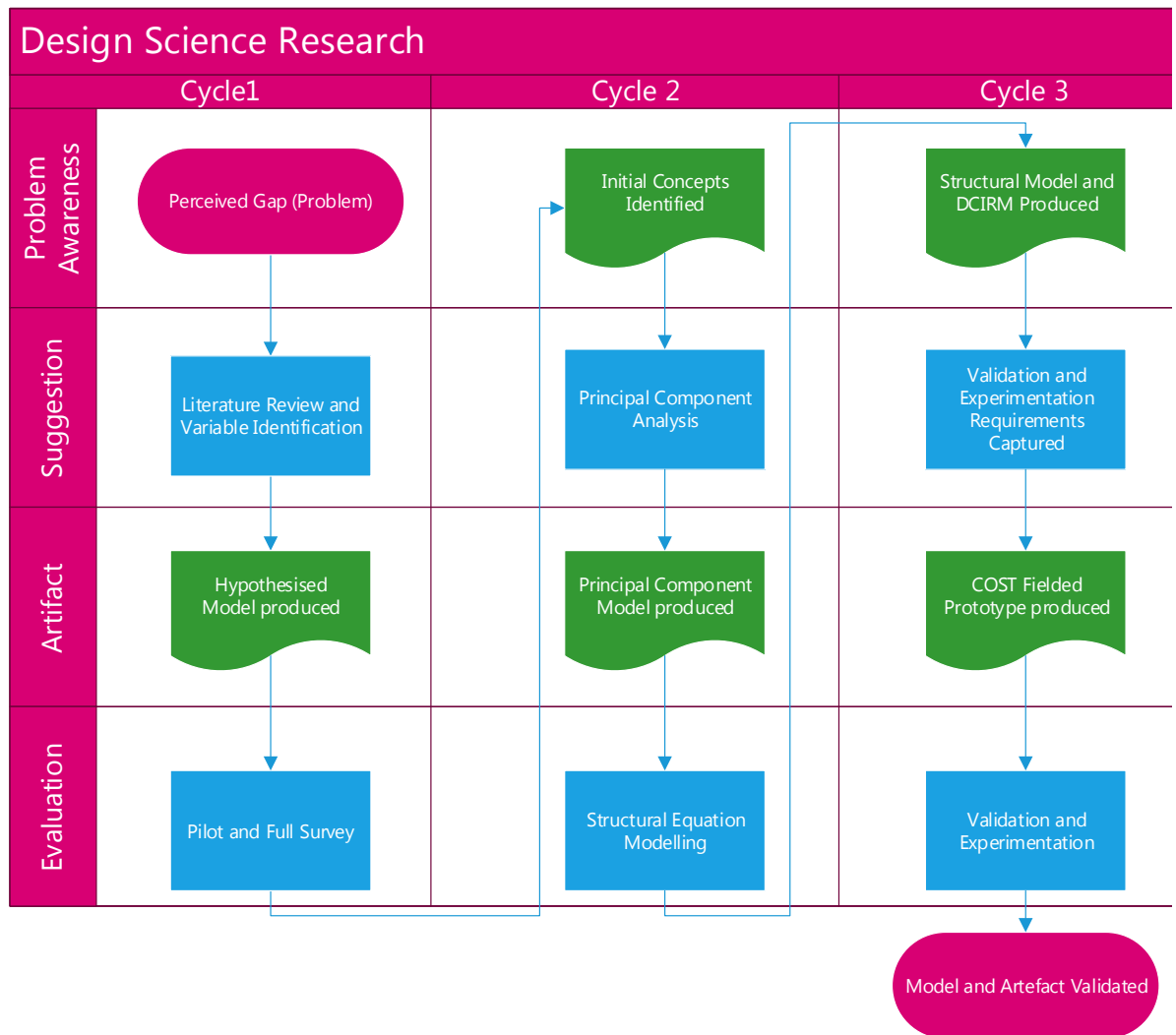


FIGURE 17-RESEARCH PHILOSOPHY USE

The starting point for the research was an identified gap from an IA practitioner’s point of view, where experience in the field had led to the belief that the commonly-used “static” incident-response processes were focused on the short-term Information Security community priorities rather than taking a more dynamic strategic long-term approach from the entire organisation’s perspective. Additionally, it was recognised, that outside of the

core Cyber Security field (from areas such as command and control, military intelligence and aerial combat) many concepts could be equally valid within the cyber domain; Cyber is after all just another domain of the conventional battlefields of land, maritime and air when considered from an “effects-based” approach. This led to the research question:

“Is there a more tailored and dynamic way of implementing Cyber Security Incident Response than by enforcing processes based on traditional static Incident Response Models?”

To put this into perspective, at the beginning of the research it was believed, after several years of experience working within the field, that not all relevant stakeholders’ interests were represented by the traditional incident response procedures. Furthermore, it was perceived that this issue extended to the risk and value of assets, which seemed to be viewed from a single perspective and were fixed despite rapidly changing environments. From the DSR approach this might be considered “awareness of the problem”, however, at this stage there would be no confirmation as to whether or not a problem existed.

To evaluate this initial perspective a literature review would be conducted in order to identify potential variables that might define the domain and, later on, provide a suitable metric for identifying the scale of any issues. The literature review would be conducted utilising a two-pronged approach; both looking at academic work that had been carried out across these areas with particular relevance to Cyber Incident Response (although not necessarily from the Cyber Security field) and also looking at best-practice documentation already used within the Cyber Security community. This revealed that the current best-practice models were not optimal in the views of many academics and professionals working in the cyber-security area (discussed in the LR chapter). From this perspective the LR would be carried out from a critical theory perspective as the models and their historical contexts were to be held up against the lens of the current evolving Cyber Security environment and the supporting academic work.

3.3 Survey

When a comprehensive list of variables had been produced, a small-scale pilot survey would be tested by NATO members and MNE7 participants. The feedback from the pilot survey resulted in modification of the questions which, in summary, concluded that 5-point Likert scales were not granular enough to accurately record the opinion that the participant wished to express; additionally, some questions needed to be reworded in order to achieve

the intended assessment of an identified variable. After these modifications, the full survey would be issued (Appendix 1 – Survey Questionnaire). By allowing rating of the importance of cyber factors using a 7-point Likert scale response (for appropriate granularity in grading relative importance of the variables) it would be possible to evaluate the opinions of the surveyed communities objectively. This would also allow statistical comparisons to be made, assessing relative importance of variables affecting cyber incident response from the perspectives of different stakeholders. Initially these would comprise the communities of experts described earlier in this text, however, to obtain sufficient respondents for objective statistical analysis this would be expanded to include respondents identified as suitable professionals on social media. These professionals were chosen from the LinkedIn communities of Cyber Counter Intelligence, Cyber Intelligence Network, Advanced Persistent Threat and Cyber Security; all professionals were chosen based on their active participation in their social media communities (i.e. actively posting articles or commenting on the posted articles).

3.3.1 Sampling Techniques

The selection of the participants in the surveyed communities could be said to constitute “judgement” (or purposeful) sampling (Marshall, 1996) as the participants were to be picked based on their assessed level of experience and willingness to express an opinion on the influence of cyber security in their domains. According to Marshall, using this method of sampling it is advantageous not to discount outliers as, when trying to conduct qualitative research it is important to capture emerging opinions as well as conflicting opinions.

3.3.2 Sample Size

With 30 variables (analysed from two different perspectives) best practice guidelines were followed (Hair Jr, Black, Babin, & Andersen, 2014): These were that for exploratory factor analysis, the sample size must:

- a. Have more samples than variables.
- b. Have an absolute minimum sample size of 50 observations.
- c. Try to maximise the number of observations per variable, ideally achieving at least 5 per sample.

This would lead to a sample size requirement of at least 150 respondents. Initially, whilst building to this number of respondents the variables were split into two logical areas to

meet the criteria. However, ultimately the minimum number of required participants was exceeded resulting in an assessment of the entire dataset utilising principal component analysis.

3.4 Statistical Evaluation

Utilising the survey results, initially principal component analysis would be carried out to establish the principal components (factors) associated with incident response. However, it was anticipated that a simple linear model would not be likely to reflect a realistic incident response model. Consequently, it was decided that Structural Equation Modelling would be employed as this not only deals with complex models, evaluating the relationships between factors but also indicates causality. The resulting structural equation model would be used as the basis for the remainder of the research.

3.5 Operational Validation

To evaluate the validity of the model produced by interpretation of the survey results it is desirable to validate the model by means of fielded prototypes (to evaluate the model effectiveness in a realistic environment) and to conduct experimentation which scientifically tests the model (MITRE Corporation, 2014). In terms of the research workflow (Figure 17-Research Philosophy Use) and the DSR context, this prototyping and experimentation provides enhanced problem awareness and allows further refinement of the model. Although it would be impossible to evaluate all aspects of the model within the scope of this research, the validation in an operational environment and the analysis of the results of a controlled experiment are described in detail in Chapters 5 and 6, these were intended to evaluate the most important and novel aspects of the model.

3.5.1 Operational Validation Methodology

The operational validation of the model (described in detail in Chapter 5) took place against the background of exercises and training for a NATO Joint Force Command as part of formal qualification to take on the responsibility of the NATO Response Force (a role which alternates between NATO Joint Force Command headquarters). Several shortcomings had been identified in the existing procedures and the author, as the technical lead in the Cyber Defence Working Group, created a tool (COST**Error! Reference source not found.**). This

tool was based on the model developed during this PhD research to address these issues. The tool is described in more detail in Section 5.2, Cyber Operational Support Tool.

At the time the tool was developed, JFCBS was preparing to take on the NATO Response Force role (a function rotated between the two NATO JFC HQs, Brunssum and Naples) and this required the successful completion of a qualification exercise (EXERCISE TRIDENT JUNCTURE). In the time leading up to the exercise battle-staff training (BST) was conducted (a pre-exercise preparation phase) for the JFCBS personnel. Immediately prior to the BST the tool was presented to the CDWG and based on immediate feedback prior to and during the BST a rapid-prototyping process was used to align the tool with the operational processes and requirements.

Having been briefed on the use and capabilities of the tool during BST, the JFCBS Cyber Defence Working Group Staff deployed to TRIDENT JUNCTURE and used the tool to respond to the exercise injects (scenarios to test the HQ capabilities).

Validation Survey

In contrast to the earlier survey, a 5-point Likert Scale (instead of 7-point) was utilised for the validation survey as it was no longer being used to identify factors where the participants expressed a desire to express a very granular opinion, but instead to evaluate the performance of the identified factors from the PhD model. The 5-point Likert Scale was considered adequate to achieve this aim.

Validation Sample Size

As the exercise was not under the control of the research, all relevant willing and available participants were asked to contribute to the survey. This resulted in 21 participants taking part in the survey. If power ($1-\beta$) is set at 0.8 and at least a Cohen's d of 0.65 is achieved (the middle of the "medium effect" categorisation) the Type I error (α) would be calculated as a maximum of 0.02 for this sample size (

Figure 18 – Type I Error Calculation: G*Power Calculator³).

³ The formulas used for the G*Power calculations are located at http://www.gpower.hhu.de/fileadmin/redaktion/Fakultaeten/Mathematisch-Naturwissenschaftliche_Fakultaet/Psychologie/AAP/gpower/GPowerManual.pdf

Typically, 0.05 would be considered a suitable maximum value for α , so this appears to be a reasonable sample size for the anticipated results.

Working backwards from this result using $\alpha = 0.05$, $1-\beta$ of 0.8 and a Cohen's d of 0.65 (i.e. effect size = 0.65), where Z represents the value from the standard normal distribution curve where the power and Type I errors are contained and the formula:

$$n = \left(\frac{Z_{1-\alpha/2} + Z_{1-\beta}}{ES} \right)^2 \quad 4$$

then the required sample size n becomes $n = ((1.96 + 0.84)/0.65)^2 = 18.6$, confirming that the sample size of 21 participants is adequate.

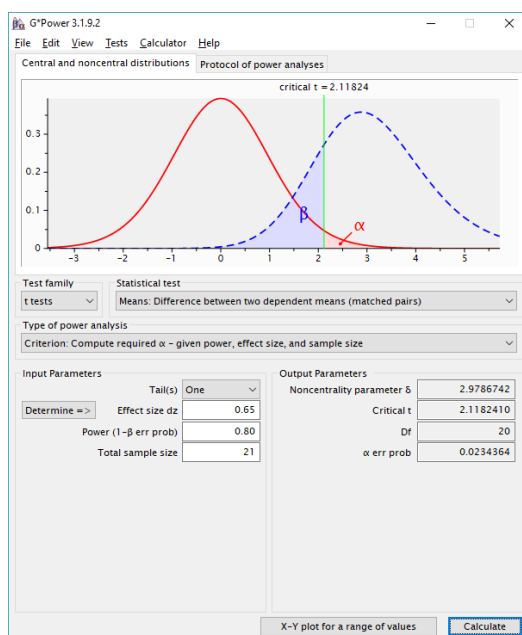


FIGURE 18 – TYPE I ERROR CALCULATION: G*POWER CALCULATOR⁵

Validation Evaluation Criteria

During this extremely busy period of NATO exercises and training during the development of the tool it was not possible to produce a controlled environment purely to evaluate the tool. Instead, it was decided to allow NATO personnel to evaluate it in their own training and exercise environments without controlling the scenarios (and as the exercise scenarios

⁴ http://sphweb.bumc.bu.edu/otlt/mph-modules/bs/bs704_power/BS704_Power_print.html

⁵ G*Power Version 3.1.9.2: Kiel University, Germany

are restricted to NATO audiences, the scenarios themselves would not have been releasable in any case). This allowed the flexibility of the tool and model to be demonstrated in a live environment without placing academic constraints on an experiment which may have introduced artificialities in the operational procedures. Whilst not meeting the normal standards of academic rigour for evaluation of a model, there are precedents in other fields for evaluating effectiveness in an operational environment (Wholey, Hatry, & Newcomer, 2010), (DiPetto, 2008). However, the downside of this approach is that it becomes impossible to evaluate the effectiveness of the tool whilst controlling specific environmental variables such as the degree to which the battlespace is congested, cluttered, contested or constrained (UK Ministry of Defence, 2015).

The assessment considered 10 areas which were evaluated both with and without the tool. These comprised factors from the decision-making area of the model, analysis of efficiency and effectiveness in providing the information and analysis of ability to cope with three of the relevant characteristics of the future battlespace (Ministry of Defence (UK), 2015); These are as follows (relevant factors or source in brackets):

- i. Cross-functional awareness of cyber impact on other branches (Collaboration).
- ii. Cyber impact on the mission (Mission impact).
- iii. Cyber impact on Intelligence (Intelligence).
- iv. Awareness of the Commander's response options and chosen response (Cyber Response).
- v. Efficiency in providing information to a cyber impact assessment (efficiency of communication).
- vi. Ability to provide relevant information to a cyber impact assessment (effectiveness of communication).
- vii. Ability to operate effectively in a congested cyber environment (Ministry of Defence (UK), 2015).
- viii. Ability to operate effectively in a contested cyber environment (Ministry of Defence (UK), 2015).
- ix. Ability to operate in a cluttered cyber environment (Ministry of Defence (UK), 2015).
- x. Awareness of dynamic targeted asset value in different mission stages (Dynamic Asset Value).

3.6 Experimental Methodology

In order to provide a controlled environment to evaluate the application of the model where factors could be manually adjusted (unlike the operational validation), a controlled experiment was carried out. The method, aim and objectives are described in the following paragraphs; the results and analysis are described in Chapter 6.

3.6.1 Experimental Aim

The aim of the experiment was to assess the contribution of the Dynamic Cyber-Incident Response Model in its support to the decision-making process for a Joint HQ commander responsible for deployed units executing missions in multi-domain warfare environments; this was compared to the support provided by the traditional Cyber-Incident Response Models and the information provided by these in the same environments. To achieve this aim, scenario-based experimentation was utilised.

3.6.2 Experimental Objectives:

The experiment was designed to achieve the following objectives:

- i. Compare perceived situational awareness (through all three levels: perception, comprehension and prediction) when using information provided by traditional response processes to that of perceived situational awareness when provided with the additional information provided by the Dynamic Cyber-Incident response model.
- ii. Compare confidence in decision-making when using information provided by traditional response processes to that of decision-making when provided with the additional information provided by the Dynamic Cyber-Incident response model.
- iii. Compare perceived capability to cope with a congested environment when using information provided by traditional response processes to that of the same capability when provided with the additional information from the Dynamic Cyber-Incident response model.

- iv. Compare perceived capability to cope with a contested environment when using information provided by traditional response processes to that of the same capability when provided with the additional information from the Dynamic Cyber-Incident response model.
- v. Compare perceived capability to cope with a cluttered environment when using information provided by traditional response processes to that of the same capability when provided with the additional information from the Dynamic Cyber-Incident response model.
- vi. Compare perceived capability to dynamically track the impact of a cyber-incident during a progressing mission when using information provided by traditional response processes to that of the same capability when provided with the additional information from the DCIRM.

Whilst primarily evaluating the situational awareness and decision-support influence of the DCIRM, the responses themselves and the timeliness of the response was also evaluated to look for any influence exerted by the model. However, by this stage of the research it had already become clear that cultural influences would serve to temper the responses from some participants dependent upon their training, experience and own environmental legal frameworks and their approach to cyber operations, even when provided with freedom to manoeuvre in the scenarios.

3.6.3 Experiment Scenario

A military decision-maker is responsible for a static military Joint HQ with deployed elements; therefore, attacks from the Internet have low mission impact despite being a nuisance. The scenario takes place in an environment where national cyber laws have been refined to provide additional rights to those under cyber-attack. However, responses are expected to be proportionate to an attack. The legally permissible responses to a cyber-attack are now:

- a. Traditional Response: stop or mitigate an attack as soon as it is detected.

- b. Passive Response: allow an attack to continue under close observation without impediment in order to gather additional intelligence. This is unlikely to warn the attacker that they have been noticed.
- c. Cyber Offensive Operations: respond to an attack by penetrating the attacker's networks and/or systems in order to gather advanced intelligence or to try to halt an attack immediately. The attacker is likely to be aware of this action and respond.

3.7 Experiment Method and Vignettes

To evaluate the structural equation model in a controlled environment suitable for an academic experiment, a simulation was used, although initially a cyber range was considered. The reasons for choosing the simulation over the cyber range were that:

- a. This would evaluate the decision-making of the responsible Commander and not the technical ability of cyber security specialists.
- b. The way the Commander received the information and his response were not tied to specific attacks, instead their response was related to the situational awareness and options provided by the model.
- c. Fewer participants would be required to run the experiment.
- d. All possible combinations of the chosen factors could be evaluated.

3.7.1 Factor Choice

For the purposes of the experiment it was decided to evaluate two key factors whilst fixing the value of an additional factor from the Dynamic Cyber-Incident Response Model, the evaluated factors were Dynamic Asset Value and Intelligence whilst Mission Impact was fixed at a value of "Low". The reasons for doing this were that during interviews throughout the research it became clear that with the current maturity of operations in the Cyber domain, any detrimental impact on a mission rated higher than "Low" would be

unlikely to result in any response other than traditional i.e. immediately try to contain, mitigate or eliminate a cyber-attack within the defender’s own network.

By choosing Intelligence (and more specifically Intelligence Value which also directly influences Mission Impact and is directly impacted by Cyber Response) together with Dynamic Asset Value a trade-off between the two would force a useful conflict in the decision-making process. Additionally, the introduction of this additional information to traditional cyber situational awareness at the Commander level could be usefully compared for contribution to the decision-making process.

3.7.2 Vignettes

With the background of the scenario described in Section 3.6.3, the vignettes in Table 3 - Vignette Combination were evaluated; these are described in Appendix 6 – Experiment Scenario and Vignettes which also provides the values for the factors for each of the vignettes. Expected responses mentioned in the table were based on discussions that took place when producing the prototype tool (COST). In general, the polled opinion would not sanction anything other than a traditional response when the Asset Value was higher than the Intelligence Value (Intelligence Gap). If the Asset Value was the same as the Intelligence Value either Traditional Response or Passive Response were expected to be chosen. However, if Intelligence Value was higher than Asset Value either Passive Response or Active Response (Cyber Offensive Operations) were expected to be chosen.

In order to minimise “learning effect” the two simulations were run in a random order (determined by the toss of a coin).

TABLE 3 -VIGNETTE COMBINATION

	Mission Impact	Asset Value	Missing Intelligence	Expected Responses using dynamic response
Value	Low	Low	Low	Traditional
	Low	Medium	Low	Traditional
	Low	High	Low	Traditional
	Low	Low	Medium	Passive/Active
	Low	Medium	Medium	Passive
	Low	High	Medium	Traditional

	Low	Low	High	Passive/Active
	Low	Medium	High	Passive/Active
	Low	High	High	Passive

3.7.3 Participant Choice and Sample size

It was decided that participants would be selected from former and current military officers, predominantly from non-cyber backgrounds with experience of operational decision-making (typically as participants in Joint Operational Planning Groups). This choice was made as this also reflects the background of many operational decision-makers at the Joint Headquarters level within Western European, North American and international military headquarters comprising personnel from these forces (a typical example is PJHQ Northwood which has fast-jet pilots, commanding officers of frigates and paratroopers as some of the former commanders). The number of participants was 20 to ensure that robust T-tests and Cohen's d could be used to assess the significance and scale of the impact of the contribution of the Dynamic Cyber-Incident Response Model. For assessing Cohen's d with a minimum effect size of 0.65 (midpoint of the "medium effect" range), a Type I error probability of 0.05 and power of 80% a sample size of 17 is required. Using the same calculation, a sample size of 19 would give power of 95% for a large Cohen's d effect size i.e. greater than 0.8 (Figure 19 - Sample Size Calculation: G*Power Calculator).

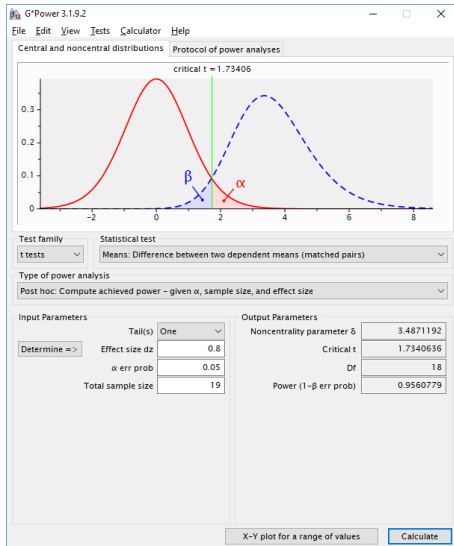


FIGURE 19 - SAMPLE SIZE CALCULATION: G*POWER CALCULATOR⁶

3.7.4 Technical Configuration

To capture the response to the vignettes set against the scenario, two simulations were run utilising Microsoft PowerPoint and captured using the Microsoft Xbox recording functionality built into Windows 10. Screenshots of the hardware and software versions used for the experiment are shown at

Appendix 7 – Equipment and Software Used for Experiment.

⁶ G*Power Version 3.1.9.2: Kiel University, Germany

4 Data Analysis

4.1 Introduction

As outlined in the methodology, the steps in producing the model were:

- a. A comprehensive systematic literature review was carried out.
- b. An initial hypothesised model was produced utilising the identified variables and grouping them logically.
- c. A pilot survey based on the literature review to date was conducted to check the appropriateness of questions, the options and range of the Likert scale provided as answers (and to solicit general feedback on the concepts and variables to date) in order to prepare for the main survey.
- d. A full survey was carried out. The results were analysed using principal component analysis.
- e. A hypothesised model utilising the identified factors was produced.
- f. Structural equation modelling (SEM) was used to produce a measurement model which confirmed the factors. The relationships and causalities between the factors were then evaluated by SEM to produce the structural model (resulting in the Dynamic Cyber Incident Response Model).

4.2 Survey Development

A limited pilot survey was carried out with participants from international military, commercial and governmental cyber security communities to evaluate the initially identified variables from the communities and the literature review.

The initial statistical evaluation of these variables, which was informed by discussions within expert communities and the remainder of the literature review led to the production of an initial model. This was also used as a starting point to describe the contribution of cyber to the operational planning process by the technical strand of MCDC-CICOA (MCDC, 2014).

This initial model shown in Figure 16 (which combines process, functions and infrastructure) attempted to describe the interaction between infrastructure and what is described here as static situational awareness i.e. the impact of an incident on the

defending environment as it is now, utilising the existing intelligence. This static situational awareness is then used as an input to dynamic risk and value assessment, where, based on the current known situation, modelling of an attack is attempted. This utilises the known vulnerabilities and paths through the infrastructure with the available attack intelligence which is then combined with the assessments by the different stakeholders for that point in time of the value of the threatened assets (recognising that different stakeholders may well place different priorities on the same asset). The output of this process would be “balance of equities” information to be provided to the key decision maker together with the static situational awareness in order to provide them with enhanced situational awareness. This information would allow them to choose the optimum response in order to meet the organisational goals; examples of these described by the response options (without reference to legal constraints) are to defend the attacked assets via passive means, gather more intelligence about an attack or attacker (via passive means) or use active means to pacify attacker infrastructure or gather more intelligence about the attacker. Referring back to the OODA loop, this whole process needs to be completed before the attacker has a chance to detect and respond to any actions taken by the defenders in order to gain an advantage over the attacker.

Utilising this initial understanding of the domain and the literature review as a starting point, a new large-scale survey was produced to evaluate the importance of identified variables in providing effective Cyber-Incident Response; this not only included respondents from the Cyber-Security communities, but also other communities involved with and impacted by cyber-incidents such as Military/Business Intelligence, Operations, Communications Information Systems Management and other support areas. The questions assessed not only the opinions of the participants as to the importance of the identified factors affecting cyber incident response but also how these factors were viewed in their communities and organisations.

4.3 Sample Frame and Procedure

As the survey was intended to address concerns of all stakeholders impacted by cybersecurity incidents, the target audience was intended to be as broad as possible. However, to ensure that some analysis of community trends was possible the respondents were divided into 6 main areas: Operations/planning, Security/IA, Intelligence/Business Intelligence, CIS Management/Engineering, other support functions, any other function (echoing a military J3/5 led working group structure and also equivalent

commercial/governmental structures). Prior to the main survey, informal discussions in expert working groups had already identified significant discrepancies between the Operations, Intelligence, CIS Management and IA/Security communities which were supported by statistical analysis so these were expected to be the primary target communities. In an early pilot, as well as providing feedback on potential bias and discrepancies in the questions the participants identified that a 5-point Likert scale did not allow enough discriminative granularity to provide an accurate reflection of their opinions so a 7-point Likert scale was used for the main survey. Initially the surveyed participants were chosen from expert working groups comprising international companies, international organisations and international military and other governmental communities. This survey process initially took place manually and then later using a combination of manual and online (SurveyGizmo) resources in order to reach a wider audience. When existing contacts in the survey communities had been exhausted, participants were chosen based on active contribution in social media communities relating to cyber security and cyber security impact (primarily from the LinkedIn communities of Advanced Persistent Threats and Cyber Security, Cyber Counter-Intelligence and Cyber-Intelligence).

In parallel, the identified variables and their context were also discussed with several professionals working in, or directly impacted by, the Cyber-Security areas within expert working groups (discussed in the Literature Review chapter) during the initial stages of the PhD research. Initially this dialogue took place with NATO and NATO member-nation experts inside security accreditation boards and cyber-defence working groups. However, later in the research, international and national experts in areas such as critical national infrastructure, commerce, defence and legal were also engaged during Multi-National Experiment 7 (MNE7), an international experiment investigating how to preserve access to the global commons of sea, air, space and cyber. During the follow-on work from MNE7, participants were also consulted from the Multinational Capability Development Campaign - Cyber Implications for Combined Operational Access (MCDC-CICOA), this community of experts expanded the survey participant base to also include specialists from non-NATO Cyber Intelligence and Operational Planning communities.

The survey was analysed in two distinct stages; the first utilising the full 60 questions which reflected both the individual and organisational perspectives (to identify discrepancies between the two perspectives of the 30 variables and allow some initial analysis). The

second, which was captured later, used 30 questions, i.e. one question per variable (only analysing the individuals' perspectives) and, as expected, had a much lower proportion of missing or disqualified responses, believed to be due to less "respondent fatigue" (Lavrakas, 2008)

The results from the first stage of the survey comprised 202 respondents of which 78 were disqualified for missing data and 2 for "straight-line responding". Outliers were not excluded from the analysis as it is believed that unconventional perspectives are also valuable when challenging conventional models (Marshall, 1996). The second stage (which only analysed the individuals' perspectives) took place approximately 6 months later and combined the original results with those of the respondents who subsequently completed only the 30 questions about the individual perspective. This comprised 315 responses of which 111 were disqualified for missing data and 3 for "straight-line responding". Utilising the first set of results and the rule-of-thumb of 5 responses per variable (Bentler & Chou, 1987), (Hair, Black, Babin, & Anderson, 2014), would have required 150 responses to evaluate each variable for both the organisational and the individual perspectives. However, at this point it was believed that there was a logical divide between the variables associated with incident detection and those constituting the incident decision-making and response processes (14 variables and 16 variables respectively) this therefore required a minimum of 80 responses for all questions which was achieved comfortably. For the second analysis, the 201 complete responses allowed the variables to be analysed in their entirety whilst meeting the same conditions.

4.4 Data Preparation

The manual and online responses were combined into a single spreadsheet to be loaded into SPSS. Prior to the analysis, all geographic, operating system and other data that could possibly be used to identify an individual were removed as this was a very strong requirement identified by the security and intelligence communities early in the pilot survey; Security and Intelligence communities are particularly sensitive about this requirement. The exception to the anonymization was where respondents specifically allowed their details to be included in order to allow further feedback/discussion.

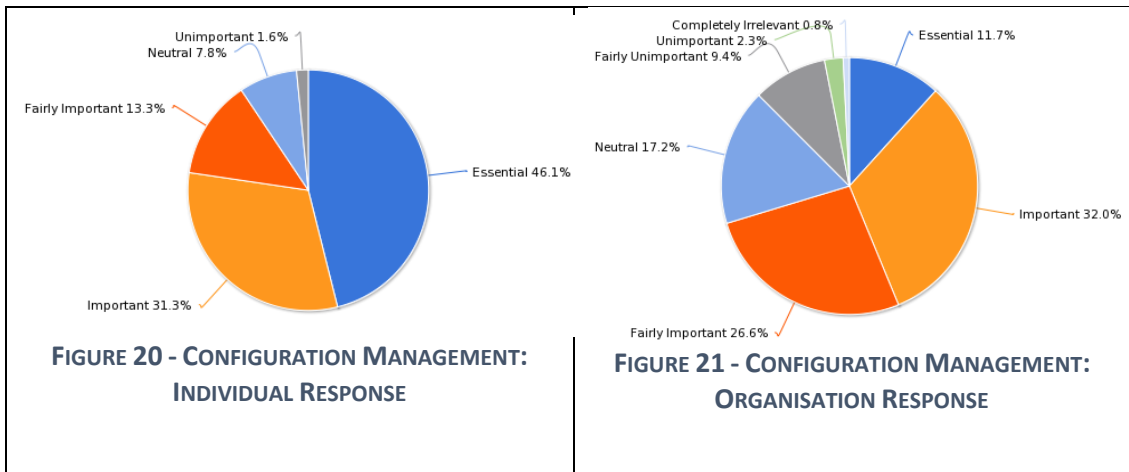
4.5 Survey Analysis and Results

4.5.1 Statistical Analysis

From the initial results (which comprised 202 responses) comparing both organisational and individual perspectives, there was a striking difference in opinion between individuals in all communities and their perception of their organisations' opinions. This assessment was confirmed by paired t-tests where all 30 variables were found to have significant results.

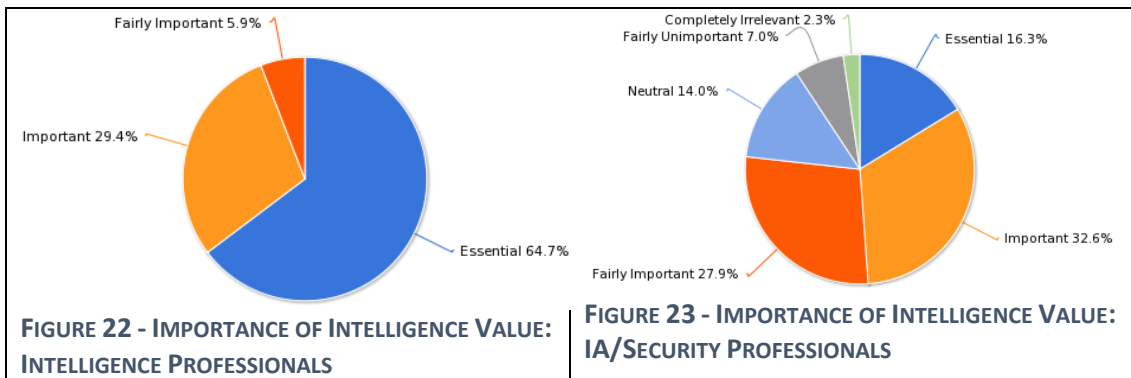
4.5.2 Stakeholder Perspectives

From the results, it appears that individuals across the communities tend to place more importance on the identified variables than their organisations or communities. A good example of this can be seen in the response to Configuration Management (CM) where almost half of the participants assessed that effective CM was essential to provide optimal Cyber-Incident Response (Figure 20) whereas in their communities and organisations just over 10% of the participants (Figure 21) believed that their communities and organisations found CM to be essential. Other notable examples of this phenomenon were reflected in the use of automatic tools for intelligent data reduction, sensors for monitoring at all levels, timeliness and reliability of data and to a lesser extent, areas such as environmental conditions that analysts work in.

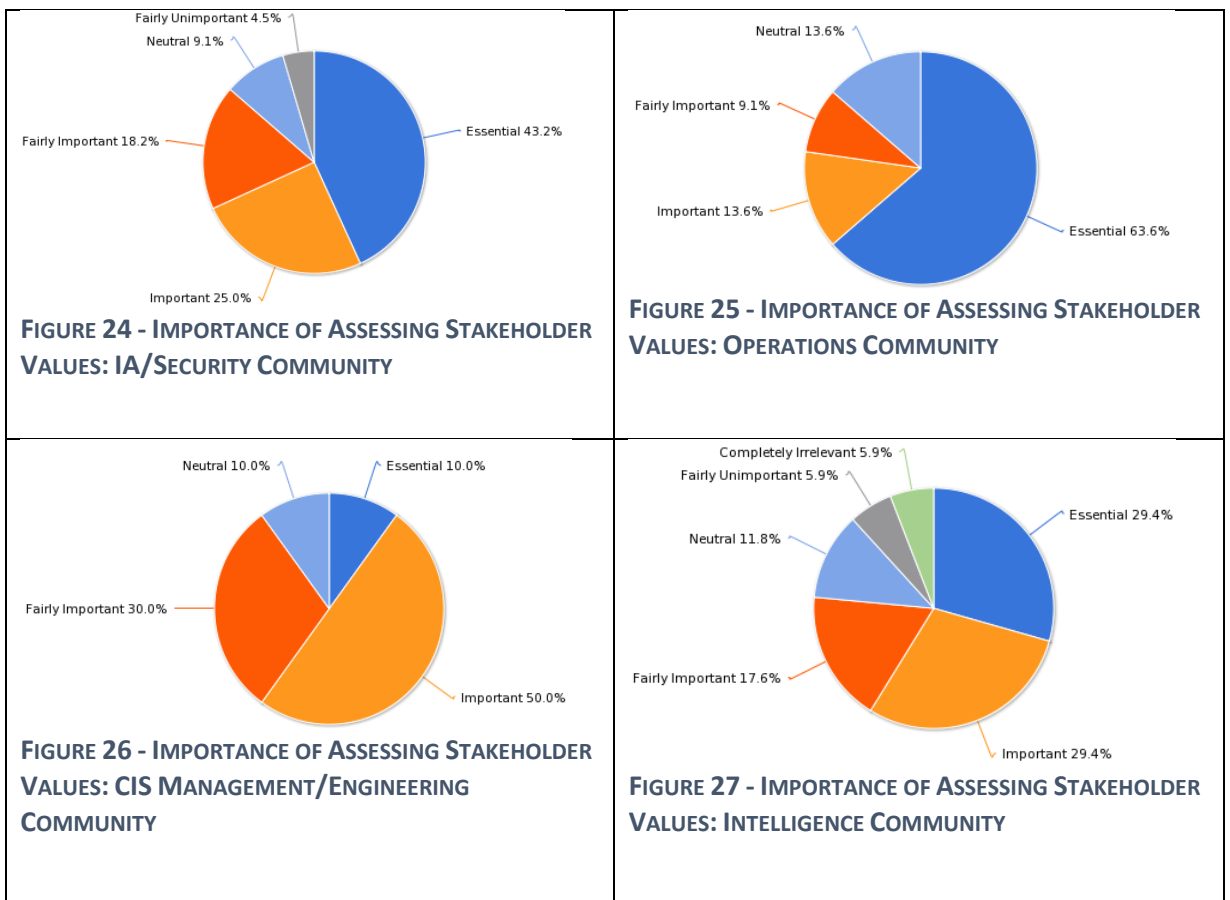


As expected, there were also significant differences in the importance placed on assigning a value to intelligence regarding the attackers and attacks between the communities. This is demonstrated below in the contrasting opinions on the importance of placing a value on

Intelligence information as part of the Cyber-Incident response process (Figure 22 and Figure 23).



However, some unexpected differences of opinion were also identified across the communities, even relating to the importance of stakeholders being able to assess the value of assets from different perspectives (Figure 24 to Figure 27). In this example, it might be surmised that the CIS Management/Engineering communities believe that they already know the priority of the assets that they maintain so it is not essential to have the functional owner's perspective.



4.5.3 Factor Determination

When the survey was initially produced, a set of 30 variables were identified which might be considered important to Cyber Incident Response; as can be seen from the draft model, this creates an almost unmanageable model from a conceptual point of view. In order to simplify this, a series of statistical processes were run to try and reduce the number of variables (i.e. to check for significant correlation between similar variables to merge them as a single factor) and these are summarized in the subsequent tables. Not only does this allow simplification of the model but also makes experimentation more realistic (as too many variables will make it almost impossible to test all inter-relationships and assess their significance on the measured output variables).

For the first time (as far as can be determined) factor analysis was carried out to determine key areas of importance in the cyber incident response process. This was achieved by analyzing the results obtained from the communities of interest (from the survey) using principal axis factoring and Varimax⁷ rotation. This dimension reduction process allows correlated variables to be grouped into common components or factors and those which are orthogonal to them are grouped into separate factors. From the sample size, it is suggested (Hair, Black, Babin, & Anderson, 2014) that a factor loading of more than 0.50 be used⁸ in order to achieve a power rating of 80%.

Initially, all variables were grouped together to carry out principal component analysis, however, this produced some nonsensical factors where completely unrelated variables were grouped together with variables which were grouped with obvious logical alignment. This led to a reassessment of the variables from a conceptual point of view⁹ and the division of the variables into two distinct areas, Incident Detection and Situational Awareness/Decision-making.

Utilizing the specified process (using the SPSS software package), for the Incident Detection grouping the following factors were identified from the data sources (Table 4):

⁷ Created by Henry F Kaiser in 1958

⁸ (Hair, Black, Babin, & Anderson, 2014) : Exploratory Factor Analysis – Judging the Significance of Factor Loadings, Table 2.

⁹ (Hair, Black, Babin, & Anderson, 2014) : Exploratory Factor Analysis – Conceptual Issues

- i) Sensors (monitoring of operating system logs, network sensor logs, application logs etc).
- ii) Collaboration (both inbound and outbound SA collaboration with trusted partners).
- iii) Information Credibility (accuracy, timeliness and reliability of information).
- iv) Incident Discrimination (analyst experience and automated tools to reduce the “noise” of routine events).

TABLE 4- PRINCIPAL COMPONENT ANALYSIS OF INCIDENT DETECTION VARIABLES

	Component			
	Sensors	Collaboration	Credibility	Discrimination
OS Monitoring	.85			
App Monitoring	.72			
Hardware Mon	.71			
Network Mon	.69			
Collaboration In		.87		
Collaboration Out		.83		
Accuracy			.75	
Timeliness			.73	
Reliability			.50	
Automated Tools				.80
Analyst Experience				.73

These variables were then grouped together to create a process that for the purposes of the model will be called Incident Detection. Utilising a series of similar reductions for the Situational Awareness/ Decision-Making grouping using the same Varimax process, the rest of the variables were analysed. This analysis is given at Table 5 and results in the following factors:

- i) Intelligence (this is an indicator of what is known about the attacker and the defended environment, i.e. “know your enemy and know yourself”).

- ii) Dynamic Risk (this could also be interpreted as Mission Impact as it takes the generated situational awareness and overlays this with potential outcomes and impact on the mission goals).
- iii) Dynamic Value (this assesses the relative values of intelligence and assets from stakeholder and operational perspectives).
- iv) Decision-Making (this is the choice between traditional responses, passive monitoring and an active response i.e. offensive cyber operations).

TABLE 5 – PRINCIPAL COMPONENT ANALYSIS OF DECISION-MAKING

	Component			
	Intelligence	Dynamic Risk	Dynamic Value	Decision
Vulnerability KB	.620			
Attacker KB	.650			
CAPEC	.753			
Simulation	.561			
Goal		.502		
SA		.714		
Prediction		.592		
RA		.465		
Asset Value			.471	
Stakeholder Value			.597	
Time Modification			.607	
Intelligence Value			.570	
Active Defence				.605
Passive Monitoring				.629
Traditional Cyber				.468

These interacting processes are then described by:

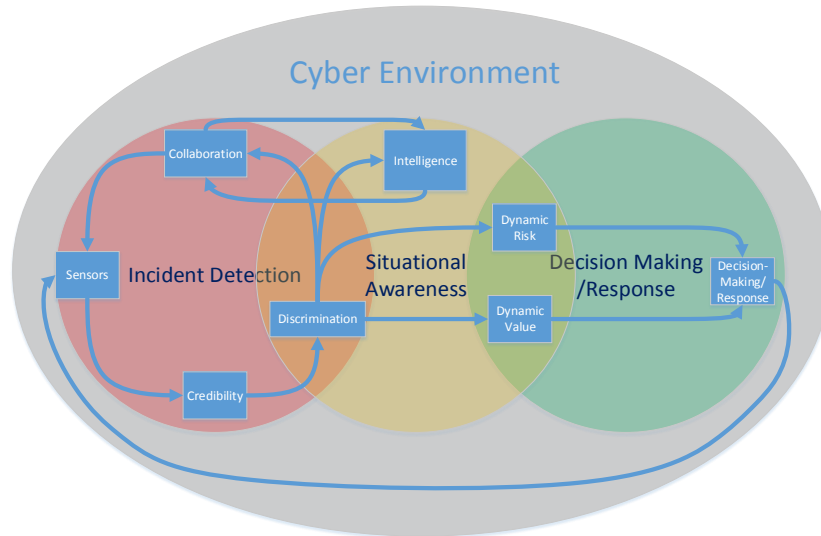
- i) Incident Detection: the gathering of information from relevant sources with the appropriate credibility including collaboration information received from partners. This comprises Sensors and Collaboration, Credibility (of sources) and Discrimination (of incidents).

- ii) Situational Awareness: receiving a feed from Incident Detection, Situational Awareness adds the context from Intelligence, the value of the targeted Asset, the dynamic risk to that asset and to the organisational goals. This is also likely to indirectly include a feedback loop from the Incident Response which will undoubtedly have an impact on the environment and attack progress.
- iii) Decision-making: based on the previous stages and the static impact evaluation, the responsible decision maker takes the organisational goals into account before deciding on a course of action. They are provided with a number of response options (which may be reduced by their legal and organisational constraints): these options are:
 - a. A conventional response, i.e. defend against the attack via conventional means (for example blacklists, IPS, etc).
 - b. Passive monitoring response, i.e. observe but show no reaction at all to the incident (as though it was undetected) in order to gain intelligence.
 - c. Active Defence comprising either:
 - i. Intelligence gathering, i.e. actively reconnoitre the attacking infrastructure by any means possible in order to gain intelligence but without intentionally causing disruption to the attacking infrastructure.
 - ii. Cyber strike, i.e. neutralise the attacking infrastructure via any available Cyber means.

Or a combination of these methods dependent upon the stage of the attack and the danger posed to the organisation.

As a result of the principal component analysis, the factors and the relationships between them are proposed in the hypothesised schematic model shown at Figure 28. In this schematic model, there is an initial cycle of incident detection where the continuous monitoring of sensors takes place, the incidents are then filtered, discriminated from the background noise and then passed on to collaboration partners (if any) whose own alerts are also fed into the detection process (effectively becoming remote sensors).

FIGURE 28 - PRINCIPAL COMPONENT ANALYSIS SCHEMATIC DIAGRAM



The situational awareness takes the existing intelligence (which is continually being updated from own and partner sources), the discriminated incidents and puts them into a context for the commander/decision-maker which is relevant for the mission. This provides the commander with not only the instantaneous value of the assets being targeted but also the risks to the mission of the attack. This culminates in the commander’s decision where he chooses an appropriate authorised response. This response either directly or indirectly influences the environment which in turn will be detected by the change in events detected by the sensors.

It should be noted that in terms of response, for the military commander other options outside of a cyber-response may be available; i.e. kinetic options may be considered (using the domains of land, air, maritime or space). Additionally, the environment, detection, SA and response should not only be considered in the network environment but also the other planes of the information environment as described in MNE7 (shown in Figure 29).

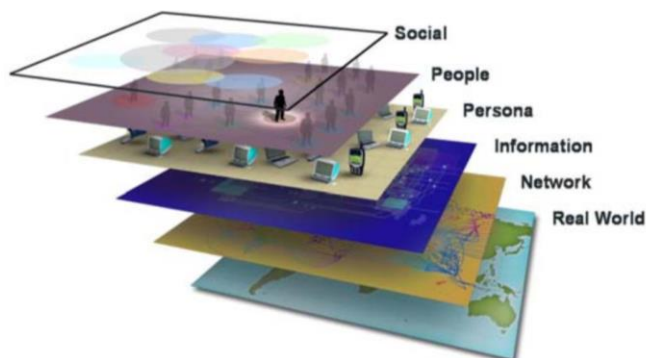


FIGURE 29 - MNE7 INFORMATION ENVIRONMENT

4.5.4 Structural Equation Modelling

However, although relationships between factors could be hypothesized as a result of the principal component analysis, resulting in Figure 28, they could not be evaluated objectively using this method. At this stage, the techniques used up to this point could only be used for validating non-complex linear models. To achieve a more thorough evaluation of the factors and to evaluate the relationship and causality between the factors, Structural Equation Modelling (SEM) was deemed to be more appropriate.

SEM can trace its roots back to the early proponents of Path Analysis as far back as 1918 (Matsueda, 2011), since then it has had several different influences and stages of development where it has continued to evolve and now arguably provides one of the most robust methods for both factor analysis and establishing causality when used in the most appropriate way for the data under analysis (Lowry & Gaskin, 2014). The SEM method utilized for this research comprises two distinct processes, a measurement model and a path (or structural) model. In the first stage, the Measurement Model analyses all measured variables together and carries out statistical tests against these to evaluate the relationships simultaneously, ultimately allowing factors to be determined from the independent variables. In the second stage, when the factorial grouping has been determined by the Measurement Model, causal relationships can be proposed and evaluated in the Structural Model.

Within this research, by the time that the SEM was commenced, completed surveys from 201 respondents had been received; however, by this point the relevance of their perception of their organizations' responses was not deemed to be relevant to the model development as the individuals were seen to be the domain experts so the results were only analyzed from the individuals' perspectives. During the initial multiple linear regression in earlier work (Mephram, Louvieris, Ghinea, & Clewley, 2014), the only method of achieving a logical grouping of factors was to split the variables into two logical groups for analysis; these were Incident Detection and Decision-Making. However, when SEM was conducted, additional respondents allowed all variables to be analyzed together in the Measurement Model thus providing a more holistic approach. When assessing data for normality one method considers that skewness and kurtosis of less than 1 are generally considered slightly non-normal and values of up to 2.3 are considered to be moderately non-normal (Lei & Lomax, 2009). However, even with severely non-normal data, in this case defined as having skewness above 0.7 and kurtosis in excess of 3.5, relatively recent

work in SEM (Lei & Lomax, 2009) confirmed that for sample sizes of 100 and above, SEM was robust for both the maximum likelihood (ML) and generalized least squares (GLS) methods (typically resulting in significantly less than 10% bias on parameter estimates). Consequently, the data being analyzed in this research was comfortably within the boundaries acceptable for SEM analysis (i.e. considerably less than 0.7 skewness and 3.5 kurtosis).

4.5.5 Measurement Model

The initial measurement model is shown at Figure 30 and the variables relating to this are described in Appendix 2 - Cyber Security Variables. In this model, each variable has an associated error term and the covariances between the factors are shown as double-headed arrows. Some variables were eliminated from during the principal component analysis phase for falling below a significant factor loading value of 0.4 contributing threshold (Hair Jr, Black, Babin, & Andersen, 2014) whilst others were eliminated for loading on more than one factor (Appendix 3 – Principal Component Analysis) or for being the only variable loading on a factor. This resulted in the 23 variables which resolved to the identified 8 factors shown in the diagram.

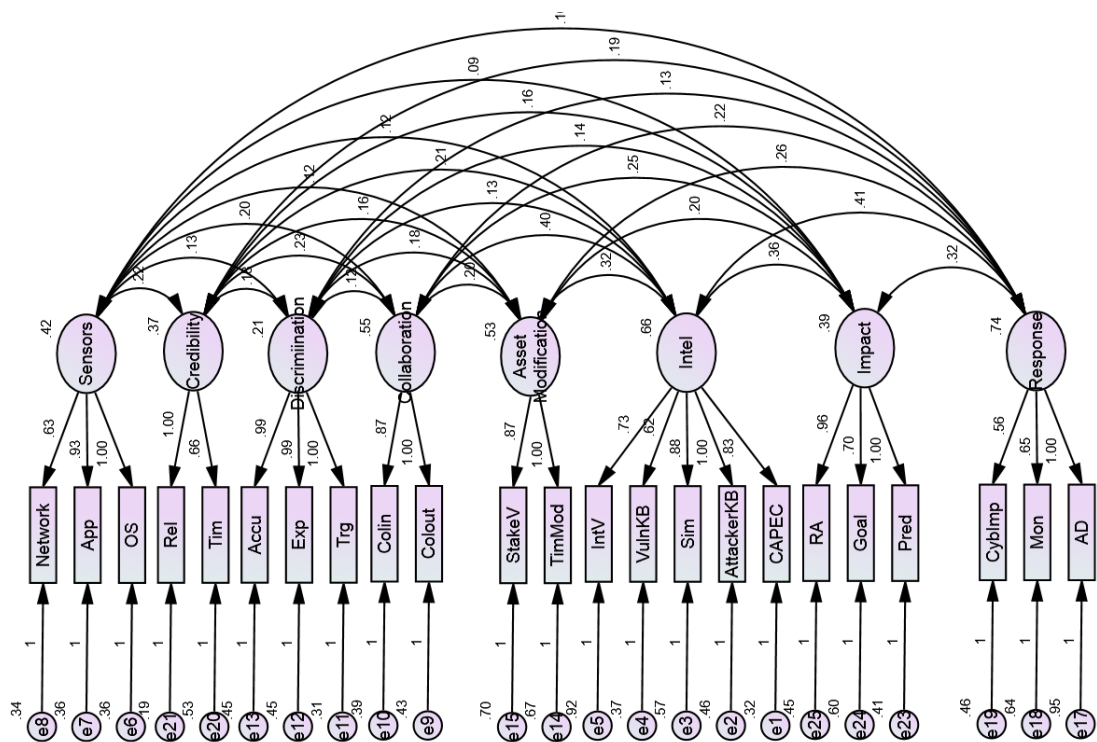


FIGURE 30 - SEM MEASUREMENT MODEL

The goodness of fit indices associated with the initial SEM model are shown at Table 6. The interpretation of the tests is presented below (an outline of the fit indices with references is described at Appendix 4 – Structural Equation Modelling: Fit Indices). The first item of note is the probability test, (based on the χ^2 calculation). Although this statistic rejects the model as non-significant, recent academic work (Hooper, Coughlan, & Mullen, 2008) suggests this test is not reliable for large sample sizes or those that deviate from normality. However, CMIN/DF falls between recommended bounds of 1 and 5 (Wheaton, Muthén, Alwin, & Summers, 1977) which is seen as a better alternative to χ^2 . Furthermore, it is advised (Lei & Lomax, 2009) that, for sample sizes below 500, NFI, NNFI and CFI are better fit indices than χ^2 .

Cyber Incident Response Measurement Model					
Fitness Test	NPAR	CMIN	DF	P	CMIN/DF
Model	74	254.3	202	.0	1.3
Test	RMR	GFI	AGFI	PGFI	
Model	.0	.9	.9	.7	
Test	NFI Delta1	RFI rho1	IFI Delta2	TLI rho2	CFI
Model	.8	.8	1.0	.9	1.0
Test	PRATIO	PNFI	PCFI		
Model	.8	.7	.8		
Test	NCP	LO 90	HI 90		
Model	52.3	15.6	97.1		
Test	FMIN	F0	LO 90	HI 90	
Model	1.3	.3	.1	.5	
Test	RMSEA	LO 90	HI 90	PCLOSE	
Model	.0	.0	.0	1.0	
Test	ECVI	LO 90	HI 90	MECVI	
Model	2.0	1.8	2.2	2.1	
Saturated Model	2.8	2.8	2.8	3.1	
Independence Model	7.1	6.6	7.8	7.2	

TABLE 6 –SEM MEASUREMENT MODEL

The other statistics marked in amber are marginally acceptable and those marked in green are well within acceptable limits. However, it is suggested (Byrne, 2010) that NFI also tends to over-reject models with instead CFI being the measurement of choice (RFI is a derivative of NFI).

Utilising this evaluated measurement model as a starting point, an initial structural model was proposed in Figure 31. However, after evaluation of the regression weight divided by the standard error for each of the causal relationships (denoted by Critical Ratio in AMOS or CR), it was found that the influence of Collaboration on Discrimination was negligible (less than 2 and probability more than 0.05, thus indicating an invalid model) but from a logical perspective a discriminated incident is important information to share with partners and by reversing this relationship it became significant and the CR increased to 4.2.

Equally the influence of Discrimination on Intel was similarly negligible in the beginning (possibly because the discriminated incidents are evaluated against intelligence information but do not directly influence the intelligence unless new information is discovered) so this relationship was deleted. However, despite the influence of the Asset Modification (i.e. modified asset value) having a similar issue of significance when tied to Impact, when the influence was directly moved to Response (i.e. the Incident Response decision), the relationship became valid (CR of 2.4 and significant) indicating that whilst the asset may not be directly considered in the mission impact, it is considered in the incident response (possibly due to strategic value/impact).

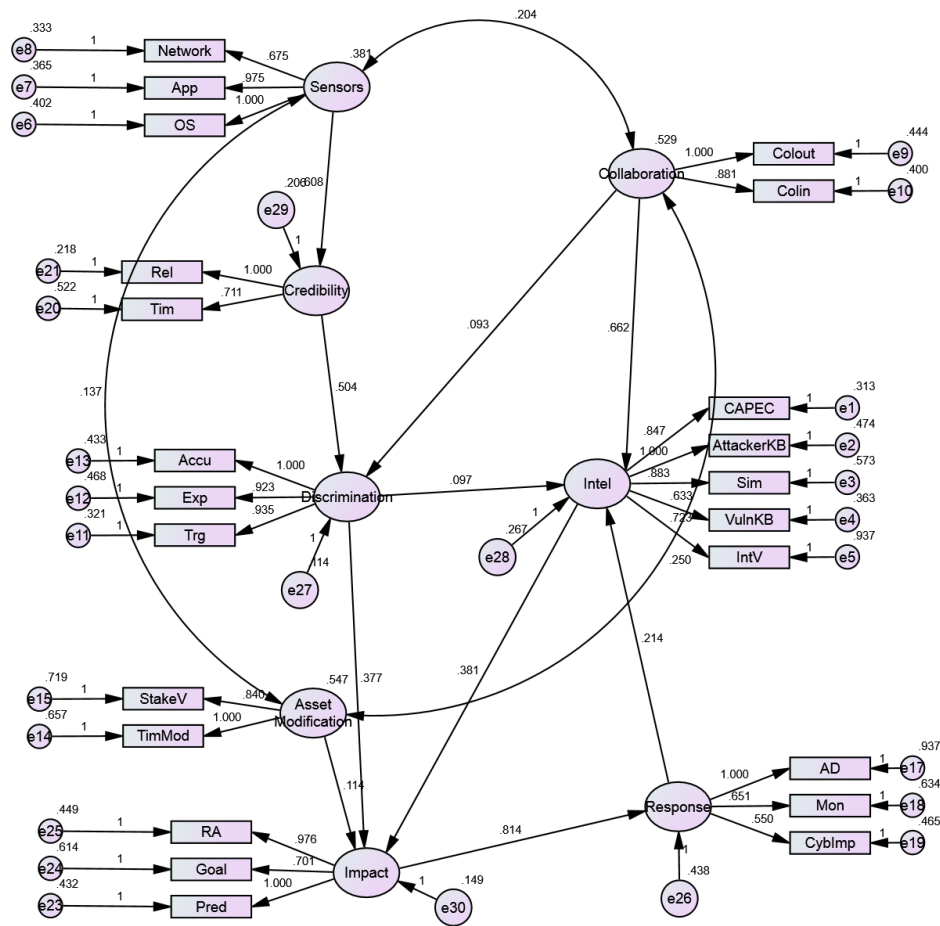


FIGURE 31- INITIAL SEM STRUCTURAL MODEL

From testing, each of the relationships in turn of the initial structural model (Figure 31) in the manner described for the relationship between Collaboration and Discrimination, Asset Modification and Response, and Discrimination and Intel, the final structural model was produced (Figure 32).

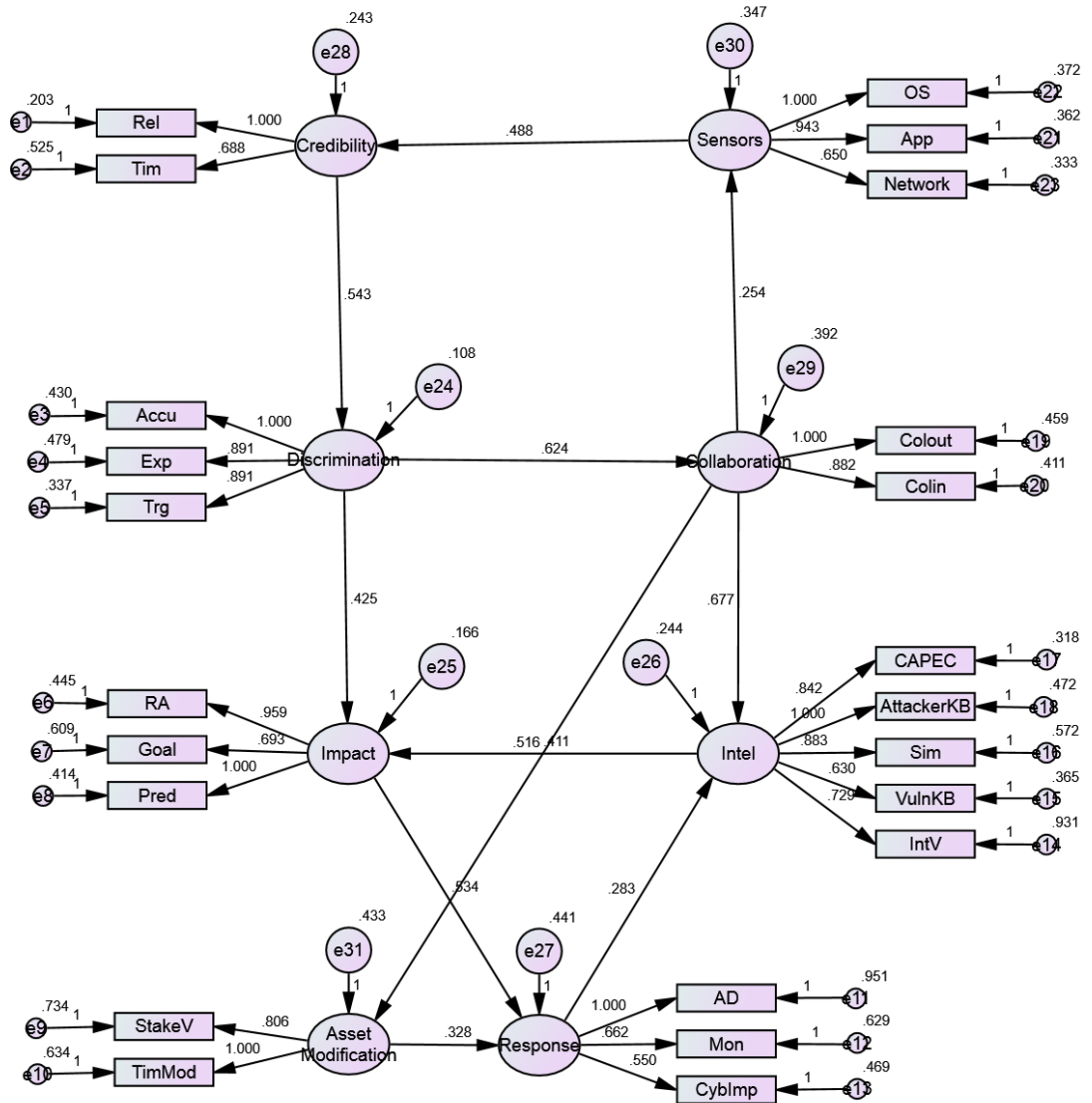


FIGURE 32- FINAL SEM STRUCTURAL MODEL

However, by analysing the relationships logically, the overlapping stages: incident detection, situational awareness and decision-making, can be seen within the structural model. By redrawing this schematically, the relationship between the factors and interconnecting processes can be seen (Figure 33), resulting in the Dynamic Cyber Incident Response Model (DCIRM). In this schematic, the three stages can be treated as follows:

- a. Incident Detection. In this model, there is a cycle of incident detection which from discriminated events will refocus the attention of the sensors (including collaboration feeds) based on any discriminated incidents, this may also include sensor tuning (to receive more rapid updates, more reliable feeds etc., thereby enhancing credibility).

- b. Situational Awareness has knowledge of the environment: i.e. collaboration, intelligence, and dynamic asset value (which is identified as Asset Modification in the SEM diagrams) and knowledge of the incident (discrimination); from these and knowledge of the mission together with an assessment of future likely events the potential mission impact can be assessed.

- c. Decision-making is directly influenced by overall impact on the targeted organisation, in terms of mission-impact and asset value which are supported by robust intelligence. The sanctioned response options are organisation specific, dependent upon resources, legal constraints and defence philosophy. Also considered in the mission impact is the value of obtainable missing intelligence information which is weighed against the risks to targeted assets and other variables contributing to mission impact.

However, one final modification to the model not realised by the SEM process was the relationship for the feedback loop to the start of the incident response process beginning at the sensors. However, in a similar manner to the MNE7 information planes (Figure 29 - MNE7 Information Environment), the external cyber environment could be seen as existing on a different plane, influenced by the incident response process (from the response decision) and feeding information to the incident detection process (via the sensors and collaboration partners).

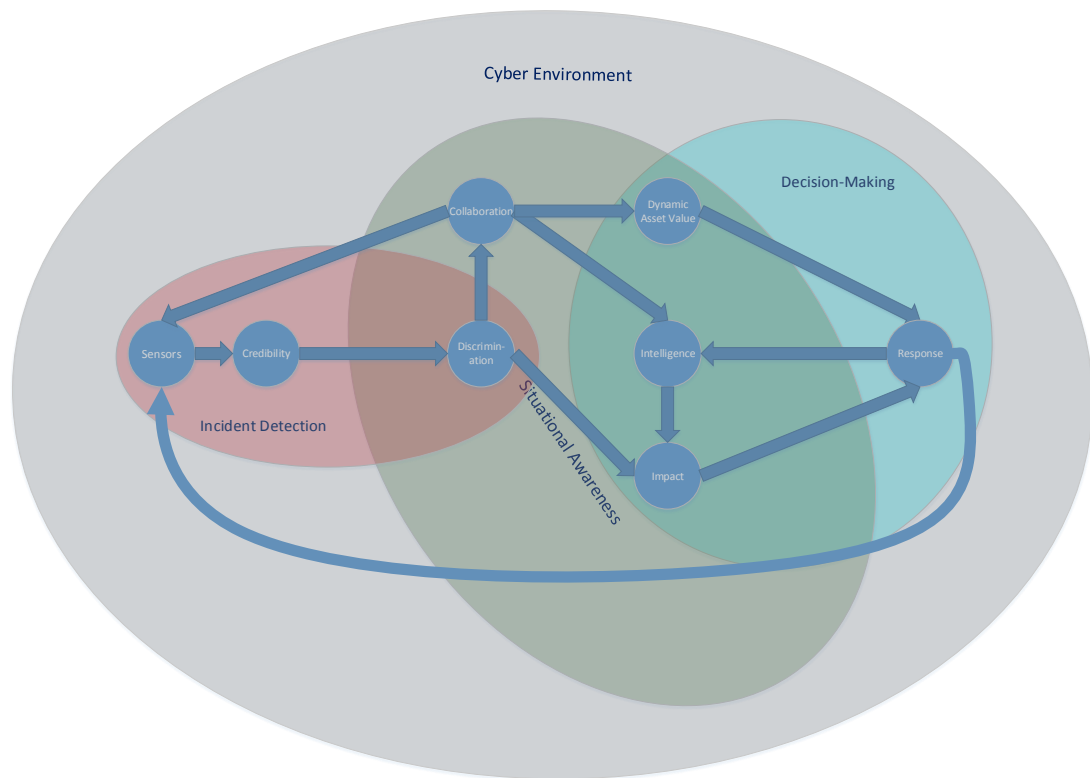


FIGURE 33-SCHMATIC DYNAMIC CYBER INCIDENT RESPONSE MODEL

4.6 Contrast with Current Models

In contrast with the traditional incident response models, (Figure 8 and Figure 9) where a single loop describes the incident response process (albeit with some additional processes outside the core in the more recent version), the derived theoretical model has separate incident detection and incident response loops. Additionally, through a feed-forward process, the detected incidents are evaluated in terms of the potential mission impact. Other points of note are that Asset Value is not fixed; this is dependent upon input from collaboration partners (visible in the diagram) as well as the independent variables relating to the stage of the mission and the internal stakeholder assessments.

This model is a significant departure from traditional incident response models such as those from the Software Engineering Institute, SANS and NIST (Figure 7, Figure 8, Figure 9 and Figure 10 respectively) as the impact of the incident on the defending organisation, the value of the potential intelligence to be gained and the value of the defended asset ultimately determine the appropriate response. It also provides more granularity in the provision of Situational Awareness specific to the Cyber Domain compared to the generic

SA model of Endsley (Figure 12), and by extending the cycle into the decision-making reaches beyond the Cyber SA Reference model of Tadda and Salerno (Figure 13).

4.7 Practical Implications

Using this model, it is anticipated that high-level policy will be developed separating the incident detection process and the incident response decision-making process. The detection process is fairly independent of organization although monitoring infrastructure and resources will vary from organization to organization. However, the decision-making will not only be constrained by resources but also the legal-framework, risk appetite and organizational objectives binding the responsible decision-maker. By defining the interfaces between these two separate stages and the creation of comprehensive situational awareness, organisation-specific processes can be created to support the decision-making regarding choice of appropriate response options.

5 Operational Validation Results and Analysis

5.1 Background

As described in detail in Section 3.5.1, at a meeting of the Joint Force Command Brunssum (JFCBS) Cyber Defence Working Group (CDWG) in Summer 2015, it was identified that although the planning processes for most of areas of operations were catered for in the NATO Common Operational Planning Document (NATO Allied Command Operations, 2013) these did not include Cyber Operations. To address this gap, a prototype tool was produced based on this PhD research which was the final artefact in the third cycle of the DSR approach (Figure 17).

5.2 Cyber Operations Support Tool

The tool was produced using a Microsoft Excel workbook and was named the “Cyber Operations Support Tool (COST). COST (Figure 34) linked the component parts of the model to the branch and internal structure of a NATO Joint Force Command HQ thus allowing the JFCBS staff to populate the tool with relevant data (such as asset values at different stages of the mission cycle). This in turn provided the key decision-maker with situational awareness at a level abstract enough to allow the choice of an appropriate response to a Cyber Incident.

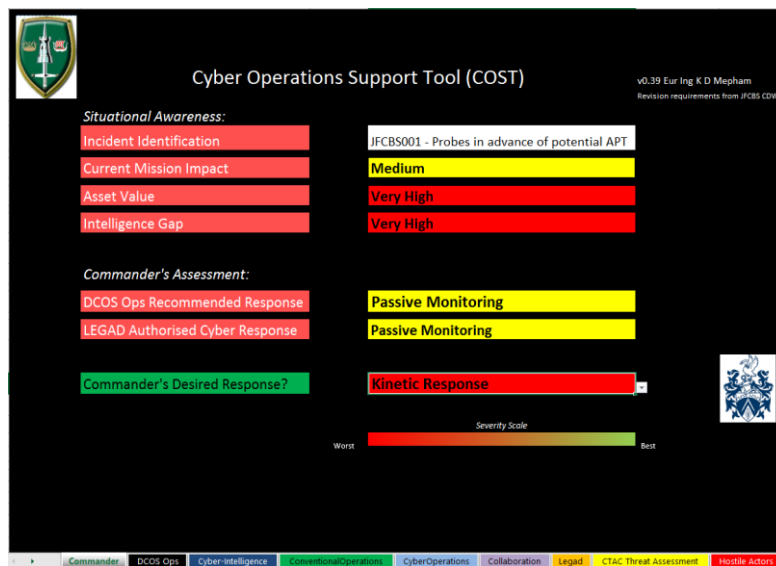


FIGURE 34 - CYBER OPERATIONS SUPPORT TOOL

In terms of following the DCIRM model, the COST demonstrated the Situational Awareness and Decision-Making phases of the model (as Incident-Detection is a well-established area

and is outside the remit of the cross-functional staff officers providing the Commander with advice). In the tool, a cross-functional working group populated the asset value for their different assets (Figure 35) for all stages of the mission (providing dynamic asset value), they also provided advice on the overall mission value for each of the assets from a mission perspective for each mission stage (populating Mission Impact). Utilising a NATO algorithm, the Cyber Threat Level was calculated from the Cyber Intelligence information and the Intelligence Value also identified by the J2 (Intelligence) specialists. The Mission Impact and Intelligence Gap were then provided together to the Commander (to make an evaluation of the relative mission merits of both values) together with the Dynamic Asset Value for him to choose an appropriate response. In choosing the response more (or possibly no) additional information would be fed back to the Intelligence specialist contingent upon the response (i.e. a traditional response would deny additional information as the attack would be stopped, a passive or offensive response would feed-back additional information).

Unfortunately, it was neither possible to see the exercise injects prior to the exercise nor to tailor them to evaluate the tool and model fully. However, COST was utilised by the CDWG during the exercise and in addition to its use as a cyber incident response tool it was reported that it had substantial utility as a planning tool for re-evaluating the initial priorities placed on critical and valuable assets (**Error! Reference source not found**.example values and names have been used as actual prioritised asset lists are classified).

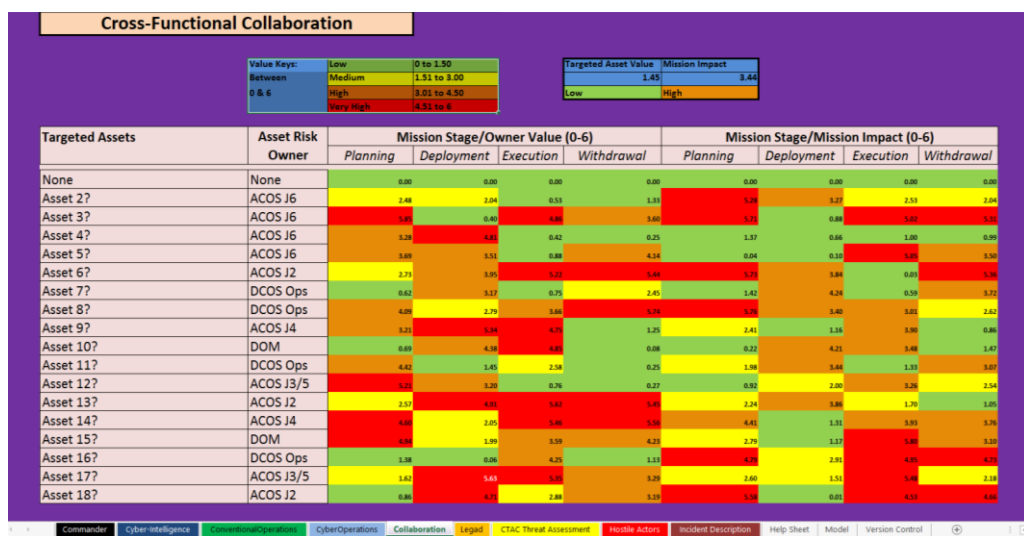


FIGURE 35 - PRIORITISED ASSET LIST

5.3 Evaluation

The evaluation of this tool considered 10 areas which were assessed both with and without the tool. These comprised factors from the decision-making area of the model, analysis of efficiency and effectiveness in providing the information and analysis of ability to cope with three of the relevant characteristics of the future battlespace (Ministry of Defence (UK), 2015); these were as follows (relevant factors or source in brackets):

- i. Cross-functional awareness of cyber impact on other branches (Collaboration).
- ii. Cyber impact on the mission (Mission impact).
- iii. Cyber impact on Intelligence (Intelligence).
- iv. Awareness of the Commander's response options and chosen response (Cyber Response).
- v. Efficiency in providing information to a cyber impact assessment (efficiency of communication).
- vi. Ability to provide relevant information to a cyber impact assessment (effectiveness of communication).
- vii. Ability to operate effectively in a congested cyber environment (Ministry of Defence (UK), 2015).
- viii. Ability to operate effectively in a contested cyber environment (Ministry of Defence (UK), 2015).
- ix. Ability to operate in a cluttered cyber environment (Ministry of Defence (UK), 2015).
- x. Awareness of dynamic targeted asset value in different mission stages (Dynamic Asset Value).

5.4 Analysis

Analysis of the responses using a paired-samples t-test provided the results given in Figure 36. The results suggest that for all areas assessed (which is a physical instantiation of the model) the tool provides a significant benefit compared to not using the tool (i.e. two-tailed significance is below 0.05 for all categories).

Paired Samples Test									
		Paired Differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference				
					Lower	Upper			
Pair 1	XFunctionalAwarenessT - XFunctionalAwareness	1.857	.910	.199	1.443	2.271	9.350	20	.000
Pair 2	MissionImpactT - MissionImpact	1.619	1.071	.234	1.131	2.107	6.926	20	.000
Pair 3	IntelligenceT - Intelligence	1.524	1.167	.255	.993	2.055	5.984	20	.000
Pair 4	CdrResponseT - CdrResponse	1.143	.964	.210	.704	1.581	5.435	20	.000
Pair 5	ProvisionEfficiencyT - ProvisionEfficiency	1.238	1.300	.284	.646	1.830	4.364	20	.000
Pair 6	ProvisionRelevanceT - ProvisionRelevance	1.333	1.354	.295	.717	1.950	4.513	20	.000
Pair 7	CongestedT - Congested	1.286	1.146	.250	.764	1.808	5.139	20	.000
Pair 8	ContestedT - Contested	1.381	1.024	.223	.915	1.847	6.183	20	.000
Pair 9	ClutteredT - Cluttered	1.381	.865	.189	.987	1.775	7.319	20	.000
Pair 10	MissionStagesT - MissionStages	1.810	.981	.214	1.363	2.256	8.455	20	.000

FIGURE 36 - PAIRED SAMPLES T-TEST

However, in order to provide a more robust measurement of the utility of the tool, Cohen’s d and associated effect size were also calculated (Figure 37). The effect size is calculated using

$$d_z = \frac{|\mu_z|}{\sigma_z} = \frac{|\mu_x - \mu_y|}{\sqrt{\sigma_x^2 + \sigma_y^2 - 2\rho_{xy} \sigma_x \sigma_y}}$$

Where d_z = the effect size index, μ_x = population mean for the control group, μ_y = population mean for the treatment group, ρ_{xy} = correlation between the control and treatment variables, σ_x = standard deviation of the control group and σ_y = standard deviation of the control group.

Using the effect size from Cohen’s d it is suggested that 0.2 to 0.5 represents a small effect size, 0.5 to 0.8 a medium effect size and above 0.8 a large effect size (Cohen, 1992). Based on this categorization, all analysed categories fall into the “medium” effect size suggesting that for the analysed properties of the model-based tool that an obvious observable improvement compared to prior practices is experienced by the users of the tool.

Paired Samples Statistics														
	Mean	N	Std. Deviation	Std. Error Mean		$(n_c-1)s_c^2$	$(n_c-1)s_c^2$	$n_c \cdot n_c$	S_{pooled}	$\bar{x}_c - \bar{x}_o$	Cohen's d	Effect size		
Pair 1	XFunctionalAwareness	2.1	21	0.831	0.181				10.952	42	0.767854	1.85	2.409311	0.769439
	XFunctionalAwarenessT	3.95	21	0.74	0.161	13.81122								
Pair 2	MissionImpact	2.24	21	0.944	0.206		17.82272	42	0.850766	1.62	1.904167	0.689542		
	MissionImpactT	3.86	21	0.793	0.173	12.57698								
Pair 3	Intelligence	2.29	21	1.007	0.22		20.28098	42	0.866451	1.52	1.754282	0.659416		
	IntelligenceT	3.81	21	0.75	0.164	11.25								
Pair 4	CdrResponse	2.76	21	0.889	0.194		15.80642	42	0.749903	1.14	1.520196	0.605133		
	CdrResponseT	3.9	21	0.625	0.136	7.8125								
Pair 5	ProvisionEfficiency	2.57	21	1.165	0.254		27.1445	42	0.930853	1.24	1.332111	0.554348		
	ProvisionEfficiencyT	3.81	21	0.68	0.148	9.248								
Pair 6	ProvisionRelevance	2.48	21	0.928	0.203		17.22368	42	0.905635	1.33	1.468582	0.591866		
	ProvisionRelevanceT	3.81	21	0.928	0.203	17.22368								
Pair 7	Congested	2.05	21	1.024	0.223		20.97152	42	0.94671	1.28	1.352051	0.560056		
	CongestedT	3.33	21	0.913	0.199	16.67138								
Pair 8	Contested	2.05	21	0.669	0.146		8.95122	42	0.725482	1.38	1.902183	0.689165		
	ContestedT	3.43	21	0.811	0.177	13.15442								
Pair 9	Cluttered	2.14	21	0.854	0.186		14.58632	42	0.814135	1.38	1.695051	0.646552		
	ClutteredT	3.52	21	0.814	0.178	13.25192								
Pair 10	MissionStages	2.19	21	0.68	0.148		9.248	42	0.711479	1.81	2.543996	0.786146		
	MissionStagesT	4	21	0.775	0.169	12.0125								

FIGURE 37 - COHEN'S D WITH EFFECT SIZE

5.5 Feedback

In the version of the tool that was used for the validation (Version 0.39) several comments were received, these are summarised in Appendix 5 – COST Feedback. Most of the comments were related to tracking multiple incidents or attackers which would be a follow-on stage, achievable by using a database back-end to the tool. However, the vast majority of the comments both verbally and written were extremely positive about the direction of the tool and the model in general.

6 Experimental Results and Analysis

6.1 Experimental Aim

As described in detail in Section 3.6, the aim of the experiment was to assess the contribution of the Dynamic Cyber-Incident Response Model in its support to the decision-making process for a Joint HQ commander responsible for deployed units executing missions in multi-domain warfare environments; this was compared to the support provided by the traditional Cyber-Incident Response Models and the information provided by these in the same environments. To achieve this aim, scenario-based experimentation was utilised.

6.2 Experimental Objectives:

The experiment was designed to achieve the following objectives:

- i. Compare perceived situational awareness with and without the additional information from the DCIRM.
- ii. Compare confidence in decision-making with and without the additional information from the DCIRM.
- iii. Compare perceived capability to cope with a congested environment with and without the additional information from the DCIRM.
- iv. Compare perceived capability to cope with a contested environment with and without the additional information from the DCIRM.
- v. Compare perceived capability to cope with a cluttered environment with and without the additional information from the DCIRM.
- vi. Compare perceived capability to dynamically track the impact of a cyber-incident during a progressing mission with and without the additional information from the DCIRM.

Whilst primarily evaluating the situational awareness and decision-support influence of the DCIRM, the responses themselves and the timeliness of the response was also evaluated to look for any influence exerted by the model.

6.3 Experimental Results and Analysis

The experimental results were divided into three distinct categories: situational awareness and decision support, timeliness and chosen response. The first of these categories relied upon the questionnaire (given at Appendix 8 – Evaluation Questionnaire). The second category measured the time taken to complete the simulation (measured from the introduction of the first inject to the completion of the experiment). The final category analysed the responses for consistency amongst the group when compared to the expected responses.

6.3.1 Situational Awareness and Decision Support

The first three questions in Appendix 8 – Evaluation Questionnaire are designed to evaluate Endsley’s three stages of SA; Perception, Comprehension and Projection (Endsley, 1995). It can be seen from Figure 46 - Paired Samples T-Test and Figure 47 - Cohen's D Calculation in Appendix 9 – Situational Awareness and Decision Support Results that not only are the results significant but that there is a large effect, determined by Cohen’s D being above 0.8, (Cohen, 1992). Questions 4 to 6 evaluated the comprehension of three of the decision-making factors from the model (Mission Impact, Intelligence and Response). From Appendix 9 – Situational Awareness and Decision Support Results it was determined that these also improved significantly and with a large effect size. Questions 6 to 9 evaluated the capability to deal with three of the five characteristics of Battlespace (Ministry of Defence (UK), 2015) and the final question evaluated the capability of the tool to deal with a dynamic environment. Questions 1 to 6 and 10 as a group can all be considered as evaluating the contribution of the enhanced situational awareness delivered by the model to the decision-making process. This grouping is borne out by both the minimum inter-item correlation value of 0.338 and Cronbach’s Alpha value of 0.908 for the set, comfortably exceeding the thresholds of 0.30 and 0.70 for reliability of a summative grouping¹⁰. These results confirmed the significant improvement with large effect. This summative effect can

¹⁰ (Hair Jr, Black, Babin, & Andersen, 2014) (Adam, 1993) p123 – Creating Summated Scales - Reliability.

be seen graphically in Figure 38 - Total Distribution SA-Related responses where the distribution a summative grouping of all responses can clearly be seen to have moved to the right (improved SA) in the treatment condition (i.e. where the model has been used to provide additional information). This summative distribution clearly indicates that the decision-makers who took part in this experiment were more confident in the information that they received to assist them in deciding upon an appropriate cyber response to an incident.

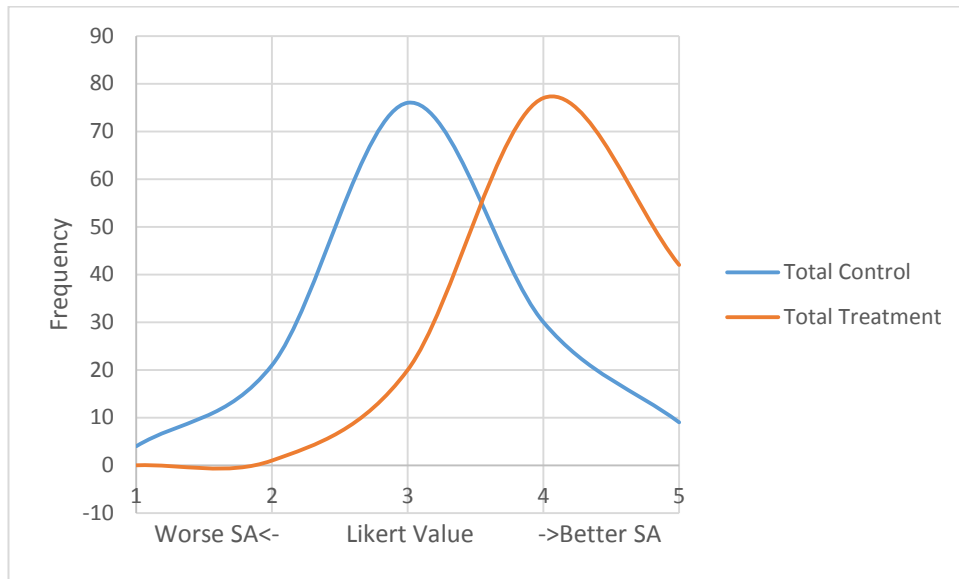


FIGURE 38 - TOTAL DISTRIBUTION SA-RELATED RESPONSES

6.3.2 Timing

The time taken to complete the entire experiment is shown in Figure 39 - Overall Time to Complete Experiment, this captures both the time taken to digest the presented information and choose an appropriate cyber response. In general, the overall time to take a decision decreased, although during interview some participants confirmed that they needed longer to consider their decision with the additional dynamic model information as they needed more time to digest the additional information. However, even these participants felt more confident in their decision-making abilities. Despite the visible differences in the distributions, the differences between the responses in the control and treatment scenarios were determined neither to be significant nor exhibit a noticeable effect on the time taken to decide on an appropriate response to a cyber incident.

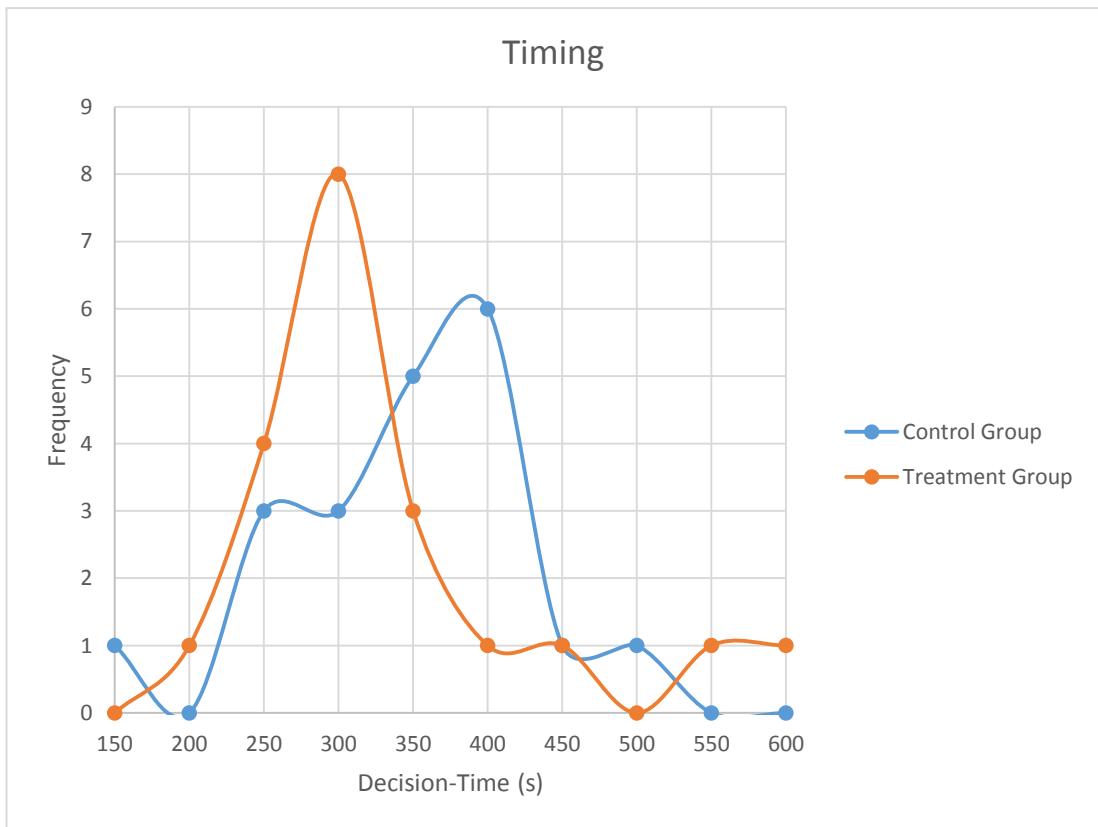


FIGURE 39 - OVERALL TIME TO COMPLETE EXPERIMENT

6.3.3 Decision Analysis

This analysis of the decisions taken makes use of a behavioural baseline based on my own perspective which is a consequence of training, experience and the interaction with experts during this research. The decisions chosen could be analysed in terms of offensiveness but from this perspective there is no “better” solution for all circumstances as the response should be based upon a perceived potential profit/loss calculation which will vary depending upon the scenario. The baseline that I produced for the advocated responses results from the following assumptions:

- a. Where Intelligence Value is low a traditional response is advocated as there is nothing to be gained from placing any asset at potential risk.
- b. Where Intelligence Value and Asset Value are equal (but not rated as Low), a passive response is advocated as this would provide the potential for Intelligence to be gained without posing a high risk to the asset.

- c. Where Intelligence Value is higher than Asset Value a passive or a cyber offensive response are advocated as these allow additional intelligence to be gained.
- d. Where Asset Value is higher than Intelligence Value a traditional response is advocated as this provides minimal risk to the asset.

Overall, the treatment group were more prepared to adopt a less traditional approach when provided with the extra information from the factors in the model (Figure 40: Frequency of Decision Choices). When examining the mean deviations from the advocated responses the differences in responses were also substantial with the tendency to align with the advocated responses increasing by more than 10% of the range i.e. a shift from 0.64 mean deviation from the advocated response to 0.43 with a total range of 2 (i.e. a traditional response was assigned a value of 1 and a cyber-offensive response a value of 3).

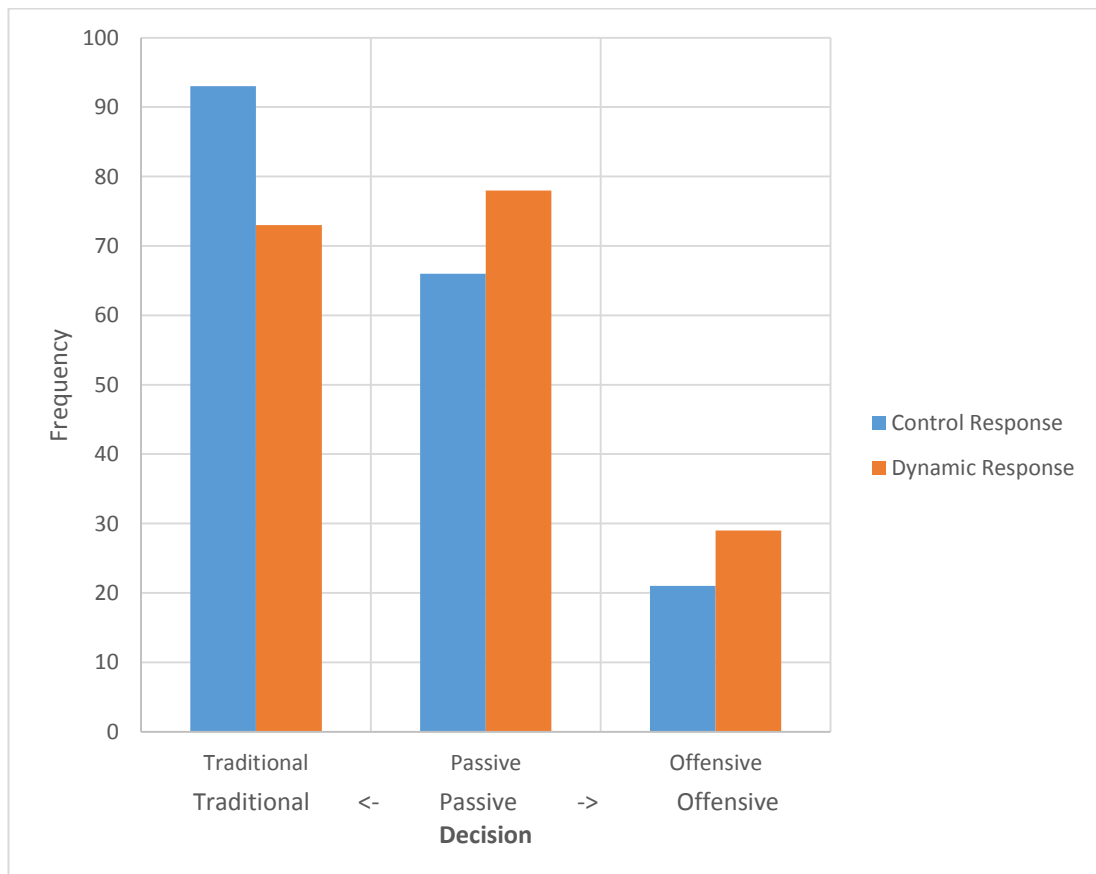


FIGURE 40: FREQUENCY OF DECISION CHOICES

7 Discussion and Conclusions

7.1 Model Comparison and Evolution

During the Literature Review and surveys, commonly used Cyber-Incident Response reference models such as the SANS model (Figure 9 - SANS Institute Incident Response Cycle, 2003), the NIST Model (Figure 10 - NIST Special Publication 800-61 Incident-Handling Process, 2012) and the CERT-CC Model (Figure 8 - CERT/CC Incident Handling Life-Cycle, 2003) were found to overlook some areas of importance in the consideration of an appropriate response when viewed from the perspective of a cross-section of stakeholders impacted by cyber incidents. These existing models prioritised the immediate protection of the defended infrastructure, with longer term improvements to the defensive measures being made as a result of the information discovered whilst resisting or neutralising the attacks.

In producing these models, although undoubtedly based on the opinions of experienced experts in the information security field, no publicly-available or discernible empirically-based foundation for these models was discovered during the literature review. This was already highlighted as an issue in 2009 when research examined the field in general (Verendel, 2009). When contrasting DCIRM with the latest of these models (Figure 10 - NIST Special Publication 800-61 Incident-Handling Process, 2012), DCIRM caters for collaboration within the detection process and also shares information with the partners during this process, in the NIST model collaboration is not explicitly stated but would mainly take place in the “detection and analysis” phase although some lower levels of collaboration would also be expected during the other phases. The concept of Dynamic Asset Value is introduced in DCIRM where the value of the attacked asset takes on a temporal nature, reflecting relative importance based on the point in the mission/business cycle that the attack takes place; this concept is absent in the NIST model as this is more general using a “one size fits all” approach although in the supporting documentation, inventories of critical assets and risk assessments are specifically mentioned as good preparation measures. In DCIRM, a separate process gives rise to an impact assessment based on available intelligence, the detected incident, the current mission and a projection of incident progression. In contrast, the NIST model describes a functional and information impact (reflecting the business and security impact) as well as a recoverability assessment;

these take place in the detection and analysis phase. Additionally, in DCIRM, Intelligence is a separate factor where not only the existing intelligence information is considered but also the potential information to be gained during an incident. This is then considered in the Mission Impact which, together with the Dynamic Asset Value informs the response. In the NIST model, the only considered response is to “contain and eradicate”; this contrasts with DCIRM where a range of responses are considered which may either stop the attack within the defended infrastructure, gather additional intelligence or actively engage with the attacking infrastructure. Finally, in the NIST model, an inner and an outer feedback loop define the incident response process allowing a faster incident analysis and eradication process to operate inside a longer lessons-learned and preparation process. Whilst an improvement over previous models, where a single cycle was defined, the DCIRM operates an independent feedback loop for incident detection and discrimination, reflecting the continuous nature of incident detection. The discriminated incidents are then fed into a situational awareness phase and then a decision-making phase, which has its own feedback loop, informing the intelligence factor based on the response decision, allowing for another reactive cycle where the response informs the intelligence which then updates the mission impact in order to make the next decision.

The DCIRM was produced as a result of the research which went through several stages of development. In order to identify additional perspectives from the cross-section of stakeholders instead of just the information security community, a comprehensive survey was carried out to evaluate potential variables discovered during the Literature Review and identify common factors using principal component analysis. The confirmation of these factors and the evaluation of the relationship between them was then analysed utilising Structural Equation Modelling (Figure 41 - Structural Equation Model).

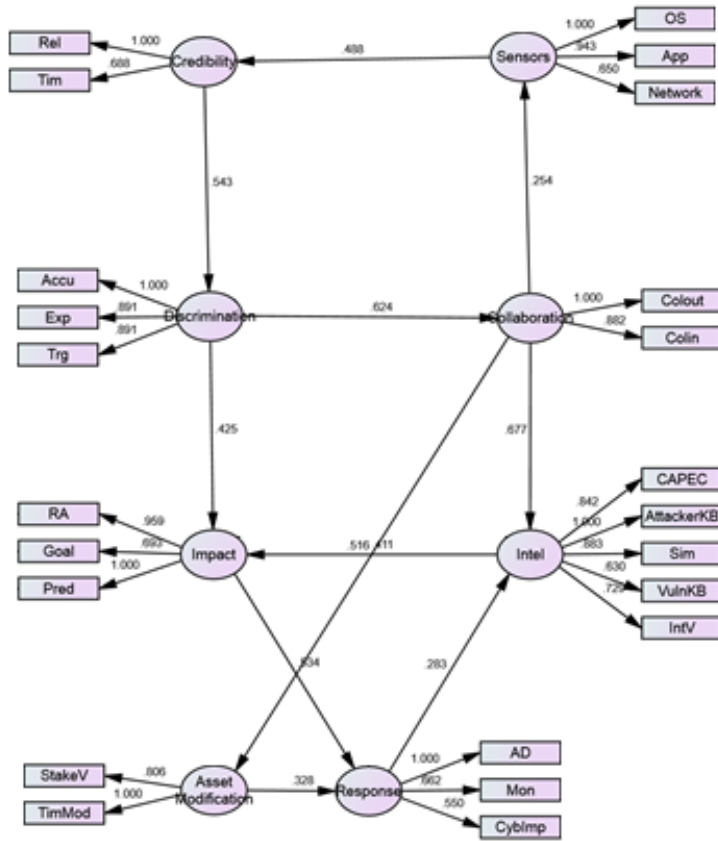


Figure 41 - Structural Equation Model

This then resulted in the Dynamic Cyber Incident Response Model shown at Figure 42 where the recognition that the cyber response influences the environment and thus the changes detected by the Incident Detection phase of the model close the loop of the entire response. This model was then evaluated in both a controlled experiment and as a fielded prototype in an exercise environment.

7.2 Key Findings

This research has identified and confirmed several concepts which must be considered in producing a comprehensive cyber-incident -response strategy:

- a. Missing intelligence value must be considered against the value of defended assets when choosing the response to an incident.
- b. Cyber-incident response must be considered as a cross-functional problem (i.e. not limited to only an IT or security specialist's

perspective) if the objectives of the whole organisation are going to be achieved. It is not only the impact of an attack on an asset to the asset owner that counts; it is the impact on the business that should take priority.

- c. Only using a traditional response to cyber-incidents potentially deprives an organisation of information/intelligence that might help it to defend itself (and its partners) better in the long-term.

Both the controlled experiment and fielded operational use of a prototype tool developed from the Dynamic Cyber-Incident Response Model (DCIRM) confirm that the factors from the model provide enhanced situational awareness and increased confidence for decision-makers to choose a considered cyber-response option when compared to a traditional approach. However, the tool developed from the model did not only allow an immediate evaluation of risk based on the local risk appetite in order to make a cyber-response decision, it also provided a framework to consider the asset value of important infrastructure in a cross-functional environment in advance of a mission being executed.

During analysis of the results from the operational validation, when compared to an expected response, the responses chosen by the participants increased their alignment with the expected response by more than 10% of the range of the utilised Likert Scale when compared to those when information was provided in a traditional manner. This indicates that the information provided by the DCIRM is more relevant for informing decision-making when passive and active responses are additional options to traditional incident response. This makes the model relevant for the modern environment where the full range of options from traditional incident response to Cyber Offensive operations are within the inventory of many nations and the risk of defended networks being compromised can be balanced against potential intelligence gains and mission/organisational objectives. From a legal perspective, this is also compatible with the framework of guidance provided by the current version of the Talinn Manual (NATO Cooperative Cyber Defence Centre of Excellence, 2016).

7.3 Evaluation of Analysis Outcomes compared to Research Objectives

The following paragraphs state the research objectives and then an analysis of how they were met.

7.3.1 Objective 1: Analyse the problem space by investigating the key variables that define its dimensions, specifically this should include all variables deemed to be influential in providing the decision maker in the cyber incident response process with the best information to decide upon a response.

During the literature review, several variables were identified from a variety of areas including intelligence, command and control, warfare and cyber security; in parallel their context and contribution was discussed during expert working groups. The importance of these variables was then evaluated statistically by means of a survey. The results were analysed using principal component analysis to identify key factors that contribute to effective cyber incident response and the analysis was developed further during the Structural Equation Modelling, where relationships between the factors were analysed, resulting in a model which was tested both operationally and in a controlled environment through instantiation in a fielded prototype.

7.3.2 Objective 2: Develop a model to represent the defined problem space and potential solutions whilst addressing perceived gaps within the prevalent cyber incident response models.

Utilising Design Science Research as a research method, an initial hypothesised model was proposed after identification of key factors from the principal component analysis. This was refined after confirming the factors and then evaluating the relationships between them utilising structural equation modelling. This led to the identification of new factors directly influencing the decision-making process as well as confirming known factors already used in traditional cyber-incident detection processes (which can be seen in Figure 42 - Dynamic Cyber Incident Response Model). The new factors were the Dynamic Asset

Value (of the assets being defended), an Intelligence factor (where the known intelligence as well as the value of existing intelligence are considered), Mission Impact (which considers impact on the immediate and long-term business objectives) and in the Decision-Making factor a number of responses were considered which, in addition to a traditional response, were passive response (allow an attack to continue unimpeded in order to gather additional intelligence) and active response (i.e. reaching out to the attacker’s network either for reconnaissance or to stop the attack). Additionally, the importance of collaboration (both in receiving and sharing information) was reinforced.

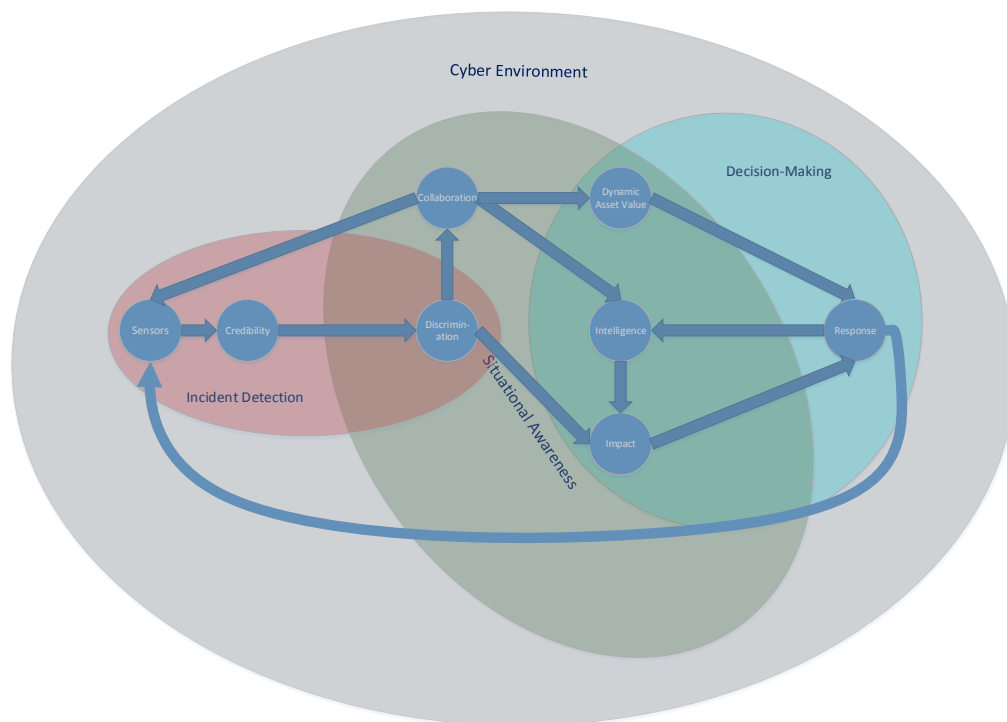


FIGURE 42 - DYNAMIC CYBER INCIDENT RESPONSE MODEL

7.3.3 Objective 3: Evaluate the developed model against the prevalent incident response models and the perceived deficiencies in those models.

Due to timing necessitated by the rolling training programme of an active Joint Force Command Headquarters, a tool based on the Dynamic Cyber-Incident Response model was developed and tested “in the field” prior to the academic experiment. The participants in the field evaluation found that the tool had significant utility and this was subsequently used as part of the training in a newly established Cyber Operational Planners’ course at the CCDCoE. The results of the analysis of the subsequent controlled experiment

determined that the tool significantly enhanced situational awareness (improving by more than 25% which equates to approximately 1 point on the Likert scale) and consequently confidence in responding to cyber-incidents. The alignment of the range of tested responses with expected response options increased markedly when using the tool developed from the model (this reduced the mean deviation of the monitored responses from the advocated responses from 0.64 to 0.43 i.e. an improvement of 33%, as described in Section 6). The static asset values, lack of information relating to cost/benefit of gathering intelligence information and impact on objectives lacking in the traditional models (Figure 8 - CERT/CC Incident Handling Life-Cycle, 2003), (Figure 9 - SANS Institute Incident Response Cycle, 2003), (Figure 10 - NIST Special Publication 800-61 Incident-Handling Process, 2012) were all addressed within the model and found to be extremely beneficial in both the operational validation and controlled experiment as is described in the anecdotal feedback in Appendix 5 as well as the results described in Chapters 5 and 6. Additionally, the new DCIRM could also be compared to more generic Situational Awareness and Command and Control Models such as those advocated by Endsley, (Figure 12), Boyd, (Figure 1) and Lawson (Figure 2), but more responsive due to the additional internal feedback loops. However, whilst following the top-level concepts of these generic models, the multiple feedback iterations and specific factors discovered during this research make this model better suited for bridging the theoretical cyber domain to the practical implementation in policy, procedures and tools.

7.3.4 Objective 4: Assess the implications of practical instantiations of the employed model against the problem space.

The model provides a logical view of Incident Detection, creating Situational Awareness and Decision-Making as three separate but integrated processes, as is demonstrated in the tool (COST), the model can be used to provide appropriate information to non-specialist decision-makers to better inform response decisions. The key improvement in the decision-making results from providing the decision-makers with the capability to directly compare intelligence priorities, asset value and mission impact. Whilst mission impact is the over-riding concern for military commanders, officers with command experience are amenable to risking assets if it is likely to result in an increase in valuable intelligence which in turn may provide strategic advantages in the longer term. In a commercial environment, similar considerations could take place in terms of Business Intelligence (in trying to establish which competitor, if any, is behind an attack), Business Impact and Dynamic Asset

Value (measured against the business cycle), however, the constraints would also need to be adjusted due to differing legal frameworks and constraints (for example PCI-DSS, GDPR etc).

7.4 Contribution to the Field

The contribution of this research to the field is summarised in the following paragraphs.

7.4.1 Theoretical Contribution:

Compared to the traditional incident response models, (Figure 8 - CERT/CC Incident Handling Life-Cycle, 2003), (Figure 9 - SANS Institute Incident Response Cycle, 2003), (Figure 10 - NIST Special Publication 800-61 Incident-Handling Process, 2012), the DCIRM identifies additional novel factors to consider during a cyber-attack. However, due to the SEM process, it also establishes the complex relationships between the factors and the feedback loops within and between the processes unlike the traditional models. Some of the novel components are recognised by others but from different perspectives e.g. the NC3A CIS Security Framework (Hallingstad & Dandurand, 2011) recognises the value of assessing dynamic risk during an attack, but in the context of a CIS security functions rather than in a response model. As far as can be determined, this research results in the first cyber incident response model to be determined through comprehensive statistical analysis of responses from a cross-section of those impacted by cyber events. The subsequent operational validation and controlled experiment serve to confirm the validity and utility of the model. The theory also extends the concepts proposed in command and control theory such as Boyd's OODA loop (Orr, 1983), Endsley's SA Model (Endsley, 1995), and Tadda and Salerno's Cyber SA Model (Tadda & Salerno, 2010). However, as the DCIRM was developed and researched specifically for cyber-incident response it is more granular than these generic models.

The model is divided into three main process areas: Detection, creation of Situational Awareness, and Decision-Making. The Detection process mirrors traditional Incident Response practices, but also includes a Collaboration factor (which may be from internal sources, external or a combination of both) as providing information to be considered as input to Sensors (along with "owned" sensors). Creation of Situational Awareness, takes the discriminated incident information, compares this with the intelligence that is known (or the value of the intelligence that may be gained from the incident), the importance of the asset and separately the value of the asset to the asset owner is evaluated (which may

also be influenced by collaboration partners). These are then considered together by the decision maker in choosing a response (which ultimately influences the environment and the intelligence to be gained. The additional feedback loops within the various stages of incident response (detection, generating SA and decision-making) allow a tighter and better-informed response i.e. because several iterations take place within the overall response cycle, more opportunity is provided to respond within an adversary's OODA loop and with more relevant information.

The novel factors and concepts utilised in this model are:

- a. Intelligence Value: this allows risk from potential compromise to be balanced against the missing information about an attacker or attack;
- b. Dynamic Asset Value: e.g. the value of an asset varies during a mission or business cycle e.g. the value of a mission plan at the beginning of a mission, immediately prior to execution, after execution and at the end of a mission;
- c. Mission Impact: the response must be weighed up against the objectives of the mission and not routinely executed without regard to the objectives.
- d. Response options: the traditional response of stopping or containing an incident within the defending network is no longer appropriate in a modern environment. More options are required which support the mission objectives including both passive (observe an attack without interference within the defending network to gather intelligence) and offensive operations. The offensive and passive responses are not considered in the traditional models mentioned in the preceding paragraphs.

Although primarily developed from a military perspective the model could be repurposed to allow the development of procedures and tools for different organisational, cultural and legal environments. The inner feedback loops within the model provide enhancement of the traditional incident response methods by providing enhanced situational awareness, enhancing information iteratively within the overall cyber-incident response cycle.

7.4.2 Artefact:

A fielded prototype tool (COST): this prototype tool has been used as a key tool within a NATO HQ as part of a qualification exercise to certify as a NATO Response Force. The Cyber Operational Support Tool developed for a NATO Joint Force Command HQ provided a physical instantiation of the model in a practical environment. This resulted in a novel method for evaluation of cyber incidents and allowed the Cyber Defence Working Group to provide relevant and timely advice to both the Joint Operational Planning Group and the Commander. During the exercise, intended to evaluate operational procedures and readiness, COST was used as an integral component of the established mission battle rhythm for the Cyber Defence Working Group as well as an immediate action tool as incidents were detected. It has also been used to train NATO cyber operations staff as part of a Cyber Operational Planners' course at the NATO CCDCoE where the utility of the cross-functional collaboration was also emphasised. The artefact, which has been validated in both controlled and operational environments, demonstrates the utility of the research in providing a bridge between theory, built upon a solid statistical evaluation of opinion, into a model which informs the production of a tool to be used in a practical environment. This was borne out by its use as a teaching aid in NATO's Cooperative Cyber Defence Centre of Excellence.

As a fielded prototype, this first instantiation of a tool based on the Dynamic Cyber-Incident Response Model provides a solid base for further development and refinement to meet the evolving needs of the organisation. The fielded tool utilised a NATO-developed algorithm for calculation of cyber risk, but this can be replaced with any algorithm for other environments, constraints and risk appetites.

7.4.3 Summary

In summary, this PhD research has produced a novel dynamic model for responding to Cyber incidents; through its implementation in a tool, it has been both tested empirically and validated operationally. The model reflects real world circumstances where assets under attack may change in value during a business or mission cycle and where discovering missing information about an attacker also has a value to the organisation. The shorter feedback loops when responding to an incident provide more of an opportunity to respond

more quickly than the opponents. Furthermore, in the controlled experiment, the tool produced from the model was shown to produce a 25% improvement in situational awareness which realised a 33% improvement in the decision taken (compared to providing traditional information when measured against an expected response).

7.5 Research Constraints, Limitations and Complications.

Several of the constraints were due to the nature of my profession, the participants and the type of information to which I had access. Additionally, other constraints were related to my geographical location. These are outlined in the following paragraphs.

7.5.1 Classified Information

Some material and participants which I had access to could not form part of the research due to the classification placed on the material by the originator or the sensitivity of the discussions. However, where this material has shaped my opinion or influenced my research I have found other verifiable unclassified material to support those views which have been appropriately referenced in this research.

7.5.2 Participants

Most participants in the surveys, experiments and expert working groups were from military or governmental agencies/organisations from NATO (or NATO-friendly) countries. This could influence the way that the participants approach cyber-incident response and the importance that they place on the factors associated with it as there is a great deal of harmonisation of policies and procedures across NATO and Partnership for Peace (PfP) nations. Additionally, many potential participants, whilst willing to provide “off the record” opinions and information were not willing to undertake surveys or be identified due to sensitivity of their positions (this is not uncommon for security/intelligence professionals). This resulted in lower numbers of official participants in the experiments and surveys than would have been hoped.

7.5.3 Geographical Location

The lack of regular access to a full academic network has necessitated more reliance on my own hardware and other resources to conduct the academic experiment than would have been possible had the research been conducted in an academic facility. Whilst certainly

not a blocking factor, the location and unpredictability of my work has frustrated my efforts to complete my research more quickly.

7.6 Future Work

Future work for this research could focus on several areas. These could be split into the processes identified in the Dynamic Incident Response Model: Incident Detection, creation of Situational Awareness, and Decision-Making. This potential research is described in the following paragraphs in this section.

7.6.1 Incident Detection

In the incident detection process additional research could be carried out, particularly in the discrimination and collaboration areas. Utilising SIEM systems, tens of thousands of events are collected every day from disparate log sources. There are correlation engines available which mainly look at the events themselves to determine patterns which may constitute attacks: by mapping these events to the known infrastructure and existing vulnerabilities, opportunistic scans could be separated from targeted attacks. Extending this concept, by describing the defended infrastructure in line with a common set of definitions and standards, is it possible to enhance the discrimination of incidents when using collaborative information? Potentially, this could provide more effective incident detection by comparing patterns in related architecture, for example across a sector such as banking or safety-critical sectors such as air-traffic management.

7.6.2 Situational Awareness

In the process where situational awareness is created, more emphasis could be created on the evaluation of cyber intelligence information; this could take the form of providing a breakdown of intelligence information (possibly using the STIX framework as a starting point) so that the overall value of (missing) intelligence information could be calculated in a repeatable and objective way. By creating a universal relative scale for the value of missing intelligence information, adjustments could be made for local environments by combining these values with local risk appetite weightings (which may also be based on the available response options). Utilising these values, the possible response options could be considered in a more objective manner when comparing the attacks against the asset values.

7.6.3 Decision-Making

In the decision-making process the 5 chosen responses used in the COST fielded prototype could be expanded upon and defined in a more coherent way. The potential consequences of each of these responses could also be investigated (using real world examples) and included in a risk management/mission impact framework to provide guidance for those making the cyber decisions at the highest levels. This could also be considered in different environments to provide best practice responses for different sectors based on risk appetite and response options within relevant international and national legal frameworks.

7.7 Final Remarks

This research has been a long but fulfilling process. Within the time that the research has taken, the cyber landscape has continued to evolve rapidly with an increasing number of NATO and non-NATO nations declaring official cyber-offensive capabilities. However, also within that time, the dangers of cyber-offensive capabilities falling into the hands of non-governmental entities such as criminal gangs have also been made apparent (such as WannaCry in 2017). Cyber-security will undoubtedly continue to evolve as a field and the model, tools and procedures which have been produced as a result of this research will need to continue to adapt to this rapidly evolving environment.

8 Bibliography

- Adam, E. C. (1993). Fighter Cockpits of the Future. *Proceedings of 12th IEEE/AIAA Digital Avionics Systems Conference (DASC)*, (pp. 318-323). Fort Worth, Texas.
- Aissa, A. B., Abercrombie, R. K., Sheldon, F. T., & Mili, A. (2011). Defining and computing a value based cyber-security measure. *Proceedings of the Second Kuwait Conference on e-Services and e-Systems* (pp. 5:1-5:9). ACM.
- Barnett, A., Smith, S. R., & Whittingdon, R. P. (n.d.). Using causal models to manage the cyber threat to C2 agility: working with the benefit of hindsight. *19th ICCRTS: C2 Agility: Lessons Learned from Research and Operations*. Annapolis: CCRP, US Department of Defense.
- Barnum, S. (2012, February 20th). *Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX)*. Online: Mitre Corporation. Retrieved February 23, 2015, from <http://stix.mitre.org>:
http://stix.mitre.org/about/documents/STIX_Whitepaper_v1.1.pdf
- Bentler, P. M., & Chou, C.-P. (1987, August). Practical Issues in Structural Equation Modelling. *Sociological Methods Research*, 16(1), 78-117.
- Boehm, B. W. (1988). A Spiral Model of Software Development and Enhancement. *Computer*, 21(5), 61-72.
- Boni, W., & Kovacich, G. L. (2000). *Netspionage — The Global Threat to Information*. Boston, MA: Butterworth-Heinemann.
- Byrne, B. M. (2010). *Structural Equation Modeling with AMOS* (2nd ed.). Ottawa, Ontario, Canada: Routledge.
- Calder, A., & Watkins, S. (2008). *IT Governance: A Manager's Guide to Data Security and ISO27001/ISO 27002*. London & Philadelphia: Kogan Page.
- Carroll, T. E., Manz, D., Edgar, T., & Greitzer, F. L. (2012). Realizing scientific methods for cyber security. *Proceedings of the 2012 Workshop on Learning from Authoritative Security Experiment Results* (pp. 19-24). ACM.
- Chapman, I. M., Leblanc, S. P., & Partington, A. (2011). Taxonomy of Cyber Attacks and Simulation of their Effects. *Proceedings of the 2011 Military Modeling & Simulation Symposium* (pp. 73-80). Society for Computer Simulation International.
- Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer Security Incident Handling Guide (Draft-Revision2)*. Gaithersburg, MD 20899-8930: National Institute of Standards and Technology.
- Clapper, J. R., Lettre, M., & Rogers, M. S. (2017, January 05). *Joint Statement by US Director of National Security, Under Secretary of Defense for Intelligence and NSA/US Cyber Command Director at a Hearing of Foreign Cyber Threats by the Senate Armed Forces Committee*. Retrieved from <https://www.armed-services.senate.gov>:

https://www.armed-services.senate.gov/imo/media/doc/Clapper-Lettre-Rogers_01-05-16.pdf

- Cohen, J. (1992, July). A Power Primer. *Psychological Bulletin*, 192(1), 155-159.
doi:10.1037/0033-2909.112.1.155
- Congress, 1. (2015, January 08). H.R. 234 (114th) Cyber Intelligence Sharing and Data Protection Act. Washington, District of Columbia, United States of America. Retrieved July 02, 2017, from <https://www.govtrack.us/congress/bills/114/hr234/text>
- Creswell, J. W. (2009). *Research Design: Qualitative, Quantitative and Mixed Methods Approaches, 3rd Edition*. Thousand Oaks, California: Sage.
- Dawson, C. (2009). *Introduction to Research Methods 4th Edition*. Oxford: Howtobooks.
- DiPetto, C. (2008). Paving the way for testing in a joint environment: the capability test methodology. *Deefence Acquisition Technology & Logistics*, 37(5), 9-12.
- Dondossola, G., Garrone, F., & Szanto, J. (2011). Cyber risk assessment of power control systems — A metrics weighed by attack experiments. *Power and Energy Society General Meeting, IEEE*, (pp. 1-9).
- Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 37(1), 32-64.
- Federal Emergency Management Agency. (2017, November 26). *Asset Value, Threat/Hazard, Vulnerability and Risk*. Retrieved from Federal Emergency Management Agency: <https://www.fema.gov/media-library-data/20130726-1455-20490-5292/fema426ch1.pdf>
- Geers, K. (2011). *Strategic Cyber Security*. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence.
- Goel, S. (2011). Cyberwarfare: Connecting the Dots in Cyber Intelligence. *Communications of the ACM*, 132-140.
- Grispos, G., Glisson, W. B., & Storer, T. (2014). Rethinking Security Incident Response: The Integration of Agile Principles. *20th Americas Conference on Information Systems (AMCIS)*. Savannah, Georgia.
- Guba, E. G., & Lincoln, Y. S. ((1994)). Chapter 6 - Competing Paradigms in Qualitative Research. In N. K. Denzin, & Y. S. Lincoln, *Handbook of Qualitative Research* (pp. 105-117). Thousand Oaks, CA: Sage.
- Hair Jr, J. F., Black, W. C., Babin, B. J., & Andersen, R. E. (2014). *Multivariate Data Analysis (Pearson New International Edition)* (7th ed.). London, UK: Pearson Education Limited.
- Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2014). *Multivariate Data Analysis - Pearson New International Edition* (7th ed.). Upper Saddle River, New Jersey, US: Pearson.

- Hallingstad, G., & Dandurand, L. (2011). *CIS Security (including Cyber Defence) Capability Breakdown*. The Hague: NATO Consultation, Command and Control Agency (NC3A).
- Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The Law of Cyber-Attack. *California Law Review*, *100*(817-885), 817-885.
- He, Y., & Janicke, H. (2015). Towards Agile Industrial Control Systems Incident Response. *3rd International Symposium for ICS & SCADA Cyber Security Research 2015 (ICS-CSR 2015)*. Ingolstadt.
- Hevner, A. R., Ram, S., March, S. T., & Park, J. (2004, March). Design Science in Information Systems Research. *MIS Quarterly*(Vol 28), 75-105.
- Hooper, D., Coughlan, J., & Mullen, M. R. (2008). Structural Equation Modelling: Guidelines for Determining Model Fit. *Electronic Journal of Business Research Methods*, *6*(1), 53-60.
- Howard, J. D., & Longstaff, T. A. (1998). *A Common Language for Computer Security Incidents*. Albuquerque: Sandia National Laboratories.
- Hu, L.-t., & Bentler, P. M. (1999). Cutoff Criteria for Fit Indexes in Covariance Structure Analysis: Conventional Criteria Versus New Alternatives. *Structural Equation Modelling: A Multidisciplinary Journal*, *6*(1), 1-55.
doi:10.1080/10705519909540118
- Hudson, L. A., & Ozanne, J. L. (1988). Alternative Ways of Seeking Knowledge in Consumer Research. *The Journal of Consumer Reserach*, *14*(4), 508-521.
- Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare and Security Research*, *1*, 80.
- Jacob, C. (1992). A Power Primer. *Psychological Bulletin*, *112*(1), 155-159.
- Kanchana, D. V., & Ganesan, R. (2013). Enhancing Security in Cyber Physical System through Policy based on Trust Management against Deception Attack. *International Journal of Computer Applications*, *70*(6), 0975-8887.
- Kerckhoffs, A. (1883, Janvier). La Cryptographie Militaire. *Journal des Sciences Militaire*, *IX*, 5-38,. Retrieved from
http://www.petitcolas.net/kerckhoffs/la_cryptographie_militaire_i.htm
- Khurana, H., Basney, J., Bakht, M., Freemon, M., Welch, V., & Butler, R. (2009). Palantir: a framework for collaborative incident response and investigation. *Proceedings of the 8th Symposium on Identity and Trust on the Internet*, 38-51.
- Killcrece, G., Kossakowski, K.-P., Ruefle, R., & Zajicek, M. (2003). *State of the Practice of Computer Security Incident Response Teams (CSIRTs)*. Pittsburgh, PA: Software Engineering Institute/ Carnegie Mellon University.
- Kovacich, D. G. (2000, April 1). Netspionage — The Global Threat to Information, Part I: What is it and Why I Should Care? *Computers and Security*, *19*(4), 326-336.

- Lavrakas, P. J. (2008). *Encyclopedia of Survey Research Methods*. Thousand Oaks, CA: Sage Publications, Inc.
- Lawson, J. S. (1980). Command control as a process,. *19th IEEE Conference on Decision and Control including the Symposium on Adaptive Processes, 1980 1980*, pp. 1-6. (pp. 1-6). Albuquerque, NM, USA: IEEE.
- Lei, M., & Lomax, R. G. (2009). The Effect of Varying Degrees of Nonnormality in Structural Equation Modeling. *Structural Equation Modeling: A Multidisciplinary Structural Equation Modeling*, 12(1), 1-27. doi:10.1207/s15328007sem1201_1
- Lowry, P. B., & Gaskin, J. (2014, April 22). Partial Least Squares (PLS) Structural Equation Modeling (SEM) for Building and Testing Behavioral Causal Theory: When to Choose It and How to Use It. *IEEE Transactions on Professional Communication*, 57(2), 123-146.
- Lucas Jr, G. R. (2014). Ethics and Cyber Conflict: A Response to the Journal of Military Ethics 12:1 (2013). *Journal of Military Ethics*, 13(1), 20-31.
- Marshall, M. N. (1996). Sampling for Qualitative Research. *Family Practice*, 13(6), 522-525.
- Matsueda, R. L. (2011). *Working Paper no 114: Key Advances in the History Of Structural Equation Modeling*. University of Washington, Center for Statistics and the Social Sciences. Seattle: University of Washington.
- MCDC. (2014). MCDC Campaign 2013-2014: First Workshop "Cyber Implications of Combined Operational Access". Retrieved from MCDC Campaign 2013-2014: First Workshop "Cyber Implications of Combined Operational Access"
- Mephram, K. D., Louvieris, P., Ghinea, G., & Clewley, N. (2014). Dynamic Cyber-Incident Response. *6th International Conference on Cyber Conflict* (pp. 121-136). Tallinn, Estonia: NATO CCD COE Publications.
- Ministry of Defence (UK). (2014). *DEFENCE STAFF, Chief.Joint Doctrine Publication 0-01: British Defence Doctrine*. (5th ed.). Shrivenham, UK: Development Concepts and Doctrine Centre.
- Ministry of Defence (UK). (2015). *Strategic Trends Programme - Future Operating Environment 2035*. Shrivenham UK: DCDC - MoD UK.
- Ministry of Defence (UK). (2016). *Cyber Primer*. Shrivenham, Swindon UK: Development, Concepts and Doctrine Centre (DCDC). Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/549291/20160720-Cyber_Primer_ed_2_secured.pdf
- Ministry of Defence UK. (2011). *Joint Doctrine Publication 2-00: Understanding and Intelligence Support to Joint Operations*. Shrivenham, UK: Development, Concepts and Doctrine Centre.
- MITRE Corporation. (2014). *Systems Engineering Guide*. Bedford, MA: The MITRE Coporation. Retrieved December 03, 2017, from <https://www.mitre.org/sites/default/files/publications/se-guide-book-interactive.pdf>

- Moore, T., Friedman, A., & Procaccia, A. D. (2010). Would a 'cyber warrior' protect us: exploring trade-offs between attack and defense of information systems. *Proceedings of the 2010 Workshop on New Security Paradigms* (pp. 85-94). Concord, MA: ACM.
- Multinational Experiment 7 Contributing Nations. (2013). *MNE7 Access to the Global Commons Concept of Employment - Outcome 3 Cyber Domain: Concept of Employment for Cyber Situational Awareness Within the Global Commons*. MNE7.
- NATO Allied Command Operations. (2013). *An Introduction to Operations Planning at the Operations Level*. Mons, Belgium: NATO Allied Command Operations.
- NATO Cooperative Cyber Defence Centre of Excellence. (2016). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. (M. N. Schmitt, Ed.) New York: Cambridge University Press.
- Northcutt, S. (2003). *Computer Security Incident Handling: Step-by-Step* (2.3.1 ed.). Bethesda, , MD, USA: SANS Institute.
- Ntalampiras, S. (2016). Automatic Identification of Integrity Attacks in Cyber-Physical Systems. *Expert Systems with Applications*(58), 164-173.
- OASIS Cyber Threat Intelligence Technical Committee. (2017, June 19). STIX Version 2.0 Part 2 Stix Objects.
- Obama, P. B. (2012). Presidential Policy Directive/PPD-20: US Cyber Operations Policy. Washington: US Government.
- Orr, G. E. (1983). *Combat Operations C3I (Command, Control, Communications, and Intelligence): Fundamentals and Interactions*. Maxwell Air Force Base, Alabama: Air University - Center for Aerospace Doctrine, Research and Education.
- Patsos, D., Mitropolous, S., & Douligeris, C. (2010). Expanding Topological Vulnerability Analysis to Intrusion Detection through the Incident Response Intelligence System. *Information Management & Computer Security*, 18(4), 291-309.
- Pethia, R. D., & van Wyk, K. R. (1990). *Computer Emergency Response - An International Problem*. Carnegie Mellon University, Software Engineering Institute. Pittsburgh, PA: Computer Emergency Response Team / Coordination Center.
- Phillips, D. C., & Burbules, N. C. (2000). *Postpositivism and Educational Research*. Lanham, Maryland: Rowan and Littlefields.
- Rid, T., & Buchanan, B. (2014). Attributing Cyber Attacks. *Journal of Strategic Studies*, 18(1-2), 4-37.
- Rowe, N. C. (2006). Measuring the Effectiveness of Honeypot Counter-Counterdeception. *Proceedings of the 39th Annual Hawaii International Conference on System Sciences* (p. 129c). Monterey CA: Naval Postgraduate School.
- Roy, A. (2010). Cyber security analysis using attack countermeasure trees. *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research* (p. Article No 28). New Yor, NY, USA: ACM.

- Schleris, W. (1988). *CERT NEWS RELEASE - No 597-88 DARPA Establishes Computer Emergency Response Team*. DARPA.
- Shackelford, S. J. (2010). State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem. *Conference on Cyber Conflict* (pp. 197-208). Tallinn, Estonia: CCD COE Publications.
- Smith, D. (1994). Forming an Incident Response Team. *Proceedings of the FIRST Annual Conference*. University of Queensland, Brisbane, Australia: FIRST.
- Tadda, G. P., & Salerno, J. S. (2010). Overview of Cyber Situation Awareness. In S. Jajodia, P. Liu, V. Swarup, & C. Wang, *Cyber Situational Awareness - Issues and Research* (pp. 15-35). Springer.
- Takahashi, T., Fujiwara, H., & Kadobayashi, Y. (2010). Building ontology of cybersecurity operational information. *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research*, 1-4.
- Tzu, S. (1963). *Sun Tzu: The Art of War (trans Samuel B Griffith)*. London: Oxford University Press.
- UK Ministry of Defence. (2015). *Future Operating Environment 2035* (First ed.). Shrivenham UK: DCDC. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/484861/20151203-DCDC_FOE_35.pdf
- United Nations. (1945). *Charter of the United Nations*. New York: United Nations.
- United Nations. (2001, December 12). Responsibility of States for Internationally Wrongful Acts. *General Assembly Resolution 56/83*. United Nations.
- Verendel, V. (2009). Quantified security is a weak hypothesis: a critical survey of results and assumptions. *Proceedings of the 2009 Workshop on New Security Paradigms* (pp. 37-50). ACM.
- Wack, J. P. (1991). *Establishing a computer security incident response capability (CSIRC)*. Gaithersburg, MD; Springfield, VA: National Institute of Standards and Technology.
- Wagner, C., Dulaunoy, A., Wagener, G., & Iklody, A. (2016). MISP: The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform. *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security* (pp. 49-56). New York: ACM.
- Wang, P., Wu, L., Cunningham, R., & Zou, C. C. (2010). Honeypot Detection in Advanced Botnet Attacks. *International Journal of Information Computing Security*, 4(1), 30-51.
- West-Brown, M. J., Stikvoort, D., & Kossakowski, K.-P. (1998). *Handbook for Computer Security Incident Response Teams (CSIRTs)*. Carnegie Mellon - Software Engineering Institute.

- West-Brown, M. J., Stikvoort, D., Kossakowski, K.-P., Killcrece, G., Ruefle, R., & Zajicek, M. (2003). *Handbook for Computer Security Incident Response Teams (CSIRTs)*. Pittsburgh PA: Carnegie Mellon - Software Engineering Institute.
- Wheaton, B., Muthén, B., Alwin, D. F., & Summers, G. F. (1977). Assessing Reliability and Stability in Panel Models. In D. R. Heise, *Sociological Methodology* (pp. 83-136). San Francisco: Jossey-Baas.
- Wholey, J. S., Hatry, H. P., & Newcomer, K. E. (2010). *Handbook of Practical Program Evaluation* (Third ed.). San Francisco: John Wiley & Sons.
- Wijnhoven, F., Amrit, C., & Dietz, P. (2014, May). Value-Based File Retention: File Attributes as File Value and Information Waste Indicators. *Journal of Data and Information Quality (JDIQ)*, 4(4), Article 15.
- Workman, M. (2012). Validation of a biases model in strategic security decision making. *Information Management & Computer Security*, 20(2), 52-70.
doi:10.1108/09685221211235599
- Yang, S. J., Stotz, A., Holsopple, J., Sudit, M., & Kuhl, M. (2009). High Level Information Fusion for Tracking and Projection of Multistage Cyber Attacks. *Information Fusion*, 107-121.
- Yuill, J., Wu, F., Settle, J., Gong, F., Forno, R., Huang, M., & Asbery, J. (2000). Intrusion-Detection for Incident-Response, using a Military Battlefield-Intelligence Process. *Computer Networks*, 671-697.

Dynamic Cyber Incident Response

General Background

Dear Respondent,

This survey has been produced as part of PhD research into Cyber Security at Brunel University. It is designed to gauge the importance of factors identified which may have relevance for efficient and effective Cyber Incident Response. It is intended to assess individual and community opinion in order to identify the discrepancies between the two. Consequently, the questions are divided into two parts; the first asking for opinion, the second asking how this is currently considered within a community.

Ultimately, the responses from this questionnaire will be used to realign current incident response models with the perceived priorities; these models will then be evaluated using experimentation.

Please note, no information will be captured with the intention of identifying individuals or organisations.

In order to identify different perspectives within organizations please identify the area which is most closely associated with your function (optional).

To gauge perspectives from different areas of an organization, please identify the most relevant category associated with your current function.

Operations,

Security/Information Assurance

Intelligence/Business Intelligence,

Engineering/Communications - Information Systems Engineering

Other Support Function

Other Function

Analyst/Implementer

Manager e.g. Section Head

Senior Manager e.g. Division, Department or Branch Head

Monitoring:

Hardware level monitoring, e.g. the capability to monitor equipment the physical or electrical status of equipment, may be used to in order to detect, monitor or analyse a cyber-attack (an example might be unexpected fault conditions generating an email alert in a digitally controlled air-conditioning system)?

Please note that for brevity in the thesis only the first question shows the Likert scale based answers, the rest follow the same format with Completely Relevant = 1 and Essential = 7.

1. In your opinion, how important is the contribution of hardware level monitoring to situational awareness during a cyber-attack? *

Essential
Important
Fairly Important
Neutral
Fairly Unimportant
Unimportant
Completely Irrelevant

2. How do you believe this is generally viewed within your wider community? *

Network monitoring is often used in order to detect, monitor or analyse a cyber-attack (this includes devices such as Network Intrusion Detection Systems, software designed to analyse network traffic such as Wireshark etc).

3. In your opinion, how important is the contribution of network monitoring to situational awareness during a cyber-attack? *

4. How do you believe this is generally viewed within your wider community? *

Operating system monitoring can often be used to identify the progress of a cyber-attack. Examples include the monitoring and alerting of audit conditions to provide evidence of logins, changes of user permissions, introduction of USB devices etc.

5. In your opinion, how important is the contribution of operating system monitoring to situational awareness during a cyber-attack? *

6. How do you believe this is generally viewed within your wider community? *

Application-level monitoring can often be used to identify a cyber-attack. Examples include alerts sent by the audit function in a database when records are deleted or permissions are changed, email applications which automatically detect egress of sensitive data etc.

7. In your opinion, how important is the contribution of application monitoring to situational awareness during a cyber-attack? *

8. How do you believe this is generally viewed within your wider community? *

In order to ensure that the appropriate monitoring is in place to protect an organisation's infrastructure, comprehensive configuration management makes a contribution to situational awareness. This includes knowing exactly which assets are located in a network and where, the versions of software that are running on them, the patch state of the items, etc.

9. In your opinion, how important is the contribution of configuration management to situational awareness during a cyber-attack? *

10. How do you believe this is generally viewed within your wider community? *

Despite having monitoring in place to detect, monitor or analyse a cyber-attack or incident it may not always meet the requirements of the analysts or decision-makers. For example, an incorrectly-tuned automated tool may report an attack when in fact it has misinterpreted normal network behaviour or if not synchronised it may report the time that events occur incorrectly.

11. In your opinion, how important is the accuracy of the information that is received from monitoring devices to situational awareness? *

12. How do you believe this is generally viewed within your wider community? *

From the same perspective, some monitoring devices may not report in real-time, instead storing log files which are uploaded or collected at regular intervals.

13. In your opinion, how important is the timeliness of the information that is received from monitoring devices to situational awareness? *

14. How do you believe this is generally viewed within your wider community? *

Also relating to the monitoring, reliability of monitoring sources cannot always be guaranteed.

Examples may include unstable network connections, maintenance issues or malfunctions which potentially cause monitoring sources to be unavailable to the analysts.

15. In your opinion, how important is the reliability of feeds from monitoring devices to situational awareness? *

16. How do you believe this is generally viewed within your wider community? *

To enhance local situational awareness, it may be advantageous to receive real-time or near real-time information regarding cyber-attacks from other organisations, businesses or national/international governmental agencies/departments. This would provide collaborative situational awareness.

17. In your opinion, how important is it to receive cyber-attack information from collaboration partners? *

18. How do you believe this is generally viewed within your wider community? *

From the other perspective as “collaboration” by its definition entails working together with partners, information-sharing is also required. In order to generate trust and good working relationships within a collaboration environment it will be required to share incident information (although filtered to remove any organization-sensitive information) with others.

19. In your opinion, how important is it to share incident information (albeit filtered) with collaboration partners? *

20. How do you believe this is generally viewed within your wider community? *

Cyber incidents can only be analysed effectively by the examination of relatively low-level data such as audit logs, network packet captures, file systems and files. However, with increasingly higher network speeds and faster processor speeds this flood of data has the propensity to overwhelm an analyst.

21. In your opinion, how important is it to have effective automated analysis tools to support the analysts? *

22. How do you believe this is generally viewed within your wider community? *

Personnel

As stated previously, cyber incidents can only be analysed effectively by the examination of relatively low-level data such as audit logs, network packet captures, file systems and files. Despite having appropriate tools which may require little detailed knowledge for daily operation the ability of an analyst or other Information Assurance (IA) professional to confirm an incident could be seen to be dependent upon their training.

23. In your opinion, how important is the training of IA personnel in their contribution to effective Cyber Incident Response? *

24. How do you believe this is generally viewed within your wider community? *

The experience of IA staff may also have an influence on the way that they respond to cyber incidents.

25. In your opinion, how important is the experience of IA personnel in their contribution to effective Cyber Incident Response? *

26. How do you believe this is generally viewed within your wider community? *

The environment where IA personnel such as analysts carry out their work may influence their effectiveness. Examples include procedures for alternating work after certain periods of time, lighting, room temperature, monitor size and resolution etc.

27. In your opinion, how important is the influence of these environmental human factors considerations in their contribution to effective Cyber Incident Response?*

28. How do you believe this is generally viewed within your wider community? *

Assets

When the target of a cyber-attack has been identified, the organisation is likely to have a perceived value for that asset.

29. In your opinion, how important is the perceived value of the asset in determining the appropriate type of incident response? *

30. How do you believe this is generally viewed within your wider community? *

Different stakeholders within the organisation may have different perceived values for the same asset, for example a customer database may be more important to a sales director than a technical director.

31. In your opinion, when determining the appropriate course of action during a cyber-attack, how important is it that stakeholders' priorities are balanced against the operational mission or objectives by the key decision-maker? *

32. How do you believe this is generally viewed within your wider community? *

Assets within the Communications and Information Systems (CIS) infrastructure are likely, by their nature, to have vulnerabilities to certain types or methods of attack if left with their "default" installation. However, for good operational reasons it is not always possible to remove these vulnerabilities as soon as they become known.

33. In your opinion, how important is it to have awareness of the exposed vulnerabilities and their disposition within the organisation's infrastructure in order to conduct effective Cyber Incident response? *

34. How do you believe this is generally viewed within your wider community? *

In addition to the relative values of assets identified in previous questions (by different stakeholders), it could be argued that the value of an asset to a company will change over time. For example, the perceived value of a server collecting event logs may increase immediately prior to an audit as the availability of the logs may be a regulatory requirement.

35. In your opinion, how important is to include a time-related modifier in the calculation for values used in the risk assessment? *

36. How do you believe this is generally viewed within your wider community? *

Intelligence

To understand a cyber-attack and predict the potential outcome or aims of the attack an up-to-date and comprehensive knowledge of vulnerabilities and their relevance to an organization's infrastructure may be advantageous.

37. In your opinion, how important is it to have access to a comprehensive and current knowledgebase of vulnerabilities to aid situational awareness? *

38. How do you believe this is generally viewed within your wider community? *

To aid the understanding of an attack and potential targets and intended outcomes, knowledge of potential attackers, their motivation, resources and methods may be advantageous.

39. In your opinion, how important is it to have access to a comprehensive and current knowledgebase of potential attackers to aid situational awareness? *

40. How do you believe this is generally viewed within your wider community? *

To aid situational awareness an up-to-date knowledge of common attack patterns and methods may be advantageous.

41. In your opinion, how important is it to have access to a comprehensive and current knowledgebase of attack patterns and methods to aid situational awareness? *

42. How do you believe this is generally viewed within your wider community? *

To provide optimal situational awareness, prediction of the likely progression of an attack may be beneficial. In order to predict attack progression, a simulation model must be constructed which is perceived to accurately reflect both the attackers' actions and the attacked infrastructure.

43. In your opinion, how important is an accurate simulation model in determining appropriate incident response actions? *

44. How do you believe this is generally viewed within your wider community? *

Although an asset (be it information or a physical system) could be considered to have an innate value from the perspective of a stakeholder, it could also be considered that intelligence relating to attacks and attackers also has a relative value (e.g. value to the defending organisation in helping to improve their infrastructure/response measures).

45. In your opinion, how important is it to allocate a value to intelligence areas of interest (examples might include attacker real-world identity, physical location, attacker motivation, attacker methods) in order to determine priorities for intelligence gathering against other incident response considerations such as physical cost of potential damage, immediate mission impact, user inconvenience etc? *

46. How do you believe this is generally viewed within your wider community? *

Decision-Making

Ultimately the highest priority for an organisation will be accomplishing the overarching organisational goals or objectives. In deciding upon the appropriate incident-response measures, this perspective may also be important.

47. In your opinion, how important is it for a key decision-maker to take account of organisation's goals or objectives when deciding upon a course of action during a cyber-incident? *

48. How do you believe this is generally viewed within your wider community? *

In order to decide the best course of action during an incident, the key decision-maker will require access to relevant information to base their decision upon.

49. In your opinion, how important is it for a key decision-maker to have access to current situational awareness information? *

50. How do you believe this is generally viewed within your wider community? *

Leading on from the previous question, predicted progress of an incident may also be relevant to decision-making.

51. In your opinion, how important is it for a key decision-maker to be aware of predicted incident progress? *

52. How do you believe this is generally viewed within your wider community? *

In order to make a fully-informed decision, the decision-maker may require risk assessments which are able to provide an assessed value for risk and potential impact of an incident.

53. In your opinion, how important is it for a key decision-maker to have access to relevant risk assessment information in order to decide the best course-of-action? *

54. How do you believe this is generally viewed within your wider community? *

To provide a full range of incident response options to the decision-maker, active defence, which may include neutralising attacker infrastructure through cyber means or actively probing attacking networks to gain additional intelligence information, may be considered as an option in some organisations.

55. In your opinion, how important is it for a key decision-maker to have access to active defence as a valid course-of-action during an incident? *

56. How do you believe this is generally viewed within your wider community? *

One possible incident response option may be to continue to monitor an attack against a low-value asset without intervening in order to gain additional insight into attacker methods, motives and capabilities.

57. In your opinion, how important is it for a key decision-maker to have monitoring (without intervention) as one of their authorised response options? *

58. How do you believe this is generally viewed within your wider community? *

General

In most organisations, cyber security has to compete with other departments for resources and budget.

59. In your opinion, in comparison with other areas, how important do you believe the area dealing with traditional cyber-security (including traditional cyber-response methods) to be in protecting the interests of the organisation? *

60. How do you believe this is generally viewed within your wider community? *

Feedback

If you feel that any areas have been missed which are particularly pertinent to Dynamic Incident Response to Cyber Incidents or wish to comment on any of the questions, please do so here.

Thank You!

Thank you for taking the time to complete this survey. To receive the full results from all respondents and analysis (when complete), please send an email to kevin.mepham@brunel.ac.uk.

For this and all subsequent surveys the consent form on the following page was used, in accordance with the University's Ethics requirements:

⊕ **CONSENT FORM:**

<i>The participant should complete the whole of this sheet</i>		
<i>Please tick the appropriate box</i>		
	YES	NO
Have you been informed about the aim of this study and how this evaluation relates to it?	<input type="checkbox"/>	<input type="checkbox"/>
Have you had an opportunity to ask questions and discuss this study?	<input type="checkbox"/>	<input type="checkbox"/>
Have you received satisfactory answers to all your questions?	<input type="checkbox"/>	<input type="checkbox"/>
Do you understand that you will not be referred to by name in any report concerning the study?	<input type="checkbox"/>	<input type="checkbox"/>
Do you understand that you are free to withdraw from the study:		
• at any time?	<input type="checkbox"/>	<input type="checkbox"/>
• without having to give a reason for withdrawing?	<input type="checkbox"/>	<input type="checkbox"/>
(Where relevant) I agree to my interview being recorded.	<input type="checkbox"/>	<input type="checkbox"/>
(Where relevant) I agree to the use of non-attributable direct quotes when the study is written up or published.	<input type="checkbox"/>	<input type="checkbox"/>
Do you agree to take part in this study?	<input type="checkbox"/>	<input type="checkbox"/>
Signature of Research Participant:		
Date:		
Name/Branch (optional)		
<u>Witness statement</u>		
I am satisfied that the above-named has given informed consent.		
Witnessed by:		
Name in capitals:	Signature:	
Date:		
Researcher name: Eur Ing Kevin Mepham	Signature:	

Appendix 2 - Cyber Security Variables

Abbreviated Name	Name	Description	Source
Hardware	Hardware Monitoring	Sensors deployed to monitor changes at a hardware level	(Calder & Watkins, 2008), MNE7, MCDC,
Network	Network Monitoring	Sensors deployed to detect anomalies or signatures in network traffic	(Calder & Watkins, 2008), MNE7, MCDC,
OS	OS Monitoring	Sensors (including built-in audit functions) deployed to detect anomalies or signatures in the operating system	(Calder & Watkins, 2008), MNE7
App	Application Monitoring	Sensors (including built-in audit functions) deployed to detect anomalies or signatures in the applications on a system	(Calder & Watkins, 2008),
CM	Configuration Management	Awareness of the defended infrastructure including deployment, hardware, software and application versions as well as configuration.	(Calder & Watkins, 2008), MNE7, MCDC,
Accu	Accuracy	Accuracy of the information supplied by the sensors e.g. the granularity and accuracy of the timestamps.	MNE7, MCDC, (Kanchana & Ganesan, 2013)
Tim	Timeliness	Timeliness of the information provided by the sensors i.e. how soon the information is received after the event e.g. real-time, every 10 minutes, hourly, daily etc.	MNE7, MCDC, (Kanchana & Ganesan, 2013)
Rel	Reliability	Reliability of the sensors i.e. the level of confidence that they will always catch and transmit the events that they are configured for also including a long mean time between failure.	MNE7, MCDC, (Kanchana & Ganesan, 2013)
Colin	Collaboration Inbound	Cyber information shared by collaboration partners which may be of use to an organisation's cyber security posture.	MNE7, MCDC, (Barnum, 2012), (Kanchana & Ganesan, 2013), (He & Janicke, 2015)
Colout	Collaboration Outbound	Cyber information shared with collaboration partners from an organisation's own sensors and analysis (in accordance with information exchange agreements)	MNE7, MCDC, (Barnum, 2012), (Kanchana & Ganesan, 2013), (He & Janicke, 2015)
Auto	Automated Tools	Tools which assist an analyst in filtering and highlighting incidents from raw data.	MCDC, (Endsley, 1995),
Trg	Training	Training of cyber analysts	MNE7, MCDC, (Calder & Watkins, 2008),
Exp	Experience	Experience of cyber analysts	(Calder & Watkins, 2008), (He & Janicke, 2015), (Endsley, 1995)
Env	Environment	Physical environment that analysts work in, i.e. human factors such as monitor size, graphical interfaces, break/shift patterns etc.	MCDC, (Adam, 1993), (Endsley, 1995)
AssV	Asset Value	Static value of asset	MCDC, (Dondossola, Garrone, & Szanto, 2011),
StakeV	Stakeholder Value	Modification of asset value by stakeholder	MNE7, MCDC
ExpVuln	Exposed Vulnerabilities	Known vulnerabilities in own infrastructure.	MCDC, (Barnum, 2012)
TimMod	Time Modification	Modification of asset value due to stage of mission cycle, business cycle, age of information, etc.	MCDC, (Wijnhoven, Amrit, & Dietz, 2014)
VulnKB	Vulnerability Knowledgebase	Knowledgebase of vulnerabilities in general (i.e. not specific to own infrastructure).	MCDC, (Barnum, 2012),
AttackerKB	Attacker Knowledgebase	Knowledgebase of known attackers (non-specific to organisation)	MNE7, MCDC, (Barnum, 2012),
CAPEC	CAPEC	Common Attack Pattern Enumeration and Classification. Knowledge base of common attack patterns/techniques and methods for categorising them.	MNE7, MCDC, (Barnum, 2012)
Sim	Simulation	Simulation of possible attack vectors or progression	MCDC, (Barnum, 2012)

		through an organisation's infrastructure	
IntV	Intelligence Value	Assigning a value to missing or gained intelligence (to be weighed against asset value).	MCDC, (Hallingstad & Dandurand, 2011), (Boni & Kovacich, 2000)
Goal	Goal	Organisation's goals and objectives	MNE7, MCDC
SA	Situational Awareness	Ability to place an incident in context of the environment and potential outcomes.	MNE7, MCDC, (Adam, 1993),
Pred	Prediction	Credible algorithms to predict an incident's progress and the effect of possible response options (to be used as engine for simulation)	MCDC, (Dondossola, Garrone, & Szanto, 2011)
RA	Risk Assessment	Use of robust techniques to provide a standardised approach to risk assessment.	(Dondossola, Garrone, & Szanto, 2011)
AD	Active Defence	Active defence (including active intelligence gathering and cyber-offensive techniques)	(Obama, 2012)
Mon	Passive Monitoring	Use of observation to gain additional intelligence rather than acting to contain or stop incidents i.e. allow incidents to continue unfettered.	MCDC, (Hallingstad & Dandurand, 2011), (Mephram, Louvieris, Ghinea, & Clewley, 2014), (Obama, 2012)
Cyblmp	Importance of Traditional Techniques	Use of standard approaches to cyber security including defence and response mechanisms.	MCDC, (Obama, 2012), (Calder & Watkins, 2008)

Appendix 3 – Principal Component Analysis

	Factor							
	Intel	Sensors	Impact	Collaboration	Discrimination	Asset Modification	Response	Credibility
CAPEC	.688							
Attacker	.652							
Sim	.621							
VulnKB	.533							
IntV	.482							
OS		.728						
App		.652						
Network		.615						
SA			.681					
Pred			.605					
Goal			.535					
RA			.448					
Colout				.652				
Colin				.582				
Trg					.703			
Exp					.466			
Accu					.403			
TimMod						.609		
StakeV						.549		
Env						.426		
AD							.733	
Mon							.489	
Cyblmp							.460	
Tim								.678
Rel								.439

Appendix 4 – Structural Equation Modelling: Fit Indices

Fit Index	Acceptable Threshold Levels	Description
Absolute Fit Indices		
Chi-Square χ^2	Low χ^2 relative to degrees of freedom with an insignificant p value ($p > 0.05$)	Unreliable for large sample sizes and deviations from normality (Hooper, Coughlan, & Mullen, 2008)
Relative χ^2 (χ^2/df)	2:1 (Tabachnik and Fidell, 2007) 3:1 (Kline, 2005)	Adjusts for sample size.
Root Mean Square Error of Approximation (RMSEA)	Values less than 0.07 (Steiger, 2007)	Has a known distribution. Favours parsimony. Values less than 0.03 represent excellent fit.
GFI (aka Gamma Hat)	Values greater than 0.95 (Hu & Bentler, 1999)	Scaled between 0 and 1, with higher values indicating better model fit. This statistic should be used with caution.
AGFI	Values greater than 0.95	Adjusts the GFI based on the number of parameters in the model. Values can fall outside the 0-1.0 range.
RMR	Good models have small RMR (Tabachnik and Fidell, 2007)	Residual based. The average squared differences between the residuals of the sample covariances and the residuals of the estimated covariances. Unstandardised.
SRMR	SRMR less than 0.08 (Hu and Bentler, 1999)	Standardised version of the RMR. Easier to interpret due to its standardised nature.
Incremental Fit Indices		
IFI (aka BL89)	Values greater than 0.95 (Hu & Bentler, 1999)	Bollen's Fit Index (1989). Non-normed, compensates for the effects of model complexity.
NFI	Values greater than 0.95 (Hu & Bentler, 1999)	Assesses fit relative to a baseline model which assumes no covariances between the observed variables.
NNFI (TLI)	Values greater than 0.95 (Hu & Bentler, 1999)	Non-normed, values can fall outside the 0-1 range. Favours parsimony. Performs well in simulation studies (Sharma et al, 2005; McDonald and Marsh, 1990)
CFI	Values greater than 0.95. (Hu & Bentler, 1999)	Normed, 0-1 range.

Appendix 5 – COST Feedback

As described in Chapter, some of the feedback from the validation of the COST tool is summarised below, with comment responding to the feedback included.

- a. *The next phase of development should allow the option of updating response options driven by the Commander’s direction and guidance; e.g. if the intelligence gap is very big, only responses X and Y are possible so option Z is not possible under condition W.*** In response to this comment, this could be possible from a logical point of view, effectively providing some automation into the decision-making. However, this would trade-off the flexibility in the response options which would have to be agreed with the risk owner (in this case the Commander).
- b. *Instead of executable response use recommended response or recommended action.*** This has been incorporated into the latest version in some respects as DCOS Ops now provides the recommended response which allows the Commander to choose the executable response.
- c. *For “Attribution” under the Intelligence tab, allow more than one attacker.*** As this is a “flat” prototype tool, allowing more than one attacker would extend this proof-of-concept significantly. However, if developed into a fielded operational version it is anticipated that this would use a back-end database in which case multiple incidents and attackers could be tracked.
- d. *The complexity should be reduced for the Commander’s decision (3 similar comments).*** This has now been done with DCOS Ops assimilating most of the information before providing a recommended response to the Commander (who now only receives the assimilated SA to assist his decision-making).
- e. *TRIDENT JUNTURE 15 didn’t allow us to use the tool to its full extent but the tool did allow us to validate our critical prioritised asset list (CPAL). Inputting the top 10 assets into the tool and associating owner value vs mission value against mission stages helped us refine priority of effort.*** This bears out the importance in the model of having dynamic asset value which is also assessed cross-functionally and against the mission impact.

- f. The challenge in the current (NATO) environment is that the Commander doesn't have an option beyond passive defence. It was hoped that the exercise would allow us to test the tool in a hybrid environment but the scenarios did not play out that way.** At the time that the tool was evaluated, NATO policy did not permit cyber offensive response to a cyber-attack. However, in response to an Article V cyber-attack (for example a devastating attack on national critical infrastructure), a conventional response was considered a valid option.
- g. The cyber tool was used during a recent exercise to validate our CPAL. This tool showed utility when it was used to validate the inputs of CPAL using the Collaboration tab. The items on the CPAL were added in the Targeted Assets section and appropriate Owner Value and Mission Impact weights were added for all stages of an operation. Based on the graphical representation we were able to see which assets should be prioritised higher or lower during each stage of an operation. This tool allowed us to focus in on the assets that should be protected more as we transition phases of the operations. Whilst not utilised during the exercise the Commander and Incident Description tabs were also assessed and analysed for utility. The Commander tab was found to provide a bottom-line up front view of a cyber incident to enable the decision-maker to have a quick overview of the cyber-situation. The Incident Description tab was found to provide basic functionality as an event log. It would be a useful area to organise events and all related trouble-tickets and incident numbers. With minor adjustments such as, ability to add more incidents within the tab or more fields (e.g. mission impact, affected organisations, etc) added for greater granularity. The bottom-line is that the Cyber Operational Support Tool has displayed significant utility in supporting operational level cyber assessments.** This detailed analysis of the tool from an experienced cyber operational analyst demonstrates the versatility of the tool. The minor deficiencies that are highlighted could reasonably be expected to be addressed in a full operational version of the tool.
- h. Splash screen with access to intelligence summary for Commander would be useful.** At present this is accomplished by going to the individual tabs (for example

Intelligence and Incident Description), however, if deemed to be a necessity this could be incorporated.

- i. **Fantastic initiative! Multiple incident tracking would improve the tool further.*** As for comment “c”, an operational version could be expected to have a database back-end where this would be possible.
- j. **LEGAD should not provide a preferred option, but instead should opine whether each of the possible options are 1) legally permissible or not permissible; 2) authorised or not authorised by RoE.*** Currently, LEGAD makes the preferred response assessment based on all legal factors so as to avoid overloading the Cdr with too much detail.
- k. **The tool is helpful to see the factors involved in the decision-making but the Commander needs more detail to determine the appropriate response. Recommend changing from an Excel spreadsheet to some type of database that can produce a PowerPoint presentation with the required details, similar to what is used for kinetic targeting packages.*** As stated in previous comments, it is agreed that a full operational version would use a database back-end. Whilst agreeing on the requirement to standardise output across branches so as to improve efficiency and decrease training requirements, this does not necessarily have to be from any one manufacturer (in fact a number of outputs such as open document format, pdf, JPG etc would probably increase the utility in a number of environments).

Appendix 6 – Experiment Scenario and Vignettes

Scenario

You are responsible for a static military Joint HQ with deployed elements; therefore attacks from the Internet have low mission impact despite being a nuisance. The scenario takes place in an environment where national cyber laws have been refined to provide additional rights to those under cyber attack. However, responses are expected to be proportionate to an attack. The legally permissible responses to a cyber-attack are now:

- Traditional Response: stop or mitigate an attack as soon as it is detected.
- Passive Response: allow an attack to continue under close observation without impediment in order to gather additional intelligence. This is unlikely to warn the attacker that they have been noticed.
- Cyber Offensive Operations: respond to an attack by penetrating the attacker's networks and/or systems in order to gather advanced intelligence or to try to halt an attack immediately. The attacker is likely to be aware of this action and respond.

Vignette 1:

Mission Impact **Low**, Intelligence Gap **High**, Asset Value **Low**

One of many boundary protection devices is being scanned from the Internet with what appears to be an unusual tool. The attacker is also unknown.

Vignette 2:

Mission Impact **Low**, Intelligence Gap **Low**, Asset Value **Low**

A known journalist hostile to your organisation is attempting to look for weaknesses in your firewalls (again). His skill level is extremely low and he is not able to configure the tools that he's downloaded in any meaningful way.

Vignette 3:

Mission Impact **Low**, Intelligence Gap **Low**, Asset Value **Medium**

Your main Internet-facing webserver is being probed with known tools. A compromise could result in some PR backlash.

Vignette 4:

Mission Impact **Low**, Intelligence Gap **High**, Asset Value **High**

Your only web proxy (a machine that caches and inspects web traffic between your internal network and the Internet) is being probed by a zero-day attack (i.e. a brand new attack) from an unknown attacker.

Vignette 5:

Mission Impact **Low**, Intelligence Gap **Medium**, Asset Value **Medium**

One of your web proxies (a machine that caches and inspects web traffic between your internal network and the Internet) is being probed by an unusual attack from IP addresses associated with a group funded by a hostile nation state.

Vignette 6:

Mission Impact **Low**, Intelligence Gap **High**, Asset Value **Medium**

Several members of your finance department have received targeted emails with links to malware (aka spearphishing). The malware and the originators are unknown to your team.

Vignette 7:

Mission Impact **Low**, Intelligence Gap **Medium**, Asset Value **High**

It appears that an attacker has exploited a known and unpatchable weakness in your IP-based security cameras on your infrastructure network.

Vignette 8:

Mission Impact **Low**, Intelligence Gap **Medium**, Asset Value **Low**

An attacker is trying to gain access to a backup webserver (used for training purposes) by using a modified version of a standard tool.

Vignette 9:


Mission Impact **Low**, Intelligence Gap **Low**, Asset Value **High**

A misconfiguration of your email server has resulted in a known teenage attacker from a developing country being able to send spam email from your server.

Appendix 7 – Equipment and Software Used for Experiment

Windows edition

Windows 10 Home
© 2016 Microsoft Corporation. All rights reserved.



System

Manufacturer: ASUSTek Computer Inc.
Model: G752VT
Processor: Intel(R) Core(TM) i7-6700HQ CPU @ 2.60GHz 2.59 GHz
Installed memory (RAM): 48.0 GB
System type: 64-bit Operating System, x64-based processor


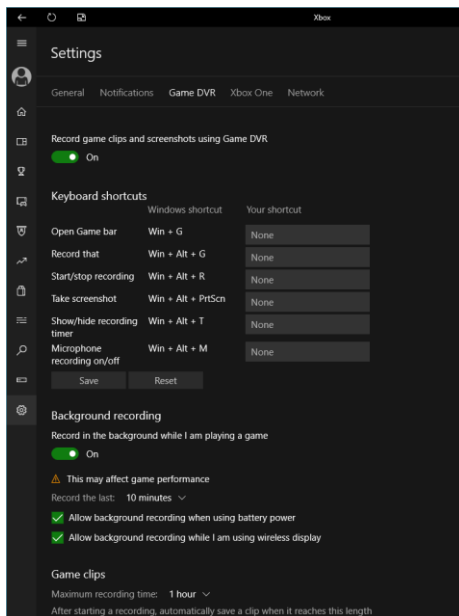


FIGURE 43 - WINDOWS VERSION AND HARDWARE



The screenshot shows the Xbox recording application settings. The 'Record game clips and screenshots using Game DVR' toggle is turned on. The 'Keyboard shortcuts' table is as follows:

	Windows shortcut	Your shortcut
Open Game bar	Win + G	None
Record that	Win + Alt + G	None
Start/stop recording	Win + Alt + R	None
Take screenshot	Win + Alt + PrtScn	None
Show/hide recording timer	Win + Alt + T	None
Microphone recording on/off	Win + Alt + M	None

The 'Background recording' toggle is also turned on. A warning message states: 'This may affect game performance'. Below this, there are three checked options: 'Allow background recording when using battery power' and 'Allow background recording while I am using wireless display'. The 'Record the last' setting is set to 10 minutes. The 'Game clips' section shows 'Maximum recording time' set to 1 hour.

FIGURE 44 - XBOX RECORDING APPLICATION

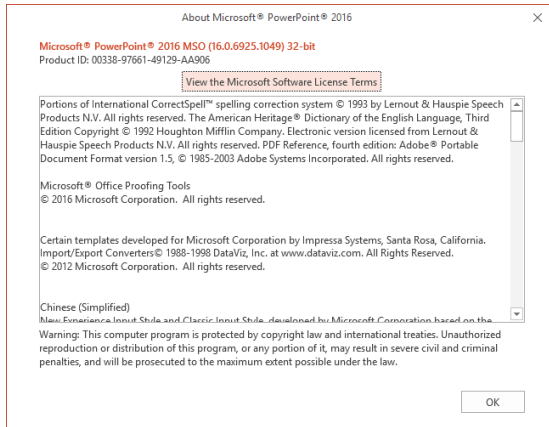


FIGURE 45 - MICROSOFT POWERPOINT VERSION

Appendix 8 – Evaluation Questionnaire

This questionnaire is part of PhD Research at Brunel University intended to produce and refine a new model for Cyber Incident Response. This section of the research is devoted to analyzing the utility of the model through the evaluation of two scenarios where both traditional and dynamic approaches are used to support the operational decision-making process. Each question is divided into two parts, the first relating to operational decision-making without the use of the information, the second to operational decision-making with the support of additional dynamic information.

Please attempt to answer all questions from your own perspective.

Any additional comments which may enhance the tool or model are very welcome.

Please note that all responses will be anonymized prior to release to the University.

Please note that for brevity the Likert scale answers follow the same format (Poor =1, Excellent = 5) for all questions so only the first question is shown in full in the thesis.

1. How was your understanding of the current environment during the experiment:

a. With the dynamic cyber-incident information?

Poor Fair Average Good Excellent

b. With the traditional approach information?

Poor Fair Average Good Excellent

2. How was your comprehension of the current situation during the experiment?

3. How was your situational-awareness with respect to allowing a prediction of the future environment?

4. How comprehensive was your awareness of the mission impact of a Cyber-Incident?

5. How comprehensive was your understanding of the Intelligence information and priorities associated with a Cyber-Incident?

6. How comprehensive was your understanding of the Commander's available and chosen response options when reacting to a Cyber-Incident?
7. How would you assess your ability to cope with a congested Cyber environment (i.e. a large and complex Cyber infrastructure)?
8. How would you assess your ability to cope with a contested environment (i.e. adversaries actively try to prevent Cyber freedom of manoeuvre)?
9. How would you assess your ability to cope with a cluttered cyber environment (i.e. several Cyber events occurring in a short space of time or simultaneously)?
10. How do you assess your ability to understand and act on the repercussions of incidents in the cyber environment as a mission progresses (i.e. gauge the effects of a Cyber Incident at different mission stages)?

Any other comments, suggestions or shortfalls relating to the tool or model?

Appendix 9 – Situational Awareness and Decision Support Results

		Paired Differences				t	df	Sig. (2-tailed)	
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference				
					Lower				Upper
Pair 1	SA1C - SA1D	-.750	.550	.123	-1.007	-.493	-6.097	19	.000
Pair 2	SA2C - SA2D	-.750	.550	.123	-1.007	-.493	-6.097	19	.000
Pair 3	SA3C - SA3D	-1.050	.686	.153	-1.371	-.729	-6.842	19	.000
Pair 4	MissionImpactC - MissionImpactD	-1.150	.745	.167	-1.499	-.801	-6.902	19	.000
Pair 5	IntelligenceImpactC - IntelligenceImpactD	-1.200	.834	.186	-1.590	-.810	-6.439	19	.000
Pair 6	ResponseOptionsC - ResponseOptionsD	-1.000	1.076	.241	-1.504	-.496	-4.156	19	.001
Pair 7	CongestedC - CongestedD	-1.100	.852	.191	-1.499	-.701	-5.772	19	.000
Pair 8	ContestedC - ContestedD	-1.200	.696	.156	-1.526	-.874	-7.712	19	.000
Pair 9	ClutteredC - ClutteredD	-1.250	.910	.204	-1.676	-.824	-6.140	19	.000
Pair 10	DynamicAssessmentC - DynamicAssessmentD	-1.150	.813	.182	-1.530	-.770	-6.328	19	.000

FIGURE 46 - PAIRED SAMPLES T-TEST

	SA1C	SA1D	SA2C	SA2D	SA3C	SA3D	MIC	MID	INTC	INTD	RESPC	RESPD	CONGC	CONGD	CLUC	CLUD	DYNC	DYND	ASSC	ASSD
XY	3	4	3	4	3	3	2	2	2	2	3	3	3	4	3	4	3	3	4	4
PR	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
BK	3	5	3	4	3	5	3	4	3	5	4	4	2	4	3	4	2	4	3	4
DG	4	4	4	4	3	4	2	4	2	4	4	4	3	4	1	4	4	4	2	4
GC	4	4	4	4	3	4	3	4	3	3	3	4	3	3	3	4	2	4	2	3
MF	4	5	4	5	3	5	3	5	3	4	3	5	3	5	3	4	3	4	3	5
MR	3	4	3	4	3	4	3	3	3	4	3	4	3	4	3	4	3	4	3	4
LDH	3	4	3	4	2	4	2	4	2	4	2	4	1	4	2	3	2	4	1	3
MC	3	4	4	4	2	3	2	3	3	4	3	3	3	4	3	4	2	3	2	3
PM	3	3	3	3	3	3	3	3	3	3	4	4	4	4	4	4	4	4	3	3
PT	3	4	3	4	3	4	3	4	3	4	4	5	3	4	3	4	3	4	3	4
LR	4	5	4	5	5	5	4	5	3	5	4	5	3	5	4	5	3	5	5	5
JS	5	5	3	4	4	5	3	4	3	4	4	5	3	4	3	4	3	4	3	4
TM	3	4	3	4	4	5	3	4	3	4	5	5	3	4	3	4	2	4	2	4
MvD	3	4	3	4	3	4	2	4	3	4	2	4	1	3	1	3	1	3	2	3
LB	3	4	3	4	3	5	3	5	3	5	4	4	2	4	2	4	2	4	3	4
MH	3	4	2	4	2	4	2	4	1	4	1	5	1	2	2	4	1	4	1	4
CP	4	5	3	4	3	4	4	5	4	5	3	5	3	4	3	4	4	4	4	5
RK	4	4	4	5	4	5	3	5	3	5	3	4	3	4	3	4	2	4	2	4
FdC	3	4	4	4	3	4	3	4	4	4	3	3	1	1	1	1	1	1	1	3
Mean	3.50	4.25	3.40	4.15	3.20	4.25	2.90	4.05	2.95	4.15	3.25	4.25	2.70	3.80	2.65	3.85	2.55	3.80	2.75	3.90
SD	0.688	0.550	0.681	0.489	0.834	0.716	0.788	0.826	0.826	0.671	0.910	0.716	1.081	0.951	0.875	0.813	0.999	0.834	1.020	0.718
Cohen's D		1.20381		1.26536		1.35111		1.42496		1.59534		1.22074		1.08028		1.42098		1.35897		1.3041
r		0.51569		0.53466		0.55979		0.58026		0.62358		0.52099		0.47524		0.57919		0.56202		0.54619
M2-M1		0.75		0.75		1.05		1.15		1.20		1.00		1.10		1.20		1.25		1.15
S_SQ	0.473684		0.46316		0.69474		0.62105		0.68158		0.82895		1.16842		0.76579		0.99737		1.03947	
S2_SQ		0.30263		0.23947		0.51316		0.68158		0.45		0.51316		0.90526		0.66053		0.69474		0.51579
S_SQ+S2_SQ(AV)		0.38816		0.35132		0.60395		0.65132		0.56579		0.67105		1.03684		0.71316		0.84605		0.77763
SQRT_SPL		0.62302		0.59272		0.77714		0.80704		0.75219		0.81918		1.01825		0.84449		0.91981		0.88183

FIGURE 47 - COHEN'S D CALCULATION