DE MONTFORT UNIVERSITY LEICESTER

Faculty of Technology
School of Computer Science and Informatics

Establishing cyber situational awareness in industrial control systems

PhD THESIS

Allan Cook

Submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy

July, 2018

For Juliette, Christine and James.

Abstract

The cyber threat to industrial control systems is an acknowledged security issue, but a qualified dataset to quantify the risk remains largely unavailable. Senior executives of facilities that operate these systems face competing requirements for investment budgets, but without an understanding of the nature of the threat cyber security may not be a high priority. Operational managers and cyber incident responders at these facilities face a similarly complex situation. They must plan for the defence of critical systems, often unfamiliar to IT security professionals, from potentially capable, adaptable and covert antagonists who will actively attempt to evade detection. The scope of the challenge requires a coherent, enterprise-level awareness of the threat, such that organisations can assess their operational priorities, plan their defensive posture, and rehearse their responses prior to such an attack.

This thesis proposes a novel combination of concepts found in risk assessment, intrusion detection, education, exercising, safety and process models, fused with experiential learning through serious games. It progressively builds a common set of shared mental models across an ICS operation to frame the nature of the adversary and establish enterprise situational awareness that permeates through all levels of teams involved in addressing the threat. This is underpinned by a set of coping strategies that identifies probable targets for advanced threat actors, proactively determining antagonistic courses of actions to derive an appropriate response strategy.

Declaration

This is to certify that:

(i) the thesis comprises only my original work towards the PhD except where indicated,

(ii) due acknowledgement has been made in the text to all other material used.

Allan Cook

Publications

Journal Papers

- **Allan Cook, Helge Janicke, Richard Smith, Leandros Maglaras** "The Industrial Control System Cyber Defence Triage Process", Computers and Security (Elsevier), Volume 70, September 2017, Pages 467-481, DOI: 10.1016/j.cose.2017.07.009

- **Allan Cook, Richard Smith, Leandros Maglaras, Helge Janicke** "SCIPS: Using Experiential Learning to Raise Cyber Situational Awareness in Industrial Control Systems", International Journal of Cyber Warfare and Terrorism (IGI-Global), Volume 7, Issue 2, May 2017, DOI: 10.4018/IJCWT.2017040101

- **Allan Cook, Helge Janicke, Leandros Maglaras, Richard Smith** "An Assessment of the Application of IT Security Mechanisms to Industrial Control Systems", International Journal of Internet Technology and Secured Transactions (Inderscience), Vol. 7, No 2, pp 144-174, 2017, DOI: 10.1504/IJIST.2017.10008030

- **Allan Cook, Richard Smith, Leandros Maglaras, Helge Janicke** "Managing Incident Response in the Industrial Internet of Things", International Journal of Internet Technology and Secured Transactions (Inderscience), Vol. 8, No 2, pp 251-276, 2018

- **Allan Cook, Andrew Nicholson, Helge Janicke, Leandros A. Maglaras, Richard Smith** "Attribution of Cyber Attacks on Industrial Control Systems", EAI Transactions on Industrial Networks and Intelligent Systems, vol. 3, issue 7, e3, pp. 1-15, April 2016, DOI: 10.4108/eai.21-4-2016.151158

Conference Papers

- **Allan Cook, Richard Smith, Leandros Maglaras, Helge Janicke** "Measuring the Risk of Cyber Attack in Industrial Control Systems", Proceedings of the 4th International Symposium for ICS & SCADA Cyber Security Research (ICS-CSR 2016), Belfast, 23-25 August 2016, DOI: 10.14236/ewic/ICS2016.12

- **Allan Cook, Richard Smith, Leandros Maglaras, Helge Janicke** "Using Gamification to Raise Awareness of Cyber Threats to Critical National Infrastructure", Proceedings of the 4th International Symposium for ICS & SCADA Cyber Security Research (ICS-CSR 2016), Belfast, 23-25 August 2016, DOI:10.14236/ewic/ICS2016.10

Book Chapters

- **Helge Janicke, Allan Cook, Andrew Nicholson, Kevin Jones** "Risks, Threats and Mitigation Strategies for SCADA Systems", Cyber-Physical-Social Systems and Constructs in Electric Power Engineering, (Siddharth Suryanarayanan, Robin Roche, Timothy M. Hansen), IET, 2016, ISBN: 9781849199360
- **Allan Cook, Michael Robinson, Mohamed Amine Ferrag, Leandros A. Maglaras, Ying He, Kevin Jones, and Helge Janicke** "Internet of Cloud: Security and Privacy issues", Chapter in Cloud Computing for Optimization: Foundations, Applications, Challenges, (Bhabani Shankar Prasad Mishra, Himansu Das, Satchidanand Dehuri, Alok Kumar Jagadev), Springer, Studies in Big Data book series, May 2018, ISBN-10:3319736752

Acknowledgements

I would like to thank my doctoral supervisors, Dr Richard Smith and Professor Helge Janicke for their friendship, counsel and good humour throughout my research. I look forward to continuing my association with them at De Montfort University for many years to come.

I would also like to thank Dr. Leandros Maglaras for his collaboration on a number of papers and his advice on the publication process.

However, none of this would have been possible without the love and patience of my wife and children. Raising a family is a team sport, the responsibilities for which I have largely handed to my wife, Juliette, during this research. Similarly, my children, Christine and James, have accepted their father sat at a keyboard for too many hours when there were probably far better things we could have been doing together. To them all I would like to express my heart-felt gratitude for their unquestioning support through this, and many other *'good ideas'* over the years. I love you.

This thesis was written using JabRef and LaTeX.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

Contents

> *"Cybersecurity is the responsibility of senior leaders who are responsible for creating an enterprise-wide culture of security. It is about aligning IT with business competencies. It is about a well-informed board and C-suite that make security decisions not based on the musings of a business show talking head but from utilizing an informed, risk-based approach."*
> Tom Ridge, former US Secretary of Homeland Security, 2014 [1].

1.1 Introduction

The cyber threat to industrial control systems (ICS) is an acknowledged security issue, but a qualified dataset to quantify the risk remains largely unavailable. Senior executives of facilities that operate these systems face competing requirements for investment budgets, but without an understanding of the nature of the threat, cyber security may not be a high priority. Operational managers and cyber incident responders at these facilities face a similarly complex situation. They must plan for the defence of critical systems, often unfamiliar to IT security professionals, from potentially capable, adaptable and covert antagonists who will actively attempt to evade detection.

The scope of the challenge requires a coherent, enterprise-level awareness of the threat, such that organisations can assess their operational priorities, plan their defensive posture, and rehearse their responses prior to such an attack. Research in the field of cyber security has focused on discrete elements of the problem, rather than the development of a cohesive framework to establish appropriate levels of cyber situational awareness across all layers of an organisation.

1.2 Overview of Research

This research explores the use of experiential learning through serious games to progressively build a common set of shared mental models across an ICS operation to frame the nature of an adversary and establish enterprise situational awareness that permeates through all levels of teams involved in addressing the threat. This is underpinned by a set of coping strategies that identifies probable targets for advanced threat actors, and proactively determines antagonistic courses of actions to derive an appropriate response strategy.

Specifically, this research encompasses:

- **Simulated Critical Infrastructure Protection Scenarios (SCIPS):** *An experiential learning environment that introduces the nature of cyber attacks on ICS and their impact on the continued operations and financial viability of an ICS operator.*
- **ICS Cyber Defence Triage Process (ICS-CDTP):** *A pre-incident coping strategy that assesses the processes and systems that would severely impact an ICS operator if degraded or denied, and develops a defensive posture and incident response playbook that can be used as the basis for exercising within a progressive collective training framework.*
- **Progressive Collective Training:** *A framework for the delivery of progressive experiential learning that integrates the SCIPS training scenarios with cyber range and table-top exercises to build shared mental models, drive policy and procedural change, build capable incident response teams, and develop pre-incident coping strategies.*

1.3 Research Aims

This research aims to determine which characteristics of experiential learning contribute to the establishment of enterprise situational awareness so that an ICS operator can target its pre-incident planning and training, using serious games and cyber exercises, to focus its defensive posture based on its operational priorities and the adversaries it faces.

1.4 Research Questions

To validate the results of this research, and assess their efficacy, six questions are proposed that can be answered through experimentation, described in Table 1.1.

No.	Research Question	Assessment Criteria
1.	*Which factors influence the development of mental models to provide cyber situational awareness?*	An assessment of any demonstrated relationships between mental models and specific characteristics observed in experimentation that shape situational awareness.
2.	*Does the adoption of coping strategies increase situational awareness?*	A demonstration, through experimentation, of an observed increase in situational awareness resulting from the use of coping strategies.
3.	*Can serious games change the risk perceptions of participants and establish a foundational level of situational awareness?*	An assessment of observed and recorded risk perceptions before and after the playing of serious games.
4.	*How can we increase the efficacy of the serious games to deliver the change in risk perceptions?*	An assessment of results from experimentation to identify which factors influence any changes in risk perception observed in Question 3.
5.	*As a result of serious games, can participants recognise the characteristics of a cyber attack and determine the possible intent and courses of action?*	An assessment of participants' recognition and comprehension of the behaviours of threat actors, and their ability to identify possible antagonistic intent and future courses of action.
6.	*Are participants of serious games able to assess the immediate and longer-term impacts of cyber attacks?*	An assessment of participants' ability to identify and quantify the consequences of the attack behaviours observed in Question 5.

Table 1.1: Research questions

1.5 Structure of Thesis

To address the six research questions described in Table 1.1, this thesis is structured as follows.

1.5.1 Background

Chapter 2 sets the scene for the research to address the questions described in Section 1.4. It provides an explanatory background that reviews the cyber threat to ICS from capable antagonists. It continues in Section 2.4 by characterising the nature of the risks associated to the threat and proposes a requirement for an enterprise-level understanding of such risks in order to adequately prepare for, and defend against, cyber attacks.

1.5.2 Related Work

Chapter 3 surveys and critically assesses the state of the art with regard to the domains and disciplines associated with this research. Sections 3.2 and 3.3 describe the scope of review and the methodology adopted. Section 3.4 then explores the characteristics of ICS through the use of a reference architecture, then reviews the application of IT security mechanisms to ICS and discusses the limitations of their use. The chapter continues with a discussion in Section 3.5 of the techniques available to measure the risk of cyber attacks in ICS, and the requirement for a qualified dataset on which to base risk assessments. This provides the basis to consider how risks are perceived, as an element of answering Question 3 - *Can serious games change the risk perceptions of participants and establish a foundational level of situational awareness?*

Section 3.6 reviews research into education for cyber security awareness to determine how serious games can be used to change the risk perceptions, understanding, and behaviours as asked in Question 1 - *Which factors influence the development of mental models to provide cyber situational awareness?*, Question 3 - *Can serious games change the risk perceptions of participants and establish a foundational level of situational awareness?*, Question 4 - *How can we increase the efficacy of the serious games to deliver the change in risk perceptions?*, Question 5 - *As a result of serious games, can participants recognise the characteristics of a cyber attack and determine the possible intent and courses of action?*, and Question 6 - *Are participants of serious games able to assess the immediate and longer-term impacts of cyber attacks?*. This includes an assessment of serious games for experiential learning, the characteristics of an effective serious game, and the strategies available to influence decision-making.

The detail of situational awareness is reviewed in Section 3.7 to further address Question 1 - *Which factors influence the development of mental models to provide cyber situational awareness?*, Question 3 - *Can serious games change the risk perceptions of participants and establish a foundational level of situational awareness?*, Question 5 - *As a result of serious games, can participants recognise the characteristics of a cyber attack and determine the possible intent and courses of action?*, and Question 6 - *Are participants of serious games able to assess the immediate and longer-term impacts of cyber attacks?*. The section includes a consideration of exercises as a means to develop situational awareness. This leads into a deeper exploration of cyber exercises in Section

3.8.

To address Question 2 - *Does the adoption of coping strategies increase situational awareness?*, Section 3.9 assesses incident response within ICS and Section 3.10 reviews intrusion analysis techniques and their applicability to ICS.

1.5.3 The SCIPS Serious Game

Chapter 4 introduces the SCIPS game, describing its evolution from an initial proof of concept during the author's MSc project, to shape risk thinking in the minds of participants, through the extended gaming framework used to deliver experiential learning to develop situational awareness and mental models for incident responders. The SCIPS game contributes to addressing Question 1 - *Which factors influence the development of mental models to provide cyber situational awareness?*, Question 3 - *Can serious games change the risk perceptions of participants and establish a foundational level of situational awareness?*, Question 4 - *How can we increase the efficacy of the serious games to deliver the change in risk perceptions?*, Question 5 - *As a result of serious games, can participants recognise the characteristics of a cyber attack and determine the possible intent and courses of action?*, and Question 6 - *Are participants of serious games able to assess the immediate and longer-term impacts of cyber attacks?*.

1.5.4 The Industrial Control System Cyber Defence Triage Process

Chapter 5 describes a coping strategy for ICS operators that allows them to address cyber threats in an effective and cost-sensitive manner that does not expose their operations to additional risks through invasive testing. It focuses on those ICS operators facing the highest levels of impact from antagonistic cyber actions, but not yet at a high level of cyber security maturity. The chapter addresses Question 2 - *Does the adoption of coping strategies increase situational awareness?*.

1.5.5 A Framework for Progressive Collective Training

Chapter 6 acknowledges that incident response teams cannot prepare for every situation, or predict every crisis. The chapter explores the requirements for collective cyber incident response training and proposes a framework to develop progressive individual and team SA to produce the levels of team cohesion and adaptability required to respond to the variety of cyber attacks an organisation might face. It contributes to addressing Question 1 - *Which factors influence the development of mental models to provide cyber situational awareness?*, Question 3 - *Can serious games change the risk perceptions of participants and establish a foundational level of situational awareness?*, Question 4 - *How can we increase the efficacy of the serious games to deliver the change in risk perceptions?*, Question 5 - *As a result of serious games, can participants recognise the characteristics of a cyber attack and determine the possible intent and courses of* *action?*, and Question 6 - *Are participants of serious games able to assess the immediate and longer-term impacts of cyber attacks?*.

1.5.6 Experiments

Chapter 7 describes the schedule and scope of the experiments that fused the SCIPS game, the Industrial Control System Cyber Defence Triage Process, and the Framework for Progressive Collective Training to generate data to allow an assessment of these concepts to answer the six research questions in Table 1.1. In particular, Section 7.5.2 introduces a novel cyber exercise format to maximise training value to participants.

1.5.7 Experiment Results

Chapter 8 articulates the results of experiments. Section 8.2 explains the key research method used, then discusses the results in Sections 8.4 - 8.12.

1.5.8 Analysis and Critical Assessment

Chapter 9 analyses the results from the experiments described within Chapter 8, assessing their impact, critically reviewing their applicability and generalisability within the cyber domain, and considers how they address the six research questions in Table 1.1.

1.5.9 Further Work

Chapter 10 summarises the areas where the analysis and critical assessment of the experimental results highlights a requirement for further research.

1.5.10 Summary Conclusions

Finally, Chapter 11 provides a summary of the conclusions of this research.

1.6 Contribution

The research described in this thesis is novel in that it combines and extends concepts found in risk assessment, intrusion detection, education and experiential learning, serious games and exercising, with safety and process models that are recognised within the operations of many ICS facilities. As such, this research:

1. Proposes a progressive collective training framework in Chapter 6 that incrementally develops the content of the five mental models defined in Section 6.3 (with

analysis in Section 9.3) necessary for SA and incident response to address Question 1 - *Which factors influence the development of mental models to provide cyber situational awareness?*

2. Characterises the results of a qualitative analysis in Chapter 8 within a set of themes summarised in Section 8.12 that shapes the nature of experiential learning within a serious gaming environment, further addressing Question 1 - *Which factors influence the development of mental models to provide cyber situational awareness?*

3. Focuses on the identification and defence of critical ICS equipment from malicious manipulation in Chapter 5, with results in Chapter 8, allowing ICS operators to actively identify and attempt to thwart malicious attacks based on an incident response *'playbook'* developed from analyses of antagonistic intent, addressing Question 2 - *Does the adoption of coping strategies increase situational awareness?*

4. Delivers a serious gaming environment in Chapter 4 with experimental results described in Sections 8.5 and 8.10 that addresses Question 3 - *Can serious games change the risk perceptions of participants and establish a foundational level of situational awareness?*, Question 5 - *As a result of serious games, can participants recognise the characteristics of a cyber attack and determine the possible intent and courses of action?*, and Question 6 - *Are participants of serious games able to assess the immediate and longer-term impacts of cyber attacks?* The game allows participants to experience the simulated impact of a cyber attack on an ICS enterprise, demonstrating how it can strategically affect shareholder value, and support the development of mental models to frame wider cyber security operations.

5. Provides a framework in Chapter 6, with experimental results described in Chapter 8, that addresses Question 4 - *How can we increase the efficacy of the serious games to deliver the change in risk perceptions?* It provides a progressive, cost-effective establishment and maintenance of situational awareness and skills proficiency through cyber range and table-top exercises that incorporate the scenarios played out in the strategic serious game environment.

6. Introduces a novel cyber defence exercise structure in Section 7.5.2, with experimental results in Sections 8.5 and 8.9, to maximise training value to participants and further address Question 4 - *How can we increase the efficacy of the serious games to deliver the change in risk perceptions?*

Chapter 2

Background

Contents

2.1 Introduction

This chapter sets the scene for the detailed discussions that follow throughout this thesis.

2.2 The Cyber Threat to ICS

A US executive order signed in 2013 stated that the *"cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront"* [2]. This infrastructure is typically underpinned by industrial control systems (ICS) that automate and manage electromechanical devices to provide services essential to a nation's wellbeing and prosperity, and as such, any antagonistic action against these represents a significant threat to the continued security of these countries [3]. ICS often use operating systems, applications and procedures that may be considered unconventional by contemporary IT professionals, and have operational requirements that include the management of processes that, if not executed in a predictable manner, may result in injury, loss of life, damage to the environment, as well as serious financial issues such as production losses that may have a negative impact on a nation's economy [3, 4, 5, 6, 7].

While the total number of ICS installations is unknown, a 2012 commercial research paper [8] estimated the global industrial automation market to be worth USD 152bn, suggesting a significant number of ICS facilities exist. In the same calendar year, the US ICS Computer Emergency Response Team (ICS-CERT) reported 138 incidents [9] to which it responded. The total number of incidents involving critical infrastructure requiring ICS-CERT to respond in the United States between October 2014 and September 2015 had increased to 295 [10]. With the costs involved in deploying ICS security, especially within critical systems, being high [11] the business case for investment must be clearly articulated [12].

An analysis by an insurance company in 2015 exercised a simulated scenario of malware causing an electricity blackout across 15 US states, leaving 93 million people without power, with a total impact to the US economy estimated at USD 243bn, rising to more than USD 1trn in one version of the scenario [13]. However, this study, and another by the North American Electric Reliability Corporation (NERC) [14], assessed the possible frequency of these incidents as low. The NERC report also cited cyber attack as only one of nine areas of concern facing the electricity sector in the period 2010-2018, and as such one must assume that there will be competing demands for resources to address these issues which may affect the appetite for investment in cyber defences.

2.3 Assessing the Risks to ICS

The potential for high-impact low-frequency (HILF) events to cause significant negative effects on an ICS facility, combined with the small sample of qualified data complicates the assessment of risks when prioritising budgets for investment. Even if the data becomes available that describes the overall attack landscape of ICS, it is unclear how to translate this into attack profiles in particular industry sectors, and more parochially, attack profiles for individual facilities.

Large ICS are typically complicated, and this complexity may deter some opportunistic actors. Advanced Persistent Threat (APT) actors, however, pose a credible risk [15]. In 2014, 55 percent of incidents investigated by ICS-CERT involved APTs or sophisticated actors [10]. By their nature, APT attacks are covert and difficult to detect, with a degree of tailoring available to the antagonist in order to achieve focussed outcomes on the target network.

There is a growing consensus that cyber security is not achievable by solely focusing on technological aspects, and that managing the risk of cyber attacks is a business problem [16]. Hence, in addition to lowering the likelihood of cyber attacks through mostly technical means, organisations can attempt to absorb losses incurred by such attacks through insurance, either through setting aside funds, or through a third-party policy. When it comes to pricing cyber risk, however, a principal problem is the scarcity of data. Regardless of how accurate and sophisticated risk models become, if there are no data to test the models against, they are of limited use [17]. Given the adaptive nature of APTs and lack of data regarding HILF events, this might prove difficult or even impossible. Faced with this ambiguity, business leaders need to decide how much they should invest and which strategy to follow. Business leaders require facts about the risk of cyber attacks to determine possible mitigation strategies [16]. Firstly, then, they require a viable definition of what should be categorised as a cyber risk. It is argued by Biener et al. (2015) [17], from an insurance perspective, that an event on a network or system must meet three criteria to be characterised as a cyber risk, as proposed in Table 2.1.

1. A critical asset such as a company server or database needs to be affected.
2. A relevant actor needs to be involved in the cause of the cyber risk incident (e.g., hackers, employees, system).
3. A relevant outcome such as the loss of data or misuse of confidential data needs to be present.

Table 2.1: Characteristics of a cyber risk, Biener et al. (2015)

However, this definition assumes an ability to assess and prioritise the critical assets of an organisation, and understanding of the antagonists who would seek to adversely affect them, along with a means to quantify the loss or misuse of data. This assessment of critical assets is focused on an individual organisation, and does not provide a basis for wider insurance policies. A central requirement for providing insurance against a specific risk is independence of risks. Following the law of large numbers[1], the larger the number of mutually independent risks in the insurance pool, the more likely it is that average aggregate losses correspond to expected losses. An empirical analysis by Biener et al. (2015) [17], however, showed that only 16.8% of cyber incidents were related to a loss in another firm. In other words, most cyber risk incidents in the sample were not correlated with other cases. The challenge of independence of risks is further exacerbated when unfamiliar technologies are employed, such as ICS. An analysis of historical incident data could be misleading if the nature of the underlying risk is based on technologies not reflective of the systems under consideration [17] and existing IT security mechanisms are mistakenly assumed to be effective technology mitigations in these environments [3].

2.4 Enterprise Understanding of Cyber Risk

In situations where the risk landscape is unclear, business leaders, operational managers, and technologists require a common language to communicate information and risk assessments. A frequent problem within the cyber security arena is the lack of viable analogies, or *mental models*, to help users assess the threats they encounter [18]. In the case of ICS security, these cognitive abstracts are even harder to develop without a dataset to quantify the risk, despite increased media coverage. Indeed, it has been observed that in the absence of credible evidence of the threat, users perceive the pur-

[1] The law of large numbers is a principle of probability according to which the frequencies of events with the same likelihood of occurrence even out, given enough trials or instances. As the number of experiments increases, the actual ratio of outcomes will converge on the theoretical, or expected, ratio of outcomes.

ported risks to be overstated by the media [19], and until they believe themselves to be in a situation where they are susceptible, they do not change their behaviours [20]. ICS operators therefore require a foundational understanding of cyber situational awareness. However, for such situational awareness to be raised to the level that individuals take action, they must address the seven aspects of situational awareness proposed by Barford et al. (2010) [21], as described in Table 2.2.

1. Acknowledge that a threat exists, and that it can be identified if it occurs.
2. Have assessed the immediate and longer-term impact of cyber attacks.
3. Be conscious of how an attack can evolve over time.
4. Understand the intent of an antagonist.
5. Recognise the circumstances under which an attack could occur.
6. Have appraised the quality of information required to make decisions during an attack.
7. Consider the possible actions an antagonist might take in order to achieve their intent.

Table 2.2: Seven aspects of cyber situational awareness, Barford et al. (2010)

To assess whether it is possible to raise ICS business leaders', operational managers', and technologists' understanding of the cyber threat by improving their awareness, we must consider the influencing factors on cyber situational awareness. We shall now review the work related to this core research theme.

Chapter 3

Related Work

Contents

3.1 Introduction

To support adequate consideration of the scope of the research problem described in Section 1.1 in the context of the wider background discussed in Chapter 2, this chapter provides a literature review of related work.

Elements of this chapter have been peer-reviewed and published in the following:

- **Allan Cook, Helge Janicke, Leandros Maglaras, Richard Smith** "An Assessment of the Application of IT Security Mechanisms to Industrial Control Systems", International Journal of Internet Technology and Secured Transactions (Inderscience), Vol. 7, No 2, pp 144-174, 2017, DOI: 10.1504/IJIST.2017.10008030

- **Allan Cook, Richard Smith, Leandros Maglaras, Helge Janicke** "Measuring the Risk of Cyber Attack in Industrial Control Systems", Proceedings of the 4th International Symposium for ICS & SCADA Cyber Security Research (ICS-CSR 2016), Belfast, 23-25 August 2016, DOI: 10.14236/ewic/ICS2016.12

- **Allan Cook, Richard Smith, Leandros Maglaras, Helge Janicke** "Managing Incident Response in the Industrial Internet of Things", International Journal of Internet Technology and Secured Transactions (Inderscience), Vol. 8, No 2, pp 251-276, 2018

- **Helge Janicke, Allan Cook, Andrew Nicholson, Kevin Jones** "Risks, Threats and Mitigation Strategies for SCADA Systems", Cyber-Physical-Social Systems and Constructs in Electric Power Engineering, (Siddharth Suryanarayanan, Robin Roche, Timothy M. Hansen), IET, 2016, ISBN: 9781849199360

3.2 Scope of Review

This research encompasses a number of subject matter areas that have influenced the direction of analysis and thesis development. Specifically, this has included;

- the characteristics of industrial control systems,

- the measurement of risk,
- techniques for the delivery of cyber security education,
- the development of situational awareness,
- the nature of cyber exercises,
- incident response planning, and
- means by which a network intrusion can be analysed.

Accordingly, this literature review addresses each of these subject areas in turn.

3.3 Review Method

Although the security of ICS is an emerging research area, the multi-disciplinary aspects of the specific subjects areas identified above were not sufficiently addressed in identified publications within the cyber domain. An initial triage based on a keyword search from open sources suggested irregular areas of research with an insufficient level of primary studies that would form a reliable base for an analysis. It was, however, apparent that primary literature was available in specific subject areas, although unrelated to ICS. A mapping study [22] was therefore employed in order to cover the breadth of the related subject matter publications to provide a basis for an analysis of this problem space.

The analysis approach assumed that a chronological sample of literature would demonstrate an evolution of thinking and provide the necessary background on which to base this research. As such, a snowballing methodology [22] was employed whereby keyword searches of Google Scholar, ACM Digital Library, IEEE and Web of Science were used in order to identify publications with a high number of citations, or applicable subject matter coverage, then their references traced in order to provide subject matter coverage. The following keywords, in a variety of combinations, were used: *cyber security, scada, industrial control system, incident response, intrusion detection, incidents, forensics. protocols, anomaly detection, critical infrastructure, risk analysis methods, process risk, safety risk, risk measurement, cyber education, situational awareness, cyber exercises, table-top exercises.* Although effective, the repeatability of a keyword searching approach is limited, and it is probable that researchers in the same field would not identify the same source materials if the exercise were to be independently repeated [23]. Therefore external, independent peer-review was used to provide an objective validation of the findings [22].

The literature review described in the following sections of this chapter surveyed the subjects of ICS, risk assessment, cyber security education, situational awareness, cyber exercises, incident response, and intrusion analysis, using existing works as a starting point. The identified works each are analysed, with preliminary conclusions proposed for each discrete research area.

3.4 Industrial Control Systems

Industrial control systems (ICS) is a general term that encompasses a family of process automation technologies including Supervisory Control and Data Acquisition (SCADA) systems and Distributed Control Systems (DCS). These control systems use Programmable Logic Controllers (PLC) or similar Intelligent Electronic Devices (IED), Remote Terminal Units (RTU) and input/output (I/O) devices to manage electromechanical equipment in either local or distributed environments. Several factors have contributed to the escalation of risks specific to control systems, including the adoption of standardised technologies with known vulnerabilities, connectivity of control systems with other networks, use of insecure remote connections, and widespread availability of technical information about control systems [3, 24, 25]. These systems provide essential services for sovereign nation's critical infrastructures, and as such, cyber attacks against them represent a significant threat to the continued security of these countries [26].

As industrial businesses and critical national infrastructure (CNI) have evolved to exploit the closer integration of services and data provided by the networking and the Internet, the isolation that secured ICS has reduced [3]. The efficiencies offered by real-time monitoring, peer-to-peer communications, multiple sessions, concurrency, maintenance and redundancy mechanisms improve the quality of the services offered to both operators and consumers [27]. As a result of this connectivity, the once isolated systems are now susceptible to an emerging range of threats. These attacks can be categorized into two classes [28]. The first class includes traditional IT attacks that target vulnerabilities in general purpose IT systems which can be mitigated by adopting IT countermeasures such as software patches, antivirus software and firewalls. The second class encompasses ICS attacks that target the elements of ICS themselves. These attacks can originate either locally, where the attacker has physical access to equipment, or remotely, where the attack is directed via unsecured connections or through the exploitation of a trusted link [28].

A review of ICS system cyber security standards by Sommestad et al. (2010) [29], depicted in Figure 3.1, highlighted the number of occurrences of specific security countermeasure keywords in the documentation. As can be seen, the most frequent terms are all related to established IT security best practice, with the implication being that IT mechanisms that support these are adequate and appropriate for ICS. By considering the effectiveness of traditional IT security mechanisms within an ICS environment we can consider areas of weakness within an ICS when traditional IT security mechanisms are deployed and assess their applicability.

ICS operations generally must execute within strict performance and time-critical boundaries, with near real-time control, requiring data to be transmitted, processed and responded to within a defined latency [30]. Unlike IT systems, ICS have typical response requirements of 1-10 milliseconds, and in motion control systems the range is further constrained to between 250 microseconds - 1 millisecond with jitter less than 1 microsecond [31]. Moreover, the main operational objectives of an ICS are to maintain

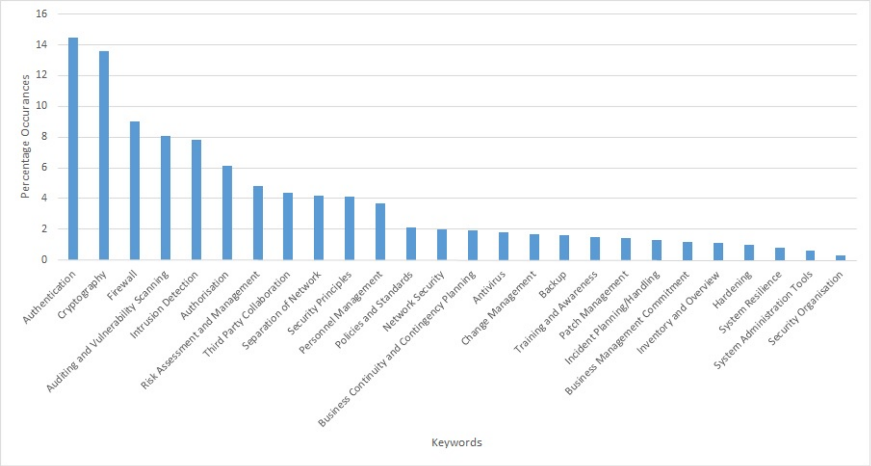


Figure 3.1: The focus of ICS standards and guidelines on countermeasure groups, Sommestad et al. (2010)

availability, reliability and safety [32]. This focus drives the behaviours of system operators to prioritise these factors when considering system change or downtime. Any modifications to the operational environment carry risks to the availability, reliability and safety of the system and as a result it is not always feasible to halt operations to install upgrades or patches [33].

ICS generally comprise two types of components: information processing elements, and field measurement and control devices. Information processing elements generally co-operate with general IT applications within the organisation and provide management information, scheduling and accounting data utilising traditional IT-based technologies. Field measurement and control devices run in the production or operational environment, often referred to as Operational Technology (OT), typically using real-time operating systems on proprietary hardware and communicate using many industrial protocols, often in a mix of IP, bus and serial technologies. Different protocols are frequently used at different levels of the ICS architecture, requiring gateways for interoperability [30]. Unlike traditional IT systems which place a higher priority on the confidentiality, integrity and availability of centralised servers (even if in a distributed architecture) rather than edge devices, an ICS places equal importance on control devices at the network or system perimeter, as these are the devices generally closest to the physical elements under control [34].

3.4.1 ICS Reference Architecture

The Purdue model, described by Williams (1991) and illustrated in Figure 3.2, is a reference architecture for control hierarchy. It describes six levels within an organisation managing an industrial control system [35, 36], and is the *de facto* model within industry [37].

ICS implementations often include a number of significant differences to traditional IT systems [30]. Typically, ICS have a deeper architecture than typical enterprises, as

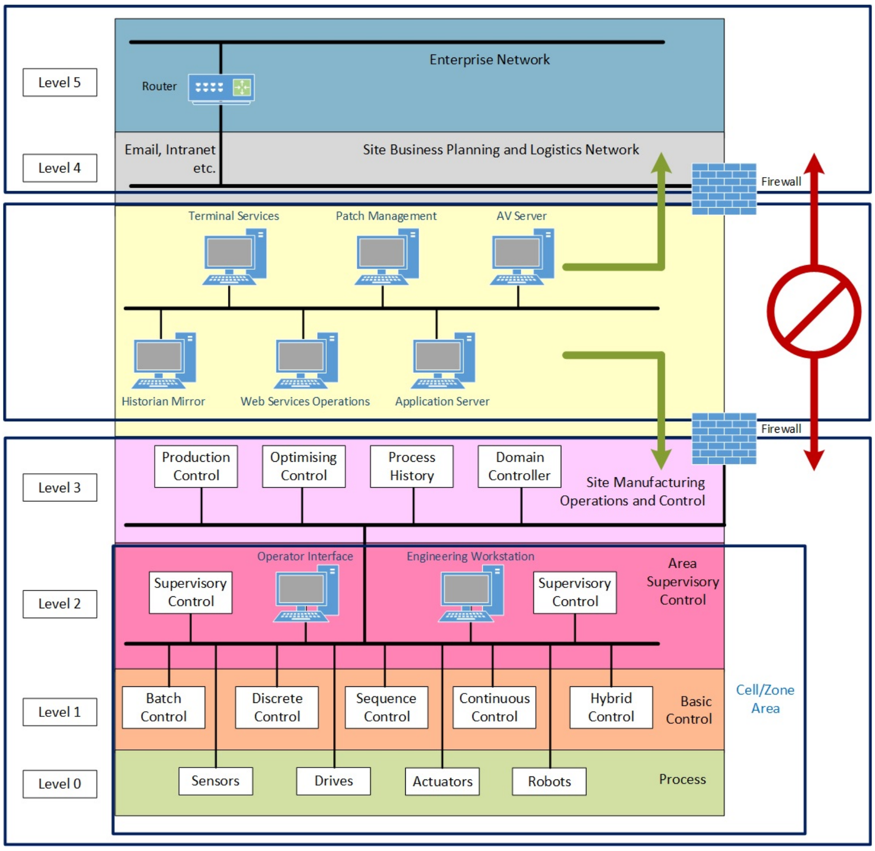


Figure 3.2: Purdue model for control hierarchy, Williams (1991)

characterised by the Purdue hierarchy. It should be noted that in reality, ICS architectures rarely adhere to clear boundaries described by Williams (1991). However, the Purdue Model provides a useful reference architecture against which we can consider security provisions. The layers of the model are summarised below:

Level 5

Encapsulates the corporate or enterprise network with Internet access managed within the layer where the centralised IT systems and function are located, along with business-to-business (B2B) and business-to-customer (B2C) services [38]. The De-Militarised Zone (DMZ) between levels 4 and 3 shows a clear demarcation between Internet-connected elements and those isolated.

Level 4

Describes the functionality that requires access to services provided by the enterprise network in Level 5. This level is more often than not viewed as an extension of the enterprise network and it relies on standard IT services, including those provided by wireless access[38].

Level 3

Level 3, the plant level, represents the traditional highest level of control in an ICS, and the highest level of OT, managing end-to-end operational functions and coordinating the workflows to produce the desired end products or utility [38].

Level 2

Level 2 is the level of supervisory control within a site or a manufacturing process that is usually responsible for controlling the end-to-end production or service, generally through SCADA or DCS [39, 40, 41]. Facilities in Level 2 encompass alarm and alert management, overall control functions and process history data collection.

Level 1 and Level 0

Although logically abstracted, it is often difficult to separate the functionality provided at Level 1 and Level 0. Level 1 comprises controllers that direct and manipulate the manufacturing process by interacting with the Level 0 devices (e.g., I/O, sensors, and actuators) [38].

The use of differing protocols at each level of the architecture requires the common use of gateway devices to transform messaging and data in order to maintain connectivity, although the adoption of IP is reducing this in new implementations. The control information sent between devices is either the input or output of a control loop implemented in a supervisory device, or diagnostic information used to monitor the health of a device. The data packets transmitted in ICS are generally small, especially at Levels 0 and 1 where only a single measurement or value may be sent. This traffic is sent both periodically, in the case of sampled data, and aperiodically when events such as a change of state or an alarm are generated. Clocks and bus contention protocols are commonplace to ensure that all data transfers occur in a timely manner and are temporally consistent [30].

3.4.2 ICS Protocols

There are between 150 and 200 different ICS protocols in use and each must be protected equally, with Modbus [42], DNP3 [43, 44], OPC [45], and the Ethernet industrial protocol (Ethernet/IP) among the most widely adopted [46, 47]. In attempts to achieve tighter integration with the upper layers of the architecture, legacy protocols such as Modbus have been encapsulated in TCP/IP (Modbus/TCP), which often blurs the control architecture layers. Many of these protocols are inherently vulnerable by design, operating without authentication mechanisms [33].

3.4.3 Review of the Application of IT Security Mechanisms to the ICS Architectural Model

Having explored the nature of ICS and its differences to IT systems, we now consider how security may be applied to each of the architectural layers.

Level 5 Protective Measures

Protocols in this layer are usually limited to IP, and as such, traditional IT technologies such as anti-virus suites, firewalls, deep packet inspection, host and network intrusion detection system (IDS) and logging and auditing techniques are all valid mechanisms for deployment within such an environment [3]. However, contemporary malware expects these tools to be in use, and the corporate network is a common attack surface for targeting OT.

The adoption of ISO 27001 and 27002 standards [48] provides frameworks in which to consider access controls in this level of the architecture. The scope of such controls should consider both preventative and detection measures and should include a full assessment of risk not just in Level 5. It must consider its context within the wider ICS, cognisant of the corporate network's potential as a distribution vector for malware to OT, and should not just focus on perimeter controls [49]. All access to corporate networks should be tightly managed, with any external connectivity, especially remote access, controlled by Virtual Private Network (VPN) technologies with Internet edge firewalls and all authentication and authorisation via Access Control Lists (ACL) maintained by the IT network operations or security teams. Separate authentication mechanisms and credentials for users of the corporate and OT networks should be used, and user accounts should not span the domains of IT and OT [3].

Level 4 Protective Measures

Level 4 shares many similarities with Level 5, and in many instances is treated as an architectural layer that encompasses both, as the two layers are inherently IP-protocol based. However, whilst Level 5 offers enterprise services and attaches to the Internet, Level 4 sits on the upper-side of the firewalls proposed in the Purdue Architecture and requires interactions with the OT [38].

The most prevalent protocol in this layer is Open Platform Communications (OPC) [47]. OPC is often used to interact with OT to provide data to management information systems such as Historians [50] and Enterprise Resource Planning (ERP) [51], thus bringing the IT and OT systems closer together. However, whilst OPC is critical to most of these interactions in many organisations, it is an infrequently monitored protocol, but a well-known pivot point for attackers [33].

Given the positioning of OPC within a layer of the architecture, these vulnerabilities should be of concern, especially, as intellectual property theft, reconnaissance and industrial espionage, economic sabotage, and positioning for possible future exploitation or attack activity are common threats to ICS [26].

Common IT best practices such as network segmentation and firewalling, regular security patching, up-to-date antivirus software that runs regularly, security-aware software development and acquisition processes are appropriate to this architectural level [52]. Given the interstitial nature of Level 4, between Level 5 with Internet access, and Level 3 and with significant OT deployments, it is essential that this layer forms a bastion of best practice in order to prevent unauthorised access to the control system, and does not provide an egress route for data from the OT to inappropriate external entities.

Level 3 Protective Measures

Level 3 represents the highest level of OT within an ICS, and acts as the lower-side boundary of De-Militarised Zone (DMZ) between itself and Level 4. The use of the IP protocol, as in the upper layers, does not mean that the behaviour in the OT levels is the same. However, in recognising the differences in OT from IT, we should not ignore the vulnerabilities that the adoption of IT technologies bring to the OT domain. To achieve adequate security at this level it is necessary to model the *'normal'* operational behaviour of an ICS in order to identify any deviations. This is often challenging as there is rarely any real-time monitoring of network data in an ICS. This allows organised cyber attacks to take place over a prolonged period of time without detection [27].

Much of the research into traffic deviation from known norms relates to intrusion detection systems, as we expect ICS traffic to differ from traditional IT systems for three reasons [53]:

1. ICS networks are expected to increase their stability over time
2. Traditional IT systems support a variety of protocols with changing applications
3. ICS traffic is expected to be periodic due to the traffic exchange mechanisms in use

In consequence, traffic patterns should not be as dependent on human activity as IT systems are. Once the traffic patterns of an ICS have been established, abnormal activity can be detected as one of three changes in the frequency domain [54]:

1. New or missing periodic burst frequency
2. Change in periodic burst size
3. Increase in the surrounding traffic noise (protocol handshakes etc.)

Level 2 Protective Measures

The theme of IDS and traffic analysis in OT continues into Level 2 where the operational elements of a DCS are typically situated [55]. In such environments it is essential for asset owners to identify the devices, applications and connections within the domain. Without this understanding an organisation cannot determine new traffic patterns or protocol interactions.

One area of research that is appropriate to this architectural layer, however, is that of log analysis. IDS and other traditional security measures cannot, by themselves, detect or mitigate process-related threats [56]. The limitations of signature- and anomaly-based detection systems do not identify threats that intend to target the *process under control*, rather than the *control system*. These can only be detected by analysing the data at a higher, semantic level. System logs capture information about process activity, which depending on the size of the industrial plant can amount to thousands of records per day, which may be valuable to attack detection. However, these logs must be adequately protected, as an attacker could potentially manipulate them by sending false data [57].

Level 1 and Level 0 Protective Measures

The primary threats to control systems in these layers include response injection, command injection or denial of service [58]. Devices in Levels 1 and 0 produce periodic traffic patterns using protocols that are insecure by design, and are therefore susceptible to replay attacks, hijacking, spoofing and manipulation. As the devices in question have limited processing resources and are inherently proprietary they will remain vulnerable until the vendors implement on-board security services, and even then, before security is improved, ICS operators would still have to accept the risk of upgrading their infrastructure.

Accepting the current limitations of the devices and protocols, security mechanisms in Level 1 and 0 lend themselves to procedural security management and configuration control. Therefore, whilst not specifically designed for ICS, the concepts of Information Security Management Systems as defined in ISO 27001 [48] offer the procedural basis for mitigations in these layers.

3.4.4 Analysis

As can be seen, the protection of ICS installations is complicated, with a range of security issues across every layer of the architecture. However, whilst the problem can be scoped and defined within an abstract concept such as a reference architecture, the reality of many ICS is that they do not follow such rigorous design demarcations, with systems and protocols crossing intangible layers at will. In recognition of this reality, we shall now consider if, where and how IT security mechanisms can be applied to ICS, cognisant of such real-world constraints.

As discussed, ICS face the same attack vectors as IT systems. Connectivity to the Internet allows reconnaissance activity around an ICS as well as an opportunity for malware delivery. Spear phishing is as much of a threat to ICS as it is to networks that incorporate IT [59]. Similarly, controls within a corporate network, or lack thereof, provide an environment in which malware can propagate and extend its reach within an organisation. However the range of attack vectors grows within an ICS as vendor engineers access control equipment either remotely or locally, with little control over the security of their devices or network connectivity [3].

In all of these scenarios, traditional IT security mechanisms are both appropriate and effective means to defend the boundaries of an organisation. Firewall architectures, email scanning, Deep Packet Inspection (DPI), VPN, Host-based IDS (HIDS), Network-based IDS (NIDS) are all established ways by which an organisation can reduce the opportunities for the ingress of malicious software into their environments [3]. As a complementary measure, the practice of locking-down unused ports, USB devices, use of access controls through corporate directories and the enforcement of least-privilege access, all reduce the insider threat attack surface [60].

From this it is clear to see the advantages of properly implemented IT security controls within the corporate and IP-enabled areas of the business, generally encompassed within Levels 5 and 4 of the reference architecture. However, the penetration of IP into the OT levels is common and not limited by doctrine [61]. OPC, in particular, spans the ICS enterprise both horizontally as well as vertically [45]. Its use of IT technologies such as IP, Distributed Common Object Model (DCOM) and Remote Procedure Calls (RPC) [62, 63], offer the opportunity to exploit proven IT security technologies to protect its use, but only if deployed using an understanding of the context of its implementation. Without limiting access to the systems using the protocol, and increasing the security of the underpinning technologies, any monitoring system, HIDS or NIDS, will be of limited effect [64, 65, 66, 5, 67, 68, 6]. As OPC and other IP-enabled technologies reach to the domain of OT, and therefore extend the reach of malware delivery, it becomes essential for the IP elements to be seen as an opportunity to harden the perimeter security for non-IP-enabled control devices further within the architectural layers [32, 69].

Once within OT it is necessary to acknowledge its inherent limitations from a security perspective, at least when discussing legacy devices. The design focus of reliability and availability using proprietary technologies and protocols, with little or no accompanying security capabilities, requires a pragmatic approach to their defence [3]. The hardening of the IP-enabled layers of the architecture will be of limited impact unless these lower layers have some means by which they can contribute to an overall defence-in-depth model. Traditional IT security mechanisms are generally not deployable within OT, as the proprietary nature of the equipment also brings proprietary warranty requirements which often preclude the addition of HIDS to any servers, for instance. This requirement for pragmatism accepts that patching opportunities are limited, and that these devices are insecure by design [33]. If authentication is not feasible within the devices then mechanisms to create whitelists of trusted connections should be considered. Where protocols can be monitored without adversely impacting the latency of the traffic, then passive tools and techniques can be considered. However, these will only be effective if the patterns of normal behaviour of traffic are modelled, as without these any deviations from the norm cannot be determined. Similarly, this overall analysis must include the industrial processes under control, as any traffic must be consistent with the proper functioning of the plant or utility. For instance, the overall traffic behaviours of a SCADA system will differ significantly from those of a DCS.

Logging has a crucial part to play in monitoring OT [57, 70, 58]. Whilst the resources within the devices often limit the maximum log size and can be overwritten as a consequence, the status updates from a device can be amended and either routed directly, or indirectly, to a central log that can maintain an overall record of the behaviour of the device. This allows for normal behaviour to be modelled, alerts to be generated for deviations from this behaviour, and provides a forensic analysis dataset.

Although these mechanisms provide a sound basis for defending the OT of an ICS, technology alone will not deliver the required results. It is necessary to define and enforce a set of risk, security, configuration and asset management procedures in order to ensure the operational activities of the plant or facility cannot be disrupted. In this respect many of the established and mature IT security standards that exist offer a basis for defining such procedures. The standards can describe the guidelines for what needs to happen in a defence-in-depth model, whereas the pragmatic approaches to IT and OT described above provide the limits and constraints of how these can be achieved. It is important that any policies that derive from this approach span both IT and OT, using expertise from each domain to take a holistic approach to security, modelling the people, processes and technology from end-to-end. Supporting this should be a rigorous approach to enterprise architecture, ensuring that every element of the business is modelled, and forming the basis for overall asset and change control.

In order for an enterprise architecture to be properly defined, the assets managed by the business must be identified. Historically this has proven to be a difficult task, especially for geographically-dispersed SCADA systems with many thousands of field devices [71]. Device scanning can expose the operation to unwarranted risk as it is common for devices to crash when having to deal with Internet Control Message Protocol (ICMP) traffic, for example [71]. A full audit of all devices must be undertaken when assessing an ICS's security, as must the physical protection of those devices if deployed outside of the organisation's main operating facilities [3]. Once identified, some means of capturing the current configuration of each device must be achieved, and procedures implemented that prevent uncontrolled change. If, as in the case of some devices, backup mechanisms are not an option, this capture of current configurations may be as simple as recording a PLC configuration, including its Relay Ladder Logic (RLL), and placing it within a configuration management system. In the event of a security incident, where a PLC or similar device is suspected of being compromised, it can be swapped out for a new device with the original configuration deployed whilst the original device is analysed.

This configuration management should also encompass patch management of devices. It has been seen in this analysis that patching presents a significant issue to ICS operators as the risk of change and potential to invalidate warranties deters many organisations from doing so. However, forward planning allows for testing ahead of deployment, discussions and agreements with vendors about the impact of patching, and contingency options such as rollback in the event of an issue.

A structure to approach the issues involved with ICS security are included in the ISA/IEC 62443 series of standards [72]. These define procedures for implementing secure ICS, providing guidance to asset owners, systems integrators, and equipment manufacturers. The document set was originally proposed by the International Society for Automation (ISA) as ISA 99, but was renamed to align to International Electrotechnical Commission (IEC) standards. The standards are organised into four categories:

1. **General:** *Provides the foundational concepts, models and lexicon to describe ICS, along with a set of security metrics and lifecycle.*

2. **Policies and Procedures:** *Addresses the aspects of implementing and maintaining an effective ICS security programme within an ICS operator.*

3. **System:** *Describes the requirements and design guidance for the integration of ICS into a secure architecture.*

4. **Component:** *Proposes the technical requirements of individual ICS components for vendors to incorporate into their products.*

IEC 62443 [72] provides a solid baseline for security, but requires the adoption of contemporary ICS components, or a significant re-working of existing ICS architectures to achieve its goals. This is likely to require significant financial investment as well as exposing an ICS operation to risks involved with change.

The UK Centre for the Protection of National Infrastructure (CPNI) ICS Good Practice Guide (2011) [73] takes US DHS best practice for ICS cyber security assessments and proposes this for adoption in the UK. In particular, it focuses on penetration testing and the processes for remediating identified vulnerabilities. Whilst it highlights the risks of such testing in ICS, it provides little advice for their mitigation.

3.4.5 Conclusions

IT security mechanisms offer the potential to increase the protection of an ICS if deployed according to best practice into those areas of the architecture that support such mechanisms. However, the deployment of these tools will not deliver the protection necessary to an ICS unless they are supported by end-to-end processes and procedures, along with measures deployed into the OT that are complementary to the IT mechanisms. IEC 62443 proposes a set of bast practices surrounding this, but requires substantial change to architectures to achieve its aims. The CPNI ICS Good Practice Guide recommends penetration testing as a means to assess security, but does not provide sufficient means to assure the ICS operation is not exposed to unnecessary risks as a result. In light of this landscape, ICS operators require a means by which they can express the risks they face to their continued operations in light of antagonistic cyber activities.

3.5 Measuring Risk

The term *risk* is often used when discussing the potential impact of a cyber attack on an ICS, yet risk may have many alternative meanings when taken in different contexts, such as business, national economics, or plant safety. In order to support rational decision-making to protect ICS from cyber attack it is necessary to develop a common vocabulary and definition of risk.

Risk is not uncertainty, nor is it a hazard. Rather, risk is a function of uncertainty and consequences, *Risk = f(Uncertainty, Consequences)*, and a hazard is a source of danger and exists as a source of risk. Risk to an ICS therefore includes the likelihood of converting a source of risk into damage, loss or injury. In order to mitigate the occurrence of a source of risk in an ICS, the hazard, one applies safeguards. Consequently, *Risk = Hazards/Safeguards*, but highlights that whilst we might reduce the risk through safeguards, we can never bring it to zero [74].

Expected Utility theory [75] also quantifies risk in terms of likelihood and loss: *R=Pr(c)C*, where *C* is the consequence in terms of negative impact to an ICS, and *Pr(c)* is the probability of a loss equal to *C*. When *n* independent events are possible, the risk is the sum of all expected values: $Pr(c_1)C_1+Pr(c_2)C_2+...Pr(c_n)C_n$. The consequences to an ICS can be measured in terms of lost revenue, productivity downtime, injuries and fatalities etc., but always in the same value as the risk itself [76], which requires a risk analysis to consider what the key measures are out the outset. However, when considering the probability and impact of loss as a quantitative measure, one should avoid describing risk as "probability *times* consequence". This definition is misleading, as in the case of a single scenario this equation would equate a high-impact low-frequency (HILF) scenario to a low-impact high-frequency (LIHF) scenario, which in the case of an ICS are clearly dissimilar and require differing mitigation strategies [74].

Another term often used in the context of ICS risk is 'vulnerability'. Conceptually, a vulnerability is a risk conditional on an event. Expressing an event as *A*, then *Vulnerability |A = Consequences + Uncertainty |occurrence of A* [77].

As we have seen, the two main factors of risk are the consequences *C* and the probability of *C*, *Pr(c)*. The probability of *C* can also be expressed as the measure of uncertainty *Q*. If we define a set of consequences of interest *C'*, we can express a general description of risk as *Risk description = (C', Q, K)* or alternatively *(A', C', Q, K)* where *K* is the background knowledge upon which *Q* and *C'* are based, including expert opinion, models, assumptions, datasets etc., and *A'* is the set of possible events. Consequently, a vulnerability to a given event can be expressed as: *Vulnerability = (C', Q, K |A)*. These definitions, however, are based upon the accuracy and coherence of the background knowledge K, on which the risk description is based [77].

Fenton and Neil (2012) [78] highlight the impact of K on risk assessment by describing the probability of an event as *P(A/K)*, demonstrating that at least some degree of subjective judgement is incorporated into an assessment, and that it is an expression of a *degree of belief* rather than an absolute value.

Cyber attacks on ICS are, to date, HILF events that lack validated datasets for analysis. This situation is similar to that faced by those responsible for quantifying the likelihood and impact of terrorist attacks, and as such it is worthwhile considering how such events are considered in terms of national security. Lewis (2014) [76] articulates threats in the context of risk as *Threat=Intent* x *Capability*, where *intent* is the propensity of an adversary to attack, and *capability* is a measure of an adversary's ability to launch a successful attack. The US National Research Council (NRC) [79], using models based on the US Department of Homeland Security (DHS) risk practices, also incorporates threat, but uses a wider definition not limited to antagonistic actions, and cannot be considered equivalent to Lewis' description. The NRC model incorporates T, vulnerabilities V, and capabilities C, as *Risk=TVC*. However, in a critical analysis of this approach in light of terrorist attacks, the NRC highlight that defining the values of T, V, and C poses a significant challenge as there is little validated data available and poor reliable knowledge of adversary behaviours. This data fits the Zio et al. (2013) [77] description of K. In this context the situation is similar to that of ICS. The NRC analysis highlights that an *intelligent adversary* who may seek to actively defeat defensive measures, causes T, V, and C to become interdependent, and as a consequence, risk becomes a factor of T, V, and C, therefore *Risk=f(T,V,C)* [79], but does not include any specific measure of antagonistic intent.

The level of uncertainty regarding both terrorist and cyber attacks requires us to consider what US Secretary of Defense, Donald Rumsfeld, in 2002 described as "unknown unknowns"[80], and how we might reduce this uncertainty. Kaplan and Garrick (1981) [74] proposed that a risk could be described by answering three questions:

1. What can happen? (i.e., what can go wrong?)
2. How likely is it that it will happen?
3. If it does happen, what are the consequences?

In order to answer these questions it is necessary to consider a set of outcomes or scenarios, which can be expressed as a triplet $\{s_i,\ p_i,\ x_i\}$ where s_i is the scenario description, p_i is the probability of the scenario occurring, and x_i is the measure of the consequences. A table of such risk triplets would describe the overall risk: $R=\{s_i,\ p_i,\ x_i\}\ i=1,\ 2 \ldots N$. However, this approach is limited by the finite set of scenarios described in the triplet. The actual list of scenarios is infinite, and as a result, any assessment made in this manner is based on incomplete data, as the model does not account for the scenarios not included in the analysis. A method for addressing this is to account for all of the scenarios not considered in the category s_{n+1}. The resulting risk analysis is now the set of triplets: $R=\{s_i,\ p_i,\ x_i\}\ i=1,\ 2...N+1$, which includes all of the scenarios defined, and provides an allowance for those not included. Whilst this might at first appear to be a contrived logical construct, it allows us to consider what probability we should assign to the residual category s_{n+1}. This allows us to contemplate the problem within a rational framework, and in particular, what elements of K are relevant, and what evidence exists for the scenarios of type s_{n+1} that, by definition, have not occurred yet but exist within the definition of A'. Ostrom and Wilhelmsen (2012) [81] list nine criteria for consequences to be considered in context of what could be viewed as s_{n+1} scenarios, in order to assess their credibility. They conclude that one should "never dismiss a consequence until it is proven not to be credible."

These methods of describing risk are dependent upon qualified data or expert opinion K, a known set of events A', an accurate quantification of probability ($Q,\ P_i$), and an ability to reduce the number of scenarios of type s_{n+1}.

We shall now explore the viability of quantifying these variables in the context of cyber attacks on ICS as a valid means of articulating risk.

3.5.1 Risk Techniques

The techniques discussed in this chapter result from a systematic review of decision science, ICS safety and counter-terrorism research, resulting in a subjective, non-exhaustive set of risk approaches based on the literature identified.

Probabilistic Risk Assessment (PRA)

Probabilistic Risk Assessment (PRA), also referred to as *probabilistic safety assessment (PSA)* and *quantitative risk assessment (QRA)* [82] is a scenario-based analysis methodology that systemises the knowledge and uncertainties about a system by answering the Kaplan and Garrick (1981) [74] three risk questions relating to what can go wrong, how likely is it, and what are the consequences? [82, 77]. The process identifies a set of undesirable *end states*, then for each state it defines a set of *initiating events* that describe disturbances to normal operation that can lead to the condition. Scenarios are then generated based upon sequences of events that start with an initiating event and conclude in an undesirable end state, allowing the evaluation of the probabilities of these scenarios using all available evidence, past experience, and expert judgement. The scenarios are then ranked according to their contribution to the frequencies of the end states, as well as the systems, structures and components that also contribute [82, 81]. PRA is typically employed for accident analyses in systems that are highly reliable and for which significant reliability data is available [83], whereas we are considering wilful, malicious cyber attacks. The techniques do not preclude such an assessment, and the steps involved would accommodate the consideration of an attack against cyber-physical systems such as ICS. The methodology allows for differing probabilistic methods to be employed during the analysis, including Bayesian networks, Monte Carlo simulations etc. [82, 77], in order to generate the probabilities of the scenarios. By itself, therefore, PRA does not provide a means to mitigate the lack of available and verified ICS threat data, previously described as K. As a scenario-based approach neither does it address those threats defined by the type s_{n+1}.

Bayesian Networks (BN)

Bayesian networks (BN) are based on the theory that belief is conditional and depends on mounting evidence that either contributes to a belief or refutes it. BN describes a belief system in terms of *conditional probabilities*, containing propositions that are either true, partially true, or false [76, 84]. The subjectivity that BN supports allows us to consider the probability of an attack without a frequentist approach to representative data. Using BNs we start with a hypothesis H and describe a *prior belief* about H expressed as $P(H)$. Using observed evidence E we can revise our belief about H in light of E and calculate a *posterior belief* about H by calculating $P(H|E)$ in terms of $P(E|H)$ [78].

BN are flexible risk analysis tools as they allow the degree of belief in a hypothesis, or a series of hypotheses, to evolve as new evidence emerges and allow greater detail to be derived over time. As such, BN offer the potential to reduce K, and allow for additional attack scenarios to be added to the model, thereby reducing s_{n+1}. However, given the lack of immediately available data regarding cyber attacks on ICS, consideration should be given to how data for BN analysis will be obtained.

Fault Tree Analysis (FTA)

Fault tree analysis (FTA) is a method primarily aimed at system safety and reliability, although as a technique used within ICS communities it may offer a valuable insight into the likelihood and impact of maliciously-caused equipment failure. It is a deductive analysis technique focusing on one error at a time, intended to ensure that all aspects of a system are identified and controlled in order to determine design aspects that could lead to potential failures [85]. The events are generally considered as Boolean representations, insomuch as they either will or will not occur [86]. FTA is often used as an element of PRA, but can be used independently. Fault trees are a graphical representation of the interaction of failures and other events in a system. The process begins by supposing that a particular failure occurs, then uses deductive logic to step through a system, considering the possible direct causes that could contribute to the condition, forming a graphical tree-like structure as the analysis progresses [81]. Once a fault tree has been developed, data regarding the failure rate for individual system components can be analysed either in series or parallel, through the application of logic gates, to estimate the likelihood of the failure event (referred to as the *top event*). The process drives the production of *cut sets* - the smallest number of system components that, if they all fail, will lead to an overall system failure, then assesses the probability of such failure [86].

According to Sutton (2014) [87], the quality of the failure rate data on which the method is based are often unreliable, and subjective measures often substituted. These measures are still considered of value as the method allows experts to contribute based on their experiences in a structured manner, and enables subsequent deeper analysis of areas where the data is deemed inconclusive. The approach has a reputation for being resource-intensive, requiring significant expertise in the system under analysis. Its resource requirements aside, FTA's major advantage is that fault trees can accommodate complex logical relationships and interdependencies between system components. It is less dependent on human thought extrapolation to recognise the effects of changes in system behaviours [86].

For the purposes of assessing the risk of cyber attack on ICS, the approach has some merit. By starting at a system failure, in our case a maliciously-caused failure, we can trace back through the components of an ICS, both OT and IT, to determine scenarios under which the events could occur. By focussing on system components and the chaining of events and connectivity to adversely affect them, as long as every system component is considered, it is likely that the set s_{n+1} will be reduced, although the method has no formal mechanism for measuring this. However, the approach is still reliant on expert opinion and qualified data, as expressed in set K. Fundamentally, the method is focused on predicting equipment failures rather than the behaviours of malicious actors. It offers no means of determining threat actor capability or target preferences, although it can contribute to a wider threat analysis process.

Event Tree Analysis (ETA)

Event tree analysis (ETA) uses the same mathematical and logical techniques as FTA, but considers the impact of a failure of a particular component through inductive reasoning. Like FTA, ETA can also be used within other risk analysis techniques such as PRA. Event trees model a sequence of outcomes which may arise after a particular *initiating event*, focusing on paths or scenarios that lead to failure. As such, ETA considers the three questions posed by Kaplan and Garrick (1981) [74] that form their risk triplet. Following each event, ETA considers the occurrence or non-occurrence of all other possible events, with probabilities calculated conditionally on all previous outcomes in the tree. The approach assumes that each event only has two outcomes; success or failure, although separate event trees can be developed for each initiating event [86, 81, 87].

ETA allows analysts to consider one path or scenario at a time, and offers some use when assessing the potential causes of an undesirable effect as it propagates through an ICS. This may facilitate the identification of unexpected system conditions. Like FTA, however, the approach is still reliant on expert opinion and qualified data K, and the subjective set of initiating events does not reliably reduce s_{n+1}.

Bow-tie Analysis

The Bow-Tie analysis method combines FTA with ETA by considering an undesirable event, then analysing deductively to the left using FTA, considering what could lead to the event, then analysing inductively to the right using ETA to consider the consequences of the event [87]. Whilst the approach does not address the shortcomings in respect of K, it may generate scenarios previously not considered, and as a result may possibly reduce the set s_{n+1}.

Attack Trees

Attack trees [88] consider the paths by which an antagonist would attempt to reach a particular target in a network, described as a root, with leaf nodes articulating the chain of attack surfaces by which the attacker could reach that target. As such, attack trees provide a similar analytic construct to FTA, ETA and Bow-tie analysis, and suffers from the same limitations in respect of K [86]. However, whilst FTA, ETA and Bow-tie approaches are primarily focused on failure scenarios, attack trees concentrate on malicious attempts to manipulate a system, so the combination of these methods may broaden the attack scenarios under consideration and potentially reduce the set s_{n+1}.

Monte Carlo Simulations

When assessing the potential for an attack on ICS, so far we have only considered those scenarios that we consider realistic. However, this bias does not address the set s_{n+1}. One option to attempt to reduce the set of unconsidered attack targets, and thereby reduce s_{n+1}, is to adopt a stochastic model that includes every element within the system. Monte Carlo analyses reflect the randomness of life, even in deterministic systems, by assigning each system element an initial operating condition and a probability of failure. A time sequence starts based on a given interval and a random number is generated for each element within the system. If the random number falls within a defined failure range, the system element transitions to a failed state. At the end of each iteration, the cut sets are analysed to determine the system's operability and availability and the results aggregated to produce an overall model of the system [87].

Monte Carlo simulations are resource-intensive and require long run times in order to achieve stable results. By itself it cannot determine the impact of a targeted cyber attack, but the technique offers a useful model as it considers all elements within a system in a random manner, possibly introducing failure conditions not previously considered, thereby reducing s_{n+1}. However, the assigned probability of failure requires expert knowledge, and as such forms part of set K. Monte Carlo simulations alone will not immediately address the qualitative improvement of K, but there is potential for using Monte Carlo simulations to feed BN analyses.

Markov Models

Another method to perform stochastic analysis is based on Markov models. These represent all of the possible states of elements within an ICS, against which it performs a series of transitions based on a defined time interval, or step in a batch process [87]. Each transition results in a system element either remaining in its current state, or moving to a new one. As such, the probability of transition from one state into another is dependent only on the current state, and not on the history of states that preceded it. This property is usually referred to as the *Markov property*. Where the future state of the system element is dependent upon both the current state and the immediate past state, it is referred to as a second-order Markov process, and so-on for further higher-order Markov processes [89].

The immediate transition between states may not accurately represent real-world considerations for ICS, where states are not binary and can introduce an indeterminate condition as large electromechanical devices execute instructions. That aside, Markov models offer similar benefits to Monte Carlo simulations, as assuming they model the complete system, may introduce failure scenarios to reduce the set s_{n+1}, and perhaps could be used in conjunction with BN analyses.

Failure Modes, Effects and Criticality Analysis

Failure Modes and Effects Analysis (FMEA) is an experience-based hazards analysis approach based on expert opinion and engineering standards. The accumulated knowledge allows hazards to be considered in light of experiential data and evaluated against *Recognised and Generally Accepted Good Engineering Practice (RAGAGEP)*. The method examines the ways in which equipment can fail and considers the consequences of such failures. Device criticality can also be analysed, in which case the method is described as Failure Modes, Effects and Criticality Analysis (FMECA). Importantly, FMEA/FMECA does not consider the causes of the failure, just the impact of its occurrence. Neither is it concerned with the sequence of events that led to the failure, or the actors or circumstances involved [87].

By focussing solely on failure modes and the resulting effects, without considering the path that led to the event, FMEA and FMECA allows scenarios to be considered based purely on impact. By itself the process will not address the quantification of risk of cyber attacks within an ICS, but as it is a commonly produced engineering artefact that many ICS facilities will already possess, it offers a means to qualitatively check the background data and expert opinion, K, used to inform the assessment process. By not limiting the impact of failure to potential cyber access routes, we may limit the set s_{n+1}. FMEA/FMECA should be considered in conjunction with FTA.

Hazard and Operability (HAZOP) Method

The Hazard and Operability (HAZOP) method is probably the most widely used hazards analysis method in industry. Its widespread use and acceptance has led to a large number of practitioners and supporting service providers. The method divides the system under analysis into nodes, each of which represent a section of the process that undergoes a significant change or transformation. Examples of nodes include pumps, reactors, heat exchangers etc. The information is generally extracted from plant piping and instrumentation diagrams (P&ID). The size of the node is a subjective decision based on the nature of the industrial process and may group devices or system elements together in order to consider an overall process change holistically [87].

A HAZOP analysis follows a consistent process whereby a system node is selected and its purpose and safe limits defined. Next, one of a set of *process guidewords* are selected, such as high flow, low/no flow, reverse flow, misdirected flow, high pressure, high temperature, polymerisation, wrong composition etc., that describe the effect that should be considered, and hazards and their causes are identified as a result. For each hazard, the process considers it will be recognised should it occur and an estimation of the consequences is reached. A set of safeguard requirements are then defined, as is the estimated frequency of the hazard's occurrence. Finally, the hazards are ranked and a set of findings and recommendations is produced.

HAZOP analyses drive a rigorous assessment of the impact of undesirable events on a process, decomposing to a detailed level. Conformance to established processes and guidewords should provide a comprehensive set of potential areas of risk. Whilst it may not be commonplace to consider these impacts from the perspective of cyber attacks, a HAZOP should identify areas where change to the process will result in adverse outcomes. The breadth of the process should reduce the size of the set s_{n+1} and by adhering to RAGAGEP, confidence in set K is arguably increased.

CARVER and MSHARPP

When considering the threat to an ICS, methods exist within the military community to describe an intelligent adversary's intent and capability. The US Department of Defense (DoD) use the CARVER assessment method to determine criticality and vulnerability in infrastructures. CARVER is an acronym for *Criticality, Accessibility, Recuperability* (a system's ability to recover from an attack), *Vulnerability, Effect and Recognisability.* The method focuses on an adversary's perspective of the infrastructure to enable an analysis of the weaknesses of a target, or the means by which its operations can be manipulated by an attacker [90]. In this manner, the capabilities of several threat actors can be considered. The output of the CARVER assessment is a critical asset list that defines a prioritised set of assets that are of value to an attacker based on their importance, whereby the asset's incapacitation or destruction would have a serious impact on the military operation or facility. The use of CARVER matrices to consider threats to critical national infrastructure by civilian agencies when preparing for terrorist attacks is emerging, as it allows organisations to consider the relative desirability of targets, although its use has been limited to the assessment of physical assets [91]. Another approach, encompassed in the acronym MSHARPP, describes the attractiveness of a target due to its importance to an operation (the *Mission*), the perception that a successful attack with generate (the *Symbolism*), the *History* of similar attacks, system *Accessibility*, *Recognisability* of target, impact on the local *Population*, and *Proximity* to other key assets. Like the CARVER approach, a matrix is derived using a numeric range that represents the perceived vulnerability or likelihood of attack, from the perspective of the defender. The respective numerical values are totalled to provide a relative value as a target or the overall assessment of attractiveness to an attacker, and thereby a prioritised list of assets to defend [90].

Game Theory

Studies of antagonistic attacks can be conducted using game situations rather than decision models [92]. Game theory techniques involving sequential multi-player scenarios such as *Stackelberg Competitions* allow players to decide upon actions that result in the best possible rewards to themselves whilst anticipating the rational actions of the other participants. The outcome of the game defines the optimal allocation of resources and investment to minimise risk on the part of the defender and maximise risk for the attacker [76, 93, 94]. In an evaluation of physical attacks against electric power networks using game theory, Holmgren et al. (2007) [92] illustrated the effectiveness of the technique, but highlighted the need for a greater understanding of the attacker's intent. It is possible that the use of CARVER or MSHARPP may address this issue in some way, as the attractiveness of a target may be used as a surrogate for intent. Holmgren et al. (2007) [92] also acknowledged a wider issue; that the results of game theoretic approaches depend upon how the scenario is framed, suggesting that it is dependent upon the set K and that s_{n+1} is not necessarily reduced by its use.

3.5.2 Deep Uncertainty

If the techniques discussed thus far do not provide sufficient means to address K and s_{n+1}, we are faced with the area of decision science referred to as *deep uncertainty*. Cox (2015) [95] describes three methods of combining models and datasets in order to reduce the levels of uncertainty:

1. Using Multiple Models and Relevant Data to Improve Decisions
2. Robust Decisions with Model Ensembles
3. Averaging Forecasts

Using Multiple Models and Relevant Data to Improve Decisions

When no validated data set is available, a *good* decision is one that assesses clearly higher and lower probabilities of undesired outcomes based on a combination of existing models that are consistent with available, albeit not directly relevant data. This combination of alternative models is described as the *uncertainty set*.

Robust Decisions with Model Ensembles

Cox (2015) [95] proposes that when faced with decision-making decisions with deep uncertainty, a technique that can be employed is to generate and analyse a large number of scenarios. Of these, a set that performs well by some criterion for most scenarios is more likely to also do well in reality, if reality is well-described by at least some of the scenarios in the uncertainty set.

Averaging Forecasts

Simple arithmetic averaging of results from different methods is reported to usually outperform an average of any single method, and by averaging across models one can reduce the error between forecast and subsequently measured true values [95].

3.5.3 Eliciting Expert Opinion

If no valid data is available to inform set K then Ezell et al. (2010) [96] recommend that the probabilities of different attacker options should be elicited from experts. However, expert opinion is not necessarily a viable replacement, and care should be taken with the validity of such judgement. In particular, Wallsten and Budescu (1983) [97] ask whether the probabilities elicited provide a valid measurement related to the frequency of the events? Merrick et al. (2015) [98] propose that calibration is one measure of validity. When an expert assesses the probability P, on what basis is the judgement that proposes that the event occurs $P\%$ of the time? Those who will act on the expert advice would assume that P should be close to the observed frequency of the event, $\hat{P}$. However, P is simply a measure of the expert's degree of belief [99], and in the case of cyber attacks on ICS, no data is available to adequately describe $\hat{P}$.

Merrick et al. (2015) [98] observe that a calibration curve formed by probability judgements is usually more extreme than the relative frequency of events, and as such, expert opinion may have a bias toward a negative perspective. Wallsten and Budescu (1983) [97] point out that when faced with judgements based on complex events, it is natural for humans to simplify the task by using heuristics, which also introduce biases into analyses. According to Hora (2007) [100] the quality of judgements is based on the background information used for the assessment, usually derived from their experience, and is reliant on the expert's ability to fuse this with other data sources. Merrick et al. (2015) [98] discusses three heuristic techniques: *representativeness* in which the probability is based on the similarity to other observed events, *availability* where humans overestimate the frequency of an event due to excessive media reporting, and *anchoring*, where humans adopt a starting position then adjust away from that in order to produce a probability. None of these methods serve to improve the accuracy of the expert opinion in order to inform the set K. However, Ravinder et al. (1988) [101] and Howard (1989) [102] demonstrate that decomposing complex scenarios into discrete events improves the overall calibration and reliability of probability judgements when eliciting expert opinion, and in this manner we may minimise the biases and errors introduced.

3.5.4 Analysis

PRA remains the de facto standard for risk assessment in large-scale critical facilities and provides an analysis framework that incorporates safety data and probabilistic methods such as BN and Monte Carlo simulations [76]. For the immediate future there does not appear to be a proven, viable alternative. Its strength lies in its scenario-based approach, which from the perspective of ICS cyber threats allows malicious activity across the electromagnetic spectrum to be included in the overall risk analysis. However, as ICS cyber attacks remain low-frequency events, details of what an ICS attack scenarios may look like are in short supply and as a consequence our ability to reduce the set s_{n+1} remains limited. PRA also requires expert opinion, which given the lack of quantifiable data on ICS cyber attacks leaves the background information K open to the biases previously described. As such, any PRA analyses undertaken using expert opinion should require that any attack scenarios comprise a set of discrete events that aggregate to form a potentially complex attack, rather than attempting to consider the incident as a whole. Sommestad and Ekstedt (2009) [103] have demonstrated some success in combining attack trees with Bayesian methods and expert assessment, but their analysis did not include the industrial processes under control or their safety characteristics, and as such does not address the holistic impact of a cyber attack on an ICS.

Red teaming and game theoretic approaches offer possible improvements on the use of expert opinions, but their efficacy is currently limited by the cross-discipline team of IT and OT staff, and a lack of common vocabulary and understanding, especially when industrial engineering is also introduced. In order to address this issue it will be necessary to describe the industrial processes and technologies using a language and framework understood by all disciplines. Without such an analysis model it is unlikely that a robust risk assessment could be produced.

Ultimately, however, the current options for assessing ICS cyber risk are limited by the available data, and accordingly we should consider how such a dataset can be produced.

3.5.5 Options for Developing a Qualified Cyber Attack Dataset

Risk analysis is an established discipline, but for quantitative methods to work satisfactorily they require a validated dataset. The limited qualified reports of cyber attacks on ICS do not satisfy this requirement, and as a consequence, risk analyses on ICS are currently dependent on subjective judgements and cannot adequately consider the breadth of attack vectors. The US DoD advisory group, JASON, argues that predictive models for rare events are unreliable [104], and like Ravinder et al. (1988) [101] and Howard (1989) [102], recommend decomposing the rare events into smaller, well-bounded problems that can be tested. The Idaho National Laboratory [105] suspended research into quantitative analysis into this field, in favour of subjective approaches more in line with the criteria found in the CARVER and MSHARPP models. Whilst data exists to define the risks of equipment failure in an ICS, the predicted rates of these events are based on deterioration rather than intentional direction. It would also need to be proven that safety cases have a direct relationship with security cases before using this data as the sole basis for cyber attack risk analysis.

Background Information

Central to the issue of providing qualified risk analyses of cyber attacks on ICS is the lack of available data, which we have referred to as the set K. Without validated background, those responsible for identifying vulnerable elements cannot elevate the investment priority in this area against other, more clearly perceived risks to the business, such as failure to meet regulatory targets, service outages through ageing equipment, and exposure to financial markets. As such, an essential first stage of improving the quality of K is to provide a means to portray the impact of HILF events in a manner recognisable to senior stakeholders. At a more detailed level, however, malicious behaviour data needs to be shared in order to allow ICS operators to gain a greater understanding of events that are indicative of potential or actual attacks. Threat intelligence sharing offers a key benefit to the whole ICS community as it allows a richer view of areas for protective analysis within an industrial operation. Bayesian networks are potentially of value in this analysis, as models for K could be constructed, tested and revised over time using threat intelligence data, thereby improving the quality of background information on which decisions are based.

Attack Vectors

The lack of available data also limits our understanding of attacker options and targets, resulting in the possibility that the set of unconsidered scenarios that we have referred to as s_{n+1} is unfavourable. Decomposing the scenarios into smaller, manageable analyses offers clear benefits, but we are still largely reliant on expert opinion to define the scenarios to begin with. Introducing Monte Carlo and Markov simulations to test all possible failure modes may add a degree of objective data to the analysis to challenge any cognitive biases introduced during the scenario construction. The wealth of safety information available, from HAZOP, FEMA, FTA and ETA, is potentially a sound basis from which to start these analyses, and would allow the consideration of the relationship between safety and security cases.

Intelligent Adversaries

Models developed for risk analyses cannot be static. Cyber attacks are conducted by intelligent adversaries who will change their approaches dependent on the security mechanisms deployed. Threat intelligence, Bayesian networks and game theoretic approaches will allow general attack behaviour to be modelled, not the specifics of an attack against a particular facility. In considering intelligent adversaries in the context of terrorist events, the NRC [79] recommend the introduction of Red Teams to probe the defences of an organisation. This may prove problematic in an ICS, as they may not be resilient to potentially destructive testing [3], and so some form of non-destructive testing is required. This does not, however, preclude red teaming as a viable concept should a safe, representative environment be made available for such activities. Sommestad and Hallberg (2012) [106] demonstrated how cyber security exercises, conducted on dedicated infrastructure, can generate valuable data for security research.

Non-destructive Testing Through Simulation

Many industrial facilities utilise simulation tools to model and predict the operations of the processes under control within an ICS. This forms an essential part of the operations of the facility, based on the steady-state behaviour of the process. These models could be revised to allow boundary conditions to be introduced to predict where potential negative outcomes can be generated [107]. The ICS elements responsible for controlling the boundary conditions could then be considered as a discrete, testable scenario. This could be used to develop synthetic environments, testbeds, or cyber ranges on which representative architectures could be deployed using a mix of virtualised environments and non-production physical devices. Attack scenarios by intelligent adversaries could then be exercised and the results fed into background information models. In order to support this, it would be necessary to produce an architectural model of the ICS that supports the description of attack hypotheses and vulnerabilities, including security events, state transitions, dependencies, and means to describe differing consequences in various measures (financial, production loss etc.).

3.5.6 Conclusions

Quantitative risk analysis does not provide the sole means of addressing the problem, and pragmatically, one may be forced to adopt a method best suited to the available data, or by the combination of partially-suited models, until a suitable critical mass of information can be derived.

Raising awareness of a threat is an acknowledged risk safeguard, as it is argued that through knowing that there is the possibility of a hazard, in this case a cyber attack, it poses less risk than if we have no understanding of its potential impact [74]. Experts within the ICS field bring domain knowledge to bear to raise awareness, but it has been observed through experimentation that a calibration curve formed by subjective probability judgements is usually more extreme than the relative frequency of events [98]. This limits the credibility of the information provided by such experts, especially in light of the low frequency of recorded antagonistic events. If senior executives within ICS operators do not believe they are potential targets for malicious actors, they will not prioritise cyber defences above competing requirements for investment budgets. Similarly, if managers and technologists do not understand which elements are likely targets for antagonists, they cannot prepare their defensive posture.

In light of this, we shall now review whether security education methods can provide the basis for raising awareness of cyber threats.

3.6 Cyber Security Education

The majority of educational programmes within the cyber security domain have been awareness campaigns [108]. These typically use lectures or presentations to articulate the issues surrounding advanced actors to a wide audience, with little tailoring to specific audiences. Results using this approach are mixed, with learning methods often designed from the perspective of the presenter, focused on delivering as much information as possible within the minimum time, instead of considering the audience and focusing on how to effectively transfer the information [109] [110]. Education theories propose that whilst the quality of the information delivering the message is important, it is not necessarily sufficient. Communication does not necessarily imply increased awareness of the part of the audience. Other influencing factors such as personal knowledge, beliefs, attitudes, perception and the efficacy of coping strategies can also have a substantial influence, as can social factors such as the responses of peers [108]. Even if training has delivered an immediate increase in understanding, it has been demonstrated that this does not necessarily reflect the long-term perspective of the audience [20]. The issue, then, is not the content of the cyber awareness programme, it is the nature of its delivery that must be considered.

We must therefore explore mechanisms to enhance didactic learning, or look to alternatives.

3.6.1 Serious Games for Experiential Learning

Experiential learning [111] is an educational technique based on the assumed importance of experimenting and involvement, proposing that active engagement in a scenario develops personal experiences that form the basis of understanding. Subsequent iteration of these experiences, followed by periods of reflection, promotes the formation of ideas, with the testing of these ideas solidifying the understanding in the mind of the participant [110]. Kolb (1984) [111] illustrates this learning cycle in Figure 3.3.

Serious Games are a form of experiential learning in which a mental contest is played in accordance with specific rules, that uses entertainment to deliver specific learning objectives [112, 113], encouraging the player to decide, choose, define priorities and to solve problems [110].

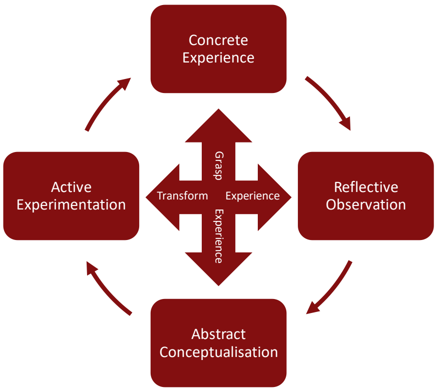


Figure 3.3: Kolb's experiential learning cycle (1984)

Whilst there are positive impacts of serious games [114], the results are inconclusive [109]. Experimentation suggests that serious games are more engaging and effective than presentations, although it is difficult to make generalisations about all serious games and presentations since the effectiveness of each learning method depends on the learning elements being included and the nature of the delivery [109]. One key observation from this experimentation, however, is that experiencing failure is an important element of learning, and that during a serious game, most of the learning occurred during debriefing when participants had the opportunity to reflect on their experiences, allowing them to develop the mental models of the situation, against which they could refine their understanding. Indeed, the results show that the more they experienced failure during the serious game, the larger the difference became in observed behaviour compared to those participants that only attended a presentation. Players predominantly experience failure when they are engaged and challenged to reach specified goals, where challenge improves the entertainment value and competition by creating barriers between the current state and the goal state. Feedback provides a tool for participants to learn from their previous actions and adjust them accordingly [115]. The opportunity to experience failure, therefore, and to reflect upon this during debriefings should be considered am element of an effective serious game, as should the definition of an end goal for the game.

3.6.2 A Review of Strategies to Influence Decision-Making

There are various personal, social and environmental factors that can influence risk awareness, decision-making and behaviour, and these interact in complex ways [108]. It is therefore not unsurprising that a number of models and approaches have been developed to describe how these factors interrelate to influence thinking and behaviour [108]. In this analysis, a subjectively-selected subset of approaches that appeared appropriate to shape the nature of serious games were reviewed.

The *Theory of Planned Behaviour* (TPB) proposes that beliefs and behaviour are interconnected [116], and that an individual's attitude, subjective norms, and perceived behavioural control, together shape their intentions and subsequent behaviour [117]. Their attitude is shaped by their beliefs about the consequences of adopting a certain course of action [116], whereas the subjective norms they perceive are influenced by those peers or seniors whom the individual considers important [116]. Perceived behavioural control is reflected in the level of governance an individual feels they may have in executing a certain behaviour or course of action [118]. Understanding threat perception is an important factor when considering how to shape an individual's attitudes [119], as well as ensuring that any influential messaging is underpinned by approval within an appropriate peer group [120]. The individual must perceive that they have an ability to influence the situation, or else their beliefs will not be translated into action [118].

Protection Motivation Theory (PMT) [121] postulates that individuals protect themselves based on four factors:

1. The perceived severity of the threatening event
2. Their perceived vulnerability or susceptibility to the probability of the occurrence
3. The efficacy of the recommended preventative behaviour (the 'response efficacy')
4. Their perceived self-efficacy

PMT has been described as an effective theory for predicting an individual's intention to engage in protective actions through its use of *fear appeals* [122, 123]. A fear appeal is a strategy for motivating people to take a particular action by arousing fear. Protection motivation stems from both a threat appraisal and a coping appraisal [108]. The threat appraisal assesses the severity of the situation, whereas the coping appraisal considers the individual's ability to respond to the situation. As such, the coping appraisal consists of both the efficacy of the response to the situation (the *response efficacy*), and the individual's ability to execute the response (the *self-efficacy*). Specific research into PMT in the cyber security domain [20] identifies further factors of the coping appraisal to include a cost/benefit analysis of carrying out the response, suggesting that the response efficacy must have some form of quantifiable return on investment.

The *Extended Parallel Process Model* (EPPM) [124] extends PMT and its use of fear appeals, to model an individual's reaction to a fear-inducing stimulus. EPPM proposes that when faced with such a stimulus individuals will either attempt to control the perceived threat through an assessment of its magnitude and consequences, or control their fear about the threat by assessing the efficacy of their ability to cope, whether through response efficacy or self-efficacy [125]. It is therefore important to balance a individual's perception of their ability to cope with a threat with their perception of their susceptibility to the threat. This ensures that they consider mitigating actions rather than just acknowledging that the threat exists [108], and take no further action.

TPM, PMT and EPPM all require an appreciation of the threat and an ability to cope with that threat. TPB highlights that an individual's peer group influences their perception of threat, and as such, educating the individual in a wider group of his or her peers may prove beneficial if the nature of the threat can be articulated effectively to, and acknowledged by, a wider audience. In the context of serious games, this leans toward multi-player environments. Both PMT and EPPM promote the use of fear appeals to develop mental models, and as such, it is appropriate for us to consider these in greater detail to determine their applicability.

3.6.3 Fear Appeals

Fear, the emotional reaction that may be aroused when a threat is perceived [126], is central to the motivational elements of PMT and EPPM, which use increased perception of a threat as a call to action. The principle is that when individuals are more cognisant of the risks they face, this should result in a greater level of engagement with the issue, ultimately resulting in some form of mitigating activity [127]. However, for fear appeals to be effective in a synthetic environment such as a serious game, we must understand what levels of fear are believable and appropriate. It has been observed that when the level of fear arousal increases from low to moderate, the level of persuasiveness of fear appeals increases [128]. However, with high levels of fear arousal, instead of accepting the position advocated in the fear appeal, individuals are likely to disengage rather than consider options to manage the threat [128]. Similarly, any fear appeal must also include strategies for self-efficacy and response efficacy to maintain the engagement of the audience and avoid disengagement [127].

For a fear appeal to be effective, it must satisfy four conditions:

1. The described scenario must be realistic and generate a low-to moderate fear reaction [128]
2. The message must be accompanied by specific recommendations on how to address the threat [118, 121, 124, 129]
3. The individual to whom the fear appeal is being addressed must believe the recommended actions will work [118, 121, 124, 129]
4. The individual must believe they have the ability to execute the recommended actions [118, 121, 124, 129]

These four conditions, therefore, should be considered within the overall characteristics of an effective serious game for experiential learning.

3.6.4 Characteristics of an Effective Serious Game

Central to any game is that players must have a meaningful decision-making experience during the gameplay - they must have *agency*. Agency means being able to act on your own behalf, or put in terms of behavioural change theory, being able to influence the situation through coping strategies. Players who can only make decisions that do not affect the state of the game do not have agency and are likely to disengage. The main characteristic of an effective game is where players are given agency in areas where they require it and to remove it in areas where they do not [130]. Of the many techniques available to give agency to players, the most useful is the introduction of a *trade-off* [130]. In a trade-off, the player is given two or more options, each with its own benefits and drawbacks, where players have to relinquish something of value in exchange for something else, and experience the consequences of their choices. Another effective decision-making technique is to offer options with less certainty and higher pay-offs pitted against options of high certainty and low pay-offs, referred to as a *risk-reward* choice [130]. However, too much choice can overload the player [131], resulting in a diminished player experience. An effective game, therefore, requires a range of choices sufficient to provide meaningful agency to a player and support trade-offs, but without too many choices to detract from the gameplay.

Game Theory

Game theory provides a theoretical framework for rational decision-making, but tends to deal with highly idealised problems where the payouts are clear, information is shared, and complexity is mediated to a reasonable level [130]. Its efficacy, however, is somewhat limited in real-world games where ambiguous situations are commonplace and no clear decision is preferable. Actual player behaviour can diverge from theoretical results and players may be influenced by irrelevant information that has no bearing on their likelihood of success [130].

Game Play

Successful games engage with players in terms of positioning their gameplay in the following five spectrums [132]:

1. **Collaborative to Competitive:** *The balance by which players are encouraged to adopt a 'winner-takes-all' mentality versus a collegiate approach to team success.*

2. **Intrinsic to Extrinsic:** *Defines how players are rewarded for their successes in the game.*

3. **Multiplayer to Solitary:** *The level to which players interact with each other, if at all.*

4. **Campaign to Endless:** *Describes the boundaries of the game, and whether it has a natural conclusion or can continue indefinitely.*

5. **Emergent to Scripted:** *Determines whether the outcome of the game is known, or evolves with the gameplay.*

Motivation

Intrinsic motivation that encourages players to draw their own conclusions [133] is more effective than extrinsic motivators such as points, badges, and achievements [130], although punishment for failure should be avoided [134]. Rewards, therefore, are not necessarily an effective motivator during a serious game, and intrinsic motivators such as competition and the desire to win may prove more beneficial. Adaptation, control, challenge, feedback and goal-setting are common elements of serious games.

Established Serious Games for Cyber Defence

Two serious games were identified in the literature as having established their utility for cyber education; CyberCIEGE and Tracer FIRE.

CyberCIEGE is a video game that presents students with computer security dilemmas within an environment that encourages experimentation, failure and reflection. The objective of the game is to demonstrate the functionality and limitations of cyber security mechanisms. Participants' adopt the role of a decision maker for a small business, making decisions within a three-dimensional office environment populated by game characters who require to access enterprise assets to achieve goals in order to progress through the scenario. An in-game economy rewards the player when users achieve goals, and punishes them for failure. Virtual assets within the game have associated motives that drive the game's cyber threats. Participants choices modify the system's vulnerabilities, thereby affecting the opportunity for the attacker to compromise the assets. The participant is penalised the value of an asset should it be compromised or made unavailable [135].

Tracer FIRE (Forensic and Incident Response Exercise) was originally developed to provide assurance that cyber forensic analysts remained current with respect to threats, tools and techniques. A Tracer FIRE exercise typically starts with a series of lectures relating to cyber security, followed by a multi-day competitive event. For the competition element, participants form teams that work collaboratively to solve challenge problems. The challenges are presented using a board layout with categories appearing in the columns and the number of points awarded for successfully solving challenges in the rows. Participants are provided identical computers and a standard suit of cyber security software tools that includes ENCASE Enterprise™, WireShark™, IDA Pro™, Volatility™, Hex Workshop™and PDF Dissector™. The challenge involves an attack against an organisation involving multiple adversaries who have differing motives, operating both independently and in coordination with each another. This is combined with individual challenges that must be solved, with each puzzle providing a clue to the overall scenario. The objective is to successfully complete the individual challenges to receive points, while simultaneously trying to determine the overall scenario. During the exercise, teams must allocate work across the members of the team, defining the order in which they work and the time they commit to individual challenges. At any given time each team member can work on an individual challenge, allowing teams to work on multiple challenges simultaneously. Points are awarded for successful submission of answers to each challenge, with point deductions for incorrect answers. The exercise concludes with teams presenting their explanation of the overall scenario [136]. Tracer FIRE has been used to measure human performance factors in cyber security forensic analysis [137], and incident response teams [138].

3.6.5 Analysis

Whilst some evidence exists to support the view that serious games offer a feasible means by which cyber education can be imparted, it remains difficult to make generalisations about all serious games. Understanding the nature of the training audience is essential, as personal knowledge, beliefs, attitudes, perceptions, peer group, and understanding of coping strategies all have a substantial influence. It is therefore essential to consider how the opportunity to fail is manifested within the game, and how this affects the participants. Not only must failure be seen to be acceptable, the associated periods of debriefing, reflection, and subsequent experimentation, must be linked to tangible frameworks to ensure appropriate mental models are developed by the training audience. The applicability of these models should be measured by their correlation to real-world cyber threats, so that any fear appeals employed by the game will be judged as realistic by the participants. Equally important is the nature of the response to the threats within the game. If the threats are to be viewed as contemporary, the responses to them must be correspondingly realistic. Accordingly, the provision of viable coping strategies that can actually influence the outcome of a real-world network intrusion must be considered an essential element of any cyber education programme.

Of the two established serious games reviewed, CyberCIEGE displayed many of the key characteristics of an effective serious game, such as experimentation, failure and reflection. The scale of its use suggests that serious games can deliver viable results for cyber education, but the scenarios observed were not reflective of a real-world, capable threat actor following an established network intrusion methodology. Tracer FIRE was designed to ensure cyber forensic analysts remained current with threats, tools and techniques, and to that end it provides the basis of a real-world problem space. However, the game is biased towards forensic analysis, and therefore deals with elements of an intrusion after the event. For an organisation considering how to proactively understand and its adversaries and defend against them, it offers few coping strategies. Neither of the games included ICS in their scope.

3.6.6 Conclusions

For serious games to be a viable mechanism to deliver cyber education that relates to real world cyber threat scenarios, the education must translate into a contemporary understanding of the cyber threat landscape and provide coping strategies that demonstrate an ability to protect an organisation and recover from an intrusion. For ICS environments, this must encompass the characteristics of industrial control and the consequences of a cyber attack on such services. Serious games should therefore be tailored to the audiences they are addressing. Whilst a technical audience will require a game that articulates the issues in a technical manner, a managerial or business leadership game should present the cyber threat in the language of business. The game should also allow the translation of the threat between the business and technical audiences through the provision of shared metal models, thereby improving communication between the two training audiences. A shared understanding will promote a common Observe, Orient, Decide, Act (OODA) decision loop [139] across the business and technical organisational units of an ICS provider. This shared situational awareness is therefore an area that requires further investigation as an element of a cyber education programme.

3.7 Situational Awareness

Capable adversaries that are characterised by sophisticated levels of expertise and significant resources are referred to as Advanced Persistent Threats (APT). Such APT actors use multiple attack vectors, such as cyber, physical, and deception, to create opportunities to pursue their objectives over an extended period of time and adapt to defenders' efforts to resist them, in order to achieve their objectives [140]. By their nature, APT attacks are covert and difficult to detect, and organisations such as critical national infrastructure (CNI) providers who present attractive targets to APT actors face a dynamic, evolving threat landscape. As a consequence, they carry an associated degree of business risk. Awareness of a risk is one of the main factors of a successful risk management programme [141]. By proactively raising awareness of threats and their impacts it poses less risk than if we have no understanding of its potential impact [74]. Situational awareness (SA) models potentially provide a framework from which risk managers can better understand the threat landscape, helping to shape the cognitive processes of incident responders, allowing the tailoring of risk mitigations to better fit the individual needs of the organisation requiring protection from APTs [142] [143]. Indeed, it is argued that a well-trained response team that understands the nature of the adversary is critical to success in responding to APT incidents [144].

Since incident response teams cannot prepare for every APT situation, or predict every crisis, training activities need to be provided to support operating in challenging situations to develop concrete guidance, procedures and tools to help individuals to collectively react in different, unpredictable situations [145]. To produce the level of team cohesion and adaptability required to respond to the variety of APT attacks an organisation might face, the training environment should include simulations to contribute to the progressive, cost-effective establishment and maintenance of situational awareness and skills proficiency [146].

SA, defined by Endsley (1995) [147], is *"the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future"* [147]. This definition comprises three levels of SA:

1. **Level 1 SA: *Perception of the elements in the environment.*** The initial step in achieving SA is to perceive the conditions, characteristics and dynamics of relevant elements in the environment [147].
2. **Level 2 SA: *Comprehension of the current situation.*** A synthesis of the disjointed Level 1 elements to form a holistic understanding of the environment and the significance of particular objects, events, or gestalt patterns [147].
3. **Level 3 SA: *Projection of future status.*** Integration of the characteristics and dynamics of the elements and comprehension of the situation (both Level 1 and Level 2 SA) to provide a projection of the future actions of the elements in the environment to support decision-making [147].

Team SA, as illustrated in Figure 3.4, is the degree to which every team member possesses the SA required for their own responsibilities, independent of any overlaps in SA requirements that may exist. It is not sufficient that one team member knows perfectly but the other not at all. Every team member must have SA for all of their own requirements [147].

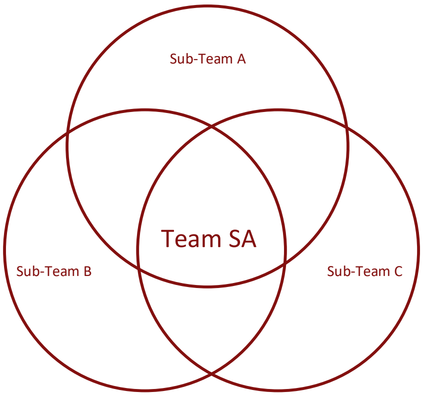


Figure 3.4: Team situational awareness, Endsley (1995)

A critical element of SA is understanding the rate at which information is changing, or how much time is available until some event occurs or some action must be taken. The dynamic nature of cyber incident response (IR) dictates that as the situation changes, so an individual's and team's situation awareness must also change or face being rendered inaccurate. In highly dynamic environments this requires operators to adopt many cognitive strategies for maintaining SA [148]. A common problem within the cyber security arena is the lack of viable analogies, or mental models, to help people assess the threats they encounter and maintain their SA [18].

Mental models allow people to predict and explain the behaviour of the world around them, to recognise and remember relationships among components of the environment, and to construct expectations for what is likely to occur next. Furthermore, mental models allow people to draw inferences, make predictions, understand phenomena, decide which actions to take, and experience events vicariously [149]. Shared mental models help members of teams to to understand the roles and responsibilities of other team members [150] and cope with difficult and changing task conditions [151] [152]. The ability to adapt is an important skill in high-performing teams, and a shared mental model is an essential element of a team's adaptability and SA. It allows team members to understand each others' task demands to predict what their team-mates are going to do, and what they require in order to do it. This requirement for shared SA is amplified in situations with excessive workload and time pressures [149, 153]. This manifests itself as four types of shared mental models, as proposed by Mathieu et al. (2000) and illustrated in Table 3.1.

Type of Model	**Knowledge Content**	**Comment**
Technology/Equipment	Equipment functioning, operating procedures, system limitations, likely failures.	Likely to be the most stable model in terms of content. Probably requires less to be shared across team members.
Job/Task	Task procedures, likely contingencies, likely scenarios, task strategies, environmental constraints, task component relationships.	In highly proceduralised tasks, members will have shared task models. When tasks are more unpredictable, the value of shared task knowledge becomes more crucial.
Team Interaction	Roles/responsibilities, information sources, interaction patterns, communication channels, role interdependencies, information flow.	Shared knowledge about team interactions drives how team members behave by creating expectations. Adaptable teams are those who understand well and can predict the nature of team interactions.
Team	Teammates' knowledge, skills, attitudes, preferences, and tendencies	Team-specific knowledge of teammates helps members to better tailor their behaviour to what they expect from teammates.

Table 3.1: Types of shared mental models, Mathieu et al. (2000)

Mental models are developed as a result of training and experience in a given environment. A novice in an area may have only a vague idea of important system components, and sketchy rules or heuristics for determining the behaviour he or she should employ with the system. With experience, recurrent situational components will be noticed, along with repeat associations and causal relationships [147]. Instruction should be structured such that new information or knowledge builds on existing knowledge. This facilitates the development of SA, as personnel are able to develop increasingly detailed mental models [154].

The requirement to develop experience-based understanding suggests experiential learning may provide a suitable vehicle by which individuals and teams can develop the mental models necessary for situational awareness in incident response situations.

3.7.1 Exercises for Experiential Learning to Develop Situational Awareness

Exercises are a proven method for delivering experiential learning [155]. The term 'exercise' is fairly broad, however, and represents many different types of activities from individual training through to large-scale, multi-team events, where teams can familiarise themselves with tools, procedures, and rehearse working together as a unit [156].

Whilst the concept and benefits of exercising are well-known and recognised [157, 156, 158, 159, 106, 160, 155], much of this is focused on table-top exercises (TTX) [158] and military exercises [161]. Exercises are typically scenario-based environments where there is a simulation of a conflict or competitive situation between a Blue Team representing the friendly forces, and an opposing Red Team as the antagonist [156]. A TTX is a facilitated, structured scenario-based discussion in which decision makers or responders work through a series of events or incidents in a low-stress environment. TTX are not intended to address all problems or policy, but are targeted on identifying areas that require resolution or further refinement. Their objective is both educational and developmental in that disconnects, perceptions, processes and procedures can be easily identified and then addressed [159, 162].

A more recent development in this field has been the emergence of cyber defence exercises (CDX) where a synthetic exercise environment is used to provide a representative network containing physical and virtual elements, referred to as a 'cyber range' [156, 157, 158, 106]. A cyber range presents a real-life situation or hypothetical security problem staged in a realistic manner, although typically in a condensed timeframe, against a Red Team who may adopt a range of techniques or intrusion set personas to improve the realism [157, 106].

Participants within a cyber exercising environment are usually described as members of one of four teams.

1. *Blue Team* comprises the exercise participants responsible for the defence of a

technology infrastructure from antagonistic actions. In a defensive exercise, the Blue Team are the primary learning audience [158, 163].

2. *Red Team* is the antagonistic counter-play organisation that attempts to disable or impair the functionality of the systems that the Blue Teams are protecting, by emulating an adversary's attack or exploitation capabilities against an enterprise's security posture. The Red Team's objective is to provide a controlled antagonist that delivers scheduled behaviours that the Blue Teams must defend against [158, 163].

3. *White Team* is responsible for the planning and management of the exercise, the development of rules of engagement, and the direction of the Red Team via an events list that is tied to the learning objectives of the Blue Team [158, 163].

4. *Green Team* provides and supports the technical exercise environment, ensuring it provides a suitable infrastructure on which to deliver the Blue Team training [158].

These exercises are forms of collective training, spanning any type of collective task from the simplicity of two people working together in different roles, to large complex tasks that span multiple teams and organisations and involve an integration of effort between them to achieve specific objectives [161, 164]. This differs from individual training, that focuses on the acquisition of skills for individual competence.

Military training emphasises a *'crawl-walk-run'* approach that begins with elementary tasks and progresses through stages with increasing complexity, to develop the training with progressive levels of realism [152, 165, 166]. This progression applies to both individual and collective training. Fundamental skills are acquired at the *crawl* stage, learning the individual components of the skill or task. During the *walk* phase, the components are integrated at a slower than normal pace. Finally, during the *run* stage, the skill or task is performed at normal speed in realistic conditions. This approach lends itself to the development of the mental models described in Table 3.1, as the progressive complexity of tasks will allow models to be refined using experiential learning to develop concrete experiences through reflection on performance, abstract conceptualisation, and active experimentation [111]. However, whilst the crawl-walk-run approach is applicable to both individual and collective training, personnel should have a sound understanding of individual roles and responsibilities before working in a group [151, 165].

The principal differences between individual training and team and collective training are associated with scale and complexity, and can be characterised by the [161]:

1. complexity of the task,

2. complexity of the context in which the task is conducted,

3. complexity of the start state of the training audience,

4. complexity of exercise planning,
5. complexity of the instructional task,
6. complexity of evaluation,
7. scale of resource requirements,
8. costs of training.

Traditionally, the crawl-walk-run model is applied sequentially through a series of training episodes. However, it has been demonstrated that providing progressive training scenarios that deliver crawl-walk-run training opportunities that are cumulative and grow in complexity, delivers far greater training benefit. Schaab and Moses (2001) proposed that by placing the responsibility for learning on the trainee, requiring them to solve problems during the scenario in a crawl-walk-run manner, experimental results demonstrate that their learning was accelerated when compared to traditional methods [152]. A comparison of the traditional and recommended methods using a crawl-walk-run model is shown in Figure 3.5.

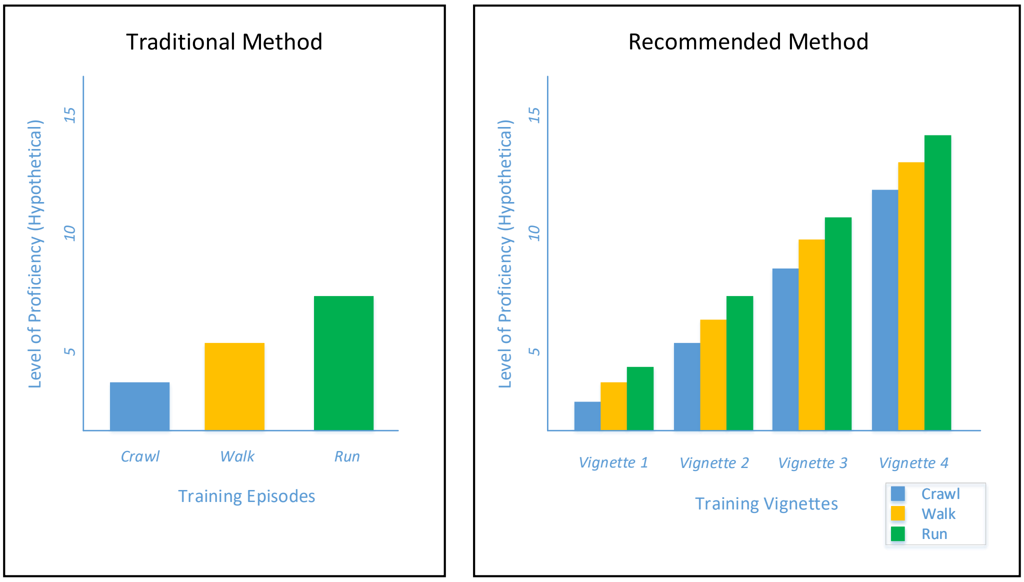


Figure 3.5: Traditional and recommended methods of collective training, Schaab and Moses (2001).

3.7.2 Analysis

Exercises are an established training mechanism for developing SA through experiential learning for military audiences. None of the literature reviewed suggested that prior military training was necessary for such education to be effective. Indeed, literature describing exercises in commercial and academic environments defines no such pre-requisites for the exercises to be successful. The mental models of Matheiu et al. (2000) [149] provide a basis to determine the scope of experiential learning for cyber SA in ICS environments across TTX and CDX. The models should support the development of shared understanding and situational awareness across business and technical audiences to ensure a common frame of reference to deal with an antagonistic actions against an ICS operation. The crawl-walk-run framework for exercises lends itself to an overall structure for progressive training, as well as progressively stretching participants within each exercise. No literature was identified in this review that articulated what such a training programme or framework would look like. Similarly, no literature reviewed fused the subjects of exercises, cyber SA, mental models, or progressive collective training.

3.7.3 Conclusions

The differing types of exercise allow for the delivery of many training scopes to a multitude of audiences. If properly designed, these could be complementary, and part of an overall training programme to build mental models. These models, however, must be equally developed for business and technical audiences in order to ensure a common frame of reference to deal with an antagonistic actions. This requires aligned scope for business-oriented training and technical training to develop not just functional cyber defence skills, but organisational processes and procedures to address APT activities. The scope should also provide a framework for progressive collective training, following the crawl-walk-run model, so that participants are incrementally introduced to more complex and challenging scenarios as elements of an overall education programme. In particular, this model should address collective training of incident response, both procedurally and technically, so that the first time an organisation experiences an APT attack is not the first time it impacts their organisation. As such, this requires us to further investigate the use of cyber exercises for such detailed training.

3.8 Cyber Exercises

We have discussed that the advantages of serious games lie in the provision of a safe training environment, where users are able to play, test and reflect without serious consequences. In a motivating, challenging environment, players acquire skills and knowledge that are transferable to real world tasks. It is this realism that makes serious games an appropriate training tool for SA skills [160, 158].

Exercises to reduce threats, risks, vulnerabilities and assess consequences in environments using ICS in CNI are vital in establishing a resilient society. The need, therefore, for exercises to train organisational leadership, management and incident responders are clear [158]. Exercises can be a powerful tool for training. If properly planned and executed, cyber exercises provide teams with the opportunity to prepare in a safe environment, to identify training gaps and demonstrate operational readiness. However, Kim and Goodall (2016) [156] point out that designing, planning, executing, and assessing cyber exercises is a poorly documented process. No standard assessment methodology has been employed across all cyber exercises, and there is no common lexicon for cyber exercise assessment.

Generally, cyber exercises have three different purposes [167]:

1. **Awareness:** *To conduct a cyber-exercise for awareness, bringing individuals together to make them aware of possible security incidents that their organisation might experience.*
2. **Education and Training:** *To prepare the individuals with the response techniques that they may require when dealing with security incidents.*
3. **Assessment:** *To test the ability to detect and respond in a coordinated manner in dealing with attack and cyber incidents.*

Cyber exercises allow participants to evaluate potential scenarios and determine their responses to the events. This can serve as both a situational awareness tool and business process model evaluation technique. Therefore collaborative cyber exercises are important aspect of cyber strategy in ICS and CNI protection. This promotes the collaborative cyber exercise as a platform for situation awareness training, incident information sharing, and cooperation in incident handling [167].

The educational benefit of cyber competitions across varying formats, including vulnerability assessments, forensic challenges, offensive and defensive competitions, or various combinations thereof, are well-established [168]. With defined goals, individuals or teams compete for some extrinsic award or recognition. Competitions that engender a cooperative learning environment within a team are more effective than individual competitions [168]. There is a significant amount of literature discussing the efficacy of cyber exercises as competitions [169, 170, 171, 168, 172, 173, 174, 106, 175, 136, 176, 177]. However, such competitions may misplace participant motivation to focus on winning rather than learning. A review of literature of 14 formal cyber competitions [168] noted that only one of the competitions had clear educational outcomes identified, and concluded that a lack of defined educational outcomes leads to incoherent training objectives and measures. As a result, consideration should be given to the rationale behind participating in such exercises [174].

One clear objective that exercises can provide is to produce data for cyber security researchers. The lack of empirical data makes it difficult to study the security of operational systems, but competitions that represent realistic attackers, defenders, and security processes may deliver tangible information for further analysis [106]. Sommestad and Hallberg (2012) proposed five topics that can be used as for experiments in cyber competitions [106]:

1. **The process model of an attack:** *An investigation of the steps taken by the antagonist.*
2. **The attributes of successful attackers and defenders:** *An assessment of the competencies of antagonists and defensive personnel.*

3. **The impact of security mechanisms on success:** *A measurement of the effectiveness of selected defensive strategies to support a defence-in-depth protective model.*

4. **The accuracy of detection and incident analysis methods:** *An analysis of incident response and forensic examination techniques.*

5. **The accuracy of security assessment methods:** *An assessment of the validity of quantitative metrics to assess vulnerabilities or weaknesses in a system.*

However, most of these competitions primarily focused on the technical characteristics of security such as memory corruption exploits, denial-of-service attacks, and detection capabilities of intrusion detection systems etc. The results lacked the properties to provide support for decision makers in an operational scenario, who must also test and develop security processes and procedures. It is this broader dataset that decision makers could potentially use to determine where to focus cyber security investment and develop a coherent defensive posture.

Berninger (2014) [178] proposed that cyber exercises could be used to provide an assessment framework to generate data for testing and measuring the efficacy of cyber mitigation methods, such that they can be used as the basis for the shaping of cyber investment plans.

In reviewing the nature of cyber exercises, two key aspects became apparent; *adversary understanding* and *progressive training*.

Adversary Understanding

In order to be able to successfully defend a network or system, it is useful to have an accurate appreciation of the cyber threat that goes beyond stereotypes. To effectively counter potentially decisive and skilled attackers it is necessary to understand their behaviour. Although the motives for attacks may remain unknown, a thorough understanding of their observable actions can still help to create attacker profiles to design effective countermeasures. These *attacker personas* have been used to assess the overall threat landscape for an organisation, and as such, form the foundation of any realistic cyber exercise [157]. In a study in which participants received either training that focused on the functionality of security software and its application in various situations, or a narrative description of software functions in the context of adversary tactics and techniques, it was noted that the narrative description allowed participants to accurately interpret intrusion events and contextualise them [179]. In particular, the study highlighted the importance of the ability of individuals to effectively work together during a cyber incident. Similarly, in an analysis of Red Teams in a small-scale ICS exercise, a team comprising ten individuals who had not met previously, were required to adapt to situations caused by Blue Team defensive actions, or as a result of errors and limited expertise [180]. The study concluded that by understanding how Red Teams cope with dynamic situations, that network defenders could better profile adversaries and anticipate their movements on a network, and that cyber range exercises were appropriate to produce this dataset.

Progressive Training

Cyber exercises must be progressively calibrated to the participants' level of expertise so that experienced personnel are sufficiently challenged, while ensuring inexperienced players are not overwhelmed. Exercises may allow participants to assume roles involving offence, defence or some combination thereof, while presenting extraneous events that simulate real-world operational demands. As a result, a distinction should be made between competition and training. Competition involves skills measurement of individuals, and perhaps, teams, whereas training concerns improvement in performance [136]. There is limited research documenting the cognitive and performance factors that distinguish novice from expert cyber security analysts, and is necessary to understand how to better structure the education and training of cyber security professionals [136]. A common challenge faced by researchers, however, involves gaining access to research samples for data collection activities, whether in controlled experiments or semi-naturalistic observations such as exercises. These events frequently entail semi-realistic challenges that may be modelled on real-world events, and occur outside normal operational settings, freeing participants from the sensitivities regarding information disclosure within operational environments.

3.8.1 Analysis

Cyber exercises allow participants to evaluate potential threat scenarios and determine their responses, to serve as both a SA development tool and business process model evaluation technique. If not overly competitive, this can be used to develop shared mental models in a collaborative manner. This is an essential element of any training programme, as the lack of empirical data makes it difficult to study the security of operational systems. Exercises with realistic antagonists, defenders, and security processes offers the opportunity to develop a tangible dataset focused on the needs of an individual ICS operator. However, to achieve this, exercises require clear training objectives, with an assessment methodology to determine whether these objectives have been achieved. These objectives may be technical in nature, but equally may be to test and develop security processes and procedures, or to capture data to cost-justify cyber security investment.

This requires significant planning on the part of the exercise planning and execution team, as exercises will require:

1. An understanding of Blue Team individual skills and collective training to date.
2. Detailed training objectives that progressively develop the participants' capabili-

ties, both individually and as a team.

3. Attack behaviours that are based on a real-world understanding of the threat landscape the exercise participants face in the real world.
4. A capable and disciplined Red Team to imitate the threat actors.
5. Realistic scenarios and supporting materials.
6. A representative exercise environment or cyber range.
7. A clear plan for the assessment of the exercise.

Most of the literature reviewed described how to run an *efficient* exercise, whilst very little was observed that discussed how to run an *effective* exercise. No literature was identified that focused on improving cyber SA and the development of shared mental models. Similarly, none of the literature encompassed the characteristics of the seven requirements above and their fusion into a coherent model for developing cyber SA and IR skills.

3.8.2 Conclusions

Cyber exercises appear viable as a means to develop shared mental models for ICS SA. However, these should be constructed as training programmes rather than overt competitions. This is not to say that competition has no place in these environments, rather it emphasises that competition should be linked to specific training objectives with tangible educational outcomes. Whilst failure is an essential element of learning, and competition provides mechanism for failure in a safe environment, without suitable time for reflection and experimentation it appears unlikely that suitable SA or mental models will be acquired. Exercises will need to be carefully planned, and fit within an overall framework of progressive collective training, for them to be effective. In particular, for incident response training, the framework will need to accommodate the varying levels of individual training of the exercise participants. It will also be essential for the incident response plans and processes of the organisation to be incorporated into the exercises, to maintain the necessary levels of realism, and also to test their applicability to real-world threat actors.

3.9 Incident Response

Preparing incident response processes, procedures and gathering data on an ICS is a critical initial stage in dealing with an incident. To facilitate the derivation of realistic scenarios, a series of circumstances should be modelled to represent the cause, the impact and what is necessary to contain and remediate the situation. A key preliminary stage in this overall approach is to determine the probable risks to a control system.

The Control Systems Cyber Security Self Assessment Tool (CS2SAT) [181] is a self-assessment tool methodology and tool to assist in the evaluation of the cyber-security risks for ICS and provide recommendations to mitigate vulnerabilities. This allows the ICS operator to consider best practices in addressing its perceived risks. The US DHS [182] highlight that the National Institute of Standards and Technology (NIST) has developed several guides and publications addressing cybersecurity, and that whilst they focus on traditional IT, they provide guidance that could be used to shape ICS incident response plans if the characteristics of control systems are considered. These publications include [182]:

- NIST SP 800-40 “Creating a Patch and Vulnerability Management Program”
- NIST SP 800-61 “Computer Security Incident Handling Guide”
- NIST SP 800-83 “Guide to Malware Incident Prevention and Handling”
- NIST SP 800-86 “Guide to Integrating Forensic Techniques into Incident Response”
- NIST SP 800-92 “Guide to Computer Security Log Management.”

Once the status of an ICS has been assessed, and the elements of the disaster recovery plan defined, and organisation should then consider the creation of a Computer Security Incident Response Team (CSIRT). The composition of the CSIRT will vary depending on the organisation’s size and structure, with responsibilities shared among different departments that have not traditionally provided support to the ICS or OT security teams. Vendor expertise can be sourced through service level agreements SLA with equipment providers, as can consultants or other specialists, especially where organisations have limited resources [183]. The scope and responsibilities of the CSIRT should include [182]:

- Providing expertise on threats and vulnerabilities to IT systems and ICS.
- Establishing facilities to serve as a clearing house for incident prevention, information, and analysis.
- Developing the policies and procedures related to incident response.
- Understanding the safety systems implemented in the ICS.
- Identifying operational impacts to the organisation in the event of an incident.
- Creating and testing the incident response plan.
- Developing the channels to act as a single point of contact for all internally reported or suspected incidents.
- Responding to incidents.

- Reporting to key stakeholders and external agencies during and after the incident.
- Gathering the forensic information to support analysis and any legal recourse.
- Implementing the safeguards to prevent a recurrence of the incident.
- Remediating the ICS after an incident.

As the range of incidents with the potential to impact an ICS are broader than traditional IT systems [3], it is necessary to document their nature in order to ensure that equal, or prioritised, consideration is given to all, so that a proper response can be formulated for each potential incident.

Whilst first responders in the physical and operational areas of critical infrastructure undergo rigorous training and evaluation, the same is not true for cyber incident responders. Similar levels of training, however, can be achieved through cyber range exercises, allowing the assessment of cyber incident responders [184].

As an element of incident response planning, organisations should assess their readiness in terms of availability of resources, both prior to an initial event, and during the average interval between the recovery time of an existing incident and the occurrence time of a new incident [185]. When responding to a network intrusion incident, evidence and analysis are required to determine if architectural and operational decisions affect adversary behaviour. Alongside this, Bodeau and Graubart (2013) [186] articulate the need for a vocabulary to describe the effects on cyber adversaries required to map cyber resiliency techniques to the different phases of an attack campaign, and by doing so, provide measures of defensive effectiveness against adversary activities.

The characteristics of effective performance amongst incident responders is not well understood. However, several social processes and dynamics that contribute to incident response effectiveness have been identified. A sophisticated, high-performing incident response team, it is argued by Tetrick et al. (2016), is a closely-connected, collaborative network of teams (or sub-teams) [187]. This manifests itself in ten areas of consideration when developing incident response teams [187], as described in Table 3.2.

1. Social maturity of the teams.
2. Methods of performance evaluation.
3. Decision-making processes.
4. Communication effectiveness.
5. Information sharing.
6. Collaborative problem-solving.
7. Understanding of team expertise.
8. Trust between teams.
9. Sustainable attention management and focus over time.
10. Continuous educations in incident response

Table 3.2: Ten development areas for incident response teams, Tetrick et al. (2016)

In research related to Tetrick et al. (2016) [187], it was identified that to improve the performance of incident response teams, a focus should be placed on SA, collective information processing, and forecasting [188]. Leaders, it was argued, can improve these processes using strategies such as pre-briefing, debriefing, simulations, and providing focused feedback.

Post-incident forensics offer an opportunity to incident responders to identify the nature of an attack and potentially prevent its recurrence. However, during an incident in an ICS, forensic opportunities to analyse evidence reduce as time goes by and volatile data is lost. Therefore, developing a forensic readiness plan is essential to determine which data sources are necessary to identify indicators of compromise, and calculating the available window of opportunity to exploit this information [189].

3.9.1 Analysis

Exercises appear appropriate to test and improve IR procedures in a variety of scenarios, especially in light of an adaptable adversary such as an APT. For ICS operators it allows IT and OT personnel to work together, developing individual and team skills. For those responsible for the development of incident response plans and procedures, it facilitates the testing of their efficacy. For a wider crisis management team that interacts with IR procedures, it allows the organisation as a whole to rehearse dealing with critical cyber incidents. However, none of the literature reviewed identified the requirement for developing mental models as an element of IR training.

3.9.2 Conclusions

Exercises provide a framework to improve the performance of IR teams' situational awareness, collective information processing, and forecasting, if they are suitably realistic and focus on the breadth of responsibilities that exist within incident management. As such, it is unlikely that a single exercise will provide sufficient coverage to address all of the issues likely within such a scenario. A range of incidents should be planned within a framework that progressively introduces complexity to the exercise scope. Alongside this, the framework will need to introduce a vocabulary to consistently articulate intrusion events in a manner that will be understandable to all parties concerned.

3.10 Intrusion Analysis

There are various frameworks in use to articulate APT intrusion behaviours on networks and systems. The frameworks are not mutually exclusive, and elements can be combined if necessary. Their primary benefit is a common vocabulary and level of reporting granularity that allows organisations to describe intrusion events, and forecast likely subsequent antagonistic actions.

3.10.1 The Diamond Model of Intrusion Analysis

The Diamond Model, defined by Caltagirone et al. (2013) [190], is an analysis framework that defines atomic intrusion events and describes the four core features of an antagonistic event, those being an *adversary* using a *capability* delivered over an *infrastructure* in order to target a *victim* and produce an outcome. This is illustrated in Figure 3.6.

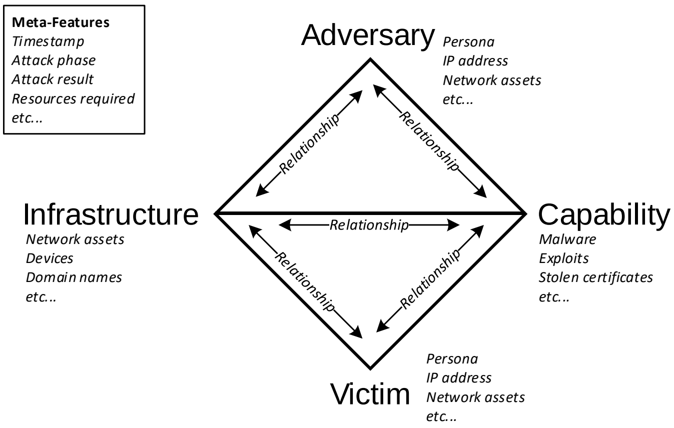


Figure 3.6: The diamond model of intrusion analysis, Caltagirone et al. (2013)

These core features, or nodes, are connected by edges that define the relationship between each. The nodes and edges are connected into a model that resembles a diamond. An intrusion event also has a number of meta-features that allow for further details of an intrusion event to be modelled. All attributes have an associated confidence level to allow for a weighting to be applied to decisions taken on the perceived accuracy of data. The advantage of the model comes from the ability to analytically pivot between the connected points on the diamond to reach other connected points. This means that common capabilities being used in different intrusion events can be correlated and identified.

A key component of the model is *Activity Threads*. An activity thread is a directed phase-ordered graph where each vertex is an event and the arcs identify causal relationships between the events along one or more paths. The arcs establish whether the path is AND (necessary) or OR (optional). Arcs can be actual (i.e. modelled during or after an event), or hypothesised, where future courses of action are predicted. The threads are organised vertically to describe all of the causal events an adversary executed, or may execute, against a specific victim, collectively aimed at fulfilling the adversary's intent.

Rather than being defined as a specific ontology or taxonomy for modelling attack behaviours, the diamond model is intended to be an extendable framework that can accommodate architectures and technologies as befits an environment. As a result, an event in the model is a variable-sized n-tuple that allows a basic tuple to be extended based on requirements. The basic diamond event, along with the standard victim definition, is depicted in Figure 3.7.

The Diamond Model provides a range of analytical methods to integrate threat intelligence and predict antagonistic actions. It models attacker courses of action, and assists with compensatory defensive activities once an intrusion has been detected.

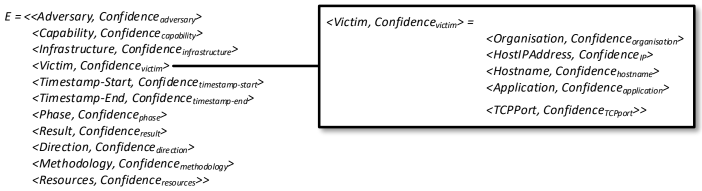


Figure 3.7: Basic diamond event and standard victim definition, Caltagirone et al. (2013)

3.10.2 Lockheed Martin Kill-Chain

Network defences can be improved by exploiting knowledge of adversaries by creating an intelligence feedback loop that establishes a position of information superiority and decreases the adversary's likelihood of success with each subsequent intrusion attempt. The Lockheed Martin™ Kill-Chain, proposed by Hutchins et al. (2011) [191], describes the phases of a network intrusion, correlating antagonistic behavioural indicators to defender courses of action, identifying characteristics that connect individual intrusions to broader intrusion set campaigns. Through this intelligence-led approach to defensive planning, the cyber security posture of an organisation can evolve at a tempo comparable to that of an APT.

The model describes seven stages of APT actions within a cyber attack [191]:

1. **Reconnaissance:** *Research, identification and selection of targets by antagonists, using open sources to determine suitable attack surfaces.*

2. **Weaponisation:** *The exploitation of the information harvested during the reconnaissance phase to tailor malware to the target environment.*

3. **Delivery:** *Transmission of the malware to the targeted environment to establish an initial foothold.*

4. **Exploitation:** *The manipulation of the device or environment in which the foothold was initially established, to escalate privileges or create a favourable situation for the continued covert execution of the malware.*

5. **Installation:** *The establishment of a persistent presence within the environment to maintain continued covert access and freedom to operate.*

6. **Command and Control (C2):** *The remote control of the malware from a C2 node typically outside the network boundary.*

7. **Actions on Objectives:** *Once persistence is achieved, the APT can progress to execute the objective of their actions, either to exfiltrate information, manoeuvre to another network, degrade or deny the operational capability of the environment in which they now have access, or any combination thereof.*

3.10.3 Mandiant Attack Lifecycle Model

Mandiant™ maintain an Attack Lifecycle Model [15] that characterises the steps involved in an APT intrusion, in a similar manner to the Lockheed Martin Kill-Chain. The Mandiant model describes an attack in eight stages:

1. **External Reconnaissance:** *Network scanning and associated research into the target organisation and systems.*

2. **Initial Compromise:** *The methods by which an attacker infiltrates the security perimeter of the target network.*

3. **Establish Foothold:** *Techniques and capabilities to establish two-way communications with implanted malware.*

4. **Escalate Privileges:** *The means by which an attacker elevates their permissions to a greater set of resources.*

5. **Internal Reconnaissance:** *Scanning and device discovery within the target network.*

6. **Move Laterally:** *Traversion of the target network across legitimate devices.*

7. **Maintain Presence:** *Ensuring continued control over key systems, nodes and devices.*

8. **Complete Mission:** *The execution of the intent of the attack.*

3.10.4 ICS Cyber Kill Chain

An ICS-specific kill-chain, developed by Assante and Lee (2015) [192], proposes that attacks against ICS requires an adversary to undertake a two-stage attack process. The initial *planning* phase comprises target reconnaissance, preparation, and the initial intrusion into an ICS network. The second phase, the *management and enablement* phase, establishes command and control of the payloads deployed on the ICS network and exploits them to achieve the ultimate attack objectives.

3.10.5 Analysis

The Diamond Model offers a rich set of analytical tools that can be used to anticipate antagonistic cyber activities, both before and during an intrusion. Although it does not directly provide support for ICS, its extendability suggests that such support is feasible. The ICS Cyber Kill-Chain provides a framework that considers ICS elements of a network, but there is little evidence of its adoption by industry. The Lockheed Martin model is widely used, but to be fully effective it requires details of how the adversary will 'weaponise' any gathered intelligence or capabilities. The Lockheed Martin Model has also been previously integrated with the Diamond Model. The Mandiant lifecycle is also adopted by various parts of industry, although at the time of review it had not been integrated with the Diamond Model.

No literature reviewed had integrated any techniques to proactively model a cyber attacker's courses of action prior to an attack, and use this as a basis for interpreting threat intelligence to determine a defensive posture prior to, and during, an attack on an ICS. Neither had any attempts been made to determine which elements of an ICS were likely targets for such attacks. These would be essential elements of overall cyber SA for an ICS operator.

3.10.6 Conclusions

The requirement to understand an ICS to sufficiently determine systems or processes attractive to an attacker provides a mechanism to determine the nature of a defensive posture. Fused with threat intelligence data, it will allow a forecast of potential adversary behaviour to be made prior to any intrusion events. Subject to a means by which an ICS's critical systems or processes can be identified, the Diamond Model offers a potential analytical framework to support a pre-incident analysis and maintain an assessment of antagonistic courses of action once an intrusion has been identified. Fused with one of the lifecycle models, this would provide a powerful SA tool for ICS.

3.11 Overall Conclusions

The defence of an ICS operation requires more than just IT security measures. It necessitates an understanding of OT and how it interacts with IT, and in particular how IT provides an attack surface to pivot onto OT. The issue is acknowledged in many published works, e.g. [27, 193, 194, 195], although the majority of these publications focus on technical mitigations. ICS security literature largely recommends significant changes to existing architectures, exposing the operator to the risk of change that has been at the heart of the issues surrounding security upgrades in general. Of pragmatic benefit to an ICS operator would be a process that allows the organisation to determine which of its systems and processes are critical to their operations, and as a consequence, which would be attractive to an attacker as a target of antagonistic cyber operations.

This should not be based on probabilistic risk models, as the dataset of these does not exist. No such process was identified in observed literature.

The process would require an understanding of the threat landscape to support the determination of where ICS operators should focus cyber security investment. This would require the organisation's leadership to acknowledge that APT actors may target their facilities and understand the circumstances under which this may occur. For the leadership of these organisations to act upon this understanding of the threat landscape, they will need to improve the quality of their background knowledge, K, and SA. In particular, as proposed by Bodeau and Graubart (2013) [186], a vocabulary will be required to describe the behaviours of cyber adversaries. Increased K and SA could be achieved by fusing the CARVER method [90] with an attack lifecycle such as the Mandiant™ Attack Lifecycle Model [15] or Lockheed Martin™ Kill-Chain [191], with the Diamond Model of Intrusion Analysis [190], to provide a framework for understanding the threat and developing a common vocabulary. The Activity Threads element of the Diamond Model provide an adaptive alternative to Bayesian Networks [76] or Attack Trees [88], in a framework that lends itself to cyber defensive planning.

This approach requires ICS operators to consider intelligent adversaries. The NRC [79] recommend the introduction of Red Teams to probe the defences of an organisation, but potentially destructive testing [3] is not feasible in such critical systems. However, Sommestad and Hallberg's (2012) [106] proposition that cyber security exercises, conducted on dedicated infrastructure, could be extended to include ICS. This would necessitate the fusion of industrial processes and technologies using a language and framework understood by all disciplines. This would support the improvement of background knowledge, K, and with continued exercising, potentially reduce the set of unconsidered scenarios s_{n+1}. However, as Kim and Goodall (2016) [156] point out, designing, planning, executing, and assessing cyber exercises is a poorly documented process. No standard assessment methodology has been employed across all cyber exercises, and there is no common lexicon for cyber exercise assessment. A means to assess the efficacy of cyber exercises is therefore required as a component of this process.

Serious games provide a vehicle by which a contextual understanding of the threats and impacts of antagonistic actions can be structured to develop a set of mental models to promote the development of K and SA. The use of 'fear appeals'[122, 123] within the games, using techniques derived from from PMT [121] and EPPM [124], offers a mechanism to engage participants and shape their understanding of the threat landscape. The development of background knowledge, K, should not be limited to individuals. It must be propagated across the entire ICS operation to anchoring enterprise-wide mental models that can be established across the leadership, management, technology, and incident response areas of a business. These games must be accompanied by coping strategies to ensure that participants' mental models are aligned to practical means to address the risks highlighted. These should be embedded within training programmes to progressively develop skills that are shaped by an understanding of the APT adversaries an organisation may face. These skills should not just be technical, they should also include the procedural and operational aspects of defending an ICS. The establishment of such enterprise SA and mental models to defend ICS from antagonistic actions was not identified in any literature reviewed.

Cyber and table-top exercises, as examples of serious games, provide a means to progressively develop an intelligence-led understanding of the adversary to drive enterprise-wide K, SA, and mental models. The flexibility of exercise frameworks allows a variety of dynamic scenarios to be tested, as well as the decomposition of complex scenarios into discrete events, as recommended by Ravinder et al. (1988) [101] and Howard (1989) [102]. This will provide a means to reduce the set of s_{n+1}. It will allow the various teams involved in IR to develop the cohesion and adaptability required to deal with the variety of APT attack behaviours they may encounter. This will require the training environment to include realistic simulations to contribute to the progressive, cost-effective establishment and maintenance of SA, and skills proficiency. The adoption of a 'crawl-walk-run' approach to training would potentially offer the most effective way to deliver this skills development in a limited timeframe [152, 165, 166]. No literature identified discussed this training in the context of cyber or ICS.

The reviewed literature does not address the six research questions posed in Section 1.4. The following three chapters describe the research undertaken to address these questions and establish cyber SA within ICS operators.

Chapter 4 - *The SCIPS Serious Game* - articulates the nature of a means to establish cyber SA within the leadership of an organisation, as well as form the basis for establishing a set of enterprise mental models to anchor corporate understanding of the cyber threat to ICS.

Chapter 5 - *The Industrial Control System Cyber Defence Triage Process* - describes a coping strategy that allows an ICS operator to identify which of its technology assets are likely targets for APT actors, and proposes a means to develop an investment strategy and set of incident response playbooks for an organisation to coherently respond to antagonistic actions on their networks.

Chapter 6 - *A Framework for Progressive Collective Training* - proposes an incremental model for cyber defence and table-top exercises to develop situational awareness, mental models, technical skills and operating procedures, to prepare for a targeted APT attack on an ICS operation.

Chapter 4

The SCIPS Serious Game

Contents

4.1 Introduction

Simulated Critical Infrastructure Protection Scenarios (SCIPS) was initially developed as a proof-of-concept by the author during his MSc project [196] to determine if it was possible to create a serious game that exposed personnel involved in the operation of ICS to a credible threat scenario in order to raise their situational awareness and promote an understanding of the challenges involved in cyber security investment. Although only implemented as a spreadsheet with some supporting materials, it provided encouraging results.

This section describes the thorough examination of the SCIPS proof-of-concept conducted during this research, and how it was re-evaluated and re-implemented as a component of the experiential learning framework described in Chapter 6.

The majority of this chapter has been peer-reviewed and published in the following:

- **Allan Cook, Richard Smith, Leandros Maglaras, Helge Janicke** "SCIPS: Using Experiential Learning to Raise Cyber Situational Awareness in Industrial Control Systems", International Journal of Cyber Warfare and Terrorism (IGI-Global), Volume 7, Issue 2, May 2017, DOI: 10.4018/IJCWT.2017040101
- **Allan Cook, Richard Smith, Leandros Maglaras, Helge Janicke** "Using Gamification to Raise Awareness of Cyber Threats to Critical National Infrastructure", Proceedings of the 4th International Symposium for ICS & SCADA Cyber Security Research (ICS-CSR 2016), Belfast, 23-25 August 2016,
DOI:10.14236/ewic/ICS2016.10

4.2 SCIPS

SCIPS raises cyber situational awareness through the use of fear appeals, played-out in a safe environment that promotes self-learning, intrinsically motivating participants and encouraging them to draw their own conclusions as a result [133, 197, 198]. Unlike generic cyber security awareness campaigns, SCIPS is intended for stakeholders protecting CNI organisations. Previous research into using serious games for cyber security education has focused on developing technical incident response skills rather than attempts to shift the perceptions of stakeholders impacted by such incidents [199, 200]. Elements of response planning training by the European Union Agency for Network and Information Security (ENISA) [201] included attempts to quantify the costs associated with cyber incidents, but did so at an operational level on IT systems, with financial impacts that could be mitigated through the purchase of insurance policies [202] and could therefore potentially be de-prioritised by an executive of a CNI facility facing competing demands for large-scale investment. In order to express the issues of cyber attack on CNI to the game's audience the scenarios illustrate an effect on the strategic viability of a critical infrastructure business. The game specifically focuses on the strategic risks facing a CNI facility, playing through scenarios in which participants experience the financial implications of a cyber attack on an ICS. Instead of an arbitrary abstract measurement of cyber defensive success within the game, SCIPS uses the currency of shareholder value and market sentiment [203]. It demonstrates that antagonistic actions by a capable threat actor have the potential to severely degrade share price in a publicly-quoted company. Players are required to balance the competing priorities of shareholders and regulators with security requirements to defend against a credible cyber threat. Each investment has a financial impact with associated trade-offs, but can protect revenues that result in maintained share price and projected dividend payments to investors, thereby promoting risk-reward considerations.

4.3 Problem Statement

To bound the scope and objectives of the SCIPS game, a set of five overall high-level requirements were produced to guide the analysis and development process:

1. Produce an educational game targeted at stakeholders to raise awareness of the business-level impact of cyber security incidents. The players will be assumed to have minimal ICS or IT security knowledge, but will understand the general objectives of a business.
2. The game and its purpose should be understandable in a reasonable amount of time (15 mins) and should not require detailed knowledge or previous experience.
3. The game should not follow a strict path and should keep the players focused on a scenario where there are no immediately apparent winning solutions.
4. The game should encourage debate within a team and promote competition between teams.
5. The game should allow the development of new scenarios and gameplay options, so that it can be repeated without significant re-working of the components.

4.4 Game Design Options

In order to achieve the game's objectives, the requirements were reviewed against gameplay options, the medium of the game, and the nature of the game design.

4.4.1 Gameplay

For the game to appeal to the target audience it was necessary to ensure that the nature of the gameplay lent itself to the players and the promotion of learning through self-discovery. An initial investigation reviewed the gameplay activity options defined by Knapp (2013), as described in Table 4.1.

4.4.2 Game Medium

The medium of the game play was analysed against the learning objectives and problem statement, again using definitions described by Knapp (2013), illustrated in Table 4.2.

4.4.3 Game Design Approach

The gameplay and medium were considered in context together, resulting in the assessment matrix shown in Table 4.3. Whilst subjective, the matrix highlighted that *role playing* and *exercises* offered the closest fit to providing a platform on which to

Matching:	In a matching game the player must match one item with another.
Collecting/Capturing:	Where the goal is to acquire a certain number of objects. The player with the largest collection wins.
Allocating Resources:	The player is required to balance the allocation of resources in order to achieve a working equilibrium. There is no competition with other players in this approach.
Strategising:	A player allocates resources in a similar manner to an 'Allocating Resources' game, but is in competition with other players.
Building:	Players try to create objects out of given materials.
Puzzle Solving:	Players are required to solve a puzzle.
Exploring:	Players interact with an environment looking for objects of value.
Helping:	Involves one player assisting another player to accomplish a task.
Role Playing:	The player assumes the role of another person, with their responsibilities defined within the confines of the game.

Table 4.1: Options for gameplay, Knapp (2013)

Board Game:	A turn-based approach with players moving around a predetermined route through roles of dice.
Role Playing:	A board-less, dice-based model where players interact with a facilitator who has a predetermined number of options for the players to explore.
Exercise:	A scenario is presented with boundary conditions in which players can manoeuvre freely.
Single Player PC Game:	An automated environment where players interact via a programmed interface with an algorithmic opponent.
Multi-Player PC Game:	Similar to the single-player approach, but pitching player against player rather than an algorithm.

Table 4.2: Options for game mediums, Knapp (2013)

address the overall problem statement and learning objective. The decision was taken to combine the two approaches in an exercise format that requires players to adopt leadership roles typical of a critical infrastructure facility running ICS operations. To derive a scenario under which a cyber attack on a critical infrastructure facility would appear feasible, it was decided to construct a fictitious sequence of events based around UK foreign policy and military intervention in a fictitious country, with a nation-state adversary that possesses an indigenous offensive cyber capability [204, 205].

	Board Game	Role Playing (facilitated model)	Exercise	Single Player PC Game	Multi-Player PC Game
Matching	*Gameplay did not lend itself to self-learning*	*Gameplay did not lend itself to self-learning*	*Gameplay did not lend itself to self-learning*	*Gameplay did not lend itself to self-learning*	*Gameplay did not lend itself to self-learning*
Collecting/ Capturing	*Gameplay was too focused on a predictable outcome*	*Gameplay was too focused on a predictable outcome*	*Gameplay was too focused on a predictable outcome*	*Gameplay was too focused on a predictable outcome*	*Gameplay was not viable in a head-to-head player environment*
Allocating Resources	*Difficult to allow players to allocate resources in a fixed board model*	Viable: Players could adopt a role, but limiting the playing time and scope of decision making could prove difficult	Viable: Players could face a given scenario and attempt to reach equilibrium of resources. However, a non-competitive environment may not be appropriate for senior executives	Viable: Players could face a scenario, but the algorithm-based approach without other player interaction would limit opportunities for self-discovery	Viable: Players could face a scenario and play head-to-head. However, the computer environment would require game-playing literate competitors and may stifle debate
Strategising	*Strategising on a board game tends to extend the time required to play*	Viable: Although limiting the scope of the decisions available to players may prove challenging	Viable: Allows for competitive decision-making in a limited scenario. However, constraining the scope of the decisions to those appropriate to the game may prove challenging	*The available development time would not fit into the project timescale*	*The available development time would not fit into the project timescale*
Building	*Gameplay did not lend itself to problem statement*	*Gameplay did not lend itself to problem statement*	*Gameplay did not lend itself to problem statement*	*Gameplay did not lend itself to problem statement*	*Gameplay did not lend itself to problem statement*
Puzzle Solving	*Gameplay lends itself to reaching a predetermined outcome, which is not appropriate*	*Gameplay lends itself to reaching a predetermined outcome, which is not appropriate*	*Gameplay lends itself to reaching a predetermined outcome, which is not appropriate*	*Gameplay lends itself to reaching a predetermined outcome, which is not appropriate*	*Gameplay lends itself to reaching a predetermined outcome, which is not appropriate*
Exploring	*Gameplay did not lend itself to problem statement*	*Gameplay did not lend itself to problem statement*	*Gameplay did not lend itself to problem statement*	*Gameplay did not lend itself to problem statement*	*Gameplay did not lend itself to problem statement*
Helping	*Gameplay did not lend itself to problem statement*	*Gameplay did not lend itself to problem statement*	*Gameplay did not lend itself to problem statement*	*Gameplay did not lend itself to problem statement*	*Gameplay did not lend itself to problem statement*
Role Playing (assuming a role or persona)	*Role playing on a predefined board game did not appear feasible*	Viable: Role playing would limit the scope of the decisions available to players, but overall game scope management would be challenging	Viable: Role playing would limit the scope of the decisions available to players, but overall game scope management would be challenging	*The available development time would not fit into the project timescale*	*The available development time would not fit into the project timescale*

Table 4.3: Game options assessment matrix

4.5 Player Experience Design Process

To drive the gameplay through the player experience, a seven-step development process from Burke (2014) [132] was adopted. These steps, and the decisions taken therein, are illustrated in Figure 4.1 and described below.

4.5.1 Outcomes and Success Metrics

In the process defined by Burke (2014) [132], the intended outcomes and measures of success must be defined at the outset to ensure the subsequent design steps adhere to the intentions of the game and player experience. As such, it was defined that the intended outcome of playing the game would be that participants realise that:

1. There are circumstances under which a cyber attack could impact a CNI facility.
2. The drivers for the attack may come from actions beyond their control.

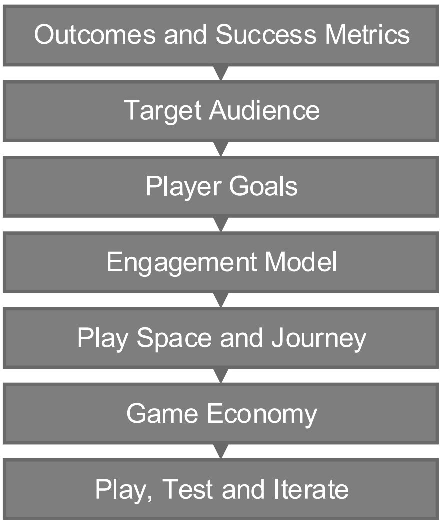


Figure 4.1: Player experience design process, Burke (2014)

3. Cyber attacks can have a direct impact on share price and shareholder value.
4. Investment in cyber security before an attack is the best way of preparing for this potential situation.

4.5.2 Target Audience

The game is intended for stakeholders involved with the protection of CNI organisations. Typically these should be participants who, during the course of their normal working activities, would not be required to balance investment decisions or interface with shareholders. In this way, technical personnel are exposed to business issues, thereby broadening their enterprise understanding.

4.5.3 Player Goals

In the SCIPS game, players are required to make a series of investment decisions based around the maintenance of a CNI facility that operates ICS equipment. In the initial version of the game this is based around an electric power generation plant. Subsequent implementations of the game are planned to address other industries within the CNI sector, supporting a broad spectrum of cyber-related scenarios.

Players are required to balance the competing priorities of shareholders and regulators with the security requirements to defend against a credible cyber threat. Each investment has a financial impact with associated trade-offs, but can protect revenues that result in maintained shareholder value. Players of the game adopt one of five roles within an organisation that operates a Combined Cycle Gas Turbine (CCGT) electricity generation plant. Their objective is to maximise shareholder value, expressed as share value and anticipated dividend per share. The winner is the team with the highest share value, and the loser is the CEO of the team with the lowest share value.

The business objectives of the game are to meet, as closely as possible, the investments stated in their annual report and to maintain market confidence. Figure 4.2 illustrates how the shared goal of each team is to maximise the share price, whilst individually, players try meet personal goals by preserving their bonuses which are impacted by the reallocation of funds within the business.

The exception to this is the Security Director. To create a player role who was more likely to champion the required security investments it was decided that the Security Director would have no bonus, and therefore have no external influences on their behaviours when considering the need for cyber protection mechanisms.

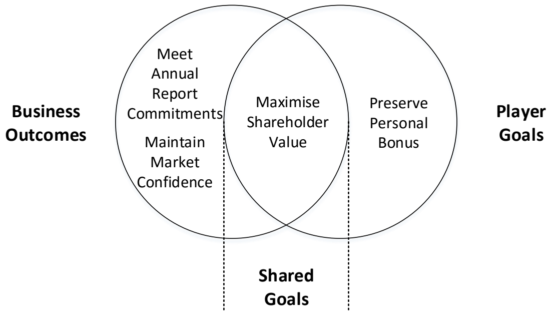

Business Outcomes
Meet Annual Report Commitments
Maintain Market Confidence
Maximise Shareholder Value
Preserve Personal Bonus
Player Goals
Shared Goals

Figure 4.2: SCIPS player goals

4.5.4 Engagement Model

Burke (2014) [132] describes the ways that games engage with players in terms of positioning their gameplay on the following spectrums described in Table 4.4.

Figure 4.3 illustrates the current SCIPS engagement model, shown as black circles, and the extended engagement model that potential further iterations of the game framework will support, as white.

The SCIPS game is essentially *collaborative* with intra- and inter-team *competitive* elements that drive debate between players about how to reallocate budgets in order to mitigate the cyber threat. Each round of the game is time constrained to drive instinctive behaviours from the executives participating [206]. A leader board is maintained throughout the game so that teams can see where their share price sits with respect to other teams.

Collaborative to Competitive:	The balance by which players are encouraged to adopt a ‘winner-takes-all mentality’ versus a collegiate approach to team success.
Intrinsic to Extrinsic:	Defines how players are rewarded for their successes in the game.
Multiplayer to Solitary:	The level to which players interact with each other, if at all.
Campaign to Endless:	Describes the boundaries of the game, and whether it has a natural conclusion or can continue indefinitely.
Emergent to Scripted:	Determines whether the outcome of the game is known, or evolves with the gameplay.

Table 4.4: Game engagement models, Burke (2014)

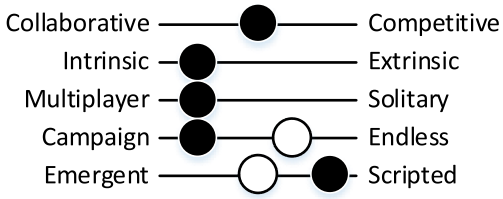


Figure 4.3: SCIPS player engagement model

Rewards within the game are *intrinsic*, focused on maintaining the fictitious organisations’ financial targets and the personal compensation packages of the player roles within each team.

The game is *multiplayer*, with multiple players within teams, and multiple teams. Players primarily interact with the other members of their team, but are influenced by the financial performance of the other teams via the leader board.

The flow of the game follows a *campaign* that models a series of incidents based on a typical cyber attack adversary lifecycle or ‘kill-chain’ [191]. Versions of the game planned for later releases will support a shift in gameplay towards an *endless* model based on attacker-defender [79] games that will support cyber warfare and ‘capture the flag’ functionality.

The current iteration of SCIPS is *scripted* to provide a credible scenario that leads to the cyber attacks. The initial version uses a US-UK coalition intervention in an overseas conflict to underpin the emerging cyber threat, and alternative scripted scenarios are also under development following a discussion between De Montfort University and the UK Computer Emergency Response Team (CERT-UK) [207]. Additionally, later versions of the game will support more emergent scenarios such as attacker-defender models.

4.5.5 Play Space and Game Journey

Play Space

The play space of the game is based around a game board, role cards, security cards, video feeds, newspaper 'cuttings', a tablet player interface and an overall leader board. All of the components of the play space interact, using a mix of soft and hard (physical) game play elements.

Game Board
The game board provides an illustration of a CCGT power plant to set the scene for the players, and to act as a focal point around which they can gather. It provides placeholders for purchased *security cards* to act as a quick reference for their increasing defensive capabilities.

Role Cards
The role cards, picked at random by the players, describe their responsibilities within the organisation and their compensation packages.

Chief Executive Officer (CEO): Ultimately responsible to the shareholders of the organisation and likely to see the cyber threat as an ongoing risk, but not an immediate priority that will affect the share value of the business.
Chief Operating Officer (COO): Responsible for the operations of the facility. The COO is likely to be aware of the possibility of a cyber threat, but likely to see the requirement for high availability and reliability as a higher priority issue.
Compliance Director: In regulated markets the Compliance Director will be responsible for ensuring that all regulatory and legal mandates are met. The role holder is not likely to focus on the cyber threat unless it corresponds to a stated requirement.
Plant Director: Responsible for the day-to-day operations of the facility and likely to report to the COO. The plant director will have detailed knowledge of the OT and the risk of any modifications or testing on plant operations. However, the Plant Director is also likely to be closer to the issues surrounding OT and the reality of the cyber threat.
Security Director: Responsible for IT and OT security and required to balance the management of both, although is unlikely to have the mandate to enforce changes on the operational environment.

Security Cards
The security cards within the game are configurable depending upon the scenario adopted. The initial version of the game uses the following:
External Firewalls: Protects the network perimeter and will limit the deployment of malware.
Email Filters: Detects potential phishing attempts.
Anti-Virus: Installs regularly updated anti-virus software to contain attempts at malware propagation.
Intrusion Detection: Identifies abnormal behaviour on networks and servers and

alert systems administrators to potential malicious cyber activity.

Virtual Private Network: Securely extends the network to trusted business partners, preventing attackers from intercepting and manipulating data to deploy malware.

Deep Packet Inspection: Monitors the traffic flowing into and out of the network to identify malicious activity.

Risk Assessment: A comprehensive analysis of the threats to the business, their likelihood and subsequent impact on operations to quantify the exposure the organisation has to service disruption through security incidents, and to allow the development of a qualified security plan.

Server Hardening: Disables all non-essential services on servers that expose known security vulnerabilities.

Patch Management: Initiates a programme to determine the current patch levels required for all devices and implements a pre-deployment environment to test them, ensuring they will not adversely affect operations.

Penetration Testing: Starts an ongoing penetration test regime to regularly test the environment for security vulnerabilities.

Operational Technology (OT) De-Militarised Zone (DMZ): Installs a DMZ between the IT and OT networks to minimise the risk of malware deployed in the IT environment propagating to industrial control systems.

Incident Response Process: Initiates an enterprise-wide programme to analyse the cyber threats to the business and develops plans to address them.

Segment IT Networks: Structures the IT networks of the organisation so that traffic is limited to the areas it needs to traverse, and limits the ability for malware to route to wider systems.

Create an IT/OT Security Team: Pulls together a team of experienced professionals from both the IT and OT domains in order to consider and defend the organisations technology assets from cyber attack in a coordinated, holistic manner.

Profile OT Traffic: Initiates a programme of OT traffic capture and analysis so that intrusion detection systems can be configured to recognise abnormal activity on the OT network.

Limit User Account Permissions: Implements a policy of enforcing the least privileges required for each user account, so that users only have access to the information they require, thereby limiting the ability of cyber attackers to access data and services.

Document Operational Processes: Produces a comprehensive set of documents that define the operational processes of the ICS systems and the control equipment that underpins them to determine which are critical to maintaining operational capability, and determine measures to mitigate the impact of their loss.

Limit External Accesses: Implements a process of continual review of external accesses to the network so that connections are only permitted from trusted partners and only allowed to exist for the minimum time required.

Protect Designs: Identifies all of the intellectual property and documentation key to the operational business and re-locates this to a repository where access is limited and audited.

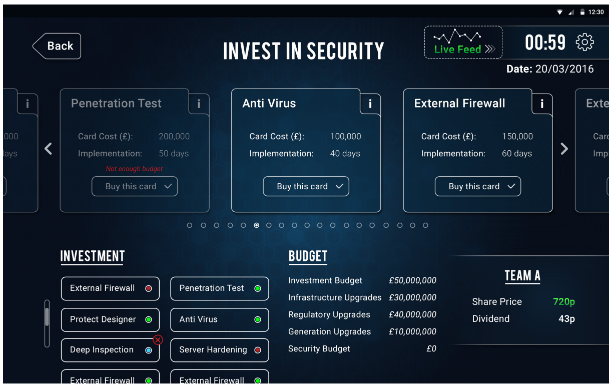
Segment OT Networks: Structures the OT networks, buses and serial communications in a manner whereby the ability to traverse from one device or protocol to another can be limited, thereby restricting the ability of malware to propagate to ICS devices.
Configuration Management Processes: Introduces a set of processes to ensure that the configuration of all known devices is recorded, and any requests to modify them are properly assessed prior to changes being made.
Secure Operational Procedures: Implements a complete review of all operations across IT, OT and associated operations and develops policies for all aspects of personnel, processes and use of technology, then introduces programme of change to establish their use.
Catalogue Assets: Implements a programme to identify and catalogue all IT and OT assets within the organisation so that they can be properly managed.

Videos and Press Cuttings

At the beginning of each round a video is played to the teams via their tablet interfaces. It presents a simulated news broadcast that explains the initial scenario that will subsequently develop as the game progresses. The videos are supplemented by newspaper cuttings that summarise the news broadcasts so that players can refer back to salient points.

Tablet Player Interface

The players within the teams interact with the game and leader board through the tablet player interface. In the example screenshot in Figure 4.4, a team purchases security cards.



Date: 20/03/2016

Penetration Test
Card Cost (£): 200,000
Implementation: 50 days
Not enough budget

Anti Virus
Card Cost (£): 100,000
Implementation: 40 days

External Firewall
Card Cost (£): 150,000
Implementation: 60 days

BUDGET

Investment Budget	£50,000,000
Infrastructure Upgrades	£30,000,000
Regulatory Upgrades	£40,000,000
Generation Upgrades	£10,000,000
Security Budget	£0

TEAM A

Share Price	720p
Dividend	43p

Figure 4.4: An example of the SCIPS tablet interface

Leader Board

The game also uses a leader board that interacts with the tablet devices to display the financial positions of each of the teams, providing a comparative evaluation of their performance at the end of each round.

Game Journey

At the start of the game the players are presented with the investment budgets committed to in their fictitious CNI company's annual report. These include provisions for upgrades to physical infrastructure, regulatory compliance, and efficiency improvements. No provision is made for increased cyber security in their plans for the forthcoming financial year. ‘Agency’ is provided through the purchase of a limited number of *security cards* that can apply defensive mechanisms to an ICS. Each card has an associated cost and implementation timescale. Players must trade-off the purchase costs from their investment budgets. Any reduction in committed inward investment results in the overall share price falling. The business objectives of the game are to meet, as closely as possible, the investments stated in their annual report and to maintain market confidence. Whilst trying to preserve the share price, players also try to maintain their personal bonus, which is also impacted by investment decisions, resulting in a tension between shared and personal objectives (Figure 4.2).

As the six rounds of the game progress, participants experience the recognised phases of an APT attack lifecycle. The game aims to provide experiences to inform a mental model for the players, with which they can assess the implications for their own ICS operations. It requires participants to work in teams, thus reinforcing the experience amongst their peers, and developing a similar understanding across the teams of players. The game uses a two-fold approach to fear appeals. Firstly, it presents a developing cyber attack scenario that results in catastrophic damage to a CNI facility, with significant resulting impact on share price and market confidence. Secondly, it stimulates a fear of losing by placing teams and individual players in a competitive scenario, where loss is visible to their peer group.

The journey that players experience through the game starts at *onboarding*, then progresses through the *game rounds* until the *game close* and the final *evaluation* of its effectiveness.

Onboarding

Prior to commencing the game, connectivity between the tablets and the leader board is established. At the start of the session players are introduced to the rules of the game by a facilitator. In later versions of the game this step will be automated and displayed on the tablet interface. Members of each team then pick a *role card* at random and enter their name against the role on the tablet.

Game Rounds

The game currently comprises six rounds, each representing a two-month period in a twelve-month financial year from April to March. In each round a new video broadcast is played, explaining the ongoing situation in the fictitious country. In the current version of the game, the players witness a UK-US coalition employing economic sanctions and military intervention resulting in hacktivists from the region threatening to retaliate against UK energy infrastructure. The CEO of the fictitious company starts with his individual bonus reduced to 80% of its possible maximum value as a result of market sentiment reducing the team’s company share price by 10% in response to the threat. After watching the video at the beginning of each round, players have a limited amount of time to decide which cyber security protection cards to purchase, and which of their existing budgets to transfer the funds from. Initially the scenario is baselined with none of the security cards selected, and a total investment budget available that is allocated between infrastructure, regulatory and generation upgrades. As the budgets are decremented, players can see the impact on their overall share price and projected dividends to shareholders, as well as their own personal bonus. As the rounds progress, cyber incidents escalate from initial reconnaissance activity to effects against the energy production capabilities of the power plant, the impact of which can be limited by the purchase of security cards in previous rounds. Each of the security cards has four values assigned to it, used in the calculations regarding its impact:

1. **Active?:** *This determines if the security card is active, based on the difference between its date of purchase and the current date, and the implementation timescale associated with the functionality.*
2. **Protection:** *Defines the maximum level of protection afforded by the security card.*
3. **Potential Impact:** *Defines the maximum impact that a cyber attack will have if that card is not purchased. This is defined as a numeric value and may be higher than the maximum Protection figure. This is to allow for realistic scenarios such as firewalls not detecting all attacks.*
4. **Actual Impact:** *If the security card is not active then this defaults to the Potential Impact figure, however if it is active then the value is set to the difference between the Potential Impact and Protection variables.*

The Protection and Potential Impact figures change from round to round, as certain security cards afford better protection against each of the stages of the cyber attack. For instance, the 'Traffic Profiling' security card in Round 1 has no impact on preventing external IP network reconnaissance of the IT systems, whereas in subsequent rounds it offers the ability to detect traffic abnormalities in the OT space. The sum of all Actual Impacts of all of the security cards is calculated and a percentage presented back to the players to indicate how much, or little, their infrastructure was protected, as does a textual description of the impact. In later rounds the summations of the Actual Impacts is divided by an impact factor to feed into the *cumulative impact of attacks* that reduces share price and impacts personal bonus figures.

Game Close

At the close of the game the players will have experienced the impacts of a cyber attack on the ICS in their power generation plant, the extent of which will have been limited, or not, by their cyber security investments. The leader board will display the overall performance of the teams, presenting the team with the highest share value as the winners, and the player in the role of CEO of the team with the lowest share price as the loser.

Evaluation

The purpose of the game is to change the perceptions of senior stakeholders in CNI organisations who possibly perceive investment in cyber security as an ongoing line on an IT budget that should be contained, to a strategic, top-line investment that protects shareholder value. Throughout the game, players develop their understanding of the impact of a well-executed cyber attack and form their own opinions as to the necessity of planned, defensive measures deployed in advance of such an incident. As players will come to the game with differing levels of experience and understanding of ICS and CNI, it is necessary to identify any shift in their views in order to evaluate its effectiveness. Players are encouraged to complete a feedback questionnaire that establishes their initial perceptions and measures any shifts in view as a consequence of the game.

4.5.6 Game Economy

At the start of the game the players are presented with the investment budgets committed to in their fictitious company's annual report. These include provisions for upgrades to physical infrastructure, regulatory compliance, and power generation equipment. No provision was made for increased cyber security in their plans for the forthcoming financial year. To purchase security cards to protect their infrastructure, players must decrement these budgets to fund their investments. A reduction in committed inward investment results in the overall share price falling. Overall market sentiment [203] is reflected in an initial 10% fall in share price as a result of the threats by hacktivists, with further changes to market confidence as a result of investment decisions and public awareness of cyber attacks. Whilst trying to preserve the share price, players also try to maintain their personal bonus, which is impacted by investment decisions, resulting in a tension between corporate and personal value.

Game Theory

Game-theoretic models are not used in SCIPS, as when one is called upon to defend against a cyber threat from an adaptable antagonist there are rarely situations where decisions result in a binary outcome. Zero-sum structures, or more complex models involving rational actors, fail to convey the essential message that an organisation cannot guarantee 100 percent security. Instead, the purchase of security cards decreases the impact of certain aspects of the attack during certain phases of the APT campaign, but does not entirely negate them. This adds to the risk-reward decisions players must consider.

4.5.7 Play, Test and Iterate

An analysis of the effectiveness of SCIPS as an element of this research is is discussed in Section 11. However, a cycle of play, test, and iterate was used to assess the early versions of the game. Although this early data was captured during the author's MSc project, it was not analysed in great depth. However, to drive the development of SCIPS, it was subjected to further scrutiny to direct the evolution of the framework as a part of this research.

As the intended outcomes were aimed at directing a change in individual perceptions, the associated success metrics were subjective. A player feedback sheet was completed at the end of the early versions of the game that asked nine key questions [196], all scored using a consistent numeric range. The use of the feedback form allowed participants to measure the shift in their understanding, and also to reinforce their changed perceptions through positive affirmation [208].

SCIPS was initially evaluated using three separate audiences [209, 210, 211] comprising a range of technical and business experience. After the first two evaluation sessions [209, 210] participants were offered the optional opportunity to complete a paper questionnaire to augment their verbal feedback. A limited number of participants chose to take-up the offer of completing the questionnaire. The third evaluation session [211] dispensed with structured questioning, instead offering participants the option to provide unstructured feedback.

Each of the sessions followed a slightly different format, tailored to the audience. The first [209] was played with an audience with cyber security knowledge, but without any ICS experience. The game was preceded by a presentation introducing ICS, using the Purdue Model (Figure 3.2), to develop visual representation of an ICS and create an initial mental model. The presentation explained ICS security vulnerabilities and how these might be exploited. The participants played a complete cycle of the game over six rounds, allowing 15 minutes per round. The second workshop [210] was played by an assembled audience with both ICS and cyber security experience. They played only three rounds of the game, with the round time restricted to 10 minutes. The audience received no ICS presentation. Finally, the third session [211] was presented to an audience of mixed ICS and cyber security expertise. They played the full six rounds of the game, allowing up to 15 minutes for each round. The audience received no ICS presentation beforehand.

Based upon the feedback questionnaires, which asked participants to respond on a scale of 1-10 (1=low to 10=high), the audience from the first workshop [209] had a low initial understanding of ICS and ICS security, with a mean of 4.8 *(n=10, σ=2.51)*. The second audience had a far higher understanding, with a mean of 8 *(n=5, σ=1.58)*. However, both audiences understood ICS security to be a strategic issue irrespective of their experience level, with mean values of 1) 7.2 *(n=10, σ=2.31)* and 2) 9.4 *(n=5, σ=0.89)* respectively. By the end of the sessions, the perception that ICS security was a strategic issue in the first workshop had risen to 8.9 *(n=10, σ=1.22)*, representing a mean increase of 1.7. The mean increase was less in the second workshop, with only a 0.4 rise to 9.8 *(n=5, σ=0.45)*, but their overall mean suggested a high level of understanding of the strategic significance of ICS cyber security to begin with.

Both audiences felt the tension between shared and personal goals, reflected in the maintenance of share price versus personal bonus, was realistic, with responses of 1) 8.1 *(n=10, σ=1.16)* and 2) 7.2 *(n=5, σ=1.92)*. The efficacy of the fear appeal was borne out in the effectiveness of the game, with mean values of 1) 7.9 *(n=10, σ=1.83)* and 2) 9.4 *(n=5, σ=0.89)*.

The unstructured feedback from the third session [211], which had no initial presentation, requested that any introductory briefing provided before the game should include an explanation of the vulnerabilities of ICS as well as the conventional attack cycle of an APT actor, and that this APT attack methodology should be referred to after each round to demonstrate to the audience the progression of the antagonist. There were also a number of requests for supporting literature for the security cards, as the benefits and impacts of their use were not adequately articulated to a non-technical audience on a small playing card.

4.6 Evolution of SCIPS

Following the feedback from the early evaluations, the game evolved to incorporate a series of security presentations at the start of the education session which introduced the risks to an ICS, as well as articulating the APT threat using an adversary lifecycle framework (or 'kill-chain') and the Purdue Model. The imagery used to articulate adversary behaviour and the Purdue Model in this initial presentation is subsequently used as the basis of interaction with the players to allow them to assess the progress of the antagonist, as well as support their Level 3 SA analysis of the likely courses of action the antagonist may follow. This inter-round period is also used to allow each team to present a summary of the rationale behind their investment decisions and an assessment of their effectiveness against the current phase of the APT attack. Players also discuss the type of information that would be required to improve their decision-making. As part of this focus on improving the quality of information used for decision-making, participants are also provided with a brochure that describes how the security cards available for purchase defend against the antagonist, articulating the technical effects of the security features, as well as their impact on reducing the operational risk to the CNI facility.

4.7 Initial Conclusions

Each evaluation session ideally requires 20-25 players in order to fully exercise the competitive nature of the game, although competition can be achieved with two teams of five players. However, the numbers of participants required limited the early experimentation opportunities. Similarly, by making the completion of a feedback questionnaire optional, the sample size of data collected was restricted. However, the early results of SCIPS were promising and warranted further experimentation. The increase in strategic awareness of ICS security by the players of the first workshop demonstrated the effectiveness of serious games as a means to deliver complex messages to an audience. However, the request for presentations to accompany the game from the audience of the third workshop suggested that serious games are not necessarily alternatives to didactic learning techniques, but complementary to them. The combination of the game with a presentation reinforces the mental models developed by participants. This allows players to picture the progression of the attacker through the architecture, augmented by the inter-round feedback sessions to discuss the antagonists progress through the ICS architecture.

The APT scenario used illustrates the reality of a capable antagonist. The game delivers a realistic fear appeal to motivate the audience, who subsequently acknowledge that a threat exists, understand its impact, have seen how it can evolve over time, what the intent of an attacker might be, and experienced the circumstances under which an attack could occur. The security cards illustrate the coping mechanisms available, and serve to demonstrate how an attack could be contained. The early versions of SCIPS only contributed to five of the seven aspects of cyber situational awareness that were defined in Table 2.2. It did not address the quality of information required to make decisions during an attack or consider the many alternative possible actions an antagonist might take in order to achieve their intent (aspects 6 and 7). The inclusion of inter-round interactive discussions with the game participants addressed these issues, allowing feedback and reflection to shape their thoughts on information requirements and Level 3 SA. The current version of SCIPS, as illustrated in Table 4.5, now satisfies all seven of the aspects of cyber situational awareness.

1.	Acknowledge that a threat exists, and that it can be identified if it occurs.	✓
2.	Have assessed the immediate and longer-term impact of cyber attacks.	✓
3.	Be conscious of how an attack can evolve over time.	✓
4.	Understand the intent of an antagonist.	✓
5.	Recognise the circumstances under which an attack could occur.	✓
6.	Have appraised the quality of information required to make decisions during an attack.	✓
7.	Consider the possible actions an antagonist might take in order to achieve their intent.	✓

Table 4.5: SCIPS Alignment to the 'aspects of cyber situational awareness' defined by Barford (2010)

SCIPS, as an element of this development programme, and through the realism of the game, contributes to Question 1 - *Which factors influence the development of mental models to provide cyber situational awareness?* of the six research questions posed in Section 1.4, that considers which factors influence the development of mental models to provide cyber SA. The nature of the scenario of the game, and its focus on strategic issues, further contributes to Question 3 - *Can serious games change the risk perceptions of participants and establish a foundational level of situational awareness?*. By providing *agency*, SCIPS also provides a potential increase in the efficacy of the manner in which risk perceptions are changed, thus contributing to Question 4 - *How can we increase the efficacy of the serious games to deliver the change in risk perceptions?*. Finally, by including an end-to-end cyber attack in the game, and the requirement for participants to assess the intent, impacts and future courses of action of the antagonist, SCIPS also contributes to Question 5 - *As a result of serious games, can participants recognise the characteristics of a cyber attack and determine the possible intent and courses of action?*, and Question 6 - *Are participants of serious games able to assess the immediate and longer-term impacts of cyber attacks?*.

Chapter 5

The Industrial Control System Cyber Defence Triage Process

Contents

5.1 Introduction

The Industrial Control System Cyber Defence Triage Process (ICS-CDTP) is a coping strategy for ICS operators that allows them to address cyber threats in an effective and cost-sensitive manner that does not expose their operations to additional risks through invasive testing. It is intended to develop SA through progressive training, developing the necessary mental models to prepare an ICS operator for antagonistic actions on their networks.

There is evidence [212, 107] that targeted attacks from capable actors look beyond an IT system focus, and instead target the industrial processes under control in order to create an effect that impacts on the operations of an industrial facility. This attack on the critical processes represents the highest level of threat to an ICS operator, especially when perpetrated by a highly capable actor such as a nation state [213]. Any approach to security of ICS hence should assume an intelligent, adaptable adversary that will focus on high-value targets.

Traditional approaches to systems vulnerability assessment rarely focus on antagonistic intent. Instead they review penetration and exploitation options, highlighting what is vulnerable as a result. A complete review of a facility using the guidance in ISA-99 [195], soon to be replaced by IEC 62443 [72], and the CPNI ICS Good Practice Guide [73] should result in a comprehensive defence-in-depth approach to cyber security. However, such comprehensive reviews are expensive, resource-intensive activities that often cannot be justified solely based on a cost-benefit analysis.

In order to deliver the maximum return on investment for an initial cyber review, and establish the basis for a subsequent complete assessment of the operations, the potential financial and safety impacts of malicious attack activity should be modelled to determine where the manipulation of industrial processes and process data have the greatest impact. It is only once the process vulnerabilities in the operational industrial processes have been identified that it is possible to establish which of the many devices within a large ICS installation are responsible for the control of the vulnerable process steps. Triage then identifies which are the highest priorities to defend from cyber attack, and against which an incident response 'playbook' can be built to deny the attacker access to critical system assets.

The ICS-CDTP described within this chapter is focused on those ICS operators facing the highest levels of impact from antagonistic cyber actions, but not yet at a high level of cyber security maturity. The intent of ICS-CDTP is to be a coping strategy for ICS operators to *begin* a progression of informing and realising a set of ICS security controls that will form the basis of subsequent, holistic analyses of the entire industrial facility using established best practices.

The majority of this chapter has been peer-reviewed and published in the following:

- **Allan Cook, Helge Janicke, Richard Smith, Leandros Maglaras** "The Industrial Control System Cyber Defence Triage Process", Computers and Security (Elsevier), Volume 70, September 2017, Pages 467-481,
DOI: 10.1016/j.cose.2017.07.009(IF: 2,85)

The ICS-CDTP framework is novel in that it combines and extends concepts found in risk assessment and intrusion detection techniques with safety and process models that are known within the operations of many ICS facilities. As such, ICS-CDTP:

1. Focuses on the identification and defence of critical ICS equipment from malicious manipulation. It models and characterises attack behaviours and supports the development of a set of potential intrusion models that significantly improve the readiness of incident responders.

2. Complements IEC 62443 [72] and the CPNI ICS Good Practice Guide [73]. It extends the Diamond Model of Intrusion Analysis [190] and integrates the CARVER

Matrix [90] to support a fundamental change from reactionary, blanket protection to targeted and focussed defence.

3. Allows ICS operators to actively identify and attempt to thwart malicious attacks based on an incident response ‘playbook’ developed from analyses of antagonistic intent.

5.2 ICS-CDTP Overview

As discussed in Section 3.5, there is a lack of validated data against which we can apply established risk models to ICS cyber threats [214]. The ICS-CDTP assumes that the courses of action an adversary will pursue when attacking an ICS are unknown to the defender. Whilst some opportunist antagonists may attempt to cause disruption without any conscious targets, highly capable attacks will develop elaborate and coordinated attacks against the highest value targets. By assuming a highly capable attacker the ICS-CDTP framework considers a worst-case scenario driving the risk assessment and SA.

Regardless of the premeditation of an attacker, an assessment of which systems are critical to the continued operation of an industrial facility is required. This includes the assessment of the vulnerabilities of the specific control devices used and the infrastructure that underpins them with the aim to establish *attractive* targets.

ICS-CDTP defines an *attractive* target as one that is:

1. Poorly protected, either through inherent flaws in the device or weaknesses in surrounding security mechanisms.

2. Critical to the correct and profitable execution of an operational process.

3. Used in processes that, if manipulated, would result in the local population or general public becoming aware of the intrusion.

4. Easily accessible via Internet-enabled devices, or poorly protected from insiders through inadequate physical security.

These characteristics focus on the adversary’s perspective of the ICS infrastructure, and their attack intent. Targets that satisfy these criteria would offer a means by which a capable antagonist could achieve significant impact on an ICS [213].

ICS-CDTP iteratively assesses the attractiveness of a device to an antagonistic actor and provides a process to remediate any vulnerabilities, as well as describing any residual risk and informing security monitoring techniques for mitigation. However, analysis alone is not sufficient to adequately defend an ICS, it must also support ongoing security monitoring to better identify intrusions and underpin subsequent incident response. As a result, ICS-CDTP addresses the eight questions listed in Table 5.1.

1. Which devices are attractive to an attacker?
2. Can we better protect these devices?
3. What routes exist to these devices?
4. What events would occur in an attempt to access and manipulate these devices?
5. Where can we deploy sensors to detect these events?
6. How will we determine which of the alternate routes to a device are being used by an attacker?
7. How can we predict an attacker's next activity?
8. What does our incident response plan need to describe and test in order to mitigate residual risks identified in the analysis?

Table 5.1: The eight questions that ICS-CDTP addresses

5.3 ICS Cyber Defence Triage Process

The scale of ICS installations often complicates the cyber security analysis process, as it is not cost-effective to defend all systems equally in such a complex environment. Given the number of devices installed it is desirable to prioritise the defence of those that support critical functionality. This should include assessments from both offensive and defensive perspectives, which are both facilitated by ICS-CDTP. Figure 5.1 depicts the ICS Cyber Defence Triage Process.

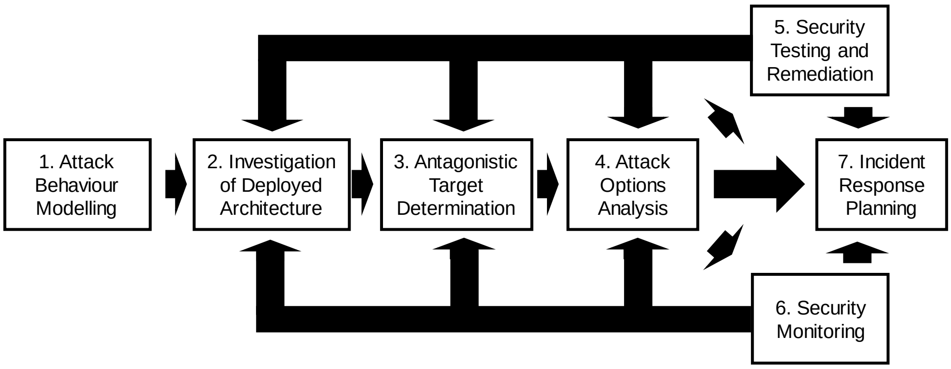

5. Security Testing and Remediation
1. Attack Behaviour Modelling
2. Investigation of Deployed Architecture
3. Antagonistic Target Determination
4. Attack Options Analysis
7. Incident Response Planning
6. Security Monitoring

Figure 5.1: ICS cyber defence triage process (ICS-CDTP)

Capable threat actors tend to follow established Advanced Persistent Threat (APT) approaches to targets [15]. In 2014, 55 percent of incidents investigated by ICS-CERT involved APTs or sophisticated actors [10]. In order to maintain a focus on such antagonists we must first decide how to represent the behaviours of an attacker. The triage process illustrated in Figure 5.1 begins in Step 1 by deciding upon an attack lifecycle model that best suits the perceived threat and available data. It then proceeds to gather documentation on the ICS network architecture in Step 2. Whilst information obtained from network enumeration is always more accurate, ICS devices are known to react unpredictably to such exercises. This will expose the operations of the facility to unnecessary risk. The network design documentation is used as a foundation for all subsequent analysis in Steps 3-7.

In Step 3 an assessment is made regarding the impact and attractiveness of key processes to an antagonist, and the underlying ICS devices, followed by a review of the possible attack threads that could permit access to the ICS in Step 4. These attacker courses of action are constrained by the characteristics of the ICS architecture implemented within the facility [215]. Accordingly, we consider the deployed infrastructure to increase the specificity of the analysis. By combining the analyses of critical devices, attacker behaviours, and the deployed ICS architecture, we produce a triage of the options available to an antagonist. This drives the detailed security analysis of the critical devices in Step 5, leading to remediation of vulnerabilities. Where this is not possible, indicators of compromise and the locations where network- and host-based sensors are identified to support targeted security monitoring in Step 6. Both options feed into the overall incident response planning process of Step 7, to underpin effective cyber defences against malicious attacks.

We will now consider each of the triage framework steps in greater detail and provide examples of their application.

5.3.1 Step 1 - Attack Behaviour Modelling

The first step of the proposed framework defines how antagonistic behaviour will be described, as a basis for subsequent analysis, by extending the Diamond Model of Intrusion Analysis [190] and integrating it with the Mandiant Attack Lifecycle [15, 216]. The Diamond Model [190] is an analysis framework that defines atomic intrusion events and describes the four core features of an antagonistic event, those being an *adversary* using a *capability* delivered over an *infrastructure* in order to target a *victim* and produce an outcome, as illustrated in Figure 3.6. These core features, or nodes, are connected by edges that define the relationship between each. The nodes and edges are connected into a model that resembles a diamond. An intrusion event also has a number of meta-features that allow for further details of an intrusion event to be modelled. All attributes have an associated confidence level to allow for a weighting to be applied to decisions taken on the perceived accuracy of data. The advantage of the model comes from the ability to analytically pivot between the connected points on the diamond to reach other connected points. This means that common capabilities being used in different intrusion events can be correlated and identified. Rather than being defined as a specific ontology or taxonomy for modelling attack behaviours, the diamond model is intended to be an extendable framework that can accommodate architectures and technologies as befits an environment. As a result, an event in the model is a variable-sized n-tuple that allows a basic tuple to be extended based on requirements.

The basic diamond event, along with the standard victim definition, is depicted in Figure 3.7.

There are many ways to express an antagonistic cyber attack. Two commercial methods were considered during this analysis; the Lockheed Martin™ 'Kill-Chain' [191] and the Mandiant™ Attack Lifecycle [15, 216]. Both techniques fitted within the process, but in this example we used the Mandiant method, as the 'Weaponisation' phase of the Lockheed Martin model would be opaque to a defender. The Mandiant lifecycle comprises eight stages:

1. External Reconnaissance: *Network scanning and associated research into the target organisation and systems.*

2. Initial Compromise: *The methods by which an attacker passes the security perimeter of the target network.*

3. Establish Foothold: *Techniques and capabilities to establish two-way communications with implanted malware.*

4. Escalate Privileges: *The means by which an attacker elevates their permissions to a greater set of resources.*

5. Internal Reconnaissance: *Scanning and device discovery within the target network.*

6. Move Laterally: *Traversion of the target network across legitimate devices.*

7. Maintain Presence: *Ensuring continued control over key systems, nodes and devices.*

8. Complete Mission: *The execution of the intent of the attack.*

The lifecycle offers the ability to model the attack methods of an antagonist in a uniform manner to allow for an assessment of behaviours towards the intended target devices. In order to consider the feasibility of these attacker options we must also take into account the deployed architecture of the ICS under analysis.

5.3.2 Step 2 - Investigation of Deployed Architecture

Security can be reduced through poor systems integration or inadequate control over communications. As a result, the ICS devices cannot be considered in isolation from the network on which they are deployed. The second step of the proposed framework investigates this deployed architecture. Whichever way the architecture has been defined within the ICS operation, whether that be through layering, grouping, functional separation etc., it must feature in the triage framework so that we can review its impact and determine common vulnerabilities that arise as a consequence of the design. ICS are typically not deployed in a consistent manner, and therefore ICS-CDTP does not prescribe any defined abstractions. For the purposes of this article we use the Purdue Model of Control Hierarchy [38] as an illustrative architecture.

The Purdue model, a reference architecture for control hierarchy [38] describes six levels within an organisation managing an industrial control system, illustrated in Figure 3.2. ICS implementations often include a number of significant differences to traditional IT systems. Typically, ICS have a deeper architecture than typical enterprises, as is characterised by the Purdue model.

Extensions to the Diamond Model: To accommodate the idiosyncrasies of ICS into the process we must extend the definition of an event within the Diamond Model.

Whilst no mandatory elements are prescribed in the model, the *infrastructure* and *victim* nodes should include the following levels of granularity to support a detailed analysis of attack options.

Input Protocol: The protocol used to access the device.
Input Bearer: The bearer over which the input protocol runs, in order to determine if it is shared.
Output Protocol: The protocol exiting the device, to accommodate protocol transformations.
Output Bearer: The bearer over which the output protocol runs, in order to determine if it is shared.
Network Segment / Identifier: Which network or bus segment, or serial identifier, is used to transit traffic over the bearers.
Architecture Layer: Which layer or zone the segment sits within.

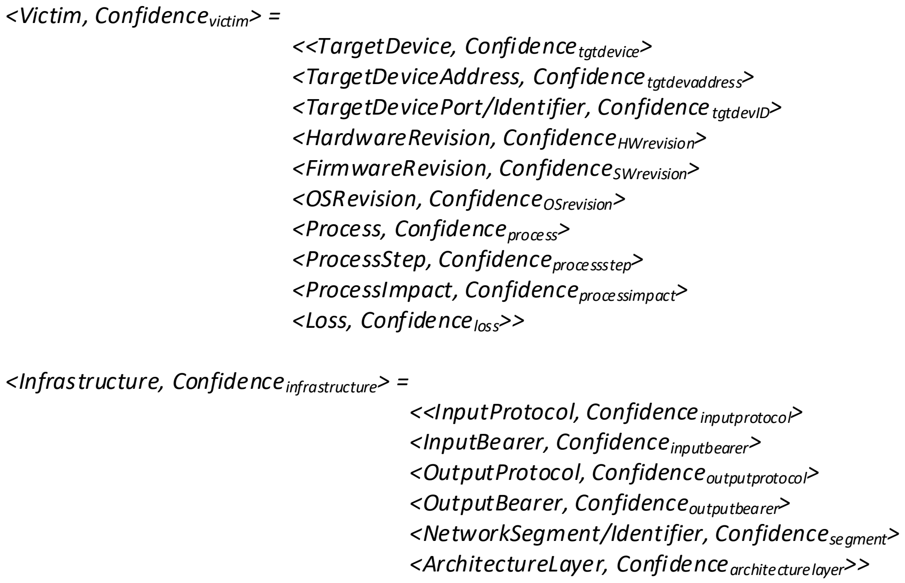
Target Device: The make and model of the device.
Target Device Address: Its address, whether IP, MAC or otherwise.
Target Device Port / Identifier: What port, or other identifier is used to communicate with the device.
Hardware Revision: The hardware revision of the device.
Firmware Revision: The firmware revision of the device.
OS Revision: The operating system revision of the device.
Process: Which process the device is used within.
Process Step: Which specific step of the process.
Process Impact: The impact, potential or real, of manipulating the device.
Loss: The associated, assessed financial loss through manipulation.

Extensions to the Infrastructure and Victim nodes are represented in Figure 5.2.

Integration of the Diamond Model with the Attack Lifecycle: The Diamond Model then needs to be integrated with the selected attack lifecycle (or *'kill-chain'*), in this case the Mandiant Attack Lifecycle [15].

Figure 5.3 shows a set of Activity Threads from the Diamond Model [190] with intrusion events modelled as diamonds. Activity Threads [190], however, lend themselves more to intrusion analysis activities, whereas we require a mechanism to develop attack routes prior to the event, in order to develop understanding of the potential attack paths.

Figure 5.4 uses Activity Threads from a single adversary to model the various options available to attack a victim device. The resulting Activity-Attack Graph allows the various possible routes to the target, and the associated events, to be modelled. The graph models, in a simple format, the alternative paths that can be considered when assessing how to defend the target device. It drives the definition of sensor and log alerts to inform on such behaviour. Should an intrusion occur, the analysis is already mature as a consequence of these models, and the attacker's next steps can be considered.



<Victim, $Confidence_{victim}$> =

<<TargetDevice, $Confidence_{tgtdevice}$>
<TargetDeviceAddress, $Confidence_{tgtdevaddress}$>
<TargetDevicePort/Identifier, $Confidence_{tgtdevID}$>
<HardwareRevision, $Confidence_{HWrevision}$>
<FirmwareRevision, $Confidence_{SWrevision}$>
<OSRevision, $Confidence_{OSrevision}$>
<Process, $Confidence_{process}$>
<ProcessStep, $Confidence_{processstep}$>
<ProcessImpact, $Confidence_{processimpact}$>
<Loss, $Confidence_{loss}$>>

<Infrastructure, $Confidence_{infrastructure}$> =

<<InputProtocol, $Confidence_{inputprotocol}$>
<InputBearer, $Confidence_{inputbearer}$>
<OutputProtocol, $Confidence_{outputprotocol}$>
<OutputBearer, $Confidence_{outputbearer}$>
<NetworkSegment/Identifier, $Confidence_{segment}$>
<ArchitectureLayer, $Confidence_{architecturelayer}$>>

Figure 5.2: Extensions to the definition of victim infrastructure nodes

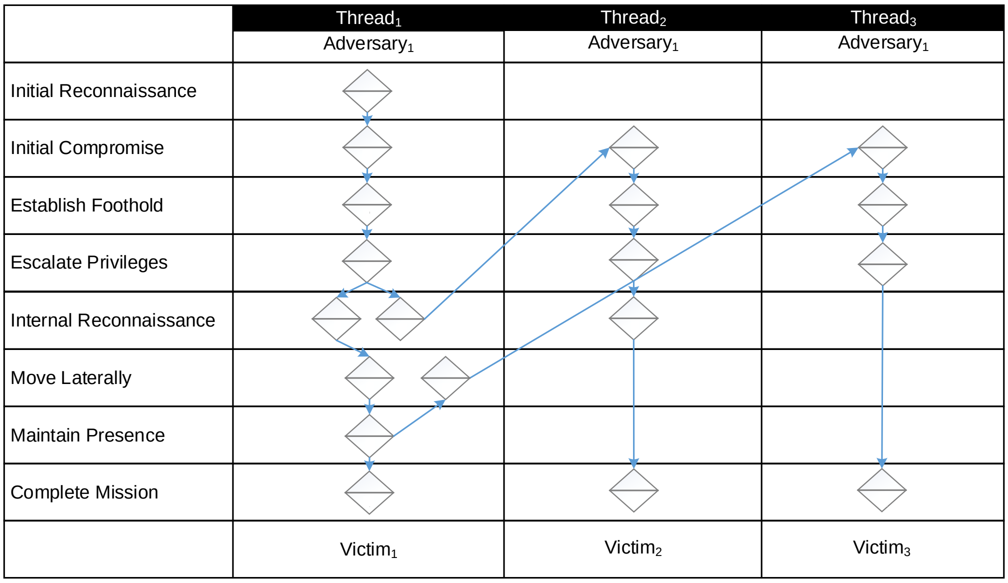


Figure 5.3: Activity threads, Caltagirone et al. (2013)

The third step of the proposed framework considers the intent and target of an attacker.

5.3.3 Step 3 - Antagonistic Target Determination

In a forensic examination of the Stuxnet malware [212] that affected uranium enrichment centrifuges, it was highlighted that the attack did not just target the vulnerabilities of the control systems in use, it also targeted the process parameters in order to create

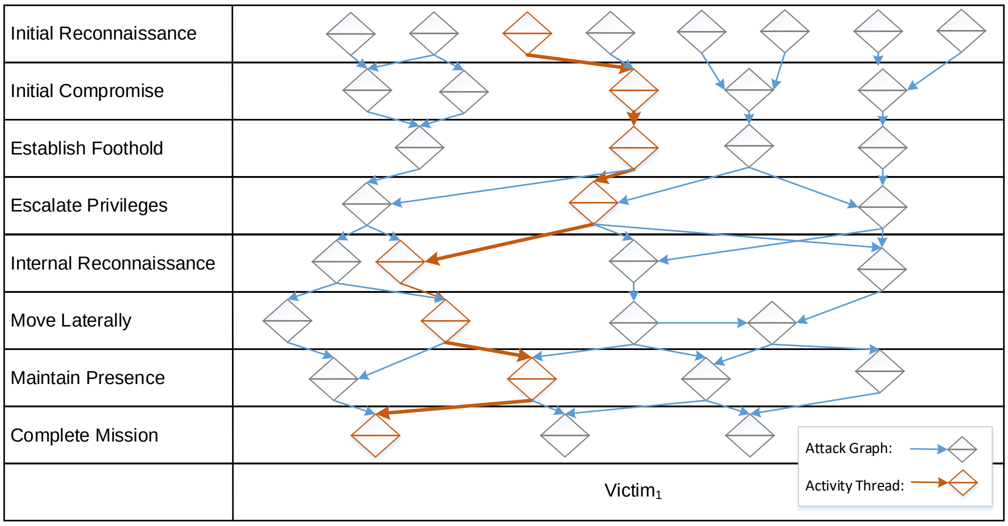


Figure 5.4: Activity-attack graph, Caltagirone et al. (2013)

an effect in the physical world. The analysis showed that unlike cyber attacks on IT systems, cyber-physical attacks involve the use of IT systems to spread malware and the manipulation of ICS elements to influence the process under control that results in damage to industrial equipment. This highlights the interdependencies of the process and the control systems in use, and how one cannot be considered in isolation from the other. Many industrial facilities utilise simulation tools to model and predict the operations of the processes under control within an ICS. This forms an essential part of the operations of the facility. These models also offer the possibility to test boundary conditions of process variable and determine which ones, if maliciously manipulated, could introduce misbehaviour within the industrial process [107].

Most simulations are focused on a model of the control strategy for the process and ensure the coherence of the overall plantwide process control [217]. However, if conditions outside of this expected system state are introduced, unanticipated consequences may be observed. For example, a change in input flow into a recycle loop can result a *'snowball effect'* [218] with outputs increasing by such a significant level that it leads to a state whereby an entire plant may have to be shutdown in order to rectify the situation. This demonstrates that if the control equipment responsible for the input flow could be maliciously manipulated, the impact on the plant could be significant. The control device therefore becomes a key asset to defend, as an attacker with knowledge of the industrial process under control may also determine the efficacy of the device as a target [107]. Such semantic attacks can lead to long-term degradation of product or services that impede the effectiveness and profitability of the operation.

Once the key vulnerable processes are defined, a further analysis of the feasibility of interfering with the control elements that are used to manage the parameters of the process is undertaken. This will determine those elements requiring remedial or protective measures to prevent the occurrence of such misuse. One method to identify areas of vulnerability that are potentially attractive to an antagonist is the CARVER

Matrix [90].

The US Department of Defense use the CARVER assessment method to determine criticality and vulnerability in enemy infrastructures. CARVER is a mnemonic for Criticality, Accessibility, Recuperability, Vulnerability, Effect and Recognisability. The method focuses on an adversary's perspective of the infrastructure to enable an analysis of the weaknesses of a target, or the means by which its operations can be manipulated by an attacker [90]. In this manner, the capabilities of several threat actors can be considered. The output of the CARVER assessment is a critical-asset list that defines a prioritised set of assets that are of value to an attacker based on their importance, whereby the asset's incapacitation or destruction would have a serious impact on the military operation or facility. The use of CARVER matrices to consider threats to critical national infrastructure by civilian agencies when preparing for terrorist attacks is emerging, as it allows organisations to consider the relative desirability of targets, although its use has been limited to the assessment of physical assets [91].
Criticality *describes the level of importance the target has and its relative value to an attacker in order to achieve a desired outcome, usually a denial or degradation in the ability of a target to function.*
Accessibility *is an assessment of how an attacker could reach an asset and the complexity of reaching the desired target.*
Recuperability *considers the time and resources required to repair or replace the target, or whether viable alternatives exist.*
Vulnerability *is a measure of the ability of attackers to deny or destroy the targeted asset.*
Effect *articulates the impact of the loss or degradation of the target.*
Recognisability *is the extent to which a critical asset can be recognised by an attacker, whether this be an understanding of its existence through to knowing the detail of its location and configuration.*

Each of the categories of the CARVER acronym are assessed for an asset, using guidelines for a subjective assessment of the ratings, based on consistent criteria described at the initiation of the analysis [90]. CARVER has a standard set of criteria based on physical assets that have been modified by the author for ICS triage. This allows an ICS operator to determine their level of exposure. These modifications to the criteria have remained close to the original intent of the CARVER process, but have been extended to accommodate the characteristics of ICS architectures. In the explanations of how we have applied CARVER within ICS-CDTP we have highlighted where we have used standard or modified CARVER criteria.

The example in Table 5.2 illustrates how criticality is typically considered using the CARVER method.

Each of the six domains of CARVER are considered in an unweighted assessment, with the overall measure of their exposure based on a simple arithmetic addition of the six values applied [90]. Using the criticality criteria above we can see how, if the processes of an industrial or critical infrastructure facility were considered, the impact

Criticality Criteria	**Score Rating**
Immediate termination of outcome; target cannot function without it	9-10
Loss would reduce operational performance considerably, or two-thirds reduction in outcome	7-8
Loss would reduce operational performance, or one-third reduction in outcome	5-6
Loss may reduce operational performance, or 10 percent reduction in outcome	3-4
No significant effect on outcome	1-2

Table 5.2: A CARVER criticality assessment using standard criteria

of their loss would become readily apparent. Take, for example, a water supply utility [76] that takes its supplies from local rivers, treats the water to remove impurities using standard control technology, maintains a four-day storage capacity of treated water and distributes to a local population via proprietary control technology. A CARVER analysis of the processes may result in the assessment described in Table 5.3.

Process Name	**C**	**A**	**R**	**V**	**E**	**R**	**Total**
Collection of water from rivers	7	4	3	5	7	5	31
Treatment of water	7	8	8	7	8	8	46
Storage of treated water	9	5	6	5	8	5	38
Distribution of water	8	7	6	5	8	3	37

Table 5.3: An example of completed CARVER matrix for a water utility

The storage of treated water appears a higher priority based on its criticality, but the lower criticality of the treatment of water is amplified by its apparent ease of access and use of standard technology that requires little industry-specific expertise to understand. This triage process allows the processes at the highest risk of being compromised to be addressed first.

Once the critical processes have been identified, the same approach can be used to identify the control devices that manage and automate them. In this manner, the scope of the analysis is immediately constrained to those systems that support the vital operational processes and provides a necessary triage. The CARVER method allows for existing, proven security methods to be brought together in a complementary framework that allows the various facets of the denial or degradation of an industrial control element to be consistently evaluated. By analysing the control logic within the device it is possible to determine which of the individual control elements, or the interactions between elements, are responsible for the key aspects of the process under control. Such analysis allows an assessment of the ability of the process to withstand variations in conditions and data during its lifetime. This measure of robustness allows for the consequences of loss to be assessed [219].

Criticality

The criticality of a device depends upon its involvement with a key process and whether or not it executes process logic or utilises process variables. Either can be manipulated to result in adverse effects on the process. These impacts can be assessed in two ways; firstly using safety analysis data; and secondly, using plant simulation data.

The Hazard and Operability (HAZOP) method is probably the most commonly used hazards analysis approach in industry [87]. Its widespread use and acceptance has led to a large number of practitioners and supporting service providers. The method divides systems under analysis into nodes, each of which representing a section of the process that undergoes a significant change or transformation. Examples of nodes include pumps, reactors, heat exchangers etc. This information is generally extracted from Piping and Instrumentation Diagrams (P&ID) [87]. The size of a node is a subjective decision based on the nature of the industrial process and may group devices or system elements together in order to consider an overall process change holistically. The groupings used for safety purposes are appropriate for antagonistic cyber analysis purposes as they describe malfunctions, and allow an assessment of impact and criticality should such conditions be wilfully caused.

A HAZOP analysis follows a consistent process whereby a system node is selected and its purpose and safe limits are defined. Next, one of a set of *process guidewords* are selected, such as high flow, low/no flow, reverse flow, misdirected flow, high pressure, high temperature, polymerisation, wrong composition etc., that describe the effect that should be considered, and hazards and their causes are identified as a result. For each hazard, the process considers how it will be recognised should it occur, and an estimation of the consequences is reached. A set of safeguard requirements are then defined, as is the estimated frequency of the hazard's occurrence. Finally, the hazards are ranked and a set of findings and recommendations is produced.

HAZOP analyses drive a rigorous assessment of the impact of undesirable events on a process, decomposing it to a detailed level. Their availability as a mechanism to assess criticality provides a rich dataset on which to base triage decisions. Where this data is not available, or when it has not covered sufficient breadth for cyber defence purposes, plantwide simulations used to model the behaviour of the processes under control can be considered as a basis for study. A study of a Vinyl Acetate Monomer (VAM) process [220] assessed the vulnerabilities using an impact vocabulary that resembled a subset of the HAZOP guidewords. The full use of the HAZOP vocabulary, however, offers a structure by which the inputs, outputs, reaction vessels etc. of an industrial facility can be analysed, using the simulation to visualise and quantify the impact. Modification of the simulation to introduce financial variables will also allow the monetary impact of manipulation to be quantified.

Once the key processes have been determined, the ICS control devices that control the vulnerable process steps can be further analysed. Within control systems, disturbances in the process result in changes to process variables (PV) and represent the value sampled for control. The measurement of the PV for the purposes of process control is described as the Controlled Variable (CV), which is provided by a Primary Element such as a sensor. The CV is compared to a setpoint within the controller, generating an error, e, representing the deviation from the desired state. Based on this data the controller determines the necessary corrective action, represented as a Manipulated Variable (mv) that drives the behaviour of Final Control Elements (FCE) such as a valve, that manipulate the mass or energy entering the process. Those control devices that act upon CV and provide logic to drive mv in the vulnerable process steps are deemed most critical [221].

Accessibility

In order for a cyber attack to be successful, the targeted control device must be accessible. Activity Threads [190] provide a formal way of representing the routes to a targeted control element. These are used to allow an assessment of their ease of use.

A set of CARVER accessibility criteria, modified for applicability to ICS triage, is described in Table 5.4. As with all of the CARVER factors described in this process, they provide guidelines to shape the consistency of the assessor's thinking, but support a subjective measure that can be derived in relatively short timescales. The accessibility criteria, modified from the original process that focusses purely on physical access to a target, guides the assessor to consider the ease with which an attacker might gain access to a critical system of device, and the likelihood of existing security mechanisms detecting such an event.

Accessibility Criteria	**Score Rating**
Remote or insider access with no means of identifying the attacker	9-10
Remote or insider access with limited means of identifying the attacker	7-8
Remote or insider access is possible with limited auditing and logging	5-6
Remote or insider access is possible with extensive auditing and logging	3-4
Remote or insider access is extremely difficult and will be identified	1-2

Table 5.4: CARVER accessibility criteria modified for ICS cyber security assessment

Recuperabilty

Recuperability is a measure of the control system element's ability to be replaced or repaired, and is a factor of the processes and procedures in place to provide a working alternative to the original device. This includes not only the replacement of the physical device, but the ability to load and execute a verified copy of the configuration necessary to operate the process. The recuperability measure can, if necessary, be tailored to the specifics of the industry under analysis. Standard CARVER recuperability criteria is applicable to ICS, and is described in Table 5.5. It guides the assessor to determine how long it would take to remediate the loss of a critical system or device.

Recuperability Criteria	**Score Rating**
Replacement, repair, or substitution requires 1 month or more	9-10
Replacement, repair, or substitution requires 1 week to 1 month	7-8
Replacement, repair, or substitution requires 72 hours to 1 week	5-6
Replacement, repair, or substitution requires 24 to 72 hours	3-4
Same-day replacement, repair, or substitution	1-2

Table 5.5: Standard CARVER recuperability criteria

Vulnerability

The vulnerability of a control device can depend on a number of factors. Common Vulnerabilities and Exposures (CVE) databases provide a library of known issues with control devices that can support an initial triage of potential avenues for exploitation. A modified set of accessibility criteria that considers the capability of an antagonist is described in Table 5.6 in order to provide accommodation for industrial equipment.

Vulnerability Criteria	**Score Rating**
Requires no industrial expertise; uses open source tools	9-10
Requires limited industrial expertise; uses open source tools	7-8
Requires extensive expertise; uses open source tools	5-6
Requires extensive industrial expertise and custom tools	3-4
Requires detailed knowledge of industrial facility and custom tools	1-2

Table 5.6: CARVER vulnerability criteria modified for ICS cyber security assessment

Effect

The effect of any cyber attack must be considered in the context of the process and the physical elements involved. This is a factor of the simulation and safety documentation review conducted in the *criticality* step of the CARVER method, and is reviewed based on the criteria in Table 5.7, modified for a critical infrastructure facility.

Recognisability

In order for an attack to be enacted upon a device it is necessary for the threat actor to be aware of its existence and be able to identify it within the control network. In order to assess the risk of knowledge of existence, it should be ascertained how much of the control system architecture has been made available on open source resources such as websites, and how much is freely discussed in communications by members of the

Effect Criteria	**Score Rating**
Large-scale impact on services and revenues; noticeable to public	9-10
Limited impact on services and revenues; noticeable to public	7-8
Minor impact on services; minor impact on revenues; noticeable to public	5-6
Minor impact on services; minor impact on revenues; public unaware	3-4
Minor impact on services; no impact on revenues; public unaware	1-2

Table 5.7: CARVER effect criteria modified for ICS cyber security assessment

facility's supply chain or maintenance service. The risk of identification of the device once on the control network is dependent on the control environment's ability to identify device enumeration behaviours, and upon a knowledge of the control network's traffic profile [54, 53].

A modified set of recognisability criteria is described in Table 5.8.

Recognisability Criteria	**Score Rating**
Requires no expertise to identify target device	9-10
Requires limited technical expertise to identify target	7-8
Requires moderate technical expertise to identify target	5-6
Requires significant technical expertise to identify target	3-4
Deception tactics deployed to minimise recognition	1-2

Table 5.8: CARVER recognisability criteria modified for ICS cyber security assessment

The modified criteria of the CARVER matrix, *criticality*, *accessibility*, *recuperability*, *vulnerability*, *effect* and *recognisability* permits the identification and comparative ranking of ICS targets that would be attractive to a capable, antagonistic actor, in order to focus the efforts and resources of defensive activities.

5.3.4 Step 4 - Attack Options Analysis

For the extent of the attack options to be considered, the fourth step of the proposed framework takes each identified course of action and decomposes it further. This analysis must also take into account the deployed architecture.

Figure 5.5 graphically presents a single Activity Thread, derived from an Activity-Attack Graph, in a novel visualisation that incorporates the deployed architecture. The usual two-dimensional representation of an Activity Thread is augmented by a third axis that shows the same attack distributed across the layers of the deployed architecture, described using the Purdue Model. The strength of this extension of the original model is that it allows common vulnerabilities or exploits to be considered over architectural layers, identifying areas of security weakness, or a concentration of potential attack behaviours, in individual layers. The standard Diamond Model approach to this uses a two-dimensional model, but this is again insufficient for an ICS. To allow for the characteristics of a deployed ICS architecture to be accommodated, a third axis is added to accommodate the architectural layers. This allows the defensive planners to review how to either detect, delay, disrupt, degrade or deceive the attacker at each layer of the architecture, considering the additional attributes defined in our extension of the *infrastructure* and *victim* nodes of the diamond event.

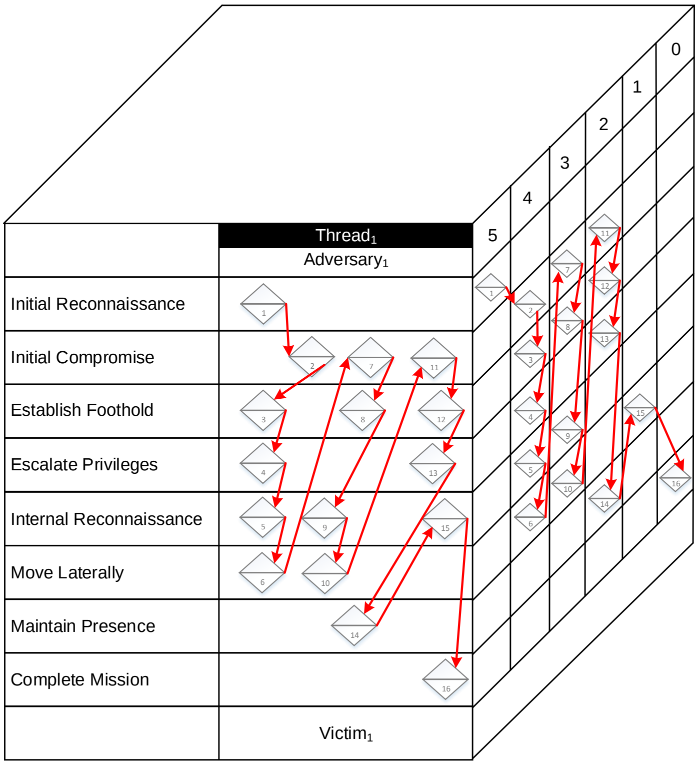


Figure 5.5: Extended activity graph incorporating the deployed architecture

The example shown in Figure 5.5 models the following APT attack behaviour:

1. External reconnaissance of internet boundary devices locates an internet-facing Third-party Access Server in the Enterprise Network.

2. An open, unprotected port is located and used to deliver an initial malware implant onto an unprotected File Server on the Site Business Planning and Logistics Network.

3. The malware communicates with an external command and control server and a fully-staged malware implant is deployed.

4. The malware uses a known operating system vulnerability to escalate its privileges.

5. Internal reconnaissance of the network identifies an Enterprise Resource Planning (ERP) [222] system in the Site Business Planning and Logistics Network.

6. The malware exploits the local network infrastructure to navigate to the Manufacturing Execution System (MES) [223].

7. A beacon is deployed to the MES.
8. The beacon communicates with the command and control server via the previously compromised internet-facing server and a fully-staged implant, tailored to the device configuration, is deployed.
9. The malware performs reconnaissance of the OT network and identifies a DCS that manages processes within the plant.
10. The malware exploits the network infrastructure to reach the DCS.
11. An initial implant is deployed on the DCS that beacons to the command and control server.
12. The command and control server, communicating via the chain of compromised devices, delivers a fully-staged implant, tailored to the device configuration.
13. The malware exploits a vulnerability in the DCS's operating system to escalate its privileges.
14. The malware modifies the configuration of the DCS in order to keep its processes continually active.
15. The malware performs reconnaissance of the PLCs connected to the DCS and exfiltrates this information.
16. The malware receives instructions from the command and control server and forces a shutdown of a targeted PLC in order to stop a critical node in the plant's processing.

The results of the Attack Options Analysis feed into the final steps of ICS-CDTP, supporting security testing and remediation, security monitoring, and incident response planning.

5.3.5 Step 5 - Security Testing and Remediation

For most large ICS it is not cost-effective to hold a pre-production environment for the whole facility on which to test changes [3]. This presents a challenge when testing against a representative system is required, as any use of the live environment can result in unforeseen consequences. In order to assess the levels of security available to the devices highlighted by the CARVER matrix analysis, it is necessary to define a means by which testing can be performed without risk to the operational environment. Step 5 of the process presented in this paper proposes a three-stage approach to security testing:

1. Simulated.
2. Isolated.

3. Synthesised.

Simulated: A *process-centric* approach to security testing that uses a simulation of the control device, modelling its logic, in order to assess the behaviours of the control strategy if the measured values, process variables, setpoints or sensor data are manipulated. The intent is to exceed normal operating parameters to test boundary conditions, and observe their impact on the process under control. The objective of this testing is not to test the security of the device, but its resilience to abnormal data and assess the error and boundary checks of the logic itself.

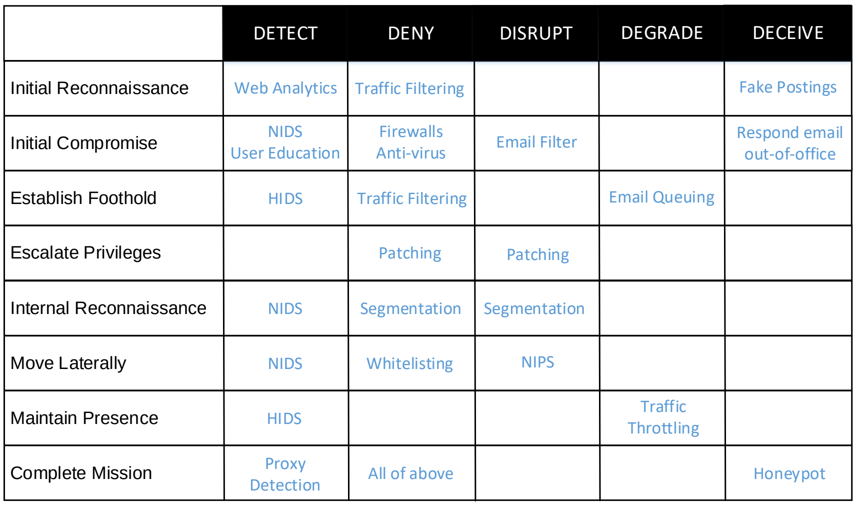
Isolated: A *device-centric* view of security that isolates a device identified as critical or attractive to an attacker, and assesses its inherent vulnerabilities. Preparation for isolated testing includes interrogating CVE databases to identify security testing performed elsewhere. Isolated testing should assess whether the recorded vulnerabilities are present within the device under test. However, not all vulnerabilities are identified or recorded within ICS equipment communities, so isolated testing should systematically test the device to assess its security. Techniques such as STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) threat modelling approach [224, 225] allow various methods of driving a vulnerability, especially those enabled by devices that are insecure by design. Depending on the licensing of the device, techniques such as fuzzing may also be adopted.

Synthesised: An *integration-centric* set of test scenarios that assesses any vulnerabilities introduced as a consequence of the integration of critical or attractive ICS devices and components. A synthetic environment such as a cyber range should be used to assess the device or interrelated devices in an architecturally representative environment that takes the output from the *simulated* and *isolated* stages to produce the requirements for testing at the synthesised stage. This allows the human aspect of control systems to be considered, as the range permits operational procedures to introduced to assess the operator's response to various situations and industrial process conditions. It also offers the additional benefit of supporting *red teams* to further analyse the attack options available to an antagonist, with the option to extend this to a CDX to assess the organisation's ability to respond to the targeting of the device or component.

As the testing iterates, the results feedback into the ongoing analysis of the *Deployed Architecture*, *Antagonistic Target Determination*, and *Attack Options Analysis* steps, allowing remedial means to address security vulnerabilities of be assessed. It also drives the development of *Security Monitoring* strategies and *Incident Response Plans*, and can feed the scenarios for a progressive collective training programme, as proposed in Section 6.

5.3.6 Step 6 - Security Monitoring

Many older ICS devices are inherently insecure [3] and hardening may not be viable. At this point the defensive analysis must move from the consideration of protection to that of active defence.



	DETECT	DENY	DISRUPT	DEGRADE	DECEIVE
Initial Reconnaissance	Web Analytics	Traffic Filtering			Fake Postings
Initial Compromise	NIDS User Education	Firewalls Anti-virus	Email Filter		Respond email out-of-office
Establish Foothold	HIDS	Traffic Filtering		Email Queuing	
Escalate Privileges		Patching	Patching		
Internal Reconnaissance	NIDS	Segmentation	Segmentation		
Move Laterally	NIDS	Whitelisting	NIPS		
Maintain Presence	HIDS			Traffic Throttling	
Complete Mission	Proxy Detection	All of above			Honeypot

Figure 5.6: The Diamond Model *Course of Action Matrix* integrated with the Mandiant Attack Lifecycle

A Course of Action (COA) Matrix [190] (Figure 5.6) is developed from the Activity Threads and Activity-Attack Graphs. It determines how to detect, deny, disrupt, degrade or deceive an attacker, and assists in the analysis of where sensors should be deployed to identify antagonistic behaviours.

5.3.7 Step 7 - Incident Response Planning

Hardening of devices and strengthening the perimeter of a networked system are essential steps towards defending an ICS from malicious activity. However, protective measures only serve to reduce the attack possibilities. When dealing with an intelligent, adaptive adversary, it is necessary to consider defensive plans to support any intrusion to allow incident responders to anticipate the antagonists' next steps. The use of Activity-Attack Graphs and COA matrices [190] considers the options available to an attacker, and describes the characteristics of each attack event using a diamond model representation, developing a set of *'competing hypotheses'* [226]. This provides a basis to build an incident response *'playbook'* that can be iteratively improved through table-top exercising and determine the most efficient means to deny the attacker access to the critical system assets. These playbooks can be assessed for the efficacy in a progressive collective training programme, as proposed in Section 6.

5.4 Analysis

As the simulation steps of the process have been demonstrated by Krotofil et al. (2014, 2015) [220, 107], and require detailed process engineering specialisms, recreating these experiments was deemed unnecessary. Isolated testing of ICS devices has been widely acknowledged as a viable means of assessing vulnerabilities of individual ICS devices [227, 228, 229], and again it would not have enhanced the evaluation of the framework by repeating analyses undertaken elsewhere. CDXs, however, provided a means by which the synthesised elements of the process could be evaluated, as well as simulating antagonistic actions against an ICS. During a large-scale CDX in July 2016 [230] it was observed that the use of the CARVER Matrix in Step 3 of an early iteration of the ICS-CDTP, with the modified assessment criteria described in this article, identified critical systems to the continued operations of ICS facilities. However, this was initially limited to systems that provided operational functionality, as opposed to technical infrastructure systems such as domain controllers etc. The Diamond Model Activity Threads and Activity-Attack Graphs in Step 4 of ICS-CDTP successfully tracked antagonistic events, using COA Matrices to determine multiple attack options, and demonstrated how analysis of Activity Thread models (a vertical analysis of the model) identified attacker progress through the networks being defended. Similarly, the horizontal analysis of the Activity Models and Activity-Attack Graphs identified common attack techniques across target networks, supporting the sharing of threat intelligence across Blue Teams. This did not prevent all Red Team activities, as systems were still compromised, but the freedom of Red Teams actions was limited to systems not assessed as critical. Red Team progress toward these systems was observed to be slower than towards non-critical systems that had not been proactively hardended, with an increased deployment of network and host sensors.

However, whilst the techniques used in the CDX demonstrated their effectiveness, they were largely paper-based, and required a significant investment of resources and effort. As the CDX progressed, the manual maintenance of paper-based data repositories became an increasing drain on the Blue Team resources, suggesting that support tools would be necessary to implement the triage process at scale.

In summary, of the eight questions posed in Table 5.1 that this framework should address, Table 5.9 describes how the various components described in this paper interact to provide a coherent model for triaging ICS.

Question	**Framework Components**	**Comments**
1. Which devices are attractive to an attacker?	CARVER Matrix	The CARVER model supports the assessment of devices that would have the most significant impact on an ICS facility, and therefore those most attractive to a capable APT actor.
2. Can we better protect these devices?	Process simulation, device testing, synthetic environments	Process simulation identifies process variable vulnerabilities, which subsequently drives the isolated and integrated security testing of the devices responsible for using these variables.
3. What routes exist to these devices?	Activity Threads, Activity-Attack Graphs, Extended Activity Graphs, COA Matrix	The modelling of event threads and graphs supports the assessment of routes towards the identified critical devices.
4. What events would occur in an attempt to access and manipulate these devices?	Activity Threads, Activity-Attack Graphs, Extended Activity Graphs	The same event threads and graphs that determine the viable route towards a critical device are also used to determine the antagonistic events that would occur as a result of an attack.
5. Where can we deploy sensors to detect these events?	Security monitoring and incident response planning	The positioning of sensors and IDS would be guided by the event threads and graphs. The responses to such event detection would then form the basis of an incident response plan.
6. How will we determine which of the alternate routes to a device are being used by an attacker?	COA Matrix	The sensor and IDS deployment would be based on the possible routes to critical devices. Any alerts would be cross-referenced to the COA Matrix to assess which of the many possible COAs is likely to be followed.
7. How can we predict an attacker's next activity?	Activity Threads, Activity-Attack Graphs, Extended Activity Graphs, COA Matrix	With the possible COAs established, the event threads and graphs can be used to assess where along the attack path the antagonist is currently positioned, and therefore which steps must be achieved before the critical device is compromised.
8. What does our incident response plan need to describe and test in order to mitigate residual risks identified in the analysis?	CARVER, Process simulation, device testing, synthetic environments, security monitoring and incident response planning	The CARVER Matrix will highlight the initial attractiveness of a system or device, and simulation and testing will determine the extent of the associated risks. This will shape the security monitoring posture and incident response plans based on the ascertained residual risk.

Table 5.9: ICS-CDTP mapped to the questions posed in Table 5.1

5.5 Initial Conclusions

ICS-CDTP provides a framework to assess the attractiveness and criticality of ICS devices that underpin industrial processes. As a validated dataset describing the nature of cyber attacks on ICS is unavailable, ICS-CDTP is based on subjective assessment of likely antagonistic targets. However, the use of safety data and simulations to drive the criticality assessment of key processes focuses on their impact on the industrial facility's ability to operate, and is based on a proven military and counter-terrorism methodology, extended for ICS. This drives the identification of those ICS devices responsible for the critical data measurements, calculations and control element manipulations that could be altered to achieve antagonistic aims, and therefore which should be triaged for immediate security testing and remediation. The approach to testing, focusing on non-destructive means that do not require access to the production environment, does not expose the ICS operator to risks that arise as a consequence of unintended consequences of security activities. As such, it provides a viable coping strategy for ICS operators establishing initial cyber situational awareness.

ICS-CDTP accepts that whilst we might define the attractiveness of a target, and identify the many routes towards it for exploitation, we cannot know *a priori* which precise route the attacker will take, or how his behaviours will change based on our defensive actions. By modelling the many courses of action available to an antagonist and overlaying this onto the deployed architecture, ICS-CDTP can determine the characteristics of malicious behaviour in each segment or layer and define the necessary signatures or heuristics by which our sensors can identify the attack. ICS-CDTP security responders can be provided with a pre-incident assessment of the courses of action available to an attacker, preventing antagonists from reaching or affecting the devices critical to the key processes of the industrial facility. This understanding and associated procedures can form the basis of a progressive series of TTX and CDX to measure efficacy and drive the development of enterprise mental models and SA.

ICS-CDTP provides a coping strategy, addressing Question 2 - *Does the adoption of coping strategies increase situational awareness?* of the six research questions posed in Section 1.4. It contributes an integrated process that combines the Diamond Model of Intrusion Analysis [190], the Mandiant Attack Lifecycle [15], and the CARVER Matrix [90]. It includes novel extensions to the Diamond Model event description and activity modelling to accommodate ICS. It further provides novel contribution by modifying the CARVER assessment criteria to support cyber impact on ICS. ICS-CDTP provides an effective triage of attack vectors and likely targets for a capable antagonist, identifying key ICS processes and their exposure to cyber threats, with the view to maintaining critical operations. These are essential elements of Question 5 - *As a result of serious games, can participants recognise the characteristics of a cyber attack and determine the possible intent and courses of action?*, and Question 6 - *Are participants of serious games able to assess the immediate and longer-term impacts of cyber attacks?* posed in Section 1.4.

Chapter 6

A Framework for Progressive Collective Training

Contents

6.1 Introduction

Capable APT adversaries are characterised by sophisticated levels of expertise and significant resources used to exploit opportunities to pursue objectives over an extended period of time, adapting to defenders' efforts to resist them [140]. Organisations such as critical national infrastructure (CNI) providers using ICS face a dynamic, evolving threat landscape as a result. Consequently, they carry an associated degree of operational risk. As we discussed in Section 3.5, to address this threat, literature asserts that we consider three questions; 1) what can happen? (i.e., what can go wrong?), 2) how likely is it that it will happen?, and 3) if it does happen, what is the impact? [74]. However, as also discussed in Section 3.5, the level of incident reporting available has not produced a sufficiently quantified and observable set of metrics for cyber attacks on ICS to answer these questions or inform generally-accepted risk models, and there is limited value in the probability judgements based on such techniques. Indeed, given the adaptability of the antagonists, preventing intrusions from well-resourced APT actors presents CNI operators with a significant challenge. Awareness of a risk is one of the main factors of a successful risk management programme [141]. By proactively raising awareness of threats and their impacts it poses less risk than if we have no understanding of its potential impact [74]. SCIPS promotes an understanding of this risk at the conceptual level, and the ICS-CDTP offers a structured process to develop a focused defensive posture. However, without a wider appreciation of the dynamic nature of the APT adversary and the necessity to maintain a trained incident response capability against such antagonists, ICS operators still carry residual risk.

SA models potentially provide a framework to better understand the landscape and raise awareness of the threats, helping to shape the cognitive processes of incident responders, and allowing the tailoring of risk mitigations to better fit the individual needs of the targeted organisation [142, 143]. It is argued that a well-trained response team that understands the nature of the antagonist is critical to success in responding to APT incidents [144].

Since incident response teams cannot be prepare for every APT situation, or predict every crisis, training activities must be provided to support operating in challenging situations to develop concrete guidance, procedures and tools to help individuals to collectively react to network intrusions [145]. To produce the level of team cohesion and adaptability required to respond to the variety of APT attacks an organisation might face, the training environment should include simulations to contribute to the progressive, cost-effective establishment and maintenance of SA and skills proficiency [146].

This chapter explores the requirements for collective cyber incident response (IR) training and proposes a framework to develop progressive individual and team SA.

6.2 Situational Awareness

To recap our appraisal from Chapter 3, SA, as defined by Endsley (1995) is *"the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future"* [147]. This definition comprises three levels of SA, as described in Section 3.7 and illustrated in Figure 6.1.

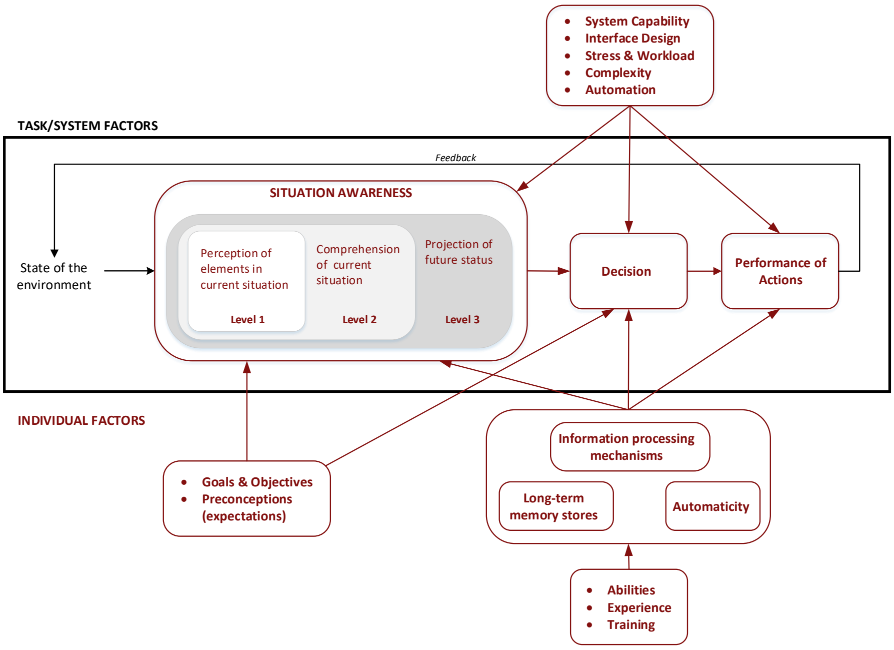


Figure 6.1: A model of situational awareness in dynamic decision making, Endsley (1995)

Figure 6.1 describes SA within the context of a decision-making process. An individual's perception of the constituent parts of the environment, from whichever sources they take their information from, forms the basis of their SA. Importantly, the selection of a decision derived from SA is separate from the resulting performance of the selected actions. There are many factors that influence the decision-making process. Key within these are the individual's innate abilities to process information, their prior training, and previous experiences. These may be further influenced by their preconceptions that can introduce a bias that affects their development of SA [147].

As discussed in Section 3.7, a critical element of SA is understanding the rate at which information changes. The dynamic nature of cyber IR dictates that as the situation evolves, so an individual's and team's SA must adapt. In rapidly changeable environments this requires operators to adopt many cognitive strategies for maintaining SA [148]. Mental models allow people to predict and explain the behaviour of the world around them, to recognise and remember relationships among components of the environment, and to construct expectations for what is likely to occur next [18, 149]. SA therefore becomes a function of the processes and systems that provide and process information before, and during, a cyber incident. In this situation the features of the task environment, including task complexity, individual workload, and stress, may also influence SA. It is important to acknowledge that SA does not encompass an individual's complete knowledge or expertise. It only refers to the elements pertinent to the dynamic environment [147]. Accordingly, it is necessary to consider the volatility of the information within the environment where SA must be established and maintained.

By separating SA from decision-making and performance of actions, we can consider the ability to comprehend the environment and project future statuses as distinct from the proficiency of response to the situation. Even experienced decision makers will make the wrong decisions if they have inaccurate or incomplete SA. Conversely, a person who has perfect SA may still make the wrong decision if they lack appropriate training and experience to comprehend the situation, or may exhibit poor performance if they do not possess the skills technical to remediate the situation. SA, decision-making, and performance, are therefore different stages within an overall process, with different factors influencing them. We therefore require a training construct that develops the mental models necessary to establish SA, along with procedural and technical skills to shape performance, that allows a set of coping strategies to be practiced and rehearsed prior to an APT event. This must look beyond individual SA, and address SA across an entire team or enterprise.

Team SA, as illustrated in Figure 3.4, is the degree to which every team member possesses the SA required for their own responsibilities, independent of any overlaps in SA requirements that may exist. It is not sufficient that one knows perfectly but the other not at all, every team member must have SA for all of their own requirements [147].

6.3 Mental Models

Shared mental models help teams to cope with difficult and changing task conditions [151, 152]. The ability to adapt is an important skill in high-performing teams, and a shared mental model is an essential element of a team's adaptability. We shall now consider the types of mental models we require to inform SA as the basis for incident response.

By their nature, APT attacks are covert and difficult to detect, with a degree of tailoring available to the antagonist in order to achieve focussed outcomes on the target network. However, it has been demonstrated that APTs follow a common attack lifecycle, performed in several phases, that can be broadly characterised as reconnaissance, preparation, execution, gaining access, information gathering and connection maintenance [231], as characterised by the Lockheed Martin™ Kill-Chain and Mandiant™ Attack Lifecycle Model. Such lifecycles allow a mental model to be constructed that encompasses the adversary behaviour discussed in Section 3.8, using an understanding of a representative antagonist's observable actions to create attacker profiles so that effective countermeasures can be designed.

Another factor that may contribute to SA and shared understanding is a model that assists each member of a team to understand the roles and responsibilities of other team members and their patterns of interaction [150]. This would need to be augmented with an understanding of the skills, expertise, attitudes and preferences of the individuals that comprise the team, to assist everyone involved to anticipate their colleagues' reactions to certain situations.

Incident responders across the enterprise require a shared mental model that describes the operational priorities of the organisation, so that their efforts are aligned to ensuring the mission-critical aspects of the operation are maintained throughout the attack. This would require a mental model that describes the operating environment of the ICS, encompassing processes under control as well as the technology estate.

These requirements manifest themselves as five shared mental models, derived from the four models proposed by Mathieu et al. (2000) [149], extending them to accommodate the characteristics of the cyber environment, recognising the volatility of the underpinning information. This extended model is presented in Table 6.1.

Type of Model	**Knowledge Content**	**Model Volatility**	**Comment**
APT Attack Behaviours	Attack methods, threat actors, intrusion sets, campaigns, malware	High	A shared knowledge of antagonistic cyber behaviours allows teams to apply this understanding to the operating environment and operational priorities. However, the adaptability of APTs requires a continual analysis of the threat landscape and recognised intrusion sets. As a consequence, this mental model is unlikely to ever be complete, and the accuracy of the model is not likely to be high.
Team Interaction	Roles and responsibilities, information sources, interaction patterns, communication channels, role interdependencies, information flow	High	Shared knowledge about team interactions drives how team members behave by creating expectations. Adaptable teams are those who understand well and can predict the nature of team interactions. The team interaction will be driven by the nature of the threat facing the organisation, and as the result of APT adaptability, team interactions and roles/responsibilities will be required to be continually refined in line with emerging threats. The model will have a strong basis on established IR practice, so although specific elements of the information requirements and flows will be highly volatile and dependent on mechanisms to detect and respond to incidents, the major elements will be stable.
Team Understanding	Teammates' knowledge, skills, attitudes, preferences, and tendencies	Medium	Team-specific knowledge of teammates helps members to better tailor their behaviour to what they expect from teammates. Personality traits are likely to be a low-volatility, the training requirement and relative knowledge of teammates skills will maintain a higher level of volatility.
Operational Priorities	Key business and operational processes, key operational and infrastructure systems	Low	Relatively stable model, but subject to changing business priorities. However, it is expected that these will be regularly communicated to the team and used for pre-incident planning, so the volatility is expected to be low as a result.
Operating Environment	Technical environment, operating procedures, system limitations, known vulnerabilities	Low	Likely to be the most stable model in terms of content, as the operating environment will have to follow established change control processes for modifications to occur. It is probable that a high degree of model stability can be achieved.

Table 6.1: Types of shared mental models for cyber SA, adapted and extended from Mathieu et al (2000)

Mental models are developed as a result of training and experience in a given environment. With experience, recurrent situational components will be noticed, along with repeat associations and causal relationships [147]. Instruction should be structured such that new information or knowledge builds on existing knowledge. This facilitates the development of SA, as personnel are able to develop increasingly detailed mental models [154]. The requirement to develop experience-based understanding suggests experiential learning may provide a suitable vehicle by which individuals and teams can develop the mental models necessary for SA in incident response situations.

6.4 Experiential Learning for Developing Situational Awareness

As discussed in Section 3.7.1, the crawl-walk-run approach to training is typically applied sequentially through a series of training episodes. However, it has been demonstrated that providing progressive training scenarios that deliver crawl-walk-run training opportunities that are cumulative, and grow in complexity, delivers far greater training benefit [152]. By placing the responsibility for learning on the trainee, requiring them to solve problems during the scenario in a crawl-walk-run manner, experimental results demonstrate that learning is accelerated when compared to traditional methods [152]. Adapting the model proposed by Schaab and Moses (2001) [152], previously discussed in section 3.7.1, to accommodate the three levels of SA defined by Endsley (1995) [147] we can provide a series of progressive crawl-walk-run developments to develop SA within a framework of increasingly complex scenarios. This is illustrated in Figure 6.2. In this way, individuals and teams can develop in a progressive manner, building their understanding, information processing mechanisms, long-term memory stores, and automaticity, as required for SA.

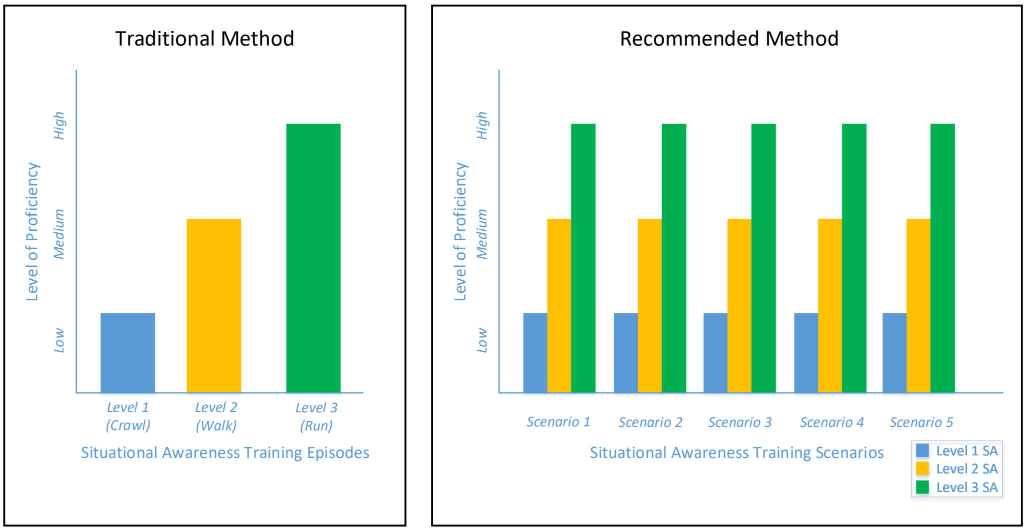


Figure 6.2: Traditional and recommended methods of collective training, adapted from Schaab and Moses (2001) to accommodate the three levels of SA from Endsley (1995)

6.5 A Framework for Progressive Collective Training to Develop Situational Awareness

Using this progressive approach, we shall now consider its application to collective training exercises, as a form of serious game. The literature review of works pertaining to collective training in Chapter 3 highlighted that much of the research in this field related to military skills development. Whitney and Vozzo (2012) [151] performed a review of experimental studies, interviews with subject matter experts, reports on military collective training, and psychological research in learning and training. They produced a set of recommended content for collective training. Zipperer et al. (2003) [165] compiled results from training questionnaires and interviews with experienced military instructors, supplemented by interviews with subject matter experts. They highlighted the evidence of the effectiveness of the crawl-walk-run approach to training. Pike and Huddleston (2011) [161] conducted a training needs analysis for team training, using a systematic process of analysing established training tasks and identifying suitable training options. They concluded the inherent complexity and scale of collective training puts it beyond the analytical reach of the techniques normally employed for individual training. Lemmers et al. (2004) [164] evaluated collective training in a distributed simulation exercise, focussing on the issues surrounding the evaluation of exercises that use synthetic environments. Schaab and Moses (2001) [152] investigated how soldiers acquire new skills, individually and collectively, using a combination of observations, surveys, and analysis of performance on practical exercises.

By combining and consolidating the concepts and results of the research by Whitney and Vozzo (2012) [151], Zipperer et al. (2003) [165], Pike and Huddleston (2011) [161], Lemmers et al. (2004) [164], and Schaab and Moses (2001) [152], a set of 17 requirements for progressive collective training for the development of SA were derived. These are proposed in Table 6.2.

A workshop facilitated by the author [232] with the leadership of a team of experienced incident responders from the research sample used for the experimentation in this research (described in section 7) reviewed the requirements in Table 6.2. The output was the definition of a framework of five levels of progressive steps to incrementally provide realistic incident response training. It introduces increasingly capable threat actors through the levels, and an associated requirements for improved SA, in an environment intended to promote learning and development. The framework spans both table-top (TTX) and cyber defence (CDX) exercises, providing common, integrated goals across the exercise types. They start at Collective IR Training (CIRT) Level 1, focusing on the development of interactions between members of sub-teams within an overall team, facing a low-level threat actor in a simple scenario, through to CIRT Level 5, where multiple incident response teams must coordinate to respond to high-level threat actors in a complex scenario. The summary of each level is provided in Table 6.3. Whilst the training objectives are common across exercise types, the assessment characteristics are specific to TTX and CDX. Accordingly, we shall now discuss the detailed use of the

Req.	Overview	Description
1.	Approach	Follow a crawl-walk-run structure.
2.	Composition	Be easily broken-down into component tasks.
3.	Understanding	Provide appropriate mental models to allow comprehension of the environment.
4.	Situational Awareness	Enhance situational awareness across levels 1 to 3.
5.	Review	Allow ample opportunity to review performance.
6.	Feedback	Provide regular feedback and opportunities for reflection.
7.	Learning Environment	Provide a learning environment in which it is safe to fail.
8.	Individual Skills	Take into account personnel's existing knowledge and skill levels.
9.	Skill Development	Build on previous knowledge and experiences.
10.	Participation	Provide opportunities for hands-on experience or active participation.
11.	Skill Maintenance	Provide sessions for ongoing maintenance of skill and knowledge.
12.	Environment	Resemble a realistic environment.
13.	Vocabulary	Develop a common lexicon for team interaction.
14.	Interactions	Drive team interactions and incident responses processes.
15.	Role Definitions	Drive greater clarity in the definition of team roles and responsibilities.
16.	Progressive Threat Model	Progressively introduce capable threat actors.
17.	Metrics	Facilitate metrics to measure improvements in capabilities and situational awareness.

Table 6.2: Requirements for progressive collective training to develop situational awareness.

CIRT levels as a progressive training framework.

6.5.1 Table-Top Exercises (TTX)

Table-top exercises (TTX), within this framework, are intended to test the completeness of operating instructions for the team, and the overall command of control (C2) during an incident. Whilst members of a response team may be individually highly-skilled, their effectiveness must be within a structure that ensures that wider Team SA is maintained, and so that individuals may be replaced if necessary. This requires complete documentation of incident response plans and techniques to address defensive cyber activities.

Collective IR Training (CIRT)	**Title**	**Description**	**Scenario Complexity**	**Threat Actor Capability**
Level 1	Sub-Team Review	Assessment of the ability of a sub-team, within an overall incident response team, to understand and execute their required functions efficiently and effectively	Simple	Low
Level 2	Team Review	Bringing together each of the sub-teams into an overall operating unit, to test the efficacy of the C2 of the team and their ability to work cooperatively.	Simple	Low
Level 3	Team Validation	Assess the ability of the team to deal with a realistic scenario that contains business or operational priorities, facing a competent threat actor.	Medium	Medium
Level 4	Team Stress Test	Progression to a complex realistic scenario supporting multiple stakeholders, whilst still facing a competent threat actor	Complex	Medium
Level 5	Multiple Teams Testing to Failure	A complex scenario involving more than one organisation, with incident response teams required to interact with outside agencies in order to deal with a large-scale, highly capable threat actor delivering coordinated attacks against all exercise participants. The intent of this level of testing is to assess at which point the teams fail to address the complexity of the situation.	Complex	High

Table 6.3: Summary of progressive collective training levels for cyber incident response.

TTX CIRT Level 1

Within a TTX, the intent of CIRT Level 1 (CIRT1) training is to assess the coherence of the operating processes and instructions used at the sub-team level within an overall incident response team. This allows any gaps in the documentation to be identified, addressed and re-evaluated. The scenario within the CIRT1 TTX should follow the crawl-walk-run model by progressively introducing more complex reports of attack activity from a low-level threat actor, to increase the requirement for SA. This necessitates the sub-team to project which antagonistic courses of action an attacker might take, and therefore which procedures are applicable to proactively defend the network.

Assessment of the sub-team within the TTX is via a measure of adherence to approved operating procedures, and the identification of gaps in the documentation that are required to be addressed for the sub-team to be effective within the overall team.

TTX CIRT Level 2

The second level of CIRT involves bringing together all of the sub-teams to assess how the operating procedures of the team and sub-teams interoperate, and how overall C2 and SA is maintained during an incident. Whilst the training at TTX CIRT1 will focus on coherence within the roles and responsibilities of a sub-team, training at CIRT2 tests the interfaces between sub-teams, and the ability to maintain shared SA in the face of a low-level threat actor within a simple scenario. Assessment at this level, as with CIRT1, is through measurement of adherence to approved operating procedures, and the identification of gaps in the documentation.

TTX CIRT Level 3

At level 3, the TTX introduces a background exercise scenario as well as an operational or business owner with dynamic priorities that extend beyond technical availability of systems. The exercise requires the incident response team to report to a management structure at regular intervals, requiring greater SA from the team, as well as the need to forecast defensive activities to respond to a mid-tier actor with the capability to manoeuvre covertly around a network and adapt to the incident responders' actions. At this level, the assessment of the team focuses far more on SA and C2 than operational procedures. It measures the adaptability of the team to manage a dynamic situation and interact with business stakeholders.

TTX CIRT Level 4

The TTX at Level 4 further increases the complexity of the scenario and the level of information to be processed by the incident response team, including external threat intelligence feeds. A greater number of malicious activities will be reported at this level, forcing the team to prioritise their activities against a set of mid-tier actors acting in a coordinated manner. This will be set in a mission-critical environment with reporting required to outside agencies such as national cyber centres and governmental regulatory bodies, as well as interacting with the press. This reporting requirement will also shape the internal stakeholder requirements for the incident response team's planned activities to mitigate the initial impacts of the attack, balanced against defending against the attackers' wider intent.

Assessment at this level is focused on C2, balancing competing priorities, and maintenance of SA in an information-rich environment.

TTX CIRT Level 5

Level 5 CIRT exercises are intended to test the participants to the point of failure. This is intended to determine at which point the C2 of the team cannot cope, and as such the scope of such an exercise may exceed the conditions anticipated for a real incident. Level 5 exercises are intended to simulate incidents that extend beyond individual organisational boundaries, such as national crises, which will involve many organisations on which the incident responders may depend, and in turn, on whom other organisations are dependent. A coordinated set of high-tier threat actors will deliver multiple, overt and covert attacks on defender's networks, forcing them to prioritise where and how to respond, interacting with other incident response teams, threat intelligence feeds, governmental and regulatory bodies, and the press. The scenario will be purposefully complex, with competing requirements and priorities for which there are no clear responses. Assessment at this level is based on individual teams' ability to maintain control and SA in a dynamic environment.

6.5.2 Cyber Defence Exercises (CDX)

Within CDX, the progressive levels of complexity described for TTXs are maintained, but as the exercises are executed on a cyber range the focus is on technical responses and the associated detail of network operations.

CDX CIRT Level 1

CDX collective training at Level 1 (CIRT1) requires minimal range infrastructure, as it is designed to train the functions of the sub-teams within an overall incident response team. As such, the training is role-specific. For instance, for a sub-team responsible for network hardening, the range provided would need to offer weakened Virtual Machines (VM) or ICS devices for the team to test their operating procedures in a realistic technical environment. Crawl-walk-run progression is offered through the level to which hardened VMs or ICS devices are tested. This does not necessarily require an *in situ* Red Team, as the evaluation of the VMs or devices could be managed via automated test scripts, although at this level they are intended to be assessed based on a low-tier threat actor. Similarly, for security analysts, scripted malicious traffic of increasing complexity could be replayed over a network, and a measure of success be defined by how much of the activity is recognised. CDX CIRT1 should assess how individuals trained in specific areas of technology can work together prior to integration into a larger incident response team.

CDX CIRT Level 2

At CIRT Level 2 (CIRT2), the entire incident response team is brought together to exercise on a cyber range. This training is based around a simple scenario featuring a low-tier actor, and provides an opportunity for the team to deal with an incident at a slower pace than in the real-world. The Red Team should be provided with a playbook of network attacks that are appropriate to this tier of threat actor. This allows the realities of incident response to be mapped against the management of SA and C2, and how information flows in a technical sense within the team. This should include how teams triage the elements of network to assess which are a defensive priority. Assessment at this level should review the progressive complexity of the network attacks and the information available to the team to determine their effectiveness and efficiency.

CDX CIRT Level 3

At this level (CIRT3), far more realism is introduced to the exercise. The exercise scenario will contain more depth than at CIRT1 and CIRT2, and as with the TTX CIRT3, a business influence will be provided via stakeholders who will dynamically define the operational priorities of the network. Much more simulated background network traffic will be generated at this level of training, providing a suitable noise floor for the mid-tier threat actor to mask activities within. The incident response Blue Team will be required to work more interactively with their sensors and logs than at CIRT1 and CIRT2, as they adapt to a dynamic adversary. At CIRT3, the C2 and SA of the team will be tested with a complexity more aligned with a real-world incident, albeit within the time constraints of a training exercise. Assessment of the team will be based upon how many of the Red Team attacks are identified and/or prevented by the Blue Team incident responders, and how well they maintained control of the situation as a cohesive team.

CDX CIRT Level 4

At CDX CIRT Level 4 (CIRT4), more external relationships are introduced to the scenario, and the scale of the range and associated network traffic levels is increased. External threat intelligence feeds will be integrated, as will the need to produce technical information for regulatory and governmental bodies. A larger Red Team will be provided to deliver coordinated attacks on the range, and whilst still acting in the character of a mid-tier actor, the frequency and breadth of attacks will be designed to progressively stress test the technical cohesion of the team, and the overall C2. Business users will be added to the scenario to bring further non-technical complexity and require the Blue Team to respond to incidents guided by business needs. This will require the maintenance of SA across both business and technical domains to ensure the overall attack is proactively defended against. Assessment at this level is based upon the incident response Blue Team not only technically defending the network, but also predicting the Red Team's malicious courses of action, to allow them to pre-empt their attacks and restrict their ability to manoeuvre on the network.

CDX CIRT Level 5

As with Level 5 CIRT TTX, the Level 5 CIRT (CIRT5) CDX is intended to test participants to the point of failure, and designed to determine at which point the C2 of the team cannot cope. In a CDX, the scenario will be based upon a complex crisis, and will involve multiple incident response Blue Teams on a range that can accommodate the defence of multiple networks from a coordinated Red Team acting as a high-tier threat actor. Blue Teams will be required to cooperate, sharing detailed threat intelligence to defend their networks. As with the TTX, assessment at this level is based on individual teams' ability to maintain control and SA in a dynamic environment.

6.6 Analysis

The requirements for a progressive collective training intended to develop SA, as described in Table 6.2, are discussed within the context of the progressive collective training framework, with comments made on the implications for TTX and CDX.

6.6.1 Approach

Within a TTX the approach will progressively increase the exercise information flow and interrogation of detail in incident response processes to provide a coherent crawl-walk-run model. In CDX the framework will provide a crawl-walk-run model across CIRT1-CIRT5, and within each of these levels the Red Team will provide the ability to progressively increase complexity as a response to the Blue Team performance.

6.6.2 Composition

CIRT1 and CIRT2 within TTX will focus primarily on component tasks, whilst CIRT3-CIRT5 will provide the ability to refine the efficacy of the components in increasingly complex situations. For CDX, the basic technical component tasks will be developed in CIRT1 and CIRT2, with greater depth of understanding of the technology required in CIRT3-CIRT5. Improvements in the technical depth required for CIRT3-CIRT5 will be achieved through more complex CIRT1 and CIRT2 exercises, executed in an overall training cycle.

6.6.3 Understanding

Mental models will be introduced during TTX that operate at a low tempo. This will allow the mental models to consolidate prior to being tested at a greater pace. Ideally, mental models will be developed on TTX prior to progression to CDX. Mental models introduced on CDX that have not been ‘walked-through’ on a TTX are likely to be less developed at CIRT3-CIRT5.

6.6.4 Situational Awareness

This will be achieved on TTX through the exercise White Team using questioning techniques to assess the Blue Team’s perception, comprehension, and projection of adversary activities so they can be progressively enhanced. This will be fused with the mental models, and ideally is rehearsed on TTX prior to CDX. On a CDX, SA will be necessary to interpret the adversary activities on the network to project antagonistic courses of action. Without this understanding the Blue Team will only ever catch-up with where the Red Team have already been. The development of information flows and mental models to enhance SA are required to have been consolidated at CIRT2 and CIRT3 prior to undertaking more complex CDX.

6.6.5 Review

Where the TTX identifies gaps in operating procedures, subsequent exercising should not be undertaken until all remedial actions have been undertaken, and the team provided with time to reflect on the consequences of new operational tasks. For CDX, post-exercise reports or assessments should be a key mechanism to record any lessons learned, and highlight areas for improvement. These comments should be reviewed and remedial actions undertaken and tested before returning to a CDX at the same, or greater CIRT level.

6.6.6 Feedback

TTX will provide an opportunity for interactive feedback from the White Team to allow the Blue Team to reflect on their actions and adjust accordingly. On CDX, regular, detailed feedback from Red Team will be required to develop Blue Team improvements on CIRT2-CIRT5.

6.6.7 Learning Environment

A non-judgemental White Team will be essential on TTX to allow an open discussion of deficiencies in operating procedures, to identify opportunities for improvement. For CDX, a mix of regular feedback from the Red Team, along with coaching from the White Team in response to Red Team feedback, will provide an environment where failure to detect a Red Team activity was seen as a learning opportunity.

6.6.8 Individual Skills

Across both TTX and CDX, those with a greater understanding of component tasks are likely to perform better. It would be prudent to use those personnel with greater experience to mentor junior staff, to bring the less experienced members of staff up to a common level of expertise.

6.6.9 Skill Development

Technical skills are likely to be less of an issue within the TTX, but knowledge of the Blue Team's processes and procedures are essential. For CDX, progression through the CIRT levels will be most effective when sequential. CDX at CIRT4 and CIRT5, in particular, will likely require iterative cycling between CIRT1-CIRT3 for maximum effect.

6.6.10 Participation

In TTX, participants should be encouraged to actively participate in their role and develop the formal interactions between teams, sub-teams and individuals. CDX will provide opportunities to test individual skills and component tasks in a hands-on manner, identifying areas for improvement as a result.

6.6.11 Skill Maintenance

The CIRT1-CIRT5 construct for TTX allows for ongoing maintenance of skills and testing of the applicability of processes and procedures in an evolving threat landscape. The provision of a cyber range for CDX, along with the progressive levels of CIRT1-CIRT5, allows for maintenance of individual and team technical skills.

6.6.12 Environment

The scenarios for the TTX should provide realistic context to consider the efficacy of processes and procedures. For CDX, a well-architected cyber range should provide a realistic, representative environment to rehearse incident response.

6.6.13 Vocabulary

The slower tempo of a TTX will provide an opportunity to assess how language is interpreted by team members, and develop a common terminology. CDX will ideally build upon the lexicon developed in the TTX, although existing, established technical language is unlikely to require any adjustment.

6.6.14 Interactions

TTX will provide a mechanism to test team interactions and assess incident response processes at a slower tempo than on CDX. However, CDX will likely drive a greater understanding of technical information flow between team members.

6.6.15 Role Definitions

TTX will likely be the main vehicle for driving the definition of roles and responsibilities, whereas CDX will verify and refine these, driving greater detail in the nature of team interactions.

6.6.16 Progressive Threat Model

Threat actors can be progressively introduced on the TTX through increasing the reported impact of antagonistic activities. The threat actors on the CDX, likely to be APT in this research, will be characterised by a progression of covertness and complexity of attacks across the lifecycle of an attack delivered by the Red Team.

6.6.17 Metrics

Qualitative or quantitative methods, or a mix thereof, can be used to capture data to assess the effectiveness of the exercises, capability development, and SA, across both

TTX and CDX, as dictated by the learning objectives.

6.7 Initial Conclusions

SCIPS provides an initial experience of an end-to-end attack where it is safe to fail. This is sufficient for some training participants for whom change in risk perceptions is desirable. However, for those responsible for planning or executing defensive policies, procedures or capabilities, the SCIPS scenario should be used as the basis for subsequent TTX and CDX. This will take advantage of the embryonic mental models established as a consequence of playing SCIPS, and progressively reinforce the developing models in the minds of participants. It therefore becomes essential to consider how scenarios developed for SCIPS will transition into TTX and CDX, to deliver a holistic training experience. Similarly, the ICS-CDTP provides a structure for defensive cyber operations within ICS operators to underpin a foundation for refinement of these mental models. This will be assessed in the experimentation described in Chapter 7.

The *APT Attack Behaviour* mental model can be developed through the fusion of cyber threat intelligence (CTI) with the use of an attack lifecycle model such as the Lockheed Martin Kill-Chain™ or Mandiant™ Attack Lifecycle Model to frame the understanding of exercise participants. The adherence to such a structure by the Red Team will allow this experience to solidify in the minds of the Blue Team.

A *Team Interaction* model will be derived from the definition of roles and responsibilities primarily within TTX, then refined on CDX in a higher tempo environment. The *Team Understanding* model is likely to come about as a result of time spent together, gelling as a coherent unit.

The *Operational Priorities* mental model will need to be based on an assessment of the operational needs of the ICS operator, and fused with the *Operating Environment* model to determine which systems and processes are essential. These models will require a coping strategy to assist in their development, especially in light of the adaptable nature of APT adversaries, and to ensure these models translate into response actions in the event of a network intrusion.

These mental models provide a structure against which experimentation can address Question 1 - *Which factors influence the development of mental models to provide cyber situational awareness?* of the six questions posed in Section 1.4. The progressive training framework described in this chapter also provides a construct in which the contribution of coping strategies can be assessed, as required by Question 2 - *Does the adoption of coping strategies increase situational awareness?*. The crawl-walk-run approach to training offers a mechanism by which the risk perceptions of participants can be progressively focussed to establish SA, thereby contributing to Question 3 - *Can serious games change the risk perceptions of participants and establish a foundational level of situational awareness?* and Question 4 - *How can we increase the efficacy of the serious games to deliver the change in risk perceptions?*. This progressive development of an understanding of adversary characteristics, and the optimising of incident response team performance through experiential learning within the framework, provides a basis to drive the comprehension and projection of APT attack behaviours required by Question 5 - *As a result of serious games, can participants recognise the characteristics of a cyber attack and determine the possible intent and courses of action?*, and Question 6 - *Are participants of serious games able to assess the immediate and longer-term impacts of cyber attacks?*

Chapter 7

Experiments

Contents

7.1 Introduction

ICS exhibit different operational characteristics to IT systems, and the threat posed by advanced, capable antagonists cannot be fully addressed by existing IT security mechanisms (see section 3.4.3). The available data relating to cyber attacks on ICS does not adequately articulate the risks faced by an ICS operator, so the potential impact cannot be demonstrated, and as a result their SA is limited. This research has proposed a number of mechanisms to develop SA to address these risks, using a mix of experiential learning, serious games, and coping strategies to establish the means to address the antagonistic threat from APT actors, encompassed in SCIPS, the Framework for Progressive Collective Training, and ICS-CDTP.

SCIPS provides an environment in which participants of the game can build the initial mental models necessary to raise awareness that a risk exists, thereby satisfying the safeguard recommended by Kaplan and Garrick (1981) [74] that it poses less risk than if we have no understanding of its potential impact.

The Framework for Progressive Collective Training proposes a set of incremental training levels constructed around TTX and CDX, described in Table 6.3 to develop coherent mental models described in this research (Table 6.1). These models extend the concepts described by Matheiu et al. (2000) [149] to underpin the three levels of SA and Team SA described by Endsley (1995) through a crawl-walk-run model adapted from Schaab and Moses (2001)[152] and extended to form the requirements for progressive collective training proposed in Table 6.2.

ICS-CDTP provides a coping strategy for organisations to focus on the identification and defence of critical ICS equipment from malicious manipulation. It uses a modified CARVER Matrix model described in Tables 5.2 - 5.8 to identify key network terrain, and an extended version of the Diamond Model of Intrusion Analysis, described in Figure 5.2, integrated with the Mandiant Attack Lifeycle (Figures 5.3 and 5.4) and the Purdue Model (Figure 5.5) to forecast antagonistic activities to develop a focused defensive posture and cyber incident response playbooks, shaped by the COA Matrix depicted in Figure 5.6.

This chapter discusses the approach proposed to address the six research questions posed in Section 1.4. It is structured as follows:

1. **Design of Study:** *A description of the approach to the study, the rationale for adopting a qualitative methodology, and within that, the selection of Thematic Analysis as the method to analyse the data.*

2. **Data Analysis:** *A summary of the Thematic Analysis process used to analyse the data.*

3. **Sample Selection:** *The selection criteria for the sample required for the study, and a description of the sample adopted.*

4. **Data Collection:** *An explanation of the methods used to collect data.*

5. **Validity and Reliability:** *The strategies used to ensure the trustworthiness of the results of the study.*

6. **Researcher Bias and Assumptions:** *An analysis of the biases of the researcher, the sample, and a statement of the principles, assumptions and constraints that shape the study.*

7. **Scope and Schedule of Experiments:** *A description of the schedule of experimentation undertaken, and the scope of each experiment.*

7.2 Design of the Study

Early evaluations of SCIPS focused on quantitative metrics, as described in Section 4.5.7. However, a review of the results from the experiments [209, 210] demonstrated that although the game effected a clear change in the risk perceptions of the participants, it only demonstrated that a change occurred, it did not address *why* participants viewed the risk differently after playing the game. So whilst we demonstrated a positive answer to research question 3 from Section 1.4 *can serious games change the risk perceptions of participants and establish a foundational level of SA?*, we were unable to address the remaining questions, in particular *how can we maximise the efficacy of the serious games to deliver the change in risk perceptions?* and *which factors influence the development of mental models to provide cyber SA?* The unstructured, open question format of the third evaluation of SCIPS [211] elicited a richer narrative as to why the game influenced the audience, and forced a review of the research methods in use. No quantitative methodologies were identified that could provide a framework in which we could assess why the changes occurred. Based on the encouraging results gathered from the unstructured responses, a review of qualitative research methodologies was therefore undertaken.

Quantitative approaches are appropriate for examining who has engaged in a behaviour or what has happened. Whilst experiments based on quantitative measures can test particular interventions, the techniques are not designed to explain why certain behaviours, or changes in behaviours, occur. Qualitative research, however, places more emphasis on the study of phenomena from the perspective of insiders, and are typically used to explore new phenomena and to capture individuals' thoughts, feelings, or interpretations of meaning and process, asking questions about knowledge and how knowledge is acquired [233, 234]. Rather than determining cause and effect, predicting, or describing the distribution of some attribute among a population, qualitative research uncovers the meaning of a phenomenon for those involved by understanding how people interpret their experiences, how they construct their worlds, and what meaning they attribute to their experiences [235].

> *"Qualitative research is an inquiry process of understanding based on distinct methodological traditions of inquiry that explore a social or human problem. The researcher builds a complex, holistic picture, analyzes words, reports detailed views of informants, and conducts the study in a natural setting."* [236]

In reviewing the methodologies available, we reviewed five types of qualitative research, comparing them across five dimensions proposed by Creswell (1998) [236] that distinguish their characteristics, as shown in Table 7.1. We shall now review these methodologies and assess their applicability.

Dimension	**Biography**	**Phenomenology**	**Grounded Theory**	**Ethnography**	**Case Study**
Focus	Exploring the life of an individual	Understanding the essence of experiences about a phenomenon	Developing a theory grounded in data from the field	Describing and interpreting a cultural and social group	Developing an in-depth analysis of a single case or multiple cases
Discipline Origin	Anthropology, literature, history, psychology, sociology	Philosophy, sociology, psychology	Sociology	Cultural anthropology, sociology	Political science, sociology, evaluation, urban studies, other social sciences
Data Collection	Primarily interviews and documents	Long interviews with up to 10 people	Interviews with 20-30 individuals to *saturate* categories and detail a theory	Primarily observations and interviews with additional artefacts during extended time in the field (e.g. 6 months to a year)	Multiple sources - documents, archival records, interviews, observations, physical artefacts
Data Analysis	Stories, epiphanies, historical content	Statements, meanings, meaning themes, general description of the experience	Open coding, axial coding, selective coding, conditional matrix	Description, analysis, interpretation	Description, themes, assertions
Narrative Form	Detailed picture of an individual's life	Description of the *essence* of the experience	Theory or theoretical model	Description of the cultural behaviour of a group or an individual	In-depth study of a case, or cases

Table 7.1: Dimensions for comparing five methodologies in qualitative research, Creswell (1998)

Biography

In a biography, a researcher studies a single individual [236]. This focus was not appropriate for the number of participants in the research sample.

Phenomenology

The philosophy of phenomenology is based upon the experience itself and how experiencing something is transformed into consciousness. Rather than attempt to develop abstract laws or theories, phenomenology focuses on *"lived experience"* [235, 237]. Patton (2015) proposes that the methodology is based on the assumption that *"there is an essence or essences to shared experience. These essences are the core meanings mutually understood through a phenomenon commonly experienced. The experiences of different people are bracketed, analyzed, and compared to identify the essences of the phenomenon, for example... the essence of being a participant in a particular program"* [238]. The role of the researcher, then, is to depict the essence, or basic underlying structure, of the meaning of the experience, using phenomenological reduction to continually return to the interpretation of the experience to derive its inner structure and meaning [235].

Grounded Theory

Grounded theory, like other forms of qualitative analysis, uses the researcher as the primary instrument of data collection, assuming an inductive posture to derive meaning from the data. The result of this type of enquiry is a theory that emerges from, or is *grounded*, in the data. Grounded theory promotes iterative collection, coding and analysis of data in order to decide what data should be collected next, and a constant comparative method involving comparing segments of data with each other to determine similarities or differences to build a substantive theory connected by a core category, a main conceptual element through which all other categories and properties are connected [235].

Ethnography

Ethnography originated in the field of anthropology [235]. The method requires the researcher to immerse themselves with the target sample [235], primarily using observations and interviews to describe and interpret a cultural or social group [236]. Such studies provide extensive data as a result of sustained exposure, often using pre-existing category schemes of social and cultural behaviours and characteristics to present their findings [235].

Ethnography has been used in software engineering as a method to elicit unstated or implicit requirements from users through observation [239] as well as developing an in-depth understanding of the socio-technological realities surrounding software development practices [240].

Case Study

A case study is an in-depth description and analysis of a bounded system, although the scope of such studies can become confused by the conflation of the unit of study (the case) and the product of this type of investigation [235]. Yin (2013) [241] defines a case study as “an empirical enquiry that investigates a contemporary phenomenon (the ‘case’) within its real-life context, especially when the boundaries between phenomenon and context may not be clearly evident” [241]. However, Merriam (2015) [235] argues that it is the unit of analysis, not the topic of investigation that characterises a case study [235]. This position is supported by Stake (2013) who proposes *“A case is a noun, a thing, an entity; it is seldom a verb, a participle, a functioning”*, arguing that *“training modules may be our cases - amorphous and abstract, but still things, whereas ‘training’ is not”* [242].

Analysis of Qualitative Methodologies

Both phenomenology and grounded theory gather data from participants involved in the phenomenon being studied, and both use iterative cycles of coding to develop an understanding of the experience. Phenomenology focuses on developing a narrative to explain the shared essence of the experience, whereas grounded theory develops a theory from data. As the focus of this study is to address the six research questions described in Section 1.4, the focus on developing a theory does not support our prime focus. The iterative interviewing of the same research sample in grounded theory also limits its applicability, as a result of limited access to the sample, without guarantee of the same membership between experiments.

Ethnography requires extensive period of intimate study and co-location with the research sample, with a deep reliance on intensive work with a few informants from the setting [235]. This level of integration with the subjects of the study has been noted to increase the likelihood of bias affecting the study [235]. As the interactions with the sample for the research is limited to specific periods of exercise execution (albeit over an extended elapsed period), the level of immersion required for an ethnographic study is not available. Also, as discussed later in Section 7.4.2, a common background shared by the author and the research sample increases the risk of familiarity bias.

The definition of a case study by Stake (2013) [242] as focusing on a *"noun"*, and his example of *"training modules"* as cases, but *"training"* as not, appears to be in conflict with questions 5 and 6 of our research questions described in Section 1.4 (*5. As a result of the serious games, can participants recognise the characteristics of a cyber attack and determine the possible intent and courses of action?, 6. Are participants of serious games able to assess the immediate and longer-term impact of cyber attacks?*)

Of the four methodologies, phenomenology best suits our analysis requirements and sample group.

Using Thematic Analysis within Phenomenology

Thematic analysis is a method for identifying, analysing, and interpreting patterns of meaning ('themes') within qualitative data, that supports a number of methodologies [243, 244] including phenomenology [245, 246].

Thematic analysis provides a systematic method for generating codes and themes from qualitative data, consistent with the intent of phenomenology. Codes are the smallest units of analysis that capture salient features of the data relevant to the research question. Codes are the building blocks for themes and patterns of meaning, providing a framework for organising and reporting the researcher's analytic observations. The aim of thematic analysis, as with phenomenology, is not simply to summarise the data content, but to identify and interpret the essence of the data, guided by the research questions. The thematic analysis process has in-built quality procedures such as a two-stage review process, where candidate themes are reviewed against the coded data and the entire data-set to promote analytical rigour [244, 247, 248, 249].

This study used thematic analysis as its phenomenological research tool. This was supported by the QSR NVivo™ qualitative analysis tool that offers functionality for thematic analysis.

7.2.1 Data Analysis

The process for analysing data using thematic analysis is outlined below.

Phase 1: Data Familiarisation

The first phase of thematic analysis requires the researcher to completely re-read all of the acquired data to ensure familiarity with the depth and breadth of the content. The repeated reading of the data supports the early identification of patterns, meanings, patterns and initial concepts within the data [243].

Phase 2: Generate Initial Codes

Once familiar with the data, and an initial set of ideas and concepts within the data has been created, the next phase of the thematic analysis process builds upon these to generate an initial list of codes from the data. Codes identify features within the data that appear interesting to the analyst, and refers to *"the most basic segment, or element, of the raw data or information that can be assessed in a meaningful way regarding the phenomenon"* [250]. These codes will differ from themes, which are often broader, and are developed later in the process [250, 243].

Phase 3: Search for Themes

Phase 3 begins when all data have been initially coded and collated, and combines codes into overarching themes that depict the data at the broader level of themes. The phase concludes with a collection of candidate themes, and sub-themes, and all extracts of data that have been coded in relation to them [243].

Phase 4: Review Themes

With a set of candidate themes available, this phase involves the review of the data to support the definition of the themes, and their refinement based on whether there is sufficient data to support them. During this phase, candidate themes may be revised, discarded, decomposed further, or may collapse into large themes [243].

Phase 5: Theme Definition and Naming

With a substantiated set of themes emerging from Phase 4, this phase further refines the themes into those that will be presented in the overall study results. This involves describing the *essence* of each theme, as well as the overall structure and relationship of the themes, determining which aspects of the data the theme captures. Each of the themes is developed into a detailed analysis that relates to the research questions, ensuring that the naming of the themes fits within the overall study narrative [243].

Phase 6: Produce Report

Phase 6 begins with set of fully defined themes, and results in the final analysis and documentation of the study. Within a thematic analysis study, the focus of the documentation is to present the complicated story of the data in a manner that convinces the audience of the merit and validity of the study findings in a concise, coherent, logical and non-repetitive manner. It must present sufficient evidence of the themes within the data, with extracts to demonstrate the prevalence of a theme, along with a compelling analytical narrative to that relates the data to the research questions [243].

7.3 Sample Selection

A review of the research questions described in Section 1.4 highlighted that as the intent of the game is to change the risk perspectives of the participants, a convenience sample would be acceptable. For the participants who would take part in the TTX or CDX, the sample must contain a mix of individuals with some experience of cyber exercises, TTX and CDX, as well as those new to exercising, and would be participating in exercises subsequent to the study. For the second group, a purposeful sample was required. The nature of convenience and purposeful sampling is discussed below.

Convenience Sampling

Convenience sampling is a type of non-probability or non-random sampling where members of the target population that meet certain practical criteria, such as easy accessibility, geographical proximity, availability at a given time, or the willingness to participate are included for the purpose of the study. The main assumption associated with convenience sampling is that there will be no difference in the research results obtained from a random sample, a nearby sample, a co-operative sample, or a sample gathered in some inaccessible part of the population, i.e. the assumption is that the members of the target population are homogeneous. As a result, it is necessary to identify how the sample would differ from one that was randomly selected, as well as to describe the subjects who might be excluded during the selection process or those who might be overrepresented in the sample. It is also necessary to identify outliers within the sample who may skew the results. The key disadvantage of convenience sampling is that it is likely to be biased, and accordingly, the results should not be considered representative of the wider population [251].

Purposeful Sampling

Purposeful sampling is a technique widely used in qualitative research for the identification and selection of information-rich cases for the most effective use of limited resources. This involves identifying and selecting individuals, or groups of individuals, that are knowledgeable about or experienced with a phenomenon of interest, with the ability to communicate experiences and opinions in an articulate, expressive, and reflective manner. Despite its wide use, there are a number of challenges in identifying and applying the appropriate purposeful sample for a study. Of these, the fact that range of variation in a sample from which purposive sample is to be taken is rarely known at the outset of a study must be addressed when interpreting the results [252].

Sample Selection Criteria

In order to address the biases introduced by convenience sampling, participants were asked to describe their knowledge of industrial control systems prior to playing SCIPS, as well as to articulate their understanding of the strategic issues surrounding the cyber security of ICS. This allowed the breadth of the sample to be assessed during the analysis of the data, and any limitations on the results to be articulated. Accordingly, there was no selection criteria for the convenience sample other than accessibility and availability. This allowed us to use the purposeful sample for the TTX and CDX as our convenience sample for SCIPS.

For the purposeful sample, where a mix of individuals with some experience of cyber exercises, TTX and CDX, as well as those new to exercising, and who would be participating in exercises subsequent to the study was required, a representative sample was identified within the British Army. The Army Cyber Protection Team (CPT) regularly engages in cyber exercises, and due to the rotation of the posting cycle within the armed forces, at least 30% of the team would be new to cyber exercises during any two-year cycle. The participants were asked to describe their technical and exercise experience when providing data so that the breadth of the sample could be assessed. A further purposeful sample from UK Armed Forces was also identified to augment the CPT for the latter experiments described in this chapter, who met the same selection criteria.

As the entirety of the sample were from a military background, this bias was considered when interpreting the results.

7.4 Data Collection

This study used three data collection methods; interviews, questionnaires, and observations.

Interviews

The interviews employed an informal, semi-structured format, focusing on those within the purposeful sample. The first round of interviews covered previous experiences of cyber exercises, and the participants' positive and negative views of exercising. These then progressed onto their experiences on the exercises run as part of the experimentation for this study, and encouraged them to compare and contrast. For those without any previous exercise experience, the interviews focused on anticipated expectations versus the experimentation exercise itself.

As the series of experiments progressed, the leadership of the CPT were re-interviewed to see how the behaviours and SA of the CPT had changed as a result of their experiences.

All interviews were recorded and transcribed.

Questionnaires

Questionnaires were the primary data collection method across SCIPS games and exercises. These contained a set of open questions intended to elicit the thoughts and feelings of the participants, based on their experiences on the experiments. These questions are included in Appendix A.

Observations

During the experiments, the behaviours of the sample were observed and recorded. The observations focused on the team interactions and SA of the participants during the experiments, and their use of coping strategy techniques. These observations were articulated as memos, extracts from which are included in Section 8 and Appendix C.

7.4.1 Validity and Reliability

To ensure that the study was trustworthy, the author maintained the following disciplines [235]:

1. **Methodological Rigour:** *Through adherence to the processes prescribed by thematic analysis to develop the themes from data coding.*
2. **Interpretive Rigour:** *Through the triangulation of data from interviews, questionnaires, and observations.*
3. **Analytical Rigour:** *Through the maintenance of an audit trail of data, and decisions based upon that data.*
4. **Reflexivity:** *Through critical-reflection as a researcher, attempting to identify assumptions, worldview, biases, theoretical orientation, and relationship to the study that may affect the investigation.*

7.4.2 Researcher Bias and Assumptions

This section provides an audit of self-perceived researcher biases and assumptions. These include:

1. The author has been a participant in many cyber exercises, and this may influence the nature of the questioning of exercise participants during the experimentation.
2. The author entered into this research with the belief that experiential learning offers a potentially viable means to establish cyber SA in the minds of participants.
3. The author is an Army Reserve Officer who has worked with the Army CPT, and may introduce a familiarity bias.
4. As an Army Officer, it is likely that the author shares many of the cognitive biases of the purposeful sample as a result of a shared military training syllabus, doctrine and operational experiences.

7.5 Scope and Schedule of Experiments

To evaluate the concepts articulated within Chapters 4, 6, and 5 of this thesis, a schedule of training programmes, SCIPS gameplay, TTX and CDX was executed over an 11 month period. The scope of the evaluation was primarily governed by access to the purposeful samples, or in one instance of a TTX, accessibility to a convenience sample via a commercial TTX that the author participated in. This required the evaluation to prioritise those exercises that would act as significant use cases to allow the concept of progressive collective training to be evaluated against the requirements defined in Table 6.2. It was decided that TTX Collective Training Level 2 (TTX CIRT2) and TTX Collective Training Level 3 (TTX CIRT3) provided sufficient coverage against the scope of the requirements to evaluate the progressive training framework's TTX efficacy. For CDX, CIRT2 and CIRT3 events were run at De Montfort University (DMU) to test the framework on a cyber range. For CDX CIRT4 and CIRT5, the author was invited to participate with the purposeful sample on exercises run by external organisations.

The schedule of experiments is summarised below in Figure 7.1.

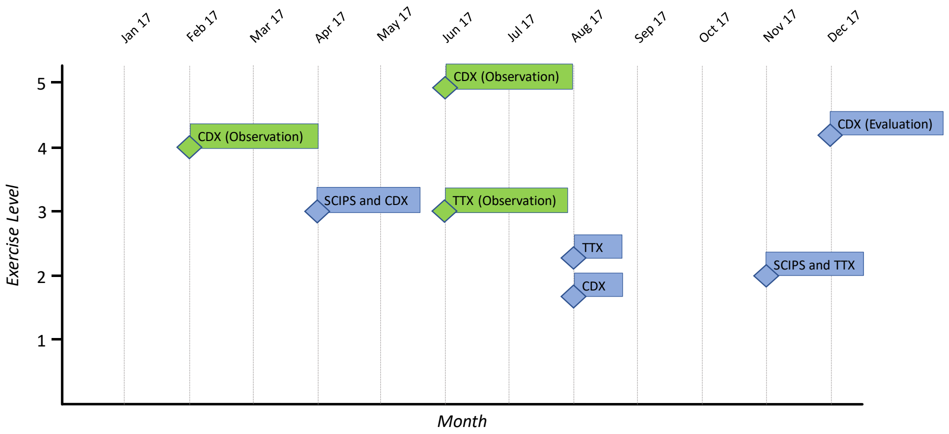


Figure 7.1: Experiment schedule

7.5.1 Cyber Defence Exercise, February 2017

The author joined 12 members of the purposeful sample on a 10 day CDX [253] involving over 150 participants. No opportunity was available to provide questionnaires to capture feedback from the sample, however, the author was allowed to record observations. An assessment of the scope, complexity and scenario of the exercise indicated that it fitted the criteria of a CIRT4 CDX, in that it required external relationships for each Blue Team that included threat intelligence feeds and the requirement to interact with governmental bodies. The CDX also integrated 10 Blue Teams into a large-scale cyber range with generated background traffic. A Red Team was provided to act as a mid-tier actor, with a frequency and breadth of attacks intended to progressively stress-test the teams.

Exercise constraints dictated the purposeful sample, the CPT, could not use their full team on the CDX, and other demands on their time meant that they could not attend any of the exercise preliminaries that allowed teams to deploy and configure sensors. The exercise afforded an opportunity to observe the CPT in an adverse situation, for which they did not have the opportunity to undertake specific training, or prepare for. As such, it allowed a baseline assessment of the sample, against which future experiments could be scoped and measured.

7.5.2 SCIPS and Cyber Defence Exercise, April 2017

This experiment was designed as a result of the observations and outcomes from the previous exercise, described in Section 7.5.1. The experiment adopted a novel exercise format and structure that combined SCIPS and a new way to conduct CDX, intended to provide the opportunity for iterations of experiences, followed by periods of reflection, to promote the formation of ideas and development of the mental models, with the testing of these ideas solidifying the understanding in the mind of the participants to establish cyber situational awareness. The experiment lasted five days, and comprised 26 Blue Team participants, an exercise facilitator (the author), and a five-person Red Team. It began by providing classroom training in:

- **Industrial Control Systems:** *A half-day introduction to ICS centred around the Purdue Model.*
- **APT Adversary Lifecycle:** *An hour-long introduction to adversary lifecycle modelling.*
- **ICS-CDTP:** *A two-hour fusion of the above, demonstrating the ICS-CDTP, and an unpublished military variant developed specifically for the CPT by the author that integrates ICS-CDTP with existing Military Intelligence processes, referred to as Intelligence Preparation of the Cyber Environment (IPCE). An overview of IPCE is included in Appendix D.*

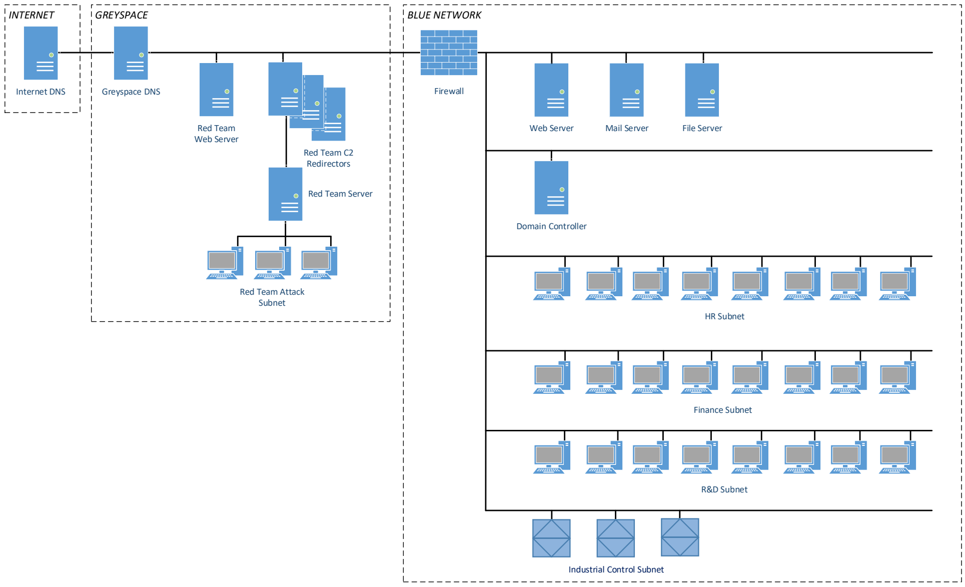


Figure 7.2: Experiment cyber range, April 2017

Following the training, the exercise participants played SCIPS, experiencing an APT attack end-to-end within the game. Each round of the game ended with teams describing their assessment of where the attackers were in the adversary lifecycle and Purdue Model, intended to develop their *APT Attack Behaviour, Team Understanding*, and *Operational Priorities* mental models.

A Novel CDX Format

The experiment then progressed to the CDX [254], using the criteria for a CIRT3 CDX within the progressive training model defined in Table 6.3. To anchor the development of all five of the mental models defined in Table 6.1, the SCIPS scenario was used as the scenario for the CDX, with participants being made aware that they were going to experience the same attack from the game, but in a detailed range environment (illustrated in Figure 7.2) that included ICS. This was accompanied by a Red Team playbook of attack techniques and attacker characteristics, along with a strict timeline for attack delivery that constrained the activities of the Red Team to a strict set of Rules of Engagement (RoE). This allowed a crawl-walk-run model to be applied that accommodated the performance of the Blue Team. The exercise comprised three days of attack activity, split into six half-days that corresponded to the activities played out in the six rounds of the SCIPS game. The Blue Team were briefed at the start of each half-day session which activities the Red Team would be undertaking against them. The Blue Team were then encouraged to discuss how these attacks would manifest themselves, and a flipchart was populated describing how they thought the Red Team would behave. These were aggregated into common themes, as shown in Figure 7.3.

The exercise then transitioned into the execution phase of that round where the Red Team would attack the network and associated ICS. Each phase was time-bound,

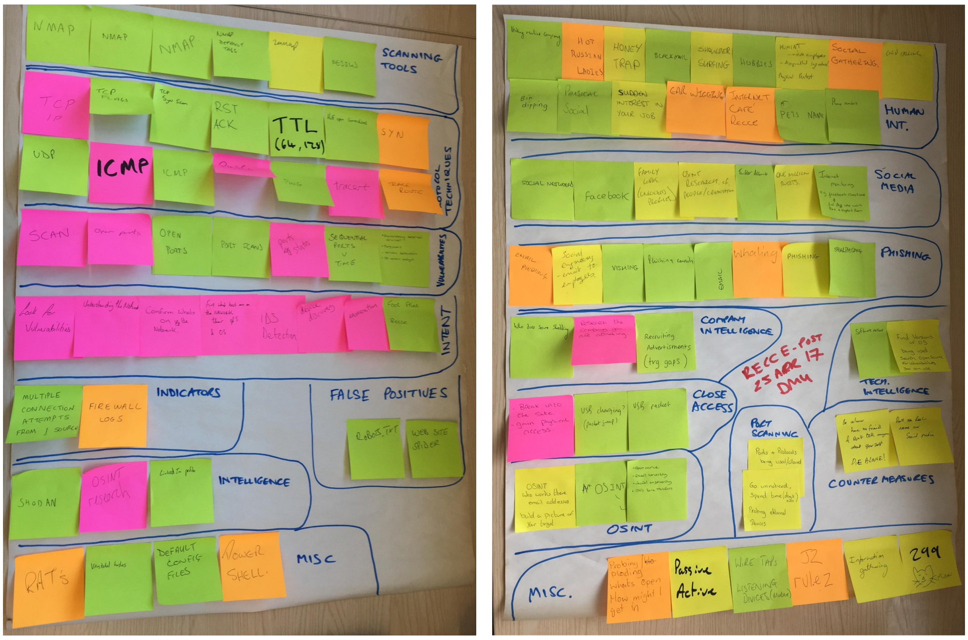


Figure 7.3: Network reconnaissance perspectives before and after Red Team activities, April 2017

and at the end the Red Team would discuss with the Blue Team which of the activities they had detected and which they had not. After a period of reflection, the Blue Team repopulated the flipchart with a description of their revised understanding of antagonistic behaviours, as well as an assessment of where the Red Team were in terms of both the adversary lifecycle and Purdue Model. This process was repeated for all six rounds of the exercise, as illustrated in Figure 7.4. At the end of the SCIPS game, and at the end of the CDX, participants were asked to complete questionnaires. Also, a subset of participants with prior cyber exercise experience were interviewed.

7.5.3 Table-Top Exercise, June 2017

The author was invited to participate in an exercise that fitted the criteria for a CIRT3 TTX with a UK CNI provider [255] that included a background scenario as well as an operational business owner with dynamic priorities that extended beyond technical availability of systems. The exercise required the organisation's crisis management team to report to a leadership structure at regular intervals, requiring accurate SA from the team, as well as the need to forecast defensive activities to respond to a mid-tier actor with the capability to manoeuvre covertly around their ICS network and adapt to the incident responders' actions. The intent of the exercise was to assess the organisational agility to deal with such a situation, and to test the adaptability of the leadership to manage a dynamic situation and interact with their wider regulatory community.

The exercise scenario related to a fictitious data breach and loss of customer data. The author provided the set of questions, summarised in Figure 7.5 and detailed in Appendix E, to drive the conversations with the leadership team as the scenario unfolded.

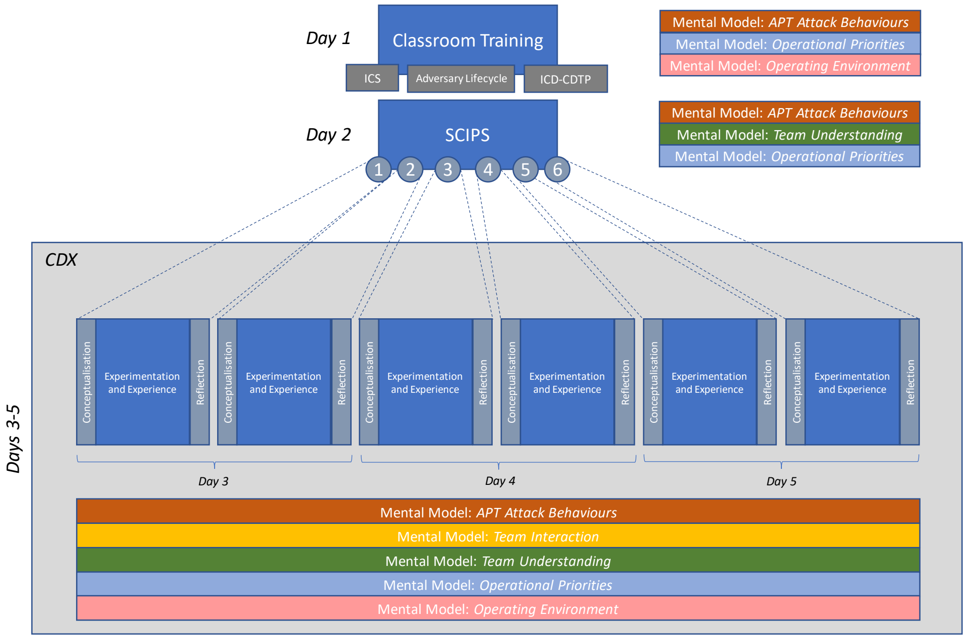
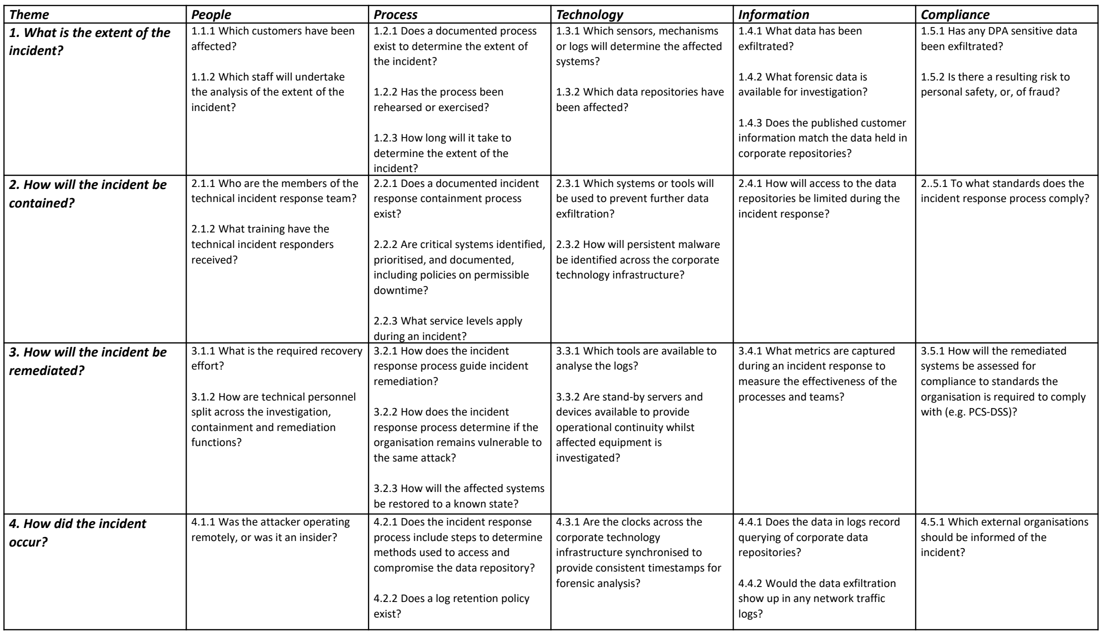

Day 1
Classroom Training
ICS
Adversary Lifecycle
ICD-CDTP
Mental Model: *APT Attack Behaviours*
Mental Model: *Operational Priorities*
Mental Model: *Operating Environment*
Day 2
SCIPS
1 2 3 4 5 6
Mental Model: *APT Attack Behaviours*
Mental Model: *Team Understanding*
Mental Model: *Operational Priorities*
CDX
Days 3-5
Conceptualisation
Experimentation and Experience
Reflection
Day 3
Day 4
Day 5
Mental Model: *APT Attack Behaviours*
Mental Model: *Team Interaction*
Mental Model: *Team Understanding*
Mental Model: *Operational Priorities*
Mental Model: *Operating Environment*

Figure 7.4: Experiment Structure and Mental Model Development, April 2017

No feedback questionnaires were completed. Only the author's observations were included as experiment results.

7.5.4 Cyber Defence Exercise, June 2017

The author joined 20 members of the CPT on an international exercise [256] involving over 1000 people across the Red, Blue, White and Green Teams, executed over 14 days. The purposeful sample (the CPT) was split between two teams, the first comprising solely personnel from the CPT, the second integrating staff from other nations. The criteria of the exercise fitted that of a CIRT5 CDX, in that it was intended to test the participants to the point of failure, and designed to determine at which point the C2 of the team could not cope. The scenario was based on an international crisis, involving Blue Team incident response teams from a number of countries, all operating within a shared threat intelligence environment. The exercise was structured on a large, complex cyber range that included significant elements of ICS, with each Blue Team assigned a network to defend from a Red Team emulating high-tier, nation-state actors. The CPT intended to further test the techniques taught the experiment described in Section 7.5.2, especially the ICS-CDTP, on which they had received further training. Their intent was to drive the development of standard operating procedures (SOP) so that new members joining the team would have a documented framework in which to integrate. It was also planned to test the new organisation structure they had adopted as a result of the experiment in Section 7.5.2 that resulted in the creation of a new team role of *Blue Terrain Manager*, that drew heavily on the concepts of the ICS-CDTP to triage and assess network terrain based on threat intelligence.



Theme	***People***	***Process***	***Technology***	***Information***	***Compliance***
1. What is the extent of the incident?	1.1.1 Which customers have been affected? 1.1.2 Which staff will undertake the analysis of the extent of the incident?	1.2.1 Does a documented process exist to determine the extent of the incident? 1.2.2 Has the process been rehearsed or exercised? 1.2.3 How long will it take to determine the extent of the incident?	1.3.1 Which sensors, mechanisms or logs will determine the affected systems? 1.3.2 Which data repositories have been affected?	1.4.1 What data has been exfiltrated? 1.4.2 What forensic data is available for investigation? 1.4.3 Does the published customer information match the data held in corporate repositories?	1.5.1 Has any DPA sensitive data been exfiltrated? 1.5.2 Is there a resulting risk to personal safety, or, of fraud?
2. How will the incident be contained?	2.1.1 Who are the members of the technical incident response team? 2.1.2 What training have the technical incident responders received?	2.2.1 Does a documented incident response containment process exist? 2.2.2 Are critical systems identified, prioritised, and documented, including policies on permissible downtime? 2.2.3 What service levels apply during an incident?	2.3.1 Which systems or tools will be used to prevent further data exfiltration? 2.3.2 How will persistent malware be identified across the corporate technology infrastructure?	2.4.1 How will access to the data repositories be limited during the incident response?	2..5.1 To what standards does the incident response process comply?
3. How will the incident be remediated?	3.1.1 What is the required recovery effort? 3.1.2 How are technical personnel split across the investigation, containment and remediation functions?	3.2.1 How does the incident response process guide incident remediation? 3.2.2 How does the incident response process determine if the organisation remains vulnerable to the same attack? 3.2.3 How will the affected systems be restored to a known state?	3.3.1 Which tools are available to analyse the logs? 3.3.2 Are stand-by servers and devices available to provide operational continuity whilst affected equipment is investigated?	3.4.1 What metrics are captured during an incident response to measure the effectiveness of the processes and teams?	3.5.1 How will the remediated systems be assessed for compliance to standards the organisation is required to comply with (e.g. PCS-DSS)?
4. How did the incident occur?	4.1.1 Was the attacker operating remotely, or was it an insider?	4.2.1 Does the incident response process include steps to determine methods used to access and compromise the data repository? 4.2.2 Does a log retention policy exist?	4.3.1 Are the clocks across the corporate technology infrastructure synchronised to provide consistent timestamps for forensic analysis?	4.4.1 Does the data in logs record querying of corporate data repositories? 4.4.2 Would the data exfiltration show up in any network traffic logs?	4.5.1 Which external organisations should be informed of the incident?

Figure 7.5: TTX Questions Matrix, June 2017

The author, along with the leadership of the CPT, observed the behaviours of the sample on the exercise, and recorded their assessment of their performance. No feedback questionnaires were completed.

7.5.5 Table-Top Exercise, August 2017

This experiment [257] was derived following a review of the performance of the CPT on the exercise described in Section 7.5.4. It was acknowledged by the team in a review of their performance that overall SA was an issue, and that their *Team Interaction* mental model and associated processes were poor. As with the exercise described in Section 7.5.2, the SCIPS scenario was used as the basis of the TTX. The familiarity with the scenario allowed the team to focus on how they work work and interact, rather than have to deal with a new set of circumstances within the exercise. A modified set of facilitation questions, based on those described in Section 7.5.3, and detailed in Appendix E, were used to drive the detail of inclusions or identification of omissions in the team's SOPs. The CIRT2 TTX was planned as a one-day exercise, and was attended by 12 of the purposeful sample. The TTX was designed to bring together representatives of the sub-teams within the CPT to assess how the operating procedures of the team and sub-teams interoperate, and how overall C2 and SA were maintained during an incident. In particular, it looked at how the elements of ICS-CDTP could be further embedded in their processes. The TTX was intended to test a proposed new SA Manager role, to sit alongside the Blue Terrain Manager, to ensure Team SA across concurrent network activities.

Feedback questionnaires were completed at the end of the exercise.

7.5.6 Cyber Defence Exercise, August 2017

As a follow-on training activity from the exercise described in Section 7.5.4, and to test the emerging SOPs emerging from the TTX described in Section 7.5.5, 16 members of the sample attended a four-day CDX designed to further build their mental models of *APT Attack Behaviours*, *Team Understanding*, and *Team Interaction*. Using the crawl-walk-run approach to training, the experiment was designed to focus on a constrained area of incident response for the CPT, and drive a greater understanding of its characteristics, thereby solidifying the *APT Attack Behaviour* mental model, and increasing the teams understanding of individual's capabilities (the *Team Understanding* mental model), and the necessary C2 and information flows (the *Team Interaction* mental model). A review of the exercise described in Section 7.5.4 highlighted that although the CPT correctly prioritised the defence of their network's Domain Controllers using the ICS-CDTP, they struggled to identify covert activities of the Red Team on the devices. To address this, a CIRT2 CDX was developed with a subset of the SCIPS scenario that focused on a low- to mid- tier threat actor in the early stages of a network intrusion, attempting to create new users on a Domain Controller. The CDX involved the Blue Team repeatedly defending the Domain Controllers in the network described in Figure 7.6, from the same attack. The intent was that the Blue Team would start to identify the attack behaviour in their sensors and logs, and with progressive use of covert techniques using a crawl-walk-run approach, the CPT would improve their understanding of how an APT takes control of a Domain Controller, and what such activities look like when interpreted via sensors and logs. Using the novel approach to CDX described in Section 7.5.2, the Red Team briefed the Blue Team on their planned attack activities. Following the attack, the Red Team discussed their actions with the Blue Team to help them interpret the data from their sensors and logs and prepare for the same attack the next day.

No feedback questionnaires were provided, but the team leader wrote a post-exercise report that assessed the Blue Team performance.

7.5.7 Cyber Exercise Training Programme, November 2017

The author was requested to develop a training programme for three cohorts of potential CPTs drawn from across the Army, as preparation from the exercise described in Section 7.5.8. The Defensive Cyber Operations (DCO) Mission Specific Training (MST) (DCO MST) was delivered to 38 attendees, in a mix of whole eight-man teams, part-teams, and individuals. It included the classroom elements delivered in the experiment described in Section 7.5.2, as well as the TTX described in Section 7.5.5, as part of a wider defensive cyber syllabus. The intent of the training was to sufficiently develop the five mental models and overall Team SA for a subset of the participating teams in the planned exercise. By only training a subset of the teams attending the exercise, it was envisaged that a tangible comparison of trained and untrained teams would be possible. The training comprised three five-day courses, covering the following:

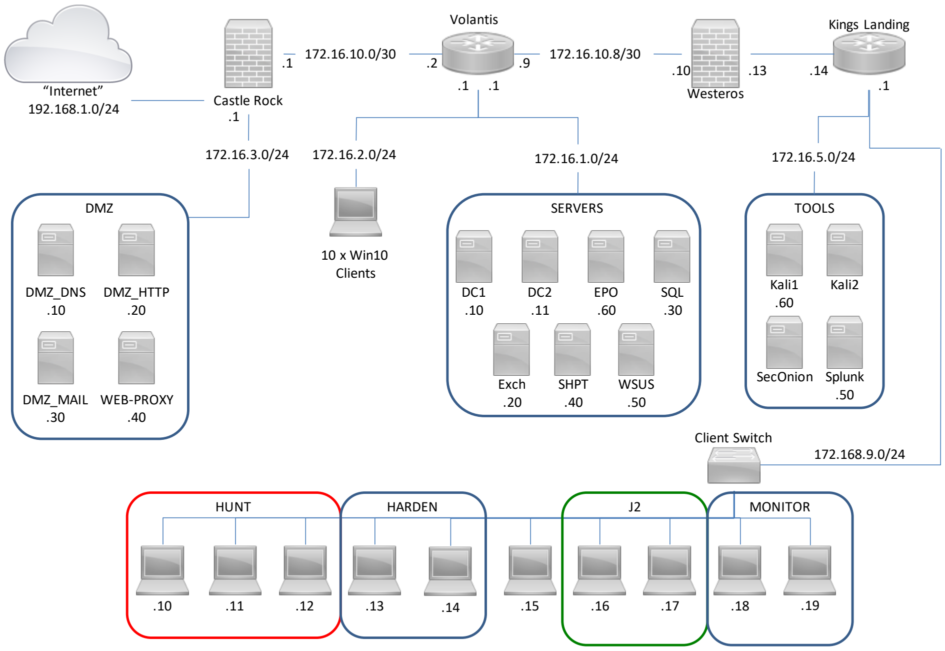


Figure 7.6: CDX Range, August 2017

1. **'Why DCO Fails?':** *A review of the results from the interviews described in Section 7.5.2 and the observations of the exercises describe in Sections 7.5.1, 7.5.2, 7.5.3, 7.5.4, 7.5.5, and 7.5.6. This specific element of the training comprised a discussion of SA and the use of mental models as a means to proactively defend a network, rather than simply react to intrusion events.*

2. **Baseline assessment of DCO capability and identification of skills gaps:** *It was acknowledged that DCO teams would be attending the exercise with differing levels of individual technical skills. This element of the training reviewed the skills required for the exercise and determined the delta.*

3. **Industrial control systems:** *It was recognised in the exercise planning that many DCO teams would have no ICS knowledge or experience. An introduction to the technology area was provided.*

4. **Threat actor characteristics and behaviours:** *A description of Red Team intrusion and evasion techniques, and the technical methods to detect them.*

5. **Intelligence Preparation of the Cyber Environment (IPCE):** *A description of the elements of ICS-CDTP integrated into existing Military Intelligence processes (described in Appendix D) to provide an understanding of the Blue Terrain that the DCO teams must defend, combined with training in the CARVER matrix to allow teams to triage the key terrain within their networks that would present high value targets for Red Teams.*

6. **Adversary lifecycle analysis:** *An specific focus on the use of adversary lifecycle models as a SA technique as part of ICS-CDTP (that were not included in IPCE)*

that allows Red Team intrusion behaviours to be modelled and forecast, then integrated into an assessment of likely Red Team COAs using the 'Diamond Model of Intrusion Analysis', along with a demonstration of how specific visual aids can enhance Team SA.

7. **DCO Team C2:** *A recommended organisational structure (illustrated in Figure 7.7) describing roles, responsibilities, information flows, and daily routine for a viable eight-man DCO team, based on the SOPs that had been developed by the CPT over the experimental period.*

8. **Development of situational awareness:** *The participants played SCIPS to experience a simulated end-to-end attack on a network and consider how they would maintain SA and manage their response. The gameplay followed the SCIPS format described in Section 7.5.2.*

9. **Exercise rehearsal TTX:** *A CIRT2 TTX based on the TTX described in Section 7.5.5, that allowed training participants to take part in a 'walk-through, talk-through' (crawl phase) of the first three days of the exercise, to refine their SOPs and immediate team activities when taking possession of a network.*

In addition to the above, it was was observed in the baseline assessment of DCO capabilities that the levels of individual skills were not consistent across the trainees. A review of skills gaps highlighted the following areas for remedial training, that were addressed through extra-curricular classes for the attendees:

1. Network traffic capture and analysis.

2. Intrusion detection systems.

3. Firewall configuration.

4. Network monitoring tools and techniques.

Feedback questionnaires were completed for the SCIPS and TTX elements of the training.

7.5.8 Cyber Defence Exercise, December 2017

Following on from the training provided in Section 7.5.7, the author attended the 10 day CIRT4 CDX that the DCO MST was provided for, to evaluate the performance of the Blue Teams, and compare the levels of SA achieved by those who attended the MST versus those who did not. The exercise comprised over 200 participants, spanning Blue, Red, White and Green teams. The exercise was already designed to be measured using a quantitative set of metrics by a third party. As such, the assessment performed in this experiment, wherever possible, fitted within the established evaluation metrics, although qualitative observations were made and recorded for the purposes of this research. The

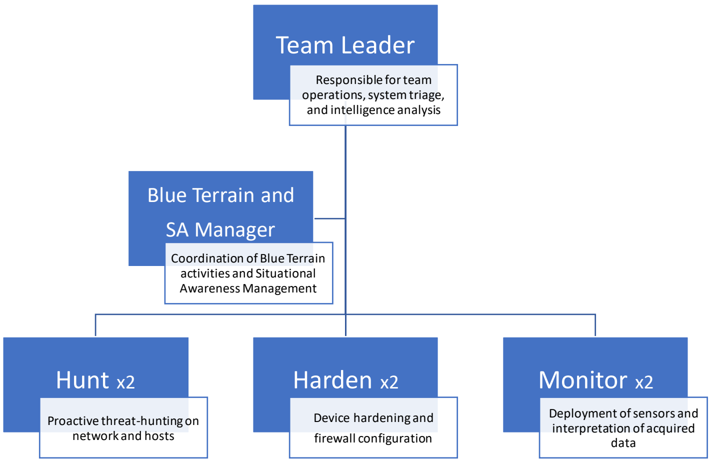

Team Leader
Responsible for team operations, system triage, and intelligence analysis
Blue Terrain and SA Manager
Coordination of Blue Terrain activities and Situational Awareness Management
Hunt x2
Proactive threat-hunting on network and hosts
Harden x2
Device hardening and firewall configuration
Monitor x2
Deployment of sensors and interpretation of acquired data

Figure 7.7: The recommended team structure for the exercise described in Section 7.5.8.

overall exercise White Team quantitative metrics assessed the Blue Teams against five criteria, on a 0-10 scale, with 10 representing the maximum positive score:

1. **Service Availability:** *A measure of the levels of availability of systems defined as critical by the exercise White Team.*
2. **Procedures:** *The adherence of the Blue Teams to procedures defined within the exercise.*
3. **Red Team Evaluation:** *A measure, by Red Team, of the levels of defence provided by an individual Blue Team.*
4. **Mission:** *An evaluation of each Blue Team's overall cognisance of the changing exercise scenario and its impact on DCO priorities.*
5. **Out of Game:** *A measure of altruistic or extra-curricular activities by Blue Teams that benefited the exercise overall.*

These measures were gauged by the exercise assessments team, with scores mediated by the White Team to maintain consistency throughout the exercise. Each day, a baseline score was assigned to each criteria, then each team's performance was mediated against this to determine how far above or below the standard score their performance was judged to have been.

To align with this approach, an assessment of Blue Teams' SA, and their use of a set of mental models with associated team structures and information management techniques taught on the Defensive Cyber Operations Mission Specific Training (DCO MST) was also measured using a mediated model, with a complementary 0-10 scale. The assessment considered the three levels of SA, plus overall Team SA, to appraise the Blue Teams' abilities to maintain a coherent understanding of a rapidly changing situation. A qualitative measure was also used to assess the teams' use of the five mental models developed on the DCO MST. Specifically, this measurement addressed:

- Team SA
- C2
- Information flows
- Understanding of adversary activities and intent

The exercise comprised 12 Blue Teams, operating within a daily six-hour exercise period. This limited the interaction time with each team to 30 minutes per day.

The cyber range contained a significant number of ICS elements to be defended by the Blue Teams.

No feedback questionnaires were provided.

7.6 Summary

The experimentation period that extended across the 2017 calendar year provided an opportunity to work with a consistent, purposeful sample, to drive the development and refinement of the use of SCIPS, TTX, and CDX as a means to deliver SA training within a progressive collective training framework, supplemented by the use of ICS-CDTP (and the IPCE variant) to provide a coping strategy for addressing the complexity of APT attacks on ICS. The DCO MST training programme provided an opportunity to refine the delivery of the training to three separate cohorts of participants, all of whom then attended the final CDX in December 2017. This allowed an assessment of the effectiveness of the training, using the exercise participants who did not attend the training as a control group.

Chapter 8

Experiment Results

Contents

8.1 Introduction

The experimental phase of this research involved exercises in which the author either observed, facilitated, or both. Those exercises that the author observed were used to shape subsequent exercises, especially where the exercise included the purposeful sample. As such, those exercises which were only observed will only reference the author's observations in this chapter. However, the influence of these observations on subsequent exercises will be clearly articulated.

Wherever possible, questionnaires were provided to gather feedback from participants for subsequent thematic analysis. Such questionnaires were not always possible, as in some instances the sample declined to complete them. In those circumstances, alternative observation data was captured.

The results of the thematic analysis were assessed in the DCO MST training programme undertaken in November 2017, and the subsequent CDX in December 2017.

This chapter discusses the thematic analysis process used to develop the qualitative themes that emerged from the experiments described in Sections 7.5.2, 7.5.5, and 7.5.7. The emerging themes are summarised within this chapter, with further detail at Appendix A. Additional observational analysis of the results from the experiments described in Sections 7.5.1, 7.5.3, 7.5.4, 7.5.6, and 7.5.8 is also included, with further detail at Appendices B and C.

8.2 Thematic Data Analysis Process

Wherever participant feedback was received, either through questionnaires or interviews, it was analysed for the emergence of themes to develop a qualitative assessment of the data. As the experimental period spanned a calendar year, and each experiment shaped the nature of the next. Phases one to five of the thematic analysis process were iterated and refined as the year progressed. The data were compiled and analysed using QSR NVivo™, using the process described in Section 7.2. The use of this process is summarised below.

8.2.1 Phase 1: Data Familiarisation

After each experiment, all of the acquired data was transcribed and re-read to ensure familiarity with the depth and breadth of the content.

8.2.2 Phase 2: Generate Initial Codes

Initial codes were generated with each iteration of experimentation, based on an analysis of the basic segments within the raw data.

8.2.3 Phase 3: Search for Themes

As the analysis of the data progressed, a total of 226 initial themes were identified. These were based on the coded data, which were combined into overarching themes and associated sub-themes. The phase concluded with a set of 12 candidate themes, with 128 sub-themes.

8.2.4 Phase 4: Review Themes

The candidate themes were then reviewed against the data to support the definition of the themes, and refined refinement based on whether there was sufficient data to support them. The themes were merged based on an identification of centres of gravity in the language, and merged based on the semantic relationships between words and phrases.

8.2.5 Phase 5: Theme Definition and Naming

The substantiated set of themes that emerged from phase four was then further refined into the nine final themes and sub-themes, with names that conveyed their essence. This included an analysis of the relationships between the themes to identify their interdependencies. A narrative was then developed to articulate the nature of the themes, with representative quotes identified that conveyed the sentiment of the content.

8.2.6 Phase 6: Produce Report

With the fully-defined themes available, the findings were assembled in the main body of this chapter to present the story that underlies the data, elaborated at Appendix A. The results are reviewed against the research questions in Section 11.

8.3 Trustworthiness of Thematic Analysis Results

For thematic analysis results to be accepted as trustworthy, researchers must demonstrate that the data analysis has been conducted in a precise, consistent and exhaustive manner [258]. Lincoln and Guba (1985) [259] proposed that trustworthiness in qualitative research could be improved by introducing the criteria of credibility, transferability, dependability, and confirmability. Each of these criteria will be assessed in turn, followed by a discussion of how possible biases were managed.

8.3.1 Credibility

Guba and Lincoln (1989) [260] claimed that the credibility of a study can be subjectively assessed by the readers if they can recognise the experience. They proposed that if a researcher could present sufficient engagement with the sample, along with supporting observations and triangulation, they could present the *"fit"* between the sample members' views and the researchers interpretation of them [258].

Along with the techniques adopted to maintain triangulation, as described in Section 7.4, the elaboration of the thematic analysis results in Appendix A contains a record of the number of sources and frequency of the references relating to the interpreted theme that emerged. This data was maintained in QSR NVivo™.

8.3.2 Transferability

Transferability, in the context of qualitative research, refers to the generalisability of the enquiry [258]. The researcher is responsible for providing a sufficient narrative from the sample so that those who wish to use the findings elsewhere can make their own assessments of the contents [259].

This chapter contains a representative example of such narratives, with greater depth of comments presented in Appendix A.

8.3.3 Dependability

For results to be considered dependable, they must be presented in a logical manner, with clear explanations [258]. Thematic analysis follows a repeatable process, although the subjective nature of the method may not deliver repeatable results. The focus, then, is therefore not on the repeatability of the themes developed, but that their structure and content must adequately represent the data.

As discussed above, the themes presented in this research in Sections 8.4 to 8.12, provide descriptions of each theme and the sub-themes they comprise, using the narrative taken from interviews and questionnaires to justify their structure and content.

8.3.4 Confirmability

The confirmability of research focuses on establishing that the themes developed are derived from the data. Confirmability is achieved when credibility, transferability, and dependability are demonstrated [258].

These criteria, as discussed above, are presented through the detail of the themes and the data used to derive them, presented in Sections 8.4 to 8.12 and elaborated in Appendix A.

8.3.5 Managing Biases

As with all forms of qualitative analysis, the researcher is the primary instrument for data collection and analysis [235]. However, humans have shortcomings and biases that may have an impact on the study. It is unlikely that these such subjective views can be eliminated from the study, therefore it is necessary to identify and monitor them.

To address this, initial potential biases were identified and recorded in Section 7.4.2. As these indicated that the common background that the author and the sample shared may influence the analysis of the data, the decision was taken to adopt an inductive approach to the development of the themes [250]. In this manner, the themes were developed solely from the data. This was assessed as preferable to a deductive approach that would attempt to fit the results to pre-existing models or theories, as any biases may have been amplified in both the selection of the theories and the interpretation of the data's fit to the models.

Additionally, when interacting with the research sample, open questions were used, with any subsequent inquiry avoiding points of detail that may influence the respondents. Where biases were recognised in the questioning, follow-on questions attempted to approach the subject from a different perspective to triangulate the answers.

We shall now explore the results of the experiments conducted.

8.4 Cyber Defence Exercise, February 2017

The author joined 12 members of the purposeful sample on a ten-day CIRT4 CDX [253] involving over 150 participants. No opportunity was available to provide questionnaires to capture feedback from the sample, however, the author was allowed to record anonymised observations. Exercise constraints dictated the CPT could not use their full team on the CDX, and other demands on their time meant that they could not attend any of the exercise preliminaries that allowed teams to deploy and configure sensors.

The exercise afforded an opportunity to observe the CPT in an adverse situation, for which they did not have the opportunity to undertake specific training, or prepare for. As such, it allowed a baseline assessment of the sample, against which future experiments could be scoped and measured.

The team were observed to possess a mid- to high-level of individual technical skills, and an operating structure that on first appearances, appeared adequate. However, as the exercise progressed it became apparent that operations within the team structure were largely on an *ad hoc* basis, with individuals responding reactively to identified network intrusion behaviours. Communications within the team were poor, and this limited SA. This was despite the adoption of a number of visual representations of network intrusion activities on whiteboards and large video screens, and a triage of priority systems to defend based upon an early version of the ICS-CDTP. It was observed that team members largely ignored the SA representations, and as a result, perpetuated their individual focuses. This was assessed to be as a result of the time pressures of the exercise, as well as there being no vehicle within the team to stimulate information exchange at anything above Level 1 SA.

Further investigations of the team performance highlighted that the team members were not correctly identifying intrusion behaviours on the network. It was observed that whilst the team possessed the technical expertise to interpret their logs and sensors, they did not have a sufficient understanding of APT attack behaviours to translate the data into an assessment of antagonistic intent.

The team's performance was assessed against the five mental models proposed in Table 6.1, with their performance described in Table 8.1.

As can be seen, the team performed well in *'Team Understanding'*. This was assessed to be as a result of previous military training and unit cohesion. However, against the other four models their performance was not as effective, and resulted in a poor outcome on the exercise. This was assessed to be as a result of the following four issues:

1. A lack of understanding of APT attack techniques and how these manifest themselves in logs and sensors.
2. Poorly defined roles and responsibilities, and no defined vehicles or mechanisms within the team to promote information sharing, communications, or SA.
3. No processes to translate the understanding of the network terrain (achieved through the use of an early iteration of ICS-CDTP) into prioritised activities within the team.
4. Although the team arrived late to the exercise, they did not have any formalised

Type of Model	Observed Team Performance
APT Attack Behaviours	Whilst the team's individual skills using defensive monitoring tools were assessed as high, they did not appear to possess an understanding of how an adversary would traverse a network, or how to predict attack behaviours.
Team Interaction	The roles and responsibilities of team members appeared loosely defined, and interactions between them were on an ad hoc basis. Communications and information flows were not formalised into a defined set of operating procedures.
Team Understanding	The understanding of the skills and personality traits amongst members of the team appeared high, as was their general morale. Despite a stressful situation, the team maintained an ordered calmness to operations.
Operational Priorities	The team had adopted an early iteration of the ICS-CDTP and triaged the high-priority systems that required defence. Upon further investigation, however, it was identified that the triage was based on an ad hoc assessment of priorities, rather than using a formalised approach such as the CARVER matrix.
Operating Environment	Due to circumstances beyond their control, the team arrived late to the exercise, and did not have time to establish a baseline before the Red Team started attacks. As a result, the team did not achieve an acceptable level of understanding of their network until almost halfway through the exercise.

Table 8.1: Observed team performance against shared mental models on the February 2017 CDX.

processes that defined the immediate activities that should be undertaken to rapidly understand the network they must defend.

These observations drove the development of the detail of the subsequent experiment schedule.

8.4.1 Experiment Outcomes

Based on the observations described in Table 8.1, it was agreed with the CPT that the priorities for improving the team's mental models would be:

1. **APT Attack Behaviour:** *The team required an increased understanding of how APTs behave on networks. This should include a means by which the attacker could be tracked through a network, how their behaviours would be represented in logs and sensors, and a means to assess future antagonistic courses of action.*

2. **Operational Priorities:** *An improvement in the ability to determine operational priorities, and use these as a basis for incident response operations, was identified as a key area for improvement. This was to include mechanisms to translate an*

understanding of key network terrain, identified using ICS-CDTP, into prioritised activities for the CPT.

3. **Team Interaction:** *A definition of clear roles and responsibilities within a recognised team structure was assessed to be required to improve the overall performance of the team. This was to include means by which individual understanding of information or events could be propagated throughout the team to develop Level 3 SA and improve overall Team SA.*

4. **Operating Environment:** *Improved techniques to understand the operational environment were identified as an opportunity to improve team efficiency. Standard operating procedures were targeted for development to reduce the time taken to understand a network, its associated ICS devices, and their exposure to possible APT activities.*

5. **Team Understanding:** *This model required the least development, and was not targeted for specific improvement within the experimental period.*

8.5 SCIPS and Cyber Defence Exercise, April 2017

This experiment was designed as a result of the observations from the exercise described in Section 8.4. The experiment comprised 26 participants, and adopted a novel exercise format and structure that combined SCIPS and a new way to conduct CDX (described in Section 7.5.2) intended to provide the opportunity for iterations of experiences, followed by periods of reflection, to promote the formation of ideas and development of the *APT Attack Behaviour*, *Operational Priorities*, and *Team Interaction* mental models.

8.5.1 Pre-Exercise Questionnaire Results

Participants were asked to complete a pre-exercise questionnaire. This provided the first of the thematic analyses of data. It highlighted the following initial themes, which are elaborated in Appendix A.2:

- *'Adversary Understanding'*
- *'Defensive Operations'*
- *'Defensive Planning'*

Adversary Understanding

The adversary understanding theme focused the participants' comprehension of the *'intent'* of the adversary, and the *'attack methods'* employed.

Attack Intent: This sub-theme discussed the intent of the antagonist. It was characterised by broad, general statements that focused on generic actors, as opposed to those who would specifically target ICS. Adversaries were stereotyped as:

> *"A person who is trying to gain information from an organisation for profit or malicious use. This can be gained initially through social engineering to target a weak point in an organisation"*

Attack Methods: The attack methods sub-theme concentrated on the nature of the network intrusion. The descriptions ranged from general, non-specific statements, to those that demonstrated at least a theoretical understanding of antagonistic techniques:

> *"Able to move quietly, using existing network capabilities or configuration issues to move laterally and escalate privileges. 2. Ability to maintain persistence, using volatile memory and injection. 3. Has a defined motive – a reason to get in and be determined to stay there. 4. Can conduct reconnaissance quietly so the network boundary penetration is not discovered"*

Defensive Operations

This theme focused on cyber defence operations, and almost exclusively discussed the need for establishing and maintaining SA when responding to a complex incident.

Situational Awareness: The comments focused mainly on communications within the team:

> *"For a Team Leader situational awareness is maintained by constantly receiving updates from the various sub-teams and integrate with intelligence and known methodologies"*

Defensive Planning

The defensive planning theme considered those activities that should be undertaken prior to an incident, and concentrated on two sub-themes; *'preparatory actions'* and *'security architecture'*.

Preparatory Actions: This focused on the actions an organisation could undertake to prepare itself for a network intrusion incident. The commentary largely focused on technical activities:

> *"Good system hardening. SIEM [Security Information and Event Management]/log correlation across all systems. Well-trained incident response*

> *team. Regular incident response drills and wash-ups of past incidents. Threat intelligence team in-house"*

Security Architecture: This sub-theme described the elements of an overall security architecture that would improve an organisation's security posture. As with the preparatory actions, the language focused on technical design:

> *"The basics of cyber security are the best. For example, keeping the systems patched, hardened, users trained and tested on good cyber security hygiene. Defence-in-depth: defender with the right tools and skills to keep ahead of threat actors"*

8.5.2 Post-SCIPS Questionnaire Results

After completing the pre-exercise questionnaire, the exercise participants undertook a period of classroom training, then all played SCIPS, experiencing an APT attack end-to-end within the game. Each round of the game ended with teams describing their assessment of where the attackers were in the adversary lifecycle and Purdue Model, intended to develop their *APT Attack Behaviour, Team Understanding*, and *Operational Priorities* mental models. Following SCIPS, all of the participants were asked to answer a further questionnaire.

The four themes that emerged from the questionnaire, elaborated in Appendix A.3 were:

1. *'Adversary Understanding'*
2. *'Stakeholder Priorities'*
3. *'Defensive Planning'*
4. *'Network Understanding'*

Adversary Understanding

This was the strongest of the themes, and encapsulated the participants' understanding of the APT actor represented in the SCIPS game. Five related sub-themes to the theme were apparent within the theme, those of attack *'intent'*, *'impact'*, *'methods'*, *'lifecycle'*, and *'threat intelligence'*.

Attack Intent: The understanding of the antagonist's intent altered from the pre-exercise questionnaire and demonstrated a strategic understanding of attacks on ICS:

> *"To force political change through disruption of public infrastructure"*

Attack Impact: Like the growth in comprehension of attack intent, the assessment of attack impact demonstrated a greater understanding of the strategic consequences of an attack on ICS.

> *"to disrupt, damage or destroy ICS which will create panic, distrust in the industry or government, as well as financial impedance"*

Attack Methods: This sub-theme continued to focus on the detail of technical attack methods and the tactics, techniques, and procedures (TTP) they would adopt. It demonstrated an increased understanding of APT behaviours:

> *"This might involve (living off the land) using tools already available on the targeted network. Such as compromising user without creating new ones. Manipulating malicious traffic to look as normal, such as exfiltration using DNS"*

Attack Lifecycle: Participants demonstrated an understanding of how the use of an attack lifecycle model, or kill-chain, could be used to determine past actions, and project future activities:

> *"you can build up a hypothesis of what and where the attacker has been"*

Threat Intelligence: Feedback from the questionnaire highlighted a growing recognition of the use of threat intelligence to inform a defensive posture:

> *"You can only be effective with the collection of relevant, accurate, and up to date information about the threat"*

Network Understanding

The need to understand a network and its associated systems, as a prerequisite for cyber defence, emerged as a strong theme. The questionnaire respondents described this theme in two forms; *'network baselining'* and *'network monitoring data'.*

Network Baselining: This sub-theme of network baselining focused on establishing a network pattern of life against which deviations from the norm could be determined:

> *"Network baseline and information flows. Network ingress/egress points. PLC/ICS process flows and critical points. Zone 0-5 boundaries and cross-boundary information flows"*

Network Monitoring Data: This sub-theme of network understanding was strongly related to supporting incident response, but the language focused on the exploitation of information acquired from sensors and logs:

> *"Any info relevant to the attack. What systems were affected? How were the systems attacked?"*

Defensive Planning

The requirement to proactively defend an ICS network, and plan ahead, emerged as a theme that encompassed both *'preparatory actions'*, and the development of a *'security architecture'*.

Preparatory Actions: This considered the need to plan ahead of a cyber incident, and ensure that appropriate plans were in place to address such a situation:

> *"I think early planning does make a big impact on the upcoming incident. So many things we would have done in the earlier stages won't work after certain time because the enemy is already in and implementing those systems is a waste of time and money"*

Security Architecture: As many of the participants playing the game had a technical background, it is unsurprising that a consideration of security architecture was discussed:

> *"In an ideal world: Secure-by-design architecture"*

Stakeholder Priorities

The priorities of the leadership within an organisation emerged as a theme, demonstrating an increasing understanding of wider business issues. The theme encompassed *'financial constraints'*, *'return on investment'*, and *'direction of investment'*.

Financial Constraints: Participants recognised, many for the first time, the financial constraints imposed by the necessity to maintain a viable, profitable business, and the limits this places on cyber security investment:

> *"had not deeply considered financial balancing act required of executives"*

Return on Investment: In a similar vein, participants started to acknowledge the requirement to demonstrate a return on security investments:

> *"Assess the risk in order to identify the best return on investment for money spent"*

Direction of Investment: Some participants started to see the value of using adversary understanding to direct investment to mitigate the threats of cyber attack:

> *"Spend wisely. Try to predict the worst attack and find a solution for it. Find the vulnerability in the system and think from the attacker's point of view"*

8.5.3 Post-CDX Questionnaire Results

The experiment then progressed to the CDX [254], using the criteria for a CIRT3 CDX within our progressive training model. To anchor the development of all five of the mental models, the SCIPS scenario was used as the scenario for the CDX, with participants being made aware that they were going to experience the same attack from game, but in a detailed range environment. The exercise comprised three days of attack activity, split into six half-days that corresponded to the activities played out in the six rounds of the SCIPS game. The Blue Team were briefed at the start of each half-day session which activities the Red Team would be undertaking against them. Each phase was time-bound, and at the end the Red Team would discuss with the Blue Team which of the activities they had detected, and which they had not.

Following the CDX, all of the participants were asked to answer a questionnaire (detailed in Appendix A.5). These questionnaires were completed at the end of the week-long experiment, by the same sample who completed the pre-exercise questionnaire. The responses discussed the participants' understanding of ICS, APT actors, and the nature of SCIPS and the CDX.

The questionnaire data was used to identify eight key themes, elaborated in Appendix A.5:

- *'Adversary Understanding'*
- *'Defensive Operations'*
- *'Defensive Planning'*
- *'Incident Response Training'*
- *'Exercise Management'*
- *'Cyber Range Quality'*
- *'Red Team Provision'*
- *'Stakeholder Priorities'*

Adversary Understanding

The adversary understanding theme focused on the *'attack lifecycle'* and the *'attack methods'* employed, reflecting on the concepts and ideas articulated after the SCIPS game.

Defensive Operations

The theme of defensive actions extended the context emerged from the SCIPS questionnaire. It elaborated four sub-themes; *'command and control'*, *'operational priorities'*, *'communications'*, and *'operating procedures'*.

Command and Control: This focused on the impact of poor leadership during exercise, and incident response in general, and reflected on issues that the team experienced during the early stages of the CDX:

> *"Too many people shouting out identified 'threats' with only a cursory investigation into that incident having being done at that point"*

Operational Priorities: The sub-theme of operational priorities discussed how an incident response team would determine where to focus resources and effort:

> *"Prioritise defence based on commander's mission, critical assets and valuable assets, and likely enemy intent drawn from threat intelligence. Solution may not defend all, but would defend most critical assets"*

Communications: Respondents commented on the need for effective communications between team members, reflecting changes in the effectiveness of their interactions as the CDX progressed:

> *"Communicate more regularly within the different areas of the team"*

Operating Procedures: The sub-theme identified the requirement for clear, detailed, SOP to guide incident responders:

> *"It would be advisable to have a clear, concise 'threat analysis' SOP, something easy to follow, especially useful to new members of the team"*

Defensive Planning

Within the defensive planning theme, two further sub-themes emerged, *'ICS understanding'*, and *'triage priorities'*. These extended the sub-themes of *'preparatory ac-*

tions' and *'security architecture'* already identified, but with no substantive change in their content.

ICS Understanding: The requirement to accurately understand the nature of ICS was highlighted as a key defensive planning requirement, reflecting how the ICS elements of SCIPS and the CDX influenced the participants:

> *"There are many threats to ICS, such as external threats (politically motivated, industrial espionage etc.), internal threats (employees with an axe to grind), human error, security challenges, securing ICS networks. Most ICS were built prior to cyber threats existing and therefore not designed with built-in security controls"*

Triage Priorities: The need to triage critical systems was identified as a key element of defensive planning, with respondents focusing on system availability:

> *"Threat to availability is more critical for ICS than for standard computer networks. Threat actors include: nation-states, individuals, criminals, political/activist groups (all with varying levels of sophistication)"*

Incident Response Training

The nature of incident response training emerged as exercise participants reflected how to effectively deliver learning outcomes. The sub-themes that arose discussed the need for a *'learning environment'*, a focus on *'training structure and pace'*, time for *'feedback and reflection'*, and the advantages of *'progressive training'*.

Learning Environment: A clear sub-theme of Incident Response Training was the nature of training environment, and its conduciveness to learning. In particular, it contrasted traditional military techniques:

> *"Good to work in an academic, non-military environment, as this promotes learning"*

Training Structure and Pace: Linked to the nature of the learning environment, the structure and pace of the training emerged as a consistent sub-theme, and in particular the management of time to allow for improved learning outcomes:

> *"The staged approach has allowed a better learning experience"*

Feedback and Reflection: Experiment participants also commented on the beneficial aspects of feedback and periods of reflection across SCIPS and the CDX:

> *"non-judgemental, structured learning environment. Sensible pace and regular discussions/debriefs. Collaboration with new individuals and academia enriches our knowledge and understanding"*

Progressive Training: This sub-theme of incident response training discussed the need for a programme that included individual training that develops into a series of progressively complex scenarios, as a means to target learning appropriately:

> *"able to focus in a progressive way on each phase of the attack cycle"*

Exercise Management

The management of CDXs emerged as a strong theme, encompassing *'exercise objectives'* in terms of positive outcomes, and *'exercise duration'*, with a focus on requests to extend the exercise execution window.

Exercise Duration: Exercise participants, whilst apparently enjoying the exercise, felt that greater training benefit could have been achieved if a longer exercising period was adopted:

> *"Longer time period for all (2 weeks would be great)"*

Exercise Objectives: Participants reflected that the exercise had clear training objectives that delivered a positive learning outcome:

> *"this was a very good exercise with much better training value. The exercise was, in my view, Blue Team focused, not just how good the Red Team is. Work and getting a better understanding of each stage of the kill chain enhanced our understanding of the required procedures in security/defending a network"*

Cyber Range Quality

Feedback from participants described issues with the range. Their comments focused on three sub-themes; *'range stability'*, *'range discrimination'*, and *'activity visualisation'*.

Range Discrimination: The sub-theme of range discrimination refers to the consequences of using a heavily virtualised architecture, and the inability of the Blue Team to determine whether characteristics of the network are as a result of a network intrusion, or simply a feature of the infrastructure:

> *"Accurate network diagram. Documented configuration"*

Range Stability: The comments on range stability largely referred to period of remediation on the network as a result of a power outage:

> *"Test stability of range more prior to exercise"*

Activity Visualisation: Participants requested the ability to record and replay attack traffic, to aid learning:

> *"Also, some sort of video replay of what the Red Team have done would be beneficial"*

Red Team Provision

The provision of a Red Team for cyber exercises, their *'discipline'*, frequency of *'feedback'* to the Blue Team, and their *'rules of engagement'*, were discussed.

Red Team Discipline: Feedback from participants focused on the benefits of the discipline of the Red Team on the exercise at DMU, as compared to previous exercises they had experienced:

> *"The exercise was, in my view, Blue Team focused, not just how good the Red Team is"*

Red Team Feedback: Participants considered the feedback provided by the Red Team to the Blue Team on the exercise at DMU, and its positive impact on learning outcomes:

> *"Each phase then concludes with feedback so Blue Team know if their actions had an effect (good or bad)"*

Rules of Engagement: The constrained rules of engagement for the Red Team on the DMU exercise were reflected upon by the participants, and its effect on their experience:

> *"Usually the Red Team will go out of scope or advance too quickly for any benefit to be gained. The constrained rules of engagement (ROE) for the Red Team allowed us to gain more from the exercise by understanding more at each phase"*

Stakeholder Priorities

The priorities of the leadership within an organisation again emerged as a theme, this time with two sub-themes; *'financial constraints'* and *'strategic viewpoint'*. The view of financial constraints did not differ substantially from the previous narrative. *'Strategic viewpoint'*, however, added a new facet to the theme.

Strategic Viewpoint: Participants discussed how SCIPS, in particular, shaped their understanding of the strategic issues surrounding cyber security, beyond just financial issues:

> *"The SCIPS game gave a high-level understanding of how security is viewed by COs [commanding officers] and company directors"*

8.5.4 Past Exercise Experience Interviews

During the exercise, a subset of participants who had prior cyber exercise experience were interviewed. A series of eight interviews were conducted with seven individuals. This highlighted seven themes, elaborated in Appendix A.4:

1. *'Incident Response Training'*
2. *'Exercise Management'*
3. *'Red Team Provision'*
4. *'Defensive Operations'*
5. *'Adversary Understanding'*
6. *'Cyber Range Quality'*
7. *'Defensive Planning'*

Throughout this section, the names of the exercises that the interviewees have attended have been obfuscated. This does not detract from the intent or understanding of the comments.

Incident Response Training

The theme of incident response training emerged as the strongest theme from the interviews. It encompassed the need for *'adversary training realism'*, a *'consistent toolkit'*, time for *'feedback and reflection'*, the need for the provision of a suitable *'learning environment'*, the advantages of *'progressive training'*, and the use of *'table-top exercises'*.

Adversary Training Realism: This sub-theme discussed the requirement for adversary understanding to translate into a realistic adversary that incident responders can train against, to allow for response techniques and processes to be thoroughly tested against specific threat actors:

> *"we'll go on an exercise and maybe it's a case of them starting off with hacktivists then evolves into an APT in that classic way that is always kind of predictable, rather than having separate training periods where you discuss a threat from X adversary"*

Consistent Toolkit: This encompassed the need to train as the team would respond in real life. Specifically, it addressed the requirement to use the tools that they would have access to should an incident occur, rather than the 'freeware' usually deployed on training infrastructures:

> *"for example, have Cisco firewalls – we never train with Cisco firewalls..., so it's usually PFSense or Vyatta on exercises. So people are tested on different tools to those we need in the real world, and it also increases the number of tools people have to learn, and we already have overload on that"*

Feedback and Reflection: Interviewees discussed the requirements for time to reflect on the events that have unfolded within an exercise, to make sense of them, and adjust their behaviours as a consequence:

> *"It gives us an opportunity to go back and look at things like the logs and see when that happened, what it looked like on the sensor. So then, from a sensor perspective, see what it looked like if it happens again, potentially write signatures for it, and stuff like that. And then also, from a Harden [Hardening Team] perspective, what can we do to remediate against it should they come in? What can we do to remediate to stop that data from being exfilled? What can we put on the firewall, what can we do on the server?"*

Learning Environment: The interviewees commented on the learning environment at DMU, and drew comparisons to previous exercises:

> *"I do think you could significantly improve individual's abilities by putting them in a more academic environment; a non-adversarial, mentored environment"*

Progressive Training: The sub-theme of incident response training further elaborated the need for a programme that included individual training that develops into a series of progressively complex scenarios for teams:

> *"So, in general terms, we have been doing CT1 through to CT5 [collective training levels 1 to 5] in one exercise, so we never get to train as individuals or as a team before [the exercise]. We tend to be doing our individual and team training on a CT4 or CT5 level exercise , so either an international or national exercise, where it's high tempo. Even if you're not being formally validated, there's an understanding that it's a test, and that it's a reflection on the capability or readiness of the team and the individual, which is not ideal because we've not had prior opportunity to iron-out any issues, or even to rehearse or exercise basic things"*

Table-Top Exercises: In discussing options for incident response training, the applicability of table-top exercises emerged:

> *"I think we could get a huge amount of value out of just table-topping and just taking away all that technical expense issue and just discussing, verbally, how you would deal with issues. It forces us to think, as well. Even in this scenario today, we've got sucked straight into "are the sensors working?", it's always the engineering issues that suck up the first few days or week, or however long, of an exercise. If that was taken away and we were just speaking in theory about how you would recognise and defend against particular kinds of threats it would force us to focus on the theory, and a more rigorous approach, and we could focus on documenting those lessons and putting them into our SOPs, rather than always just going on an exercise and just fighting through, and just trying to keep our heads above water, and then breathing a sigh of relief and going home"*

Exercise Management

All of the interviewees had experience of previous cyber exercises, and reflected on the issues they had encountered. The theme comprised four sub-themes; *'objectives'*, *'preparation'*, *'realism'*, and *'control'*.

Exercise Objectives: The subject of exercise objectives was emotive, as the interviewees had experienced unclear objectives in the past, with confusion over who the training audience were. This led to the perception that the Blue Team were never going to be put in a position where they could adequately defend against the Red Team:

> *"So you're put into that environment, yes, the attacks are escalating, but if you're not training toward a defined objective, how do you get there?"*

Exercise Preparation: The *exercise preparation* sub-theme is closely associated with the *consistent toolkit* sub-theme of the *incident response training* theme. Interviewees cited how the preparation of exercises had not considered the requirement for the Blue Team to baseline the network they were defending, or supply the tools necessary for their objectives:

> *"Other exercise points; probably another point would be admin stuff leading up to deploying – there's either not enough information, or we get information too late to act on it. For example, [EXERCISE], it's probably unavoidable because it's international so we're at the behest of our [INTERNATIONAL] partners' decisions, but not only do we not often get to choose and deploy our own tools, we don't even know what tools we're going to have until we get there"*

Exercise Realism: For cyber exercises to be of benefit to incident responders, the interviewees commented on the need for realism, in terms of scenario, and the aspects of the network that can be modified to improve their defensive posture:

> *"So there's always been that unrealistic aspect where we've had to make all these network changes, and engage with these people, that either don't exist in reality or would not give you permission in reality. So it makes you wonder what the point is, because what would you do in the real world?"*

Exercise Control: The control of the exercise by the White Team on previous exercises emerged as a strong sub-theme, with interviewees highlighting the need for strong management of the exercise to deliver the training objectives:

> *"there's a lack of a management layer that understands both the requirements of the training serials and the Blue Teams, the training audience, and has enough knowledge of Red Team activity that they can actually control it"*

Red Team Provision

The provision of a Red Team for cyber exercises, and their rules of engagement, was a point of contention for the interviewees. This theme encompassed the *'discipline'* of the Red Team, their *'capability'*, and the nature of how they provide *'feedback'* to the Blue Team.

Red Team Discipline: The sub-theme of Red Team discipline on previous exercises encompassed both the positive and negative aspects of Red Team behaviour, and the requirement to play within the agreed rules of engagement:

On the positive side, interviewees commented:

> *"Red Team activity was scripted to match the intelligence function, which means that training audience getting realistic, managed serials"*

However, on the negative side, interviewees cited:

> *"Because there was no-one reigning them in, they weren't staying within their arcs [agreed limits of responsibility], and were doing things they really shouldn't be doing. Because there was no control of the Red Team that then meant that they were able to go and do it. Not so much the guy sat at the keyboard's fault, there was no overarching layer of control to reign people in"*

Red Team Capability: This sub-theme focused on the capabilities of a Red Team, including their availability, skillset, and agreed attack playbooks:

> *"At the moment, if we do that ourselves, and we tried it, it's very much 'script kiddy' because we don't concentrate on the same sort of skills. People say 'you're Blue Team you can do Red Team' – I disagree entirely. It's a completely different point of view, I think, in the way you look at your network. A different set of skills really. It absolutely is. I want good network engineers, whereas a good pen tester doesn't actually have to be a good engineer himself. He just needs to know how he can exploit stuff and understand more coding and underlying structures rather than understanding what he needs to make the service work"*

Red Team Feedback: This covered the requirement for the Red Team to provide feedback to the Blue Team, so that the Blue Team have the opportunity to learn from their experiences. In particular, the comments of the interviewees focused on the need for a *shotval* on previous exercises, a military term that describes a period evaluation and reflection period delivered immediately after the end of a day's play on the exercise range:

> *"We didn't have any shotval wash-up with the Red Team players, so it almost felt like we were sailing into the wind. We didn't know where we were going"*

Defensive Operations

The defensive operations theme encapsulated the *'roles and responsibilities'*, *'communications'*, and *'situational awareness'* of the incident response team. Although no substantive additional narrative was provided to the 'roles and responsibilities' and 'communications' sub-themes, important aspects of developing 'situational awareness' were discussed.

Situational Awareness: Underpinning the whole of the defensive operations theme was the requirement for situational awareness, and how this was maintained. It included not only the techniques to maintain situational awareness, but also how the layout of the room used by the incident response team affects such cognisance:

> *"Another very useful thing to do is every hour or two, force everyone to have hands-off keyboard and the TL [Team Leader] or watchkeeper if necessary, would point at individual respective teams and they would brief quickly what below was going on. Very often we would find that two teams that were working in the same room, suddenly someone would join the dots all of a sudden and realise that actually they were working on the same thing. Arguably, every hour or so, just that five minutes to chance have a chat rather than people going down a certain, specific tasking can be very useful"*

> *"So what we find is there's a couple of factors that will affect how information passes around the team and overall situation awareness. The first one is where everyone's sitting. So if you look at [INTERNATIONAL EXERCISE], everyone will sit facing each other in a circle [open square]. The layout of that room [the room at DMU used for the April 2017 exercise] is all these little islands, and you'll find that the people will naturally drop into the macro problem, they'll start looking at their logs, they'll work on the Splunk server, but they won't talk across each other"*

Adversary Understanding

Within the context of understanding the threat actors that face an organisation, the sub-theme of *'threat intelligence'* was discussed. This did not substantially add to the previously identified content of the sub-theme.

Cyber Range Quality

The interviews highlighted the dependency of cyber exercises upon the quality of the ranges that they operate. It focused on two distinct sub-themes, those of *'range stability'* and *'range discrimination'*, although it did not significantly change the previously identified sub-theme content.

Network Understanding

The theme, in this instance, focused on network terrain analysis.

Network Terrain Analysis: The network terrain analysis highlighted the need to proactively assess the valuable network assets that would be attractive to an attacker:

> *"and that evolves into integrating a genuine Cyber IPE [ICS-CDTP] key terrain analysis"*

8.5.5 Experiment Outcomes

As a result of the experiment, the CPT added the role of the Blue Terrain Manager (BTM) to their organisational structure. The role of the BTM was to coordinate all activities across the network the team are defending, to ensure that the network terrain has been analysed and prioritised, and to focus defensive efforts based on an understanding of the adversary.

8.6 Table-Top Exercise, June 2017

The author was invited to participate in an exercise that fitted the criteria for a CIRT3 TTX with a UK CNI provider [255]. The exercise required the organisational crisis management team to report to a leadership structure at regular intervals, requiring accurate SA from the team, as well as the need to forecast defensive activities to respond to a mid-tier actor with the capability to manoeuvre covertly around a network and adapt to the incident responders' actions. The intent of the exercise was to assess the organisational agility to deal with such a situation, and to test the adaptability of the leadership to manage a dynamic situation and interact with their wider regulatory community.

No feedback questionnaires were completed. Only the author's observations are included.

This was the first time the leadership had been brought together for such an exercise, and it was observed that whilst the individuals responsible for managing each operating component had proven response processes, the integration of these to deal with a significant cyber event had not been tested. It was assessed that this may have been as a result of not progressively exercising the scenario.

It was assessed that leadership had established mental models for the *'Operational Priorities'* and *'Operating Environment'*, based on their in-depth understanding of the business. However, their *'APT Attack Behaviours'*, *'Team Understanding'* and *'Team Interaction'* mental models were poor, no doubt as this was their first exposure to such a scenario.

8.6.1 Experiment Outcomes

It was observed that no processes were in place to establish the triage of systems during a crisis, which contributed to the leadership's lack of focus. Similarly, no processes were defined to establish and maintain SA, which provided the information available to base decisions upon. The outcome of the exercise was a review of the processes, and the planning of a further exercises to drive-out the necessary improvements.

These observations shaped the scope of the TTX facilitated by the author in June 2017, the results of which are reported in Section 8.8.

8.7 Cyber Defence Exercise, June 2017

The author joined 20 members of the purposeful sample, the Army CPT, on an international exercise [256] involving over 1000 people across the Red, Blue, White and Green Teams that was executed over 14 days. The sample was split between two teams, the first comprising solely personnel from the CPT, the second integrating personnel from other nations. The exercise fitted the criteria of a CIRT5 CDX, in that it was intended to test the participants to the point of failure, and designed to determine at which point the C2 of the team cannot cope.

The CPT intended to further test the techniques from Section 8.5, to drive the development of SOPs so that new members joining the team would have a documented framework in which to integrate. It was also planned to test the new organisation structure they had adopted as a result of the experiment in Section 7.5.2 that resulted in a new team role of Blue Terrain Manager, that drew heavily on the concepts of the ICS-CDTP.

The author, along with the leadership of the CPT, observed the behaviours of the sample on the exercise, and recorded their assessment of their performance. No feedback questionnaires were completed by the exercise participants.

It was commented by the team leader that, as a result of the exercise described in Section 8.5, that on this exercise:

> *"the [intrusion detection] and [network hardening] aspects of the [team] displayed a high level of confidence"*

He further commented that:

> *"the slow time walk through and red team feedback received at DMU was directly correlated to the actions of the red team on [this exercise]. As the red team progressed along the cyber kill chain we anticipated, as a team, the next steps they would take"*

The personnel from the sample were split across two teams. Those that were integrated into a multi-national team comprised a smaller subset of the more experienced members of the CPT, with the majority remaining in the UK team.

It was observed that the multi-national team, led by the most experienced member of the CPT, operated with greater efficiency than the UK team. However, neither team were using detailed operating procedures. It was highlighted that most of the processes of the CPT resided in the heads of a few individuals. This resulted in ad hoc approaches to responding to incidents. The more experienced the individual leader, the better the response, but it was assessed that this was not a repeatable process. This inefficiency was in some way mitigated by the high levels of individual skills observed, but the team interactions were far from optimal, suggesting a weak *'Team Interaction'* mental model. Similarly, SA across the teams was inconsistent.

Although the introduction of the Blue Terrain Manager, as discussed in Section 8.5, provided a sound triage of critical systems, and coordinated the activities of the team across the network to prevent 'blue on blue fratricide', team SA remained poor. It was observed that no formal processes to maintain SA had been developed.

It was further observed by the Red Team in their feedback, that the CPT had failed to correctly interpret key attack behaviours on the network. In particular, the team had not seen attempts to compromise the Domain Controller. It was assessed by the Team Leader that this was as a result of having to interpret covert activity from logs and sensors, and that this would be a key learning activity for the immediate future.

8.7.1 Experiment Outcomes

It was decided, as a result of the analysis of the exercise, that:

1. SA processes would be developed for the team.
2. A new role of SA Manager would be introduced in the short-term to ensure these processes were adhered to.
3. The new SA processes would be tested on a TTX to assess their completeness and effectiveness, along with the wider set of standard operating procedures in use by the team.
4. A CDX would be planned to target the development of detecting covert adversaries on networks, and assess the effectiveness of standard operating procedures.
5. Consideration should be given to developing software tools to support the techniques within ICS-CDTP.

8.8 Table-Top Exercise, August 2017

This experiment [257] was derived following a review of the performance of the CPT on the exercise described in Section 8.7. It was acknowledged by the team that overall SA was an issue, and that their *'Team Interaction'* mental model and associated processes were poor. In line with the training priorities identified in Section 8.7.1, a TTX was developed to assess the effectiveness of the team's processes.

The SCIPS scenario was used as the basis of the CIRT2 TTX, as the familiarity with the scenario allowed the team to focus on how they work and interact. A modified set of facilitation questions, based on those summarised in Section 7.5.3 and detailed at Appendix E, were used to drive out the detail of what was included, or omitted, in the team's SOPs. The TTX was executed as a one-day exercise that was attended by

12 of the purposeful sample. The TTX was designed to bring together representatives of the sub-teams within the CPT to assess how the operating procedures of the team and sub-teams interoperate, and how overall C2 and SA was maintained during an incident. In particular, it looked at how the elements of ICS-CDTP could be further embedded in their processes. The TTX was intended to test the proposed SA Manager role, to sit alongside the Blue Terrain Manager, to ensure Team SA was maintained across concurrent network activities.

Feedback questionnaires were completed at the end of the exercise. A total of 12 questionnaires were received. Unsurprisingly, all of the responses focused on the theme of *defensive operations.*

Defensive Operations

The theme encompassed *'communications'*, *'information flow'*, *'roles and responsibilities'*, *'situational awareness'*, and *'operating procedures'*.

Communications: The TTX participants emphasised the need for effective communications, and how the assumption of a *'Team Understanding'* mental model does not always equate to its realisation:

> *"It has highlighted parts we take for granted that we perceive people should already be aware of – how 'things', 'tasks' are carried out. Also that we need to feed or record all events so they can be correlated for the bigger picture"*

Information Flow: The TTX highlighted shortcomings in the informations flows around the team as a result of poor, or non-existent procedures and proceses:

> *"Better understanding of sub-team information dependencies"*

Roles and Responsibilities: Questionnaire respondents highlighted an increased understanding of team roles and responsibilities as a result of driving out operating procedures:

> *"It has clarified who sits under what team and how they are likely to operate in an operational/exercise environment"*

Situational Awareness: Situational awareness again emerged as a sub-theme, and in particular, the team leader and sub-team leads commented on the need to maintain SA:

> *"Has made me think a great deal more as to what the processes should be. I will need to have oversight on all areas, as well as the big picture, and ensure*

> *that communications up and down happen regularly to keep an all-informed net"*

Operating Procedures: As the focus of the TTX was to drive-out the detail of the team's operating procedures, it emerged as a strong sub-theme, and resulted in the scoping of seven new standard operating procedures:

> *"Our SOPs [standard operating procedure] are massively outdated and mostly unfit for purpose -> the new seven consolidated SOPs will be much more appropriate and useful for new teams starting up"*

8.8.1 Experiment Outcomes

The TTX highlighted a number of deficiencies in the team's operating procedures. It also highlighted seven new operating procedures that should be written, and confirmed the role of SA Manager as essential to their incident response capability.

8.9 Cyber Defence Exercise, August 2017

As a result of the priorities described in Section 8.7.1, a three-day CDX was facilitated to improve the team's ability to identify covert attack behaviour on a network, and assess their ability to maintain SA. A day's preparation was included (Day 0) that preceded the three days of exercise execution, to allow the range to be assessed, to set up Blue Team tools, and trial team operations. The Blue Team was split into four sub-teams:

1. **Hunt:** *Responsible for active threat hunting on the network.*
2. **Monitor:** *Monitoring the security tools deployed on the network and inspecting for possible malicious activities.*
3. **Harden:** *The sub-team responsible for hardening all of the network devices.*
4. **Intelligence:** *Responsible for threat intelligence fusion and the Blue Terrain triage.*

A Red Team was assembled that would repeatedly run the same set of attacks over the three days to allow the Blue Team to improve their effectiveness at detecting them. The primary attack was the delivery of an implant that would beacon out to a Red Team C2 node in greyspace, and from there, receive instructions to laterally move to the network Domain Controller (DC). The Red Team rules of engagement restricted the beacons to Reverse HTTP and HTTPS, with the Server Message Block (SMB) protocol as the only permitted mechanism to laterally move on the network. The use of Mimikatz™ was permitted to harvest credentials from memory, as was the manipulation of Microsoft Windows™ Management Instrumentation (WMI) events to create persistence on devices. It was an acknowledged limitation of the experiment that no dedicated malware or forensic examination tools were available to the CPT, and the timeframes limited the opportunities to identify memory-resident malware.

As with the CDX described in Section 8.5, the Red Team briefed the Blue Team on the planned activities at the beginning of each day, and provided feedback to the Blue Team at the end of the day. The Red Team logged their activities in the Red Team server. The Blue Team recorded their activities in an event logging system that was updated by each team member at least once an hour. This allowed the progress of Blue Team activities to be tracked. Along with voice communications, the Blue Team also used a chat application to interact.

The event logs were used to assess Blue Team activity and determine the time between the deployment of a Red Team effect and Blue Team detecting it. They were also used, along with the chat logs, to analyse the nature of the communications, and characterise the interactions as Levels 1, 2 or 3 of SA.

Observations were made regarding the levels of SA achieved by the team, and the effect of the role of SA Manager.

The durations of each of the days of the exercise were as below:

1. Day 1 - 6.5 hours
2. Day 2 - 5.75 hours
3. Day 3 - 3.0 hours

8.9.1 Red Team Activity Detection

The activities of both Red and Blue teams were compiled into a single log for analysis, detailed at Appendix B. The activities are summarised below.

Day 1: Two client devices were implanted with malware that beaconed out to C2 servers in the greyspace of the range. The compromised devices were used to laterally move to a SharePoint (SHPT) server, before reaching the target devices of DC1 and DC2 Domain Controllers, as depicted in Figure 7.6. Finally, DC2 was then configured to communicate directly with the greyspace C2 servers to see if the Blue Team would detect this.

The Blue Team took *97 minutes* to identify one of compromised devices beaconing via HTTP talking to SHPT and DC1 over SMB. They took *178 minutes* to detect the second compromised device beaconing to greyspace, as well as communications via SMB to the first compromised device. A total of *169 minutes* were required to identify DC2 interacting directly with greyspace C2 nodes.

The Blue Team did not identify Mimikatz running on any devices, or malicious WMI events on DC1.

Day 2: Two distinct streams of attack activity were conducted, with no interrelationships between the attacks until they reached their ultimate target of DC1. The first stream compromised a subset of client devices that subsequently took control of SHPT before navigating to DC1. The second stream created a similar chain of separate compromised client devices, with extensive use of malicious WMI events, before finally reaching DC1.

It took the Blue Team *11 minutes* to detect the first compromised device in the first chain communicating to a greyspace C2 node, and to DC1. The team then took *25 minutes* to detect a device in the chain of the second stream, correctly identifying a Reverse HTTPS beacon. A malicious file running Mimikatz and communicating with greyspace was identified *71 minutes* after deployment.

Day 3: Additional beacons were dropped onto client devices late in Day 2 to prepare for Day 3. Covert malicious DLLs were injected into existing processes on a chain of client PCs to establish SMB communications between devices and to DC1. Password data from DC1 was exfiltrated to greyspace C2 nodes.

The Blue Team took *20 minutes* to identify the first reverse HTTP beacon, and a total of *60 minutes* to identify the chain to DC1.

A separate Blue Team stream of activity was established after identifying the communications chain, to identify the malicious processes. This process took *180 minutes.*

Assessment: The Blue Team demonstrated a marked improvement between Day 1 and Day 2 of the exercise, which was observed to be as a result of the detailed feedback provided at the end of Day 1. By Day 3 the team had become proficient in identifying the intrusion activity, so the investigation of malicious processes was undertaken as a *'stretch target'*. The time taken to identify the malicious processes was probably affected by the lack of analysis tools available to the team.

8.9.2 Situational Awareness Observations

One of the key objectives of the exercise was to assess the team's ability to maintain SA. Observations of the team started at Day 0, to review their starting position, and any changes in behaviour and effectiveness as the exercise unfolded.

Day 0: The pre-exercise day saw the team configure the room into an 'open square' configuration, as discussed in Section 8.5.4. A four-hour window was provided to set-up security monitoring tools. The Red Team deployed two implants onto client devices, with one chaining the other, so that only one beaconed to greyspace C2 nodes using a

Reverse HTTP connection. Neither of these implants were detected by the Blue Team. The team's new, incoming Team Leader assumed the role of the SA Manager. It was observed that team cohesion was initially poor, with a visible lack of SA and little sub-team communication. It was further noted that the Blue Team were not completing the event logs that would be used to record their understanding of Red Team behaviours and assess SA. At this point the team had not setup a chat service. It was also noted that the team were not adhering to the hourly 'heads-up' brief, as mandated by the team's new SA SOP, where they would stop work for five minutes each hour to brief the rest of the team. As a result, it was agreed that the Blue Team would have hourly exercise 'freeze points' where the event logs would be updated, and the SA briefs given to the team.

Day 1: The outgoing Team Leader started to mentor the incoming Team Leader, which provided guidance to shape the day's operations. The Intelligence sub-team did not produce a triage of the Blue Terrain until the afternoon, which left the Blue Team without a strategic direction for half of the day. The Monitor sub-team were focused on finalising the installation of their network monitoring tools and were not focusing on the attacks that the Red Team had told them they would deliver. It was observed that the Monitor sub-team identified SMB traffic between a client PC and a DC, but did not understand it was potentially malicious. This suggested a lack of Level 2 SA.

The Hunt sub-team did not focus on the client PCs, where the Red Team had told them their implants would land, or the DCs, which they were advised would be the attack targets. They also did not acknowledge the critical systems defined in the Blue Terrain analysis by the Intelligence sub-team that was delivered in the afternoon. This included the SHPT server in the list of priority devices, that again, went ignored by Hunt.

Overall, despite the hourly freeze point, team SA was assessed as poor by midday. This was fed back to the Blue Team, with a noticeable improvement in communications and SA in the afternoon. A significant increase in the use of whiteboards and other visual material was noticeably apparent, and a clear flow of information between sub-teams was observed. Similarly, the Hunt and Monitor teams improved their focus and performance after the midday feedback. By the end of the day, the Monitor sub-team had sensors deployed on all of the critical systems. The day-end feedback by Red Team demonstrated how the implants were delivered, and how lateral movement to the SHPT and DC servers was achieved.

Day 2: The precursor to the day's proceedings included a review of the previous day's performance. This included the key point that whilst individual SA started to emerge by midday, team SA only started to coalesce at the end of day feedback on Day 1.

Day 2 started with a far better team understanding of Red Team attack techniques and the detection of compromised devices and lateral movement. Initially, the hourly briefs were not adhered to, but this was addressed mid-morning. These briefings started out very much at Level 1 SA, focusing on what had occurred, without providing any Level 2 SA contextualisation. This was balanced, however, by the Intelligence sub-team briefs that used visual aids, demonstrating activities within the adversary lifecycle and using the Diamond Model. These focussed exclusively on Level 3 SA and the forecast of Red Team likely courses of action. Discussions ensued that demonstrated the emergence of Level 2 SA and overall Team SA, shaped by the Intelligence sub-team Level 3 briefs.

Towards the end of the day the team were demonstrating high levels of Team SA, with discussions becoming far less focused on the details of Level 1 SA, and far more about Level 2 SA contextualisation and Level 3 SA projection.

The day-end feedback session started with a review by the Red Team, who explained the two attack streams that had been undertaken, highlighting where the CPT's increased understanding from Day 1 had been effective. A subsequent review of overall SA focused on how it had improved once visual aids and graphical representations had been used, and how the whole team used these to understand the entirety of what was being detected on the network.

Day 3: The final day of the exercise started with the Red Team again briefing the Blue Team on the day's planned attacks. From the start of the day's activities, the Blue Team demonstrated far greater confidence and cohesiveness, with increased communications between the sub-teams and a far greater emphasis on maintaining Level 3 SA individually and across the team. Much more effective use was made of visual aids, with the adversary lifecycle and the Diamond Model being used as common frames of reference for the whole team. Hourly briefs were maintained (although the day's activities only lasted three hours) with each sub-team operating far more efficiently.

The day-end review contained positive feedback from Red Team on the speed and efficiency with which Blue Team had identified and countered their attack activities. Feedback from the Blue Team on the exercise included a consensus that they were operating far more effectively and with greater confidence than at the beginning of the experiment.

8.9.3 Situational Awareness Log Analysis

Two logs were maintained over the course of the exercise; an event log used to record Blue Team observed network events, and a log of all chat conversations between team members. These logs were reviewed after the exercise.

Event Logs: The event logs recorded observed network and host events over the full thee days of the exercise. The recorded commentary was analysed and classified based on the categories below:

- **Level 1 SA:** *Where the technical identifiers of an attack were observed, without* *any discussion of their relevance or context.*

- **Level 2 SA:** *Where Level 1 identifiers were fused to provide a greater comprehension of network attack activity, or where the recorded narrative highlighted the significance of an identified activity.*
- **Level 3 SA:** *Commentary that fused Level 1 and Level 2 events or information to provide a projection of the future activities of the Red Team, or where an individual analysis of acquired data forecast possible antagonistic courses of action.*
- **Miscellaneous:** *General commentary with no relevance to SA.*

As can be seen from Figure 8.1, on Day 1, whilst Level 1 and Level 3 SA records were identified, Level 2 understanding was low. This may have accounted for the misinterpretation of Red Team activities, i.e. the contextual understanding of Level 1 indicators was not fully comprehended, resulting in inaccurate assessments at Level 3.

By Day 2, the number of Level 1-only comments reduced significantly, with parity almost achieved between Level 2 and Level 3. This coincided with in an increase in observed Team SA.

On Day 3, the Blue Team were far more confident in their understanding of identified attack behaviours, and this was reflected in the high number of Level 3 records.

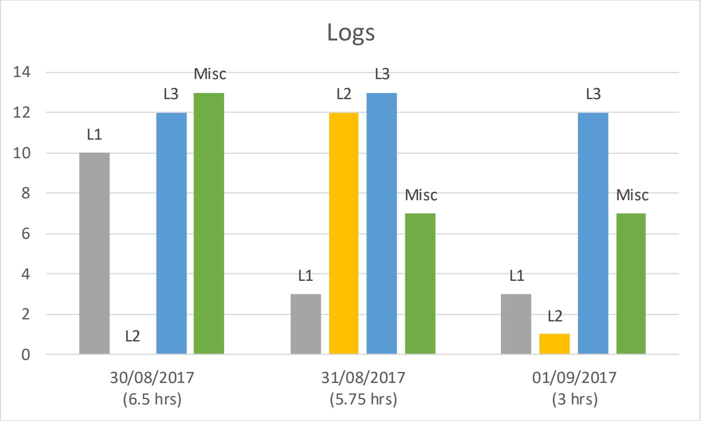


Figure 8.1: Event Logs

Chatroom Communications: Due to technical issues, the chat service was only available for two days of the exercise. The chats were classified using the same definitions of Level 1 to 3 SA as used to assess the Event Logs. However, the definitions were extended to filter out chat acknowledgements, requests for information that had no relevance to SA, status updates that had no relevance to SA, and general administrative conversations.

As can be seen, the majority of chats focused on Level 1 and Level 2 SA, with very little Level 3 observed. This, it was assessed, was due to the real-time nature of chat, and the use of the Event Logs to record the projection of Red Team activities, supplemented by the voice communications of the hourly SA briefs.

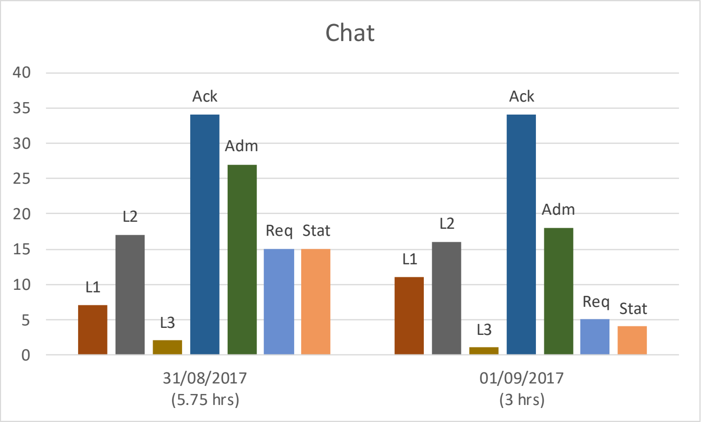


Figure 8.2: Chatroom Communications

Team Leader Feedback

The outgoing Team Leader provided some insightful feedback regarding the performance of the team, and the effectiveness of the exercise. He commented that at the start of the exercise the:

> *"Overall direction and leadership was lacking, individuals lacked context for their technical skills and communication was poor"*

He reflected on the improvement made by the team as the exercise progressed:

> *"As the serial [period of training] progressed, sub-teams improved their internal communication and processes as they were able to place context around their activities. With assistance, they were able to improve cross-team communication and information flows which, in turn, developed overall CPT situational awareness. Implementing an hourly update/team brief, supported by a J2 [Intelligence sub-team] update ensured that the sub-teams were aware of what the other teams were doing and able to place their activities into the big picture. The management team were able to maintain control of their assets and re-direct resources or activities when the situation changed. The overall improvement was evidenced by a comparison of the noise level in the trg [training] room on day 1 [Day 0] and on day 4 [Day 3]. In the beginning, the room was quiet with analysts focussed on their screens. By day 4 [Day 3] there was a noticeable difference, with analysts talking to their sub-team leads, sub-teams talking and sharing information between each other and the management team were visibly interacting with the team as a whole, particularly during the hourly briefs. There is still a tendency when the tempo*

> *increases for the hourly briefs to slip as the team is drawn to their respective screens. The TL [Team Leader] and Situational Awareness Manager (SAM) are responsible for maintaining the battle rhythm [operational cycle of activities] of the CPT and should therefore ensure that these updates are conducted. The relationship can be seen as similar to a commander and chief of staff (COS). The commander may get drawn into a particular scenario or problem and the COS is there to pull them out when required so that the overall mission functions are completed."*

He discussed the use of whiteboards and the graphical representations of Red Team behaviours using the Adversary Lifecycle Model and the Diamond Model from the ICS-CDTP:

> *"This was the first opportunity to show APT TTPs [tactics, techniques and procedures] and projected actions as a graphical overlay. This, combined with the situation and network boards, enabled the team to be able to look up and gauge the current situation and operational tempo at a glance"*

The wider challenges of a the team's role, and the complexity of the incident response situations they face was also discussed. The Team Leader focused on the need to triage the Blue Terrain to prioritise defensive actions:

> *"The CPT deploys to networks with little to no prior knowledge of their configuration, information flows or patch states. This is significant as the CPT must understand the network as quickly as possible in order to develop situational awareness. A key discussion concentrated on where to direct analysis and technical effort in the initial arrival stages with dissent around the network boundary v Domain controllers. This is a valid conversation with no right or wrong answer. There are, however a number of considerations. Focussing on the boundary requires there to be some understanding as to what should and shouldn't be crossing it and how internal assets route to it. This is not always immediately obvious as the network configuration is not as it should be. Concentrating on key services is good if there is an understanding of how these should be running (which is not the same as how they are running). Cognitive overload is a significant factor- the team are seeing the network for the first time and it takes time and effort to understand what they are seeing and then, crucially, to place it into the context of the situation and the adversary. No single person can do this and therefore the flow of information around the team is essential. J2 [intelligence] and the management team need this information flow in order to develop their overall situational awareness and understanding so that they can conduct their estimates and provide direction as the team moves into the PROTECT phase. It is therefore suggested that initial ME [main effort] should be directed that*

> *the monitor team concentrate on the boundary whilst the hunt team focus directly on the KCT [Key Cyber Terrain] Tier 1 assets – in this case the Domain Controllers. The sub-teams can then increase their view outwards as their SA increases. A horrible military analogy would be the monitor team are acting as a sentry whilst the hunt team go forward and clear the Tier 1 location."*

The Team Leader concluded by summarising the effectiveness of the exercise, and its applicability to further training:

> *"In Summary, a useful exercise that took a team with a lacklustre performance on [INTERNATIONAL EXERCISE] to one that demonstrated key skills and concepts required for DCO [Defensive Cyber Operations] in the deployed space. Further work is required to develop team cohesion, information flows, processes and procedures. The progressive format of the exercise proved key to developing the team's performance. It is recommended that this serial should be repeated as a regular team activity as part of in-barracks training."*

8.9.4 Experiment Outcomes

The nature of the CPT's operations requires a prioritised approach to data ingest. Subteams were observed in the early stages of the exercise to be ignoring the Team Leader's direction and working to ingest data outside of the stated priorities. It was agreed that data acquisition would be shaped by time boundaries as a means to ensure consistency in setting sensors and log collectors against agreed priorities. An outline set of priorities was agreed:

1. **Priority 1:** *Installing a Network Intrusion Detection System (NIDS) with passive traffic taps.*
2. **Priority 2:** *Integration of the NIDS feeds to a Security Event and Information Management (SIEM) tool.*
3. **Priority 3:** *Deployment of Host Intrusion Detection Systems (HIDS) and log collectors on key network terrain assets, such as Domain Controllers, Boundary Firewalls etc., with feeds to SIEM.*
4. **Priority 4:** *Deployment of HIDS and Log Collectors on all remaining network assets.*

Based on the principle of *'assumed breach'*, this prioritisation was defined to allow the team to begin to assess network behaviours almost immediately and start to acquire a critical mass of network traffic to start to identify anomalies. The feeds integrate into a SIEM to allow for more ready access to, and analysis of, this data. Priority 3 activities deploy HIDS and log collectors onto key network terrain assets to allow monitoring of triaged, likely targets. Priority 4 encompasses the rest of the network, brought under the monitoring of the SIEM as resources and time permit.

8.10 Cyber Exercise Training Programme, November 2017

A DCO MST training programme (described in Section 7.5.7) for participants for the exercise described in Section 7.5.8 was held, educating 36 individuals over three, one-week training programmes, each including SCIPS and a TTX.

For the SCIPS element, a total of 36 questionnaire responses were received. From these, four themes emerged:

1. *'Adversary Understanding'*
2. *'Defensive Planning'*
3. *'Network Understanding'*
4. *'Stakeholder Priorities'*

For the TTX component, a total of 38 questionnaire responses were received. Four themes were apparent:

1. *'Adversary Understanding'*
2. *'Defensive Operations'*
3. *'Network Understanding'*
4. *'Stakeholder Priorities'*

The resulting, merged, thematic results are summarised below. They are elaborated in Appendix A.7.

8.10.1 Adversary Understanding

This was again the strongest of the themes, and encapsulated the participants' understanding of the APT actor represented in the SCIPS game. Seven related sub-themes to the theme were apparent within the theme, those of attack *'intent'*, *'impact'*, *'methods'*, *'lifecycle'*, *'courses of action'*, *'capability'*, and *'threat intelligence'*.

Attack Intent: The *intent* theme discussed the strategic goals of the antagonist, including how this intent may be focused to apply wider political pressure by an asymmetric adversary:

> *"Political coercion on the bigger scale, however, also a show of force from a below-peer potential enemy"*

Attack Impact: The *impact* of the attack reflected the manifestation of the antagonists actions in the SCIPS game:

> *"It made me more aware of how an attack can snowball over time"*

Attack Methods: Attack methods described the participants' understanding of the techniques employed by APT actors, and how they would behave in an intrusion into an ICS network. They included the initial attack vector through to lateral movement and wider impact, linking this sub-theme strongly to the adversary lifecycle:

> *"Dropping malware onto the computer and branching out using peer-to-peer connections"*

Attack Lifecycle: This sub-theme reviewed the game participants use of the adversary lifecycle and Purdue Model to assess the attacker's progress through a network, triaged using the CARVER matrix:

> *"Be less reactive, but predict what the adversary will do next. Take into consideration CARVER matrix"*

Adversary Courses of Action: The assessment of the possible *courses of action* an adversary could pursue whilst on an ICS network was inherently linked to the use of the adversary lifecycle. However, this sub-theme emerged as a distinct element within overall adversary understanding:

> *"Trying to figure out where the attacker was and trying to plan. What to do next to prevent the attacker from damaging the network and infrastructure"*

Adversary Capability: In discussing the capability of the adversary, the experiment participants differentiated between intent and capability:

> *"Just because they have the capability doesn't prove malicious intent"*

Threat Intelligence: This theme discussed the exploitation of using intelligence to shape network defence activities.

> *"Intelligence feeds, news, social media"*

8.10.2 Defensive Operations

Defensive operations encompassed *'communications'*, *'information flows'*, *'roles and responsibilities'*, *'situational awareness'*, and *'operating procedures'*.

Communications: The communications between members of the team emerged as a sub-theme of defensive operations:

> *"It highlighted the importance of communication and that to be aware of what each team is doing will mean as a whole you can work together better"*

Information Flows: The participants were advised to adopt the role of Blue Terrain Manager within their TTX team structure, to manage activities on the network and prevent 'blue on blue' incidents caused by a lack of coordination:

> *"Helped me understand to communicate the information to the BTM [Blue Terrain Manager] to keep team operations smooth"*

Roles and Responsibilities: The TTX emphasised the definition of clear role descriptions within the team:

> *"TTX has highlighted the individual roles and responsibilities of each member. Also it has contextualised the training to the degree that all members of the team feel more confident going into the [next] exercise"*

Situational Awareness: As the TTX progressed, the participants became far more aware of the need for maintaining SA:

> *"vastly improved my knowledge of cyber and has introduced many new concepts which will now feed directly into my situational awareness and improve my overall ability as a Team Leader"*

> *"Visual situational awareness is always better"*

Operating Procedures: One of the key outcomes of the TTX was to highlight the need for standard operating procedures:

> *"The TTX was one of the most useful exercises this week and allowed me to pull together the techniques and tools learnt and place them in the appropriate point of the SOPs. It gave me a good overview of how the team members fit together and highlighted the interchangeable nature of skill sets"*

8.10.3 Defensive Planning

Defensive planning, in this instance, focused on defensive *'triage priorities'*, *'preparatory activities'*, and *'security architecture'*.

Triage Priorities: The participants of the SCIPS game highlighted the need to assess the network under defence to determine the likely targets of interest to the attacker:

> *"It brings to bear the meaning of prioritisation and the long-term impact of triaging based on the services that are more important in relation to the posed risks"*

Preparatory Activities: The pre-incident preparatory process was cited as a sub-theme of the defensive planning theme:

> *"Mitigation is better than reaction"*

Security Architecture: Participants of the SCIPS game highlighted the need for a robust security architecture as an sub-theme of the overall defensive planning process:

> *"Ring fence our assets and capabilities with layer of security"*

8.10.4 Network Understanding

Understanding the network being defended focused on *'network baselining'* and *'network monitoring data'*.

Network Baselining: A focus on creating a foundational understanding of recognised assets, traffic flows, and behaviours, against which anomalies could be assessed:

> *"[with] hindsight the order in which we implemented the defence was wrong. Highlighted the need for a full understanding of the network processes and functions"*

Network Monitoring Data: This sub-theme of network understanding was related to the exploitation of information acquired from sensors and logs:

> *"Source and destinations in order to determine where they are and what box they are operating from"*

Network Terrain Analysis: The questionnaire respondents focused on network terrain analysis in particular:

> *"By categorising the network and its importance"*

8.10.5 Stakeholder Priorities:

The financial implications and constraints of an organisation's expenditure on cyber security emerged.

Financial Constraints: This sub-theme focused on the relationship between security and financial expenditure limitations:

> *"It gave a deeper understanding how money is a large aspect of cyber defence"*

8.10.6 Experiment Outcomes

The intent of the DCO MST was to assess if the training provided to the purposeful sample of the CPT could be condensed and delivered within a reduced timeframe, and to allow the assessment of the effectiveness of the training in the subsequent exercise described in Section 7.5.8. A subset of exercise participants were trained in the DCO MST, with the teams not attending the training acting as the control group. The results of the exercise are discussed in Section 8.11.

8.11 Cyber Defence Exercise, December 2017

Following on from the training provided in Section 7.5.7, the author attended the 10 day CIRT4 CDX that the DCO MST was provided for, to evaluate the performance of the Blue Teams, and compare the levels of SA achieved by those who attended the MST versus those who did not. The exercise was already designed to be measured using a quantitative set of metrics by a third party. As such, the assessment performed in this experiment, wherever possible, fitted within the established evaluation metrics, although independent, qualitative observations were made and recorded by the author. These are recorded in memos at Appendix C.

8.11.1 Team Profiles

The exercise comprised 12 teams. Each is profiled below. Detailed characterisations from memos and observations are included at Appendix C.

Team 1: Team 1 comprised a mixed team of five individuals from the UK who had not worked together before, and five from an international partner. No members of the team attended the DCO MST. After arrival at the exercise, the team chose adopt a structure similar to that recommended on the MST, comprising a Team Leader, a second-in-command (2IC), with the rest of the team forming 1 x Intelligence, 2x Protect (their own definition that included network hunt activities), 2x Monitor, 2x Harden. The UK personnel described themselves as having a low level of technical competency, with the international partners exhibiting more experience.

Team 2: A subset of the team attended the DCO MST, but were joined on the exercise by a Team Leader, 2IC, and an intelligence embed, none of whom had any training prior to the exercise and had no previous cyber experience. The team claimed a low level of technical competency. They comprised 9 personnel in total, and formed into the team structure recommended on the DCO MST (Figure 7.7), with a Team Leader, Blue Terrain Manager (BTM), 1 x Intelligence, 2 x Hunt, 2x Monitor, 2x Harden.

Team 3: The team claimed a low level of technical competency at the DCO MST, which was supplemented by additional individual training to raise their overall understanding of DCO tools. They comprised 8 personnel in total, and formed into the recommended team structure (Figure 7.7), with a Team Leader (also managing threat intelligence), BTM, 2x Hunt, 2x Monitor, 2x Harden. They were not a formed team before the exercise.

Team 4: The five-person team described themselves as having a mix of cyber technical competencies, from mid- to high-level. They organised themselves based on the networks to be defended, with two personnel assigned to each network. They demonstrated a dynamic approach to work; they regularly came together for planning sessions, then broke away to carry-out assigned tasks. The team did not attend the DCO MST and were not a formed team prior to the exercise.

Team 5: The team described themselves as having a low level of cyber competence, and were not a formed unit before the exercise. Part of the team attended the DCO MST, including the Team Leader. They aligned themselves to the force structure similar to that taught in the DCO MST (Figure 7.7), providing 1x Team Leader, 1x BTM, 2x Hunt, 2x Monitor and 1x Harden. They integrated an intelligence embed who had not received any training prior to the exercise and had no previous cyber experience.

Team 6: The team described themselves as having a very low level of cyber competence, and were not a formed unit before the DCO MST and exercise. They aligned themselves to the structure taught in the DCO MST (Figure 7.7), providing 1x Team Leader, 1x BTM, 2x Hunt, 2x Monitor and 2x Harden.

Team 7: Team 7 comprised personnel from the CPT that formed the purposeful sample for this research. They attended the exercise with a relatively high level of training and experience. The team comprised 1x Team Leader, 1x BTM, 3x Monitor, 3x Hunt, 2x Harden and 1x Intelligence.

Team 8: The 11-person team was not formed prior to the exercise, but comprised a significant element from an established network operations team. They claimed a medium level of technical competence in the cyber domain. The team appeared to adopt the methods of working used by the network operations team and chose not to use any of the DCO MST. Only one (junior) member of the team attended the DCO MST.

Team 9: The team comprised four international partners who described themselves as competent with cyber technologies, although they had not worked together prior to the exercise. They also integrated an intelligence embed who had not received any training prior to the exercise and had no previous cyber experience. None of the team attended the DCO MST and did not adopt any of the methods taught.

Team 10: The team was not formed prior to the exercise. Only one member of the team, the Team Leader, attended the DCO MST, but not for the whole course duration. The team claimed a low-to-medium level of cyber competence. The team was structured along the lines of the DCO MST, with 1x Team Leader/BTM, 2x Hunt, 2x Monitor, 2x Harden, 1x Intelligence, with individuals focusing on different network segments to allow concurrent activity.

Team 11: The team comprised five personnel. They described their technical competence as low to medium. Given the small size of the team, the Team Leader adopted a flexible structure to allow resources to be deployed as required. None of the team attended the DCO MST.

Team 12: The team described themselves as having a low level of cyber competence, and were not a formed unit before the DCO MST and exercise. They aligned themselves to the structure taught in the DCO MST (Figure 7.7), providing 1x Team Leader, 1x BTM, 2x Hunt, 2x Monitor and 2x Harden. The majority of the team attended the DCO MST, including the Team Leader.

8.11.2 Development and Application of Mental Models

Each of the teams were assessed for their effectiveness during the exercise. The structure provided by the mental models proposed in this research was used to frame their performance.

Team 1

APT Attack Behaviours: *The team did not attempt to model the attack behaviours identified on their network to provide a greater understanding of the nature of the antagonists. They retained a reactive approach to incidents that did not use the previous intrusions to shape their network hunt capability.*
Team Interaction: *As a team of individuals from two nations, the team had little time to fuse. As a result, the team structure, roles, responsibilities, and interactions were under development for almost the whole exercise.*
Team Understanding: *They international partners provided a greater technical depth of understanding of networks than their UK counterparts. This led to an imbalance in the distribution of effort, and the effectiveness of the 10 personnel in the team was reduced as a result.*
Operational Priorities: *The team did not produce a coherent triage of the systems under management on their networks. Much of the team's early focus was to request changes to their RoE, which were repeatedly rejected.*
Operating Environment: *The team maintained a reasonable understanding of their network, but Team SA was observed to be repeatedly poor.*

Team 2

APT Attack Behaviours: *Team 2 were disadvantaged by a poor level of individual technical skills that limited their ability to identify and interpret Red Team behaviour on their networks. Their mental model started to coalesce towards the end of the exercise, but only on activities identified at the start of the exercise.*
Team Interaction: *The team adopted the structure and information flows recommended in the DCO MST, and despite only coming together as a team for this exercise, they maintained a reasonably high level of Team SA and overall C2.*
Team Understanding: *As a team coming together just for this exercise, and with poor levels of individual technical skills, their team understanding did not reach sufficient levels of team understanding until the end of the exercise. The time together on the DCO MST did appear to contribute to a collective understanding of team member capabilities.*
Operational Priorities: *The team collectively understood the operational priorities of the exercise, and reprioritised based on the evolving scenario.*
Operating Environment: *The team maintained a reasonable level of understanding of their operating environment, albeit constrained by their poor individual technical skills.*

This understanding was maintained for the whole of the exercise.

Team 3

APT Attack Behaviours: *The team demonstrated a high level of understanding of APT behaviours and were proactive in attempting to assess their courses of action, and as a result, means to mitigate their threats. Despite an initially poor level of individual technical skills on the DCO MST, the remedial training provided, plus follow-on activities prior to the exercise, had increased their abilities to an intermediate level. This was reflected in their technical understanding of Red Team activities.*
Team Interaction: *The team were not a formed unit before the exercise. The team adopted the structures and techniques taught on the DCO MST rigorously. Team interaction was well managed, with strong C2 and information flows. Team SA, in particular, was high, with continuing improvements observed over the whole exercise.*
Team Understanding: *The majority of the team had a week together on the DCO MST that clearly assisted with cohesion and understanding of capabilities. Team 3 were observed to work well together.*
Operational Priorities: *The team adapted to the changing operational priorities well, assessing and re-assessing likely Red Team COAs and targets.*
Operating Environment: *Team 3 spent a significant amount of time understanding their networks. Once achieved, they leveraged this knowledge extensively in their monitoring and hunt activities.*

Team 4

APT Attack Behaviours: *Team 4 focused primarily on network hardening as their primary means of defence, and did not focus on Red Team behaviours as indicators of likely actions.*
Team Interaction: *Team interaction was ad hoc, but to a large extent it was effective. The team did not adopt a recognisable structure until day 3 of the exercise.*
Team Understanding: *Although a team formed solely for the exercise, they meshed well. This may have been a factor of their relatively small team size. Team members were observed to be cognisant of other team members' strengths and weaknesses.*
Operational Priorities: *Team 4 maintained an approach based on hardening of the network infrastructure, irrespective of changing operational demands. However over-hardening, in some instances, denied their networks to their users.*
Operating Environment: *The team maintained a reasonable technical understanding of the networks under their management, but did not demonstrate a similar level of understanding of the needs of the user community operating on those networks.*

Team 5

APT Attack Behaviours: *The team maintained a continuous assessment of Red Team activities and likely COAs. Although limited by their individual technical skills, these assessments were realistic, and acknowledged the probable changes in targets as the exercise progressed.*
Team Interaction: *The team comprised a lower level of manning than many other teams. Despite this, they managed to adhere to a structure in-line with that taught on the DCO MST. This provided a clear set of roles and responsibilities for team members, and an operational cycle that maintained acceptable levels of Team SA.*
Team Understanding: *Team understanding was acceptable. Although only formed for the exercise, team members were observed to be aware of each others' technical competencies.*
Operational Priorities: *Team 5 maintained a detailed view of operational priorities, and adjusted as the exercise progressed.*
Operating Environment: *The low level of individual technical skills initially hampered the team's understanding of the networks under their control. Once enumerated, however, they used their understanding to full advantage.*

Team 6

APT Attack Behaviours: *Despite a low level of individual technical skills, the team used their observations of Red Team activity to shape subsequent actions. This level of understanding, however, was not included in formal reporting within the exercise.*
Team Interaction: *The team adopted the structures, information flows and C2 recommended on the DCO MST, providing clear definitions of roles and responsibilities.*
Team Understanding: *The team started with probably the lowest level of individual technical skills on the exercise, but compensated by solely focusing on the skills required for their assigned role. This allowed a rapid development of capability, as well as a clear understanding of which skills sat with which team member.*
Operational Priorities: *The team maintained strong Team SA, and a solid understanding of the priorities of the networks under their control.*
Operating Environment: *The team's limited individual technical skills constrained their ability to enumerate their networks quickly, but once complete, they maintained a continuing understanding of the detail.*

Team 7

APT Attack Behaviours: *Team 7 developed a full IPCE with assessments of key terrain, avenues of approach, and Red Team COAs which informed their operations on the exercise. This provided the basis for their proactive approach to network defence.*
Team Interaction: *As an established CPT, the roles and responsibilities of the team members were well understood, and established processes were followed.*

Team Understanding: *It was observed that the technical skills of each team member were well understood.*
Operational Priorities: *Team 7 displayed a clear understanding of the priorities of each phase of the exercise.*
Operating Environment: *The team rapidly enumerated their networks and maintained an ongoing brief to check for changes.*

Team 8

APT Attack Behaviours: *Team 8 focused their efforts on network hardening and did not attempt to maintain an assessment of Red Team COAs.*
Team Interaction: *The nucleus of the team was based around an existing network support team, with a medium level of technical competence. The team adopted a structure based around the existing nuclei's normal operations. This proved effective, and allowed newer personnel to be integrated. However, it was noted that C2 and Team SA were centred around the Team Leader, who whilst efficient, was a potential single point of failure.*
Team Understanding: *Team understanding was governed by the Team Leader, who operated as a hub for the team. It was observed that when the Team Leader was not available, the operations of the team reduced in efficacy.*
Operational Priorities: *The team focused on hardening, and this approach did not alter over the course of the exercise.*
Operating Environment: *Team 8 maintained a strong understanding of their networks.*

Team 9

APT Attack Behaviours: *The team did not maintain a view of Red Team activities.*
Team Interaction: *The team had not worked together prior to the exercise. The maintained an informal team structure, and operated with limited levels of Team SA. They used a OneNote database to record data, rather than visual aids, which it was observed reduced verbal communications within the team.*
Team Understanding: *The team maintained a high level of understanding of each others' technical expertise.*
Operational Priorities: *The team did not demonstrate a high level of understanding of operational priorities during the exercise.*
Operating Environment: *Team 9 understood the networks under their control, but did not prioritise any elements as a defensive priority.*

Team 10

APT Attack Behaviours: *Team 10 maintained strong Team SA, and conducted ongoing assessments of Red Team activities.*

Team Interaction: *The team adopted the structure and techniques taught in the DCO MST. Roles and responsibilities were observed to be clearly defined with clear C2 and information flows.*
Team Understanding: *The team demonstrated an understanding of each others' skills despite only coming together for the exercise.*
Operational Priorities: *An ongoing assessment of priorities was maintained throughout the exercise, allowing reprioritisation as necessary.*
Operating Environment: *The team maintained a technical understanding of their networks, but lacked awareness of the impact of particular actions on the user community that resulted in significant loss of service.*

Team 11

APT Attack Behaviours: *Team 11 did not maintain a view of Red Team activities or TTPs. Their focus was primarily focused on hardening.*
Team Interaction: *The team was amongst the smallest on the exercise and did not adopt any recognised structure. Team SA was low. Roles and responsibilities were unclear.*
Team Understanding: *Team members appeared cognisant of each others' general technical abilities, although it was not always clear who was assigned to which task.*
Operational Priorities: *Initially the team maintained an acceptable level of understanding the exercise mission priorities, but this reduced over time as the team's focus shifted to the purely technical aspects of the networks.*
Operating Environment: *The team's understanding of their networks grew at a slower rate than many of the other teams. It is assessed that the team size may have been a contributory factor.*

Team 12

APT Attack Behaviours: *The team maintained a continuing assessment of Red Team activities that informed a highly-developed level of Team SA. This, however, was limited in its efficacy due to an overall low level of individual technical skills.*
Team Interaction: *The team fully adopted all of the structures, tools and techniques taught on the DCO MST, and displayed solid C2 with a strong understanding of roles, responsibilities, and information flows.*
Team Understanding: *The team was observed to understand the technical competencies of the members.*
Operational Priorities: *The team maintained a high level of understanding of the operational priorities, with this competence only dropping below average for one of the exercise days.*
Operating Environment: *The team successfully enumerated their network, but levels of understanding were constrained by their limited individual technical skills.*

Overall Summary of Use of Mental Models

It was observed that where the Team Leader or BTM had attended the DCO MST, the team adopted the structure recommended in the training. The structure was based upon the CPT SOPs specifically to accelerate the development of mental models, and had been demonstrated to deliver such coherence over the CPT development timeframe. The structure, however, required a minimum of 8 technical staff for it to be viable, which automatically precluded three of the teams attending. For those teams that adopted the structure, they organised faster than those teams that arrived without an organisational plan. These teams also had pre-planned their immediate activities on the networks, which was a major element of the teaching on the DCO MST, and further contributed to their increased performance during the early stages of the exercise.

Of the teams that did not adopt the structure, it is notable that none of the Team Leaders attended the DCO MST. Interviews with Teams 1 and 8, who had the manning profile necessary to adopt the structure, but chose not to, highlighted that Team 1 intended to maintain a dynamic structure, whereas Team 8 adopted the structure of the team that comprised the majority of its team members were already a part of.

Discussions with the Team Leaders of the teams that did adopt the structure (Teams 2, 3, 5, 6, 7, 10 and 12) all felt it provided a framework in which to operate, and reduce cognitive overload.

8.11.3 Assessment of Performance Using the Derived Themes

The overall exercise, including the 12 Blue Teams, along with the Red and White Teams, are now reviewed against the themes that emerged during this research.

Adversary Understanding

The theme of Adversary Understanding was used to assess the Blue Teams' performance on the exercise, to determine if this contributed to their defensive posture.

Attack Intent: Teams 1, 4, 8, and 11 did not maintain an understanding of the Red Team activities on their networks, or only adopted such techniques late into the exercise. In particular, they did not attempt to identify the Red Team's intent to shape defensive activities. This was observed to be a caused by a combination of two factors; firstly the belief that network hardening was sufficient to address Red Team actions, and secondly, a lack of understanding that DCO teams must be proactive to defend against an adaptable adversary. These behaviours were not observed in Blue Teams that attended and adopted the DCO MST (Teams 2, 3, 5, 6, 10, and 12), Team 7 (CPT) who were trained during this research, or Team 9, who displayed high levels of cyber experience.

Attack Impact: The same teams (1, 4, 8, and 11) that did not maintain an assessment of attack intent also struggled to articulate the risks carried by the (White Team) commander as a result of Red Team activities. This was assessed to be as a result of a lack of understanding of adversary intent, and resulted in a subsequent inability to project an outcome of such antagonistic behaviours.

Attack Methods: It was observed that many teams lacked an understanding of network attack techniques (Teams 1, 2, 4, 5, 6, 10, 11, 12). Whilst this subject was covered during the DCO MST, insufficient time was available to adequately correlate attack behaviours to data in sensors and logs. This inability to translate Red Team activities recorded by sensors and logs was raised a number of times during discussions with the Blue Teams.

Adversary Capability: The lack of understanding of attack methods extended to impact the ability to assess the adversary's capabilities. All teams, except Team 7, failed to characterise the nature of the threat actor and use this to shape their defensive posture and COAs.

Adversary Lifecycle: Those teams that attended and adopted the DCO MST (Teams 2, 3, 5, 6, 10, and 12) utilised adversary lifecycle modelling to assess where in the kill-chain the Red Team were. When combined with visual aids, this made a significant contribution to Team SA and the prioritisation of defensive activities.

Adversary Courses of Action: The teams that chose to adopt the Diamond Model of Intrusion Analysis (Teams 2, 3, 5, 6, 7, 10, and 12) were observed to fuse their analyses with the adversary lifecycle modelling and outputs from the CARVER matrix, to determine the likely next steps by the Red Team.

Threat Intelligence: The intelligence embeds in Teams 2, 5, 8, and 9 had no cyber experience. The assumption by the exercise planners (without consultation with the author) was that general intelligence analysis expertise would be sufficient to support cyber defence operations. Teams 2, 3, 4, 9 used intelligence reporting from the White Team to their advantage, but generated no actionable intelligence reporting based on Red Team activities on the networks they were defending. Only Team 7 demonstrated the production of detailed intelligence reporting based on their observations of Red Team intrusion behaviours on their networks. This was assessed to be as a result of detailed technical training provided for intelligence operators within the CPT.

Adversary Understanding Summary

It was observed that teams that did not attempt to understand the adversary did not undertake a comprehensive analysis of Red Team intent and likely targets, and did not therefore triage their defences and resources against Red Team COAs appropriately. Discussions with Blue Teams highlighted that, for the duration of the exercise, a belief that focus on network hardening was sufficient to survive the limited attacks provided by the Red Team. In reality, the approach would not have stopped a capable threat actor. This was assessed as a factor of training on exercises where inter-team competition was promoted, and behaviours were shaped by a desire to move up the league table, rather than work as they would need to in a real-world situation.

Defensive Operations

The theme of Defensive Operations was used to assess the operations of the Blue Teams during the exercise, to determine if this contributed to improved defensive impact.

Situational Awareness: The SA of Blue Teams was assessed against Level 1-3, as well as Team SA. Against a mean average of mediated, subjective scores (illustrated in Figures C.2 to C.13), Teams 1, 7, 8, and 11 demonstrated high levels of Level 1 SA, whilst Teams 2, 4, 5, 6, 10, and 12 were observed to demonstrate poor Level 1 SA. No correlation between Level 1 SA and skills or experience was observed. However, it should be noted that the measures of skills and experience, illustrated in Figure C.1 were self-assessed against measures provided by the existing exercise White Team, without strong controls over the selection criteria.

Level 2 SA was observed to be high (against a mean average of mediated, subjective scores) in Teams 3, 7, and 11. It was low in Teams 1, 4, 5, 6, 9, 10, and 12 (illustrated in Figures C.2 to C.13). As with the Level 1 SA, no correlation between self-assessed skills and experience was apparent, nor between Level 1 SA and Level 2 SA.

High levels of Level 3 SA (against a mean average of mediated, subjective scores) was observed in Teams 2, 3, 5, 7, 10, and 12, whereas low levels were seen in Teams 1, 4, 6, 8, and 9. No correlations were apparent between self-assessed skills and experience, or Level 1 or 2 SA.

Team SA was assessed as high (against a mean average of mediated, subjective scores) in Teams 2, 3, 5, 6, 7, 10, and 12, whilst it was low in Teams 1, 4, 8, 9, and 11. No correlation was apparent between Team SA and Levels 1-3 SA, or self-assessed skills and experience. However, there was a correlation with those teams that attended and adopted the DCO MST (Teams 2, 3, 5, 6,10, and 12) or were previously trained using its techniques (Team 7).

Communications: The teams that attended and adopted the DCO MST (Teams 2, 3, 5, 6, 10, and 12), as well as the CPT (Team 7) were observed to demonstrate more effective team interactions than those teams that did not attend. The efficacy of the communications was based on clear, established information exchange patterns. The teams that demonstrated these effective communications were all observed to have adopted the role of combined BTM and SA Manager, as recommended in the DCO MST (Figure 7.7).

Roles and Responsibilities: Discussions with the Team Leaders of teams that attended the DCO MST indicated that they believed their teams performed better as a result of the training than if they were to have attended the exercise without it. Teams that did not attend the DCO MST determined their structure, roles, responsibilities dynamically upon arrival at the exercise. This was observed to be an inefficient process, and detracted from network defence activities. The CPT (Team 7) used their established and model developed as a result of the activities described in this thesis. This model formed the basis of the team structure, and roles and responsibilities, taught on the DCO MST (Figure 7.7). Those teams with significantly less than eight personnel (Teams 4, 9 and 11) were unable to adopt this structure.

Operating Procedures: All of the teams attending the exercise were provided with the CPT SOPs developed by Team 7 (the purposeful sample) as a result of the experiments described in this thesis. Team 7 naturally adopted the these SOPs. Team 8 used the operating procedures used by the majority of the team in their day-to-day roles. Those teams that attended and adopted the DCO MST (Teams 2, 3, 5, 6, 10, and 12) had developed operating procedures as a result of the TTX undertaken at the training sessions that were based upon the CPT SOPs. Those that did not attend the training (Teams 1, 4, 8, 9 and 11) were observed to operate in an ad hoc manner (Teams 1, 8, 9 and 11) or adopt processes focused on network hardening (Team 4).

Command and Control: Teams with established operating procedures such as Team 7 (CPT), Team 8 (who were a largely formed team), and those that attended and adopted the DCO MST (Teams 2, 3, 5, 6, 10, and 12), demonstrated coherent C2. Teams 4, 9 add 11 all adopted dynamic models of C2, with varying degrees of effectiveness throughout the exercise. As the level of Red Team activity increased towards the end of the exercise these models were assessed to be less effective.

Operational Priorities: The teams that attended and adopted the DCO MST (Teams 2, 3, 5, 6, 10, and 12) demonstrated effective operating procedures and the ability to adapt to the changing operating priorities of the exercise. Those that did not attend the training (Teams 1, 4, 8, 9 and 11) were observed to demonstrate an inflexible approach to deal with changing operational priorities. These teams were observed to ignore the provided CPT SOPs and chose to develop their own.

Defensive Operations Summary

It was observed that where the Team Leader had attended the DCO MST, their team adopted the structure recommended in the training. The structure was based upon the CPT SOPs developed throughout this research, cognisant of the limitations of an eight-person team, but covering all of the essential roles (Figure 7.7). Team size was a factor of team effectiveness, and for the scope of this exercise a team of less than eight personnel degraded performance. The combined role of BTM and SA Manager was observed to contribute to Team SA, effective communications, and the ability to respond to changing operational priorities. The use of established, tested SOPs, was also observed to contribute to effectiveness of the Blue Teams. Those that adopted ad hoc processes were observed to operate with reduced effectiveness as the Red Team increased their network activities.

Incident Response Training

The Incident Response Training theme was used to assess the effectiveness of the learning opportunities provided by the exercise.

Adversary Training Realism: The Red Team provided a range of attack options intended to provide a realistic adversary. The primary delivery mechanism for malware was phishing attacks that were enabled by simulated user activity by White Team users. These initial implants beaconed to Red Team C2 infrastructure in the exercise greyspace using a variety of Reverse HTTP and HTTPS connections. Lateral movement was facilitated via SMB, with data exfiltration delivered via HTTPS and DNS. Attacks on the exercise ICS utilised Siemens Step-7™and Modbus. The activities of the Red Team were managed by a Team Leader to ensure compliance to behaviours consistent with an APT.

Consistent Toolkit: The toolkit provided to Blue Teams was Security Onion™. This was consistent with the tools taught on the DCO MST, although this training was largely ad hoc and intended to fill gaps in individual skills. The tools did not reflect the nature of software that teams would encounter if called upon to defend a network.

Training Reflection: The exercise execution period was between 9am and 3pm every day, allowing time for reflection by the Blue Teams. However, due to the number of Blue Teams, the Red Teams did not have time to individually debrief each day. Instead, the Red Team Leader provided a collective debrief to all Blue Teams. This was observed to be of limited value, as it did not provide details pertinent to each individual team. As Blue Teams were operating with differing levels of skill and effectiveness, and intrusions onto their networks were at differing stages and using varying Red Team techniques, this collective debrief offered little opportunity for Blue Teams to focus their subsequent efforts.

Progressive Training: For those teams that attended the DCO MST, they progressed from a CIRT2 TTX to a CIRT4 CDX in single step. For those that did not attend the DCO MST, they had no progression at all. Team 7 had experienced the exercises described in Sections 7.5.1, 7.5.2, 7.5.4, 7.5.5, and 7.5.6, in a progressive build-up to this exercise. The majority of the Blue Team personnel lacked the necessary individual skills to maximise the value of this CIRT4 CDX, and would have benefited from incremental learning opportunities beforehand. It should be noted that Team 7 won the exercise.

Table-Top Exercises: Those teams that attended the DCO MST participated in a CIRT2 TTX intended to develop their SOPs prior to the exercise. Discussions with attendees highlighted that they felt this was of significant value, and provided a framework to define their C2, communications and information flows to manage the defence of their networks and coordinate their incident response activities.

Training Structure and Pace: Whilst the structure of the exercise was well thought through, with a pace intended to allow time for participant reflection, the planning had not accommodated the levels of individual skills within the Blue Teams. The issue was exacerbated by the lack of tailored Red Team feedback to the Blue Teams.

Incident Response Training Summary

The exercise was well-planned, but its execution suffered as a result of a lack of progression in training beforehand. Blue Teams did not have the opportunity to form cohesively prior to the exercise, had significantly different individual technical skills, and did not receive the detail of information in Red Team feedbacks to properly facilitate reflective learning.

Exercise Management

The theme of Exercise Management was used to assess the effectiveness of the planning, execution, and measurement of the exercise.

Training Objectives: The training objectives for the exercise were pitched at a high-level by the White Team to allow for flexibility to adapt to the training audience, rather than adherence to a strict Main Events List (MEL). However, it was observed that the Red Team spent too long trying to adapt these into serials against which the Blue Teams could be tested. This was an inefficient use of resources and resulted in the Red Team being unavailable to provide detailed debriefs to the Blue Teams to facilitate their reflective learning.

The Blue Teams were assessed on a number of metrics defined by the White Team that included service availability, adherence to procedures etc. (defined in Section 7.5.8). Each Blue Team was assigned an individual assessor to review their performance against the metrics defined by the White Team. However, this review did not feed into any training coordinators to determine how to best stretch Blue Teams to maximise training value. None of the Blue Team assessment metrics were linked to the training objectives of the exercise, and therefore an objective assessment of the effectiveness of the training curriculum was not possible.

Exercise Preparation: The Blue Teams were provided with two days to map their networks and deploy security tools before the Red Team started attack activities. This provided an adequate exercise preparation period.

Scenario Realism: The exercise was based on a comprehensive scenario that was underpinned by realistic updates, injects, and cyber threat intelligence, that was coordinated with Red Team activities. This allowed Blue Teams that adopted adversary lifecycle modelling and used the Diamond Model to track and forecast Red Team activities.

Exercise Control: The White Team was observed to maintain a strong grip on the MEL and the coordination of Red Team activities to ensure they were aligned to the scenario and were consistent with the threat actors described in the collateral materials. Individual assessors were assigned to each Blue Team, and these fed back to the White Team twice per day in a formal review of performance. This shaped the Red Team activities undertaken against each Blue Team.

Exercise Duration: The duration of the exercise condensed a significant number of attack activities into the seven days of execution. Given the low levels of individual skills within the Blue Teams, an extended execute phase would have allowed for greater learning to be achieved. Potentially this could have been combined with further education in the tools used on the exercise.

Exercise Management Summary

The exercise provided a comprehensive scenario, against which the Red and Blue Teams were managed. The training objectives did not align to the metrics against which the Blue Teams were measured by White Team, and as a result, an objective measure of its effectiveness is not possible.

Defensive Planning

The Defensive Planning theme was used to review the pre-incident planning undertaken by Blue Teams.

Preparatory Activities: Those teams that attended and adopted the DCO MST (Teams 2, 3, 5, 6, 10, and 12), as well as Team 7 (CPT), had developed SOPs to address the pre-incident planning phase of a network intrusion. For those that did not attend the DCO MST (Teams 1, 4, 8, 9 and 11), such preparatory activities were undertaken on an ad hoc basis, even though they were provided with the CPT SOPs. Discussions with these teams suggested they felt they did not have the time to read, absorb and implement the processes described in the CPT SOPs.

Triage Priorities: The CARVER matrix proved effective for Teams 1, 2, 3, 5, 6, 7, 10, and 12 as a means of shaping the planning of defensive activities. Team 8 used a prioritisation process focused on server hardening, whilst Team 11 adopted an ad hoc approach.

Security Architecture: The cyber range used on the exercise was provided with firewalls and monitoring tools that Blue Teams could request the Green Team deploy in configurations of their choosing. Timescales prevented large-scale changes to the networks being defended, but they did allow a defence-in-depth architecture to be adopted.

ICS Understanding: ICS were new to nearly all exercise participants. A significant element of the DCO MST was dedicated to ICS in order to try and address this, but it is a large and complex field and could not realistically provide the necessary depth of expertise required in the time available. Those teams that did not attend the DCO MST, apart from Team 7, had no ICS experience. This was observed to limit the effectiveness of their defensive planning, especially those with no knowledge of Siemens Step-7™or Modbus.

Defensive Planning Summary

The exercise timeframe did not allow for detailed pre-incident planning processes to be developed in parallel with network defence activities. Those teams who arrived with established SOPs, an understanding of how to triage systems on the network, and an understanding of ICS, were observed to significantly reduce their cognitive burden during the early stages of the exercise.

Cyber Range Quality

The cyber range provided for the exercise ensured each Blue Team had access to their own network enclaves that allowed them to operate independently of other Blue Teams on the exercise. The Red Team was provided with a suitable greyspace infrastructure to deliver attacks. The theme of Cyber Range Quality is now considered.

Stability: No significant exercise downtime was observed to be due to a lack of range stability.

Discrimination: The extent of the virtualisation of the networks on the range, and the elements required to produce background network traffic etc., often caused range discrimination issues for Blue Teams, who subsequently had to submit Requests for Information (RFI) to the Green Team to determine the true nature of the network elements they had observed. More comprehensive range documentation would have alleviated this issue.

Activity Visualisation: No automated means to visualise the Red Team attack activity was available on the exercise. However, at the end of the final day, the Red Team demonstrated how a number of their attacks had been delivered. It was noted in comments from the Blue Teams that an understanding of the detail of the attacks earlier in the exercise would have enabled them to more adequately apply their defences.

Cyber Range Quality Summary

The cyber range provided was demonstrated to be robust and supported the exercise with high levels of availability. The extent of the virtualisation used in the range proved confusing for Blue Teams who lacked the necessary documentation to determine whether issues with deploying and interpreting sensors were due to misconfiguration or the nature of the architecture. This slowed defensive progress by the Blue Teams and increased the Green Team workload.

Red Team Provision

To assess the efficacy of the cyber threat emulation, the theme of Red Team Provision is considered.

Discipline: The Red Team displayed strong operational discipline and attempted to remain within agreed RoE. Activities were not observed that were contrary to the exercise scenario or behaviours of the threat actors fed to the Blue Teams via cyber threat intelligence updates.

Capability: The Red Team were formed purely for this exercise, and displayed a range of skills and technical competencies. It was observed that there was not a baseline set of skills across the entire team, which resulted in key personnel having to work on attacks on multiple Blue Team networks. This was inefficient and led to attack timing and coordination issues.

Feedback: Feedback to the Blue Teams was limited to a collective debrief at the end of each day. This was as a result of the requirement for the Red Team to prepare the attacks for the next day and revise their execution in light of the Blue Team defensive actions. Whilst this allowed for the next day's exercise period to execute as planned, it was observed that the learning opportunities for the Blue Teams were limited by this approach. The Red Team Leader indicated his ability to provide detailed feedback to Blue Teams was a factor of the limited number of personnel within his team.

Rules of Engagement: As discussed above, the Red Team operated within agreed RoE. However, although effective, the Red Team RoE were not formalised and required significant interaction with the White Team to achieve the necessary outcomes. This was assessed to be inefficient.

Red Team Provision Summary

The Red Team for the exercise maintained strong discipline, but their effectiveness as a learning aid to the Blue Teams was of limited value. As the Blue Teams were the training audience for the exercise, a greater emphasis on feedback from the Red Team was required. The Red Team were unable to provide this feedback due to limitations on their numbers and the premium of particular skills.

Stakeholder Priorities

The theme of Stakeholder Priorities considers how the requirements of an organisation's leadership are addressed.

Financial Priorities: Financial priorities did not form a part of this exercise scenario.

Strategic Viewpoint: The scenario that underpinned the exercise developed throughout the execution phase, with notional mission commanders in the White Team being forced to change their operational priorities as a result of a nation-state adversary's actions. These changes in priority required changes in defensive posture by the Blue Teams. Those teams that attended and adopted the DCO MST (Teams 2, 3, 5, 6, 10, and 12), and Team 7, were observed to accommodate these changes in priorities more readily than other teams.

Return on Investment: Return on investment did not form a part of this exercise scenario.

Stakeholder Priorities Summary

Established procedures that guide the prioritisation of assets to be defended allows the accommodation of changing strategic priorities.

Network Understanding

The theme of Network Understanding allows us to consider the time afforded to the Blue Teams to review the networks under their defence.

Network Baselining: The first two days of the exercise had no Red Team activity on the Blue Teams networks. This allowed time for the teams to understand the assets they were to defend and establish a viable baseline.

Network Terrain Analysis: Teams that attended and adopted the DCO MST (Teams 2, 3, 5, 6, 10, and 12), and Team 7, were observed to use the CARVER matrix, as well as elements of Diamond Model Activity Thread models to forecast potential Red Team activity against an adversary lifecycle model.

Network Monitoring Data: The first two days of the exercise allowed the Blue Teams to deploy their sensors and logs, and establish a pattern of life of network traffic prior to the Red Team starting their intrusion behaviours.

Network Understanding Summary

The two days permitted at the start of the exercise to assess the network architecture, deploy defensive tools, and to establish a pattern of life for network traffic, allowed Blue Teams to understand the networks they were to defend.

8.11.4 Experiment Outcomes

Attendance of the exercise allowed the themes developed over the experiments described in Chapter 7 to be tested for applicability to exercise audiences beyond the purposeful sample of the CPT. This applicability is discussed further in Chapter 9.

8.12 Summary of Themes

The themes developed as a result of the experiments described in Chapter 7, and elaborated in Appendix A, describe the common threads of commentary in interviews and questionnaires. The themes were used to shape the assessment of the exercise described in Section 7.5.8, and are reflected in Section 8.11 above. These themes, and their subthemes, are summarised below.

8.12.1 Adversary Understanding

Defensive cyber postures should be driven by an understanding of the nature and characteristics of adversaries. In the case of this research, the stereotype of threat actors is APTs. Without an understanding of the adversary, organisations cannot proactively plan their defensive policies or response strategies.

Table 8.2 summarises on the sub-themes that comprise Adversary Understanding.

Sub-Theme	**Description**
Attack Intent	The outcome that the antagonist wishes to achieve.
Attack Impact	The consequences of the threat actor's actions on the organisation that operates the services manipulated by the attacker.
Attack Methods	The tactics, techniques and procedures available to, or characteristic of, the antagonist and a description of how they may be employed.
Adversary Capability	A wider consideration of the capabilities of the threat actor, beyond the initial scope of the systems or services under analysis.
Adversary Lifecycle	An understanding of the nature of APT attacks, with the ability to identify and classify antagonistic behaviours within such a model.
Adversary Courses of Action	A description of the various COAs available to an attacker to achieve their intended aims.
Threat Intelligence	The acquisition, production, and dissemination of information likely to improve adversary understanding.

Table 8.2: Adversary Understanding Sub-Themes

8.12.2 Defensive Planning

Proactive defensive policies, procedures and plans allow an organisation to consider how they will adjust to a changing threat landscape and respond to network intrusion incidents, should they occur. The sub-themes within Defensive Planning are summarised in Table 8.3.

Sub-Theme	**Description**
Preparatory Activities	Pre-incident planning that supports procedural and technical threat mitigations.
Triage Priorities	A determination of which systems and services are essential to the continued operations of the organisation.
Security Architecture	The definition and implementation of mechanisms designed to impede the progression of an attacker through a network.
ICS Understanding	The detailed descriptions of the ICS elements within an organisation, their operating requirements, connectivity to IP-enabled devices, vulnerabilities, and current configuration.

Table 8.3: Defensive Planning Sub-Themes

8.12.3 Defensive Operations

The theme of Defensive Operations is concerned with the coordination and execution of activities once an incident has been identified. Its sub-themes are summarised in Table 8.4.

Sub-Theme	Description
Situational Awareness	The establishment and maintenance of levels 1-3 of SA, as well as Team SA.
Command and Control	The management of the response to an incident.
Communications	The requirement for regular, clear and concide communications within the team, and outside its boundaries to other teams and stakeholders.
Roles and Responsibilities	The definition of, and adherence to, a set of defined scopes for personnel involved in responding to an incident.
Operational Priorities	An understanding of the static and dynamic priorities of an organisation to maintain its continued services, and those systems that underpin them.
Operating Procedures	A definition of a set of SOPs that define how an incident will be responded to.

Table 8.4: Defensive Operations Sub-Themes

8.12.4 Stakeholder Priorities

Defending an organisation from cyber attack involves more than technical teams, and is usually governed by a leadership structure with a wider perspective of the requirements of managing risk. The sub-themes within Stakeholder Priorities are summarised in Table 8.5.

Sub-Theme	Description
Financial Priorities	An understanding of the fiscal imperatives of an organisation, and the risk-prioritised facets of cyber security that impact them.
Strategic Viewpoint	A perspective of the superordinate goals of an organisation, and how they may be affected by a cyber attack.
Return on Investment	A measure of the perceived benefits that investment in cyber security will bring.
Direction of Investment	A prioritised view of where cyber investment should occur, and how this aligns with wider stakeholder priorities.

Table 8.5: Stakeholder Priorities Sub-Themes

8.12.5 Network Understanding

Network Understanding encompasses a comprehension of all aspects of the networks to be defended. This includes the sub-themes in Table 8.6.

Sub-Theme	**Description**
Network Baselining	The creation of an understanding of the nature of the network, its assets, configurations, traffic profiles, deficiencies and constraints.
Network Terrain Analysis	The assessment of the network baseline to establish a view of the vulnerabilities that arise as a consequence.
Network Monitoring Data	A determination of the source and quality of sensor and log data in order to support network monitoring.

Table 8.6: Network Understanding Sub-Themes

8.12.6 Incident Response Training

The theme of Incident Response Training discusses the requirements for a successful cyber defence education programme. The associated sub-themes of such training are summarised in Table 8.7.

Sub-Theme	**Description**
Adversary Training Realism	The Red Team in any exercise should adhere to the behaviours of representative threat actors likely to target the organisation's systems or services.
Consistent Toolkit	The need for training programmes to use the tools that incident responders will use in a real-world intrusion.
Training Reflection	The requirement for feedback and periods of reflection within training programmes, so that mental models can be anchored in the minds of participants.
Learning Environment	Training is achieved better in an environment that is not judgemental, allows mistakes, and encourages exploration.
Progressive Training	With a subject as complicated as cyber incident response, educational programmes should adopt a crawl-walk-run approach to incrementally developing skills and team cohesion.
Table-Top Exercises	TTX provide a mechanism to develop and test operating procedures in a relatively stress free environment, that does not incur the costs of a cyber range.
Training Structure and Pace	Educational programmes should be developed with the training audience in mind, and structured to deliver the training objectives at a pace commensurate with their current level of understanding.

Table 8.7: Incident Response Training Sub-Themes

8.12.7 Exercise Management

For CDX to be successful, they must be coordinated and executed in a controlled manner to deliver the required outcomes to the training audience. The Exercise Management theme encapsulates the requirements of such control, as well as the characteristics of exercises that support effective experiential learning for participants. The sub-themes of Exercise Management are included in Table 8.8.

Sub-Theme	Description
Training Objectives	Cyber exercises must be developed with clear training audiences and objectives to ensure their effectiveness.
Exercise Preparation	The training audience must be allowed time to prepare for exercises. This should include time to read background materials as well as scheduling range time to understand the networks they will defend, and to setup sensors and logs.
Scenario Realism	It is essential that the scenarios used for exercises are based in reality and, wherever possible, are representative of the environments and characteristics they will have to deal with should an incident arise.
Exercise Control	The White Team of an exercise must maintain strict management of the planning and execution phases to ensure the training objectives are met.
Exercise Duration	The execution phase of the exercise must be sufficient to ensure the training objectives are met, and that participants have adequate time to reflect on experiences and adjust their activities.

Table 8.8: Exercise Management Sub-Themes

8.12.8 Red Team Provision

The skills and behaviours of the Red Team are critical to the success of a CDX. They must ensure they deliver the attack activities necessary to provide the opportunities for the Blue Team to experience the planned training serials in the MEL, in accordance with the training objectives. The sub-themes of Red Team Provision are summarised in Table 8.9.

Sub-Theme	**Description**
Discipline	The Red Team must ensure their activities are intended to deliver the training requirements of the exercise, rather than simply demonstrate the attacking team's network intrusion skills.
Capability	The skillset of the Red Team must be sufficient to deliver the training requirements, and must be distributed across the team to prevent bottlenecks.
Feedback	The Red Team must be scaled to provide regular, detailed feedback to the Blue Teams to ensure they have the opportunity to learn from their previous actions or failures.
Rules of Engagement	The Read Team must engage with the Blue Teams within strict criteria, to remain in the character of the threat actor they are portraying, and to align to exercise training objectives.

Table 8.9: Red Team Provision Sub-Themes

8.12.9 Cyber Range Quality

The complexity, resilience, flexibility and documentation of a cyber range is a critical factor in delivering CDX. The Cyber Range Quality theme addresses these characteristics. The sub-themes that address these facets are included in Table 8.10

Sub-Theme	**Description**
Stability	The range must be designed to maintain high levels of availability whilst the Red Team attempt intrusions and the Blue Team modify configurations to defend against these activities, with rollback facilities in the event of accidental misconfiguration by exercise participants.
Discrimination	The use of virtualisation to construct the range must be supported by appropriate briefings to the Blue Teams, along with the provision of appropriate design documentation to allow Blue Teams to determine whether issues are due to in-game activities, or as a result of features of the range implementation.
Activity Visualisation	Wherever possible, tools to capture traffic and intrusion behaviour should be used to support the Red Team debriefs to Blue Teams.

Table 8.10: Cyber Range Quality Sub-Themes

Chapter 9

Analysis and Critical Assessment

Contents

9.1 Introduction

This chapter analyses the results from the experiments described within this thesis, assessing their impact, and critically reviews their applicability and generalisability within the cyber domain. Specifically, it considers the following seven aspects of the research:

1. **Thematic Analysis:** *An assessment of the themes, their development and their relationships.*
2. **Mental Models:** *An analysis of the models proposed, their applicability to IR, and their relationships with the results of the thematic analysis.*
3. **Research Questions:** *A discussion of whether or not this thesis has answered the questions posed.*
4. **Effectiveness of the Experiments as an Experiential Learning Platform:** *A review of the serious games and exercises developed during this research, and an assessment of their efficacy as a platform to deliver experiential learning.*
5. **Limitations of Research:** *A consideration of the experiments and an assessment as to how generalisable the results are.*
6. **Alignment to Related Work:** *How this research addresses the identified gaps in literature.*
7. **Contribution:** *A proposal of the novelty of this research.*

9.2 Thematic Analysis

The thematic analysis was conducted using the results from the experiments described in Sections 7.5.2, 7.5.5, and 7.5.7, iteratively developing the themes from participant feedback. The purposeful sample provided data from the experiments in Sections 7.5.2 and 7.5.5, with a wider audience drawn from across a military audience in the experiment described in Section 7.5.7. This distinction of training audience is essential to understanding the context of the results, and to allow us to draw meaning from them.

The pre-exercise questionnaire results, summarised in Section 8.5.1 and elaborated at Appendix A.2 resulted in a limited set of themes, those of *'adversary understanding'*, *'defensive operations'* and *'defensive planning'*. The content of the sub-themes within these themes highlighted a narrative with little reference to the detail of the specifics of the adversary's intent or potential impact, and simply included a general commentary on the nature of defensive cyber operations and planning, without reference to the adversary or ICS. This contrasts significantly with the results of the thematic analysis of the post-exercise questionnaires. Two sets of questionnaires were provided to participants, one immediately after playing SCIPS, the other at the end of the CDX. An analysis of the feedback after playing SCIPS, summarised in Section 8.5.2 and elaborated in Appendix A.3, resulted in four themes; *'adversary understanding'*, *'stakeholder priorities'*, *'defensive planning'*, and *'network understanding'*. Whilst *'adversary understanding'* and *'defensive planning'* arose in the pre-exercise questionnaire, their content was much richer in the post-SCIPS feedback, demonstrating an increased understanding of the nature of the adversary's intent, the impact of their actions, the benefits of threat intelligence, the need for pre-incident preparatory actives and an overall security architecture. The latter two facets, encompassed in the *'defensive planning'* theme are significant as SCIPS does not include a hands-on technical aspect in the game. The change in perspective arose from projection of events in the game into the real world. The new themes that emerged, those of *'stakeholder priorities'* and *'network understanding'* demonstrated further changes in the perspectives of the participants. *'Stakeholder priorities'* saw an acknowledgement of business priorities that may be superordinate to cyber security issues, and the requirement to consider how the leadership of an ICS organisation will perceive and act upon investment requirements. *'Network understanding'* highlighted the need to understand the nature of an ICS network, and the assets it contains, in order to adequately consider its defence.

This enhanced understanding of ICS and its defensive context was developed further in the post-CDX results, summarised in Section 8.5.3 and elaborated at Appendix A.5. Eight themes emerged from the results. Four focused on the nature of ICS cyber defence; *'adversary understanding'*, *'defensive operations'*, *'defensive planning'*, and *'stakeholder priorities'*, and four discussed the nature of CDX, their planning and execution; *'incident response training'*, *'exercise management'*, *'cyber range quality'*, and *'red team provision'*. *'Defensive operations'* highlighted the need for improved communications, C2, priorities and SOPs to efficiently defend against an intrusion into an ICS network, whilst *'defensive planing'* extended the theme to encompass the need for greater ICS understanding and the necessity to have triaged the critical systems and services of an ICS as an element of pre-incident planning. The themes that focused on the planning and delivery of CDX highlighted a range of issues and requirements surrounding the effectiveness of CDX as an experiential learning platform.

The nature of CDX was further discussed in the interviews undertaken during the experiments. Of the seven themes that emerged from the interviews, four focused on the characteristics of poor exercises. Much of the commentary described the shortcomings experienced by the participants, and drove the requirements for strong exercise management, a disciplined Red Team with defined RoE, a resilient cyber range on which to conduct the exercises, and the necessity to incrementally develop the complexity of the training to maximise the training benefit to participants.

The next experiment from which feedback was provided, described in Section 7.5.5, included a subset of the purposeful sample. The experiment was conducted after the CPT participated in an international exercise, described in Section 7.5.4, whose output (described in Section 8.7) highlighted the need to develop documented, repeatable SOPs for DCO. The focus of the experiment was to drive these SOPs as an output of a TTX (Section 7.5.5), which was influenced by the corporate TTX that the author participated in (described in Section 7.5.3). The results of the experiment, perhaps unsurprisingly, focused on SOPs within the *'defensive operations'* theme. This highlighted the requirement for clearly defined roles and responsibilities, along with the means to share information and maintain SA during an incident. The TTX resulted in the development of a set of SOPs that were used as the basis for subsequent CPT operations, and for the DCO MST, described in Section 7.5.7.

The DCO MST involved 36 participants, none of whom were a part of the purposeful sample. They had limited technical experience, and were to take part in a trial held by the British Army to assess the transferability of general networking skills to DCO. During the three, one-week sessions of the DCO MST, participants played SCIPS and took part in a TTX. The results of gathered from questionnaires conformed to the previously-defined thematic model, aligning to the themes of *'adversary understanding'*, *'defensive planning'*, *'network understanding'*, and *'stakeholder priorities'*. *'Adversary understanding'* repeatedly demonstrated over the three weeks that participants recognised the intent, impact, methods and capability of an adversary, and could identify their behaviours using an attack lifecycle and determine their possible courses of action as a result. The narrative of *'Defensive operations'* provided a richer commentary that aligned to the sub-themes previously identified. It described the requirements for clear communications and information flows between defined roles, each with bounded responsibilities. Specifically, it discussed SOPs and the mechanisms to maintain SA during an incident. *'Defensive planning'* articulated the need to triage the systems of a network to determine which elements required prioritised defence, and how the preparatory activities of an organisation would mitigate the impact of a targeted cyber attack. This supported the contents of the *'network understanding'* theme, that highlighted the requirement for an analysis of the network terrain to be defended, the baselining of traffic and behavioural analysis, fed by network monitoring data that is delivered in a form understood by network defence personnel.

To articulate the themes that emerged from the analysis of the feedback from the experiments described above, figure 9.1 illustrates the themes, their sub-themes, and the nature of their relationships in a class diagram.

The themes are inter-related, and together describe a holistic view of cyber defences, shaped by adversary understanding and stakeholder priorities, the use of this understanding to direct defensive posture, and the elements of effective training for incident response teams.

The emergence of this rich set of themes, given the far smaller set derived from the pre-exercise questionnaires of the initial data gathering exercise (Section 7.5.2), illustrates a far greater comprehension of the nature of DCO and incident response training. The alignment of commentary from the two separate samples demonstrates a consistency of understanding from the audiences as a result of the training provided.

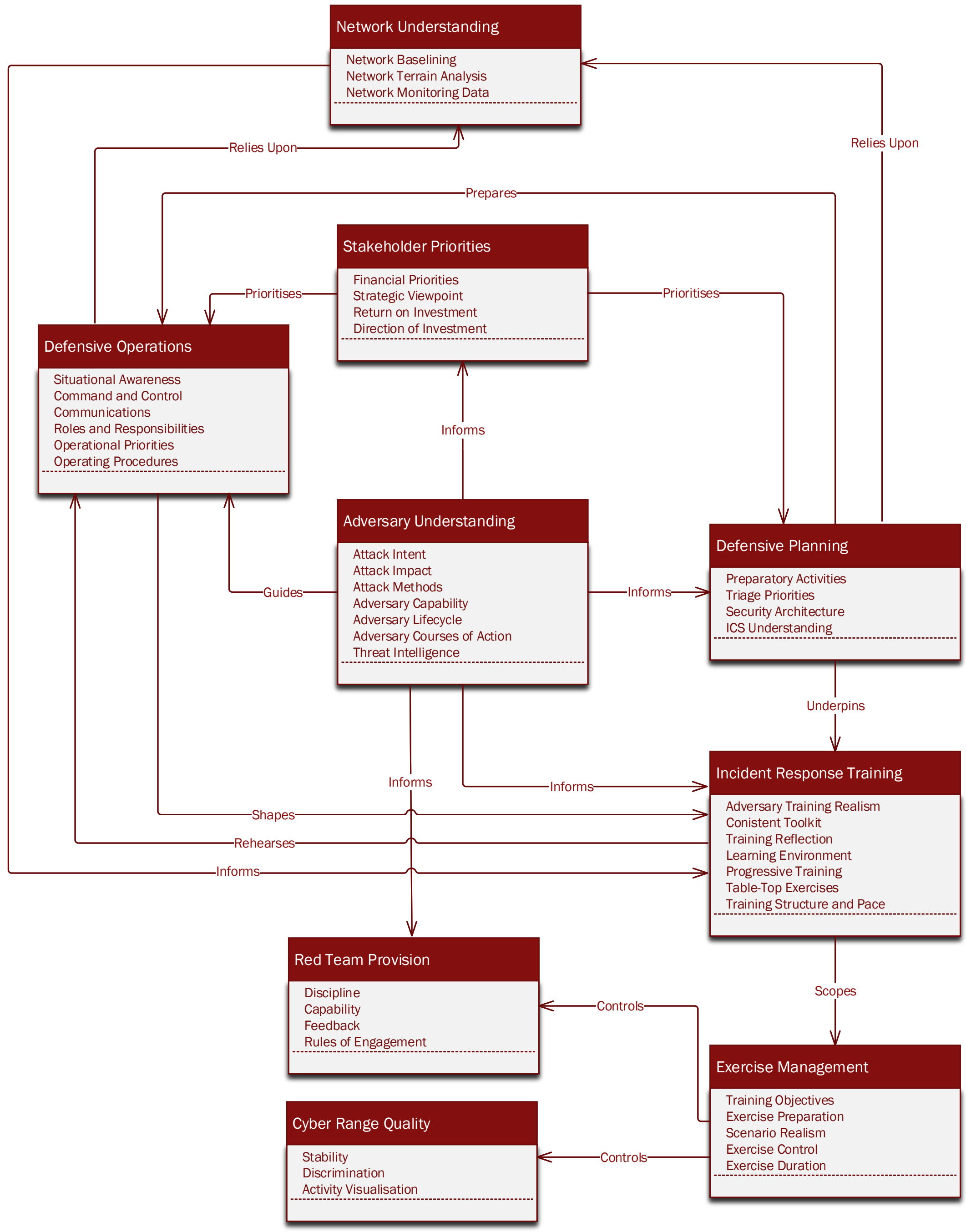


Figure 9.1: Class diagram of themes and their relationships

9.2.1 Critical Review

Whilst the themes described above suggest encouraging results, there are a number of influencing factors that must be considered before drawing conclusions. These can be summarised into three critical questions:

1. Did the questions in the questionnaires influence the respondents' answers?

2. Do the themes simply represent the structure of the training provided?
3. How generalisable are the themes?

Did the questions in the questionnaires influence the respondents' answers?

The pre-exercise questionnaire used to establish the baseline before the first full exercise (Appendix A.2) asked general questions to assess the participants perceptions of SA, the nature of the adversary, and their approach to cyber defence. In that respect, the focus of a question on the nature of the adversary likely drove the responses that folded into the subsequent *'adversary understanding'* theme. However, the sub-themes of *'attack intent'* and *'attack methods'* differentiated the nature of the responses. Similarly the question that discussed SA was likely to have influenced the development of the *'situational awareness'* sub-theme of *'defensive operations'*. The *'defensive planning'* elements that arose may possibly have been influenced by the question that asked how participants would go about cyber defence if it was under their control, although the diversity of answers does not suggest a direct correlation. Questionnaires from subsequent experiments do not use such leading language, and asked wider questions. These were not perceived to influence the answers in the same way.

It should be noted that the themes did not coalesce from the numerous candidate themes that the thematic analysis process generates until far later in the experiment schedule. Given the limited number of themes and sub-themes that arose from the initial pre-questionnaire, and the subsequent strengthening and extension of these as a result of further questionnaires, the influence of the early responses is assessed to have not overly affected the final thematic model.

Do the themes simply represent the structure of the training provided?

The themes were developed from interviews, observations and questionnaires. The interviews focused on the characteristics of past exercises, but did not ask the same questions as the questionnaires used to gather feedback from TTX and CDX particpants. The observations of the author were used as part of the triangulation process to limit biases in interpretation. The questionnaires focused on asking questions to assess the effectiveness of the training, so the answers are likely shaped by the training, but there is no evidence they are a simple representation of the structure.

There is a possible researcher bias in the generation of the themes. The immersion of the author in the series of experiments with the purposeful sample (the CPT) may had introduced a narrowed perspective. However, as Merriam and Tisdell (2015) [235] point out;

> *"Because human beings are the primary instrument of data collection and analysis in qualitative research, interpretations of reality are accessed directly through their observations and interviews. We are thus "closer" to reality*

> *than if a data collection instrument had been interjected between us and the participants."* [235].

The use of triangulation of data limits the cognitive biases of the author, and combined with the volume of data gathered, the nature of themes developed does not appear to exhibit any overt adverse influences.

How generalisable are the themes?

Qualitative research based on a limited sample potentially reduces the generalisability of results [235]. However, in the case of this research, the use of the separate sample for the final analysis (as part of the DCO MST), and the consistency of the fit of the data into the themes, suggests a wider generalisability of the results. The correlation of the themes to the mental models, discussed in the next section, further suggests a consistency with wider concepts. Empirically, the DCO themes (*'adversary understanding'*, *'stakeholder priorities'*, *'network understanding'*, *'defensive planning'*, and *'defensive operations'*) fit with established concepts within cyber security. The novelty of the progressive training methods used within this research provided a contrast for participants to the requirements for exercises that drove the themes of *'incident response training'*, *'exercise management'*, *'red team provision'*, and *'cyber range quality'*. The use of the DCO themes as a structure to assess behaviours of teams during an exercise, and of the exercise themes to assess the exercise itself, as demonstrated in Section 8.11, displays a coverage of subject matter to suggest wider generalisability of the results. Confirmation of this theory requires further work.

9.3 Mental Models

Shared mental models are essential to the performance of a team operating under conditions where time pressures, complexity of tasks, or excessive workloads limit the opportunities to develop coherent coping strategies. Such models allow teams to predict their information and team requirements and act on the basis of an understanding of the demands of the tasks at hand, allowing the team to adapt quickly in dynamic environments [149].

The models proposed in this research, described in Table 6.1, span three distinct domains:

1. The characteristics of antagonist (*APT Attack Behaviour*)
2. The nature of the cyber defence operations (*Operational Priorities, Operating Environment*)
3. The interplay between team members (*Team Understanding, Team Interaction*)

They are an extension and augmentation of the four models of ‘*Technology/Equipment*’, ‘*Job/Task*’, ‘*Team Interaction*’, and ‘*Team*’ described by Mathieu et al. (2000) [149], that in turn, were built upon the works of Converse and Cannon-Bowers (1993) [261] and Koehler and Castellan (1993) [262]. As such, there is a body of work that underpins the theoretical foundations of the models. Our assessment is therefore focused on the appropriateness and applicability of the extended model to DCO, and how the experiential learning and coping strategies proposed in this research develop these models.

As discussed in Section 3.9, the characteristics of effective performance amongst incident responders are not well understood [187]. However, several social processes and dynamics that contribute to high-performing incident response teams have been identified, summarised in Table 3.2. The ten areas proposed by Tetrick et al. (2016) in this table are cross-referenced to the five mental models proposed in this research in Table 9.1.

Ref.	**Development Areas for IR Teams**	**Shared Mental Models**
1.	Social maturity of the teams.	Team Understanding
2.	Methods of performance evaluation.	*Not addressed*
3.	Decision-making processes.	Operational Priorities, Team Interaction
4.	Communication effectiveness.	Team Interaction
5.	Information sharing.	Team Interaction
6.	Collaborative problem-solving.	Team Interaction, Team Understanding
7.	Understanding of team expertise.	Team Understanding
8.	Trust between teams.	Team Understanding
9.	Sustainable attention management and focus over time.	*Not addressed*
10.	Continuous education in incident response	*Partially addressed*

Table 9.1: Ten development areas for incident response teams, defined by Tetrick et. al (2016), mapped to shared mental models

As can be seen in Table 9.1, two of the ten development areas are not addressed in the shared mental models proposed in this research, with a further area only partially addressed. *‘Continuous education in incident response’* is an element of the progressive collective training model described in Chapter 6 and used during the experiments described in this thesis. *‘Sustainable attention management and focus over time’* and *‘methods of performance evaluation’* are beyond the scope of this research programme, and identified for further work.

The development of the shared mental models by teams in the exercise described in Section 8.11.2, and elaborated at Appendix C, demonstrated how early development of the models though the use of operational procedures and techniques for incident response teams improved overall performance. Those teams that attended and adopted the DCO MST displayed far earlier Team SA, and despite low levels of technical expertise, demonstrating that the tools and techniques of the ICS-CDTP (elements of which are included in the IPCE process described in Appendix D) provide a framework to maintain these models during situations where cognitive overload is likely. This is significant, as to date, the works of Mathieu et al. (2000) [149] and Endsley (1988-2015) [263, 147, 264, 265, 148, 266, 267, 268] have not been fused. The performances of teams who attended and adopted the DCO MST indicate that the shared mental models proposed by this research support the development of Team SA. The purposeful sample (the CPT) have demonstrated in experiments described in Sections 8.9 and 8.11 that with appropriate individual technical training, the models, supported by the ICS-CDTP, develop SA across levels 1-3.

The relevance of each of the five shared mental models is discussed in Sections 9.3.1 to 9.3.6.

9.3.1 APT Attack Behaviours

A shared knowledge of antagonistic cyber behaviours, driven by threat intelligence, allows a continual analysis of the threat landscape and recognised intrusion sets to determine the probable intent, impact, and characteristics of a targeted intrusion. The acknowledgement of such threats introduces the safeguard recommended by Kaplan and Garrick (1981) [74] that, by recognising the possibility of a hazard, it poses less risk than if we have no understanding of its potential impact. The use of SCIPS drives the strategic understanding of antagonists, HILF events, and targets the three characteristics of a cyber risk proposed by Biener et al. (2015) [17], described in Table 2.1. TTX and CDX, using the ICS-CDTP in a progressive collective training environment, iteratively develops a detailed understanding of how attacks would manifest themselves on an ICS network, and steer the development of incident response policies, procedures, and playbooks driven by a synthetically-derived understanding of APT attack behaviours. The use of synthetic environments, fused with threat intelligence, drives an increase in background information, K, and through exercising the scope of unconsidered scenarios, s_{n+1}, can be reduced.

9.3.2 Team Interaction

Shared knowledge about team interactions drives operational effectiveness. In particular, the development of Team SA and the understanding of the rate of change of information and its relationship to the dynamic nature of incident response is essential [147]. Levels 1-3 of SA, plus Team SA are developed through the progressive collective training framework described in Chapter 6, building adaptability through defined C2, roles and responsibilities, communications and information flows, using the common lexicon and tools prescribed in the ICS-CDTP (chapter 5). In particular, the TTX described in Section 8.8 illustrates how the *'Team Interaction'* model can be driven through the development of SOPs.

9.3.3 Team Understanding

Much of the understanding of a team comes from time spent working with each other, and training. The development of a strong *'Team Interaction'* model can compensate for a lack of time together if team members are allocated defined roles and responsibilities, with clear control and information flow channels between them, as observed in Section 8.11. Training is an essential element of developing team understanding. The progressive collective training framework described in Chapter 6 provides a basis for this, as demonstrated in Section 8.10.

9.3.4 Operational Priorities

The understanding of the operational priorities of an ICS operator is essential to determining which elements must maintain assured availability during a cyber attack. The ICS-CDTP provides a means to determine which systems and processes are a high priority for defence, using the output of a CARVER matrix (section 5.3.3). This supports a triaged prioritisation of where to deploy defensive mechanisms and incident response resources.

9.3.5 Operational Environment

The appreciation of the operational environment is necessary to ensure that an ICS operator understands all of the assets under its management, and determine how these may be exploited by an attacker. The ICS-CDTP addresses this specifically, as described in Section 5.3.2.

9.3.6 Relationship Between Themes and Mental Models

Many of the facts of the mental models relate to the sub-themes that emerged within the thematic analysis described in Section 9.2. The themes and mental models provide mutual support to each other; the themes describe how the mental models can be developed, and an understanding of gaps within the mental models can be used to target which areas of the themes require development within a specific training audience.

The relationship between the themes and mental models is illustrated in Figure 9.2.

9.3.7 Critical Review

The mental models proposed in this thesis are based on initial work by Mathieu et al. (2000) [149] that built on research by Converse and Cannon-Bowers (1993) [261] and Koehler and Castellan (1993) [262]. As such, there is a body of work that underpins the theoretical foundations of the models. However, we must consider the novelty and value of the findings of the experimentation.

What is the value of the extension of Mathieu et al's work?

Mathieu et al. (2000) [149] sought to examine the influence of convergence, or *'sharedness'*, of team members' mental models as related to team processes and performance by using 56 undergraduate dyads to undertake a series of low-fidelity personal-computer-based flight-combat simulations. The research focused on whether sharedness, as well as team processes and performance, developed over time. The results, whilst positive (and cited in over 2,300 articles) did not use a representative sample of participants experienced in the field of the experiments (i.e. they were not pilots) or used simulations based on a known and characterised adversary. The research in this thesis has extended Mathieu et al's models and tailored them for DCO, then tested them in a series of incident response scenarios based on real-world threats using a purposeful sample of experienced personnel to establish their appropriateness and applicability. Furthermore, the introduction of the ICS-CDTP provides mechanisms to develop the mental models in the minds of participants of SCIPS, TTX and CDX, incrementally improving the quality of the models through the use of the progressive collective training framework. The value of the extension of Mathieu et al's work is that we have defined mental models to accommodate the cyber domain and demonstrated that a focused training structure can improve the performance of experienced professionals in representative simulations.

Are the themes and models simply two views of the same concepts?

As discussed in Section 9.3.6, the themes and models are mutually supporting. Figure 9.2 demonstrates the relationships, and importantly, illustrates where the themes extend beyond the models. In that respect, the themes can be considered a further development of the aspects of the mental models. Further work is required to determine any further cohesiveness between the themes and mental models.

How generalisable are the mental models?

The research sample used for Mathieu et al's experiments [149] were, as previously discussed, not representative of the professionals who would undertake flight combat missions in real-world situations. They also used a low-fidelity simulation, with no defined relationship to recognised adversaries. The research described in this thesis, however, has used representative samples in exercises that use complex scenarios based upon real-world adversaries. In this respect, the results are broadly applicable within the cyber defence domain when considering APT attacks on ICS.

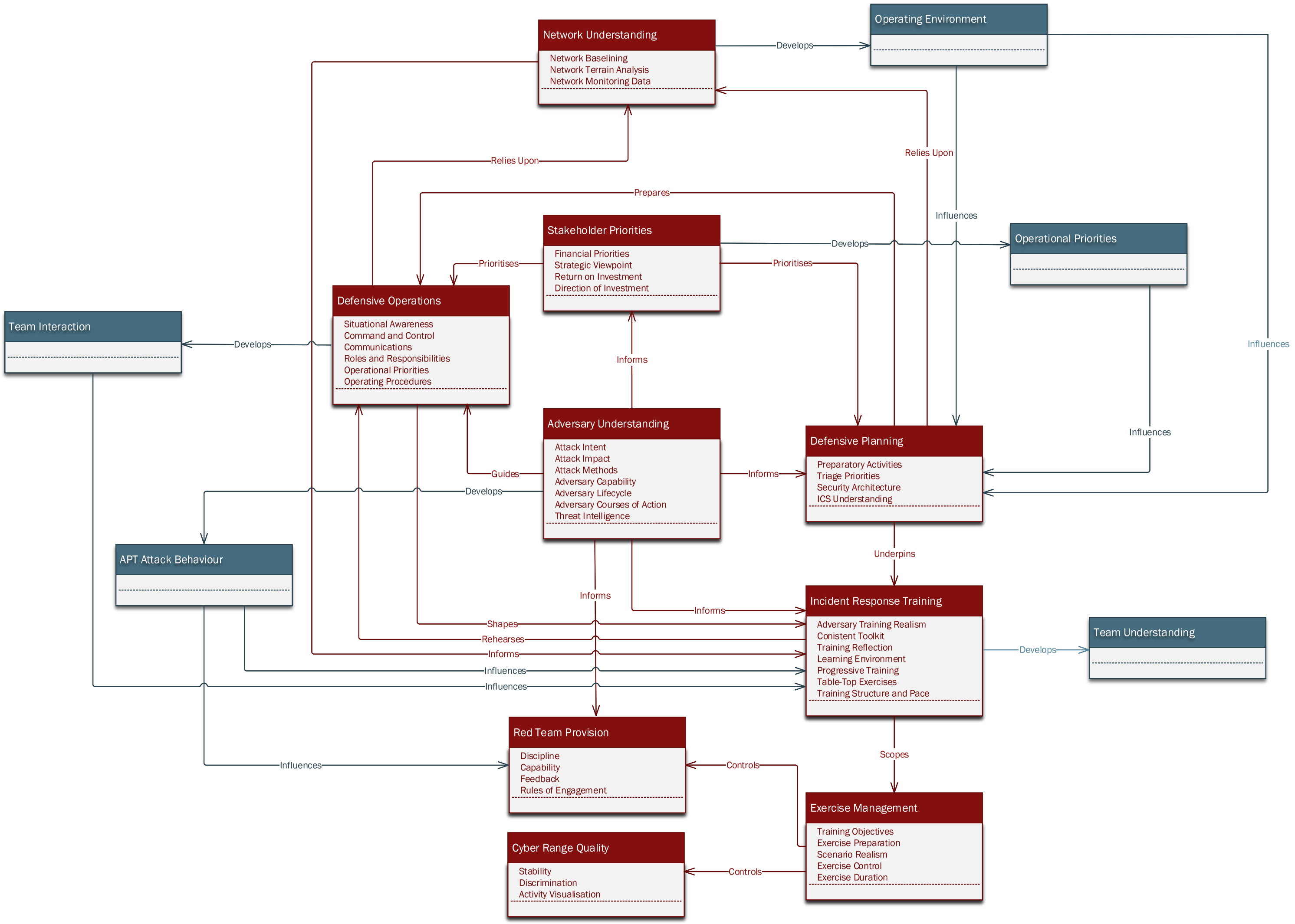


Figure 9.2: Class diagram of themes and their relationships to the mental models

9.4 Research Questions

Section 1.4 posed six questions to assess the efficacy of the models, tools and techniques proposed in this research. We shall now consider each of these in turn.

9.4.1 Which factors influence the development of mental models to provide cyber SA?

The relationships between themes and mental models highlights that it is a contextualised understanding of the real-world aspects of the adversary, ICS defences, and how these interrelate to deliver structured incident response training, that develop the mental models. This is significant, as Endsley (2000) [148] points out that SA is essentially the current state of the mental model in the context of a particular situation [148]. Therefore, the realism of a scenario can be considered the most critical aspect in the development of mental models to provide cyber SA. However, as discussed in Section 6.4, this reality must be delivered within a progressive cycle to incrementally develop mental models [152, 165, 166]. The development of mental models for cyber SA should be developed using a progressive framework of training based on realistic scenarios.

9.4.2 Does the adoption of coping strategies increase SA?

A comparative analysis of the team performances in the exercise described in Section 8.11 highlighted a difference in Team SA between teams that attended and adopted the DCO MST, and those that did not.

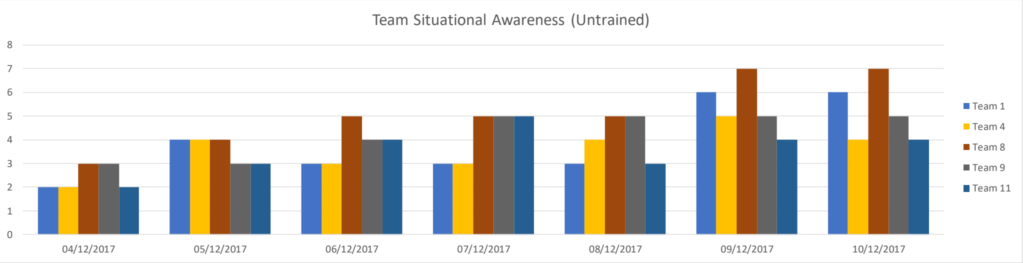


Figure 9.3: Team SA of teams that did not attend and adopt the methods taught on the DCO MST

Figure 9.3 summarises the Team SA of teams that did not attend the DCO MST. As can be seen, Team SA in the early stages of the exercise is poor. Team performances improved towards the latter stages of the exercise, but it should be noted that this coincided with a summary of the techniques taught on the DCO MST being presented to the entire exercise audience in an extra-curricular session. Subsequent adoption of these techniques resulted in an overall improvement Team SA.

By contrast, the Team SA of those that did attend and adopt the DCO MST, illustrated in Figure 9.4, achieved higher levels of Team SA from the outset. The observed drop in Team SA by Team 7, the CPT, was as a result of them not sharing their SA with the White Team. Within the team, however, their SA was consistently high.

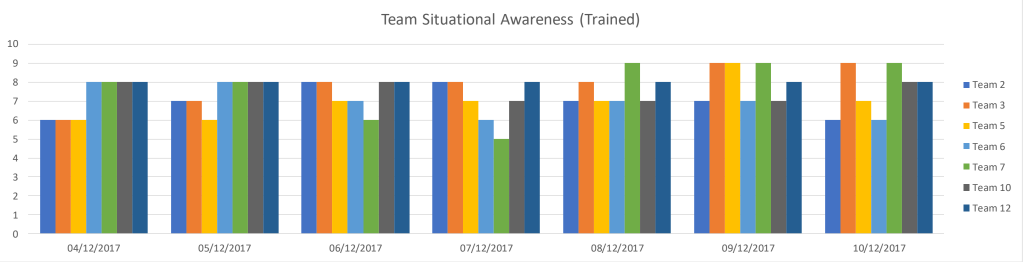


Figure 9.4: Team SA of teams that did attend and adopt the methods taught on the DCO MST

From these observations it is apparent that adopting the coping strategies of the ICS-CDTP, taught on the DCO MST, resulted in increased Team SA.

9.4.3 Can serious games change the risk perceptions of participants and establish a foundational level of SA?

The difference in strategic risk perceptions between respondents to the pre-exercise questionnaire (section 8.5.1) and post-SCIPS questionnaire (section 8.5.2) highlighted a marked change. The narrative in the *'adversary understanding'* theme shifted from an initial description of high-level, non-specific, technical threats, to strategic descriptions that focused on adversary intent and impact, and the need for intelligence to adequately maintain an understanding of the threat landscape. Similar strategic comprehension was seen in the results from the DCO MST (section 8.10).

A far richer set of themes were observed at the end of training at both experiments (sections 8.5.3 and 8.10), showing a shift in overall understanding and resultant SA as a consequence. These results demonstrate that serious games can change the risk perceptions of participants and establish a foundational level of SA.

9.4.4 How can we increase the efficacy of the serious games to deliver the change in risk perceptions?

Section 3.6.4 discusses the characteristics of effective serious games, and in particular the requirement for games to have *agency*; the ability to influence the situation through meaningful decision-making and coping strategies. It further reviews experiential learning [111] as an educational technique that proposes that active engagement in a realistic scenario develops personal experiences that form the basis of understanding. Subsequent iterations of game experiences, followed by periods of reflection, promotes the formation of ideas, with the testing of these ideas solidifying the understanding in the mind of the participant [110]. This cycle is illustrated in Figure 3.3. This cycle should include the opportunity to experience failure, as during a serious game, most of the learning occurs during debriefing, when participants have the opportunity to reflect on their experiences, allowing them to develop the mental models of the situation, against which they could refine their understanding.

SCIPS exhibits the characteristics of an effective serious game, as well as addressing the seven aspects of cyber SA defined by Barford (2010) [21] (illustrated in Table 4.5), and the three characteristics of a cyber risk proposed by Biener et al. (2015) [17], as portrayed in Table 2.1.

The results discussed in Section 9.4.3 above, suggests that SCIPS, as a serious game, is effective at changing risk perceptions. Similarly, the feedback following the CDX described in Section 8.5.3 suggests that the realism of the exercise scenarios, using a progressive crawl-walk-run approach to the execution of the exercise, with sufficient time allocated for reflection to allow the formation of ideas for subsequent testing, significantly increases the effectiveness of serious games.

The structure of the progressive collective training framework, using SCIPS, TTX and CDX, demonstrates significant, tangible results, increasing the effectiveness of standalone training packages.

9.4.5 As a result of serious games, can participants recognise the characteristics of a cyber attack and determine the possible intent and courses of action?

SCIPS has been used to present an end-to-end cyber attack within a serious game. The evolution of the game to include periods of reflection based on adversary models and the Purdue Model anchors the development of the *'APT Attack Behaviour'* mental model, based on the assessed relationship between *'APT Attack Behaviour'* model and the *'Adversary Understanding'* theme. It was observed at the CDX described in Section 7.5.8 that those who attended and adopted the DCO MST were aware of the characteristics of an attack, mapped these characteristics to adversary lifecycle models and projected courses of action. Based on the triage processes of the ICS-CDTP, and the identification of the key network terrain, these same teams were able to assess the likely intent of the attackers.

Similarly, at the CDX described in Section 7.5.6, the members of the CPT that had played SCIPS and used the same scenario on a TTX (section 7.5.5), were able to develop detailed SOPs that formalised the assessment of the network terrain, identify intrusion events, and work to forecast and future courses of action.

The results from the experiments described in Sections 8.9 and 8.11 demonstrate improved Level 2 and 3 SA, indicating the mix of didactic and experiential learning aspects of the serious games used in this research support the development of recognition of characteristics of a cyber attack, and the derivation of intent and future courses of action.

9.4.6 Are participants of serious games able to assess the immediate and longer-term impacts of cyber attacks?

The observed increases of Level 2 and Level 3 SA in experimentation results, particularly those described in Sections 8.9 and 8.11, demonstrate that participants of the serious games used in this research were able to assess the immediate and longer-term impacts of cyber attacks. Much of the understanding that underpinned this capability was derived through the use of the CARVER matrix, Diamond Model, and adversary lifecycle techniques structured within the ICS-CDTP. The experiential learning aspects of the SCIPS, TTX and CDX facilitated the development of the mental models that allowed this understanding to be exploited.

9.5 Effectiveness of the Experiments as an Experiential Learning Platform

Feedback from the research samples, acquired through questionnaires and interviews, and combined with observations of behaviour and performance on TTX and CDX, indicates that the requirements defined in the proposed framework provide a comprehensive structure in which to develop progressive collective training exercises. Whilst research exists that suggests that crawl-walk-run training may occur out of sequence [151], the evidence compiled within this evaluation of the framework indicates that adherence to crawl-walk-run through sequential collective training levels 1 to 5, across TTX and CDX, provides maximum training value. Furthermore, the data highlight how TTX provide advantages in developing SA using the mental models of *'operational priorities'*, *'team interaction'*, and *'team understanding'*. CDX, on the other hand, provide strong support for the development of *'operating environment'* and *'APT attack behaviour'* mental models.

The samples used for the experimentation in this research were IT professionals in the process of transitioning to the cyber domain. As such, the experimentation allowed the real-world impact of the training and experiential learning techniques to be assessed. The observations of the CPT at the CDX described in Section 8.4, drove the establishment of a baseline understanding of the team's mental models, and identified the subsequent areas for improvement that framed the experimentation programme. The use of SCIPS and the integration of its scenario into a novel CDX, described in Section 7.5.2, drove the addition of the role of Blue Terrain Manager (BTM) to the CPT's organisational structure, to coordinate all network terrain analysis and defensive activities, based on an understanding of the adversary. The TTX described in Sections 7.5.3 and 7.5.5 drove the development of new operational processes to drive efficient and effective incident response. In particular, the adoption of a new SA Manager role (section 8.8) established the maintenance of SA as critical to effective cyber incident management. This led to the definition of a prioritised approach to data ingest in the early stages of an incident (section 8.9), targeted to drive team efficiencies and increased understanding. Ultimately, the performance of the CPT and the teams that attended and adopted the DCO MST at the CDX described in Section 7.5.8 demonstrated the effectiveness of experiential learning as an educational platform.

On the basis of these results, it is assessed that the experiments demonstrated that experiential learning is an effective educational platform for cyber security.

9.6 Limitations of Research

The logistics of coordinating the large numbers of personnel required for the experiments described in this thesis, along with the complexity of maintaining a cyber range for CDX, limited the experimental window of this research to a one-year period. Availability of personnel and equipment could not be guaranteed outside of this timeframe. As such, the results are limited to a restricted sample. Whilst the final experiments were framed to assess the validity of the previous results, the repeatability cannot be demonstrated. Therefore, the results are restricted to a military sample within a defined training cycle.

9.7 Comparison to Related Work

The literature review in Chapter 3 cited many works that influenced the scope of this thesis. The following sections discuss the alignment of the results of this research to those publications most closely related.

9.7.1 Risk Assessment

The paucity of a qualified dataset to support probabilistic risk models is not solved by this research. Through the use of the ICS-CDTP and the application of threat intelligence, however, an individual ICS operator can assess the *Intent* and *Capability* of an adversary to inform Lewis's (2014) model [76] that proposes that *Threat=Intent* x *Capability*. Similarly, the ICS-CDTP supports the NRC model [79] that incorporates threat T, vulnerabilities V, and capabilities C, as factors of risk $Risk=f(T,V,C)$, if threat can be treated at the output of the CARVER matrix. The use of synthetic environments aligns with Sommestad and Hallberg's (2012) [106] view that cyber security exercises, conducted on dedicated infrastructure, can generate valuable data for security research. This has been extended to focus on ICS to provide data for an ICS operator model to include in their risk models. In particular, this includes the consideration of background knowledge, K, and what evidence exists for Kaplan and Garrick's (1981) [74] unconsidered scenarios of type s_{n+1}. The research is complementary with Sommestad and Ekstedt (2009) [103] who combined attack trees [88] with Bayesian methods [78] and expert assessment, but did not consider the industrial processes under control or their safety characteristics. In particular, the use of the Purdue Model [35] allows an industrial enterprise to be assessed, rather than solely the OT. This permits the perceived limitations of IT security mechanisms in ICS to be viewed holistically, to provide a mechanism to address the concerns raised by Sommestad et al. (2010) [29], illustrated in Figure 3.1.

9.7.2 Mental Models and Team Performance

This research extends the shared mental models proposed by Mathieu et al. (2000) [149] and the characteristics of high performing teams reviewed by Mathieu et al. (2008) [153] into the cyber domain, to demonstrate their effectiveness in incident response. This is aligned with the development areas for incident response teams proposed by Tetrick et al. (2016) [187]. In particular, this research demonstrates how incident response teams can develop targeted mental models and organisational structures through experiential learning, to accelerate their pre-incident planning and response capabilities.

9.7.3 Situational Awareness

Endsley's work in SA, from 1988 to 2015, is extensive [263, 264, 147, 265, 148, 266, 267, 268] and forms the basis of the SA elements of this research. Endsley's work is extended in this thesis through the application of techniques to drive the prerequisites of ICS network understanding and threat analysis, described in the ICS-CDTP, and the adoption of the crawl-walk-run approach [152, 165, 166] within the progressive collective training framework. It is further extended through the integration of Barford et al. (2010) [21] seven aspects of cyber SA and Biener et al. (2015) [17] characteristics of a cyber risk.

9.7.4 Serious Games

The SCIPS serious game is complementary to both Cyber CIEGE and Tracer FIRE. CyberCIEGE [269, 270, 271, 272], whilst effective, does not provide scenarios based upon real-world, capable threat actors following an established network intrusion methodology. Tracer FIRE [136] focuses on the forensic aspects of a cyber attack. Neither of the games include ICS in their scope. SCIPS provides an end-to-end attack on an ICS operator from an APT actor, following an established kill-chain.

The focus on constraining the Red Team's RoE within the novel CDX included in the progressive collective training framework developed during this research provides detail to support Brynielsson et al. (2016) [157] proposition that exercises can be used to capture data to improve attacker profiling, and provides an alternative to competitive cyber exercises [169, 170, 171, 168, 172, 173, 174, 106, 175, 136, 176, 177].

9.8 Contribution

The research described in this thesis is novel in that it combines and extends concepts found in risk assessment, intrusion detection, education and exercising, with safety and process models that are known within the operations of many ICS facilities. As such, this research:

1. Proposes a progressive collective training framework in Chapter 6 that incrementally develops the content of the five mental models defined in Section 6.3 (with analysis in Section 9.3), necessary for SA and incident response to address Question 1 - *Which factors influence the development of mental models to provide cyber situational awareness?*

2. Characterises the results of a qualitative analysis in Chapter 8 within a set of themes summarised in Section 8.12 that shapes the nature of experiential learning within a serious gaming environment, further addressing Question 1 - *Which factors influence the development of mental models to provide cyber situational awareness?*

3. Focuses on the identification and defence of critical ICS equipment from malicious manipulation in Chapter 5, with results in Chapter 8, allowing ICS operators to actively identify and attempt to thwart malicious attacks based on an incident response *'playbook'* developed from analyses of antagonistic intent, addressing Question 2 - *Does the adoption of coping strategies increase situational awareness?*

4. Delivers a serious gaming environment in Chapter 4 with experimental results described in Sections 8.5 and 8.10 that addresses Question 3 - *Can serious games change the risk perceptions of participants and establish a foundational level of situational awareness?*, Question 5 - *As a result of serious games, can participants recognise the characteristics of a cyber attack and determine the possible intent and courses of action?*, and Question 6 - *Are participants of serious games able to assess the immediate and longer-term impacts of cyber attacks?*, to allow participants to experience the simulated impact of a cyber attack on an ICS enterprise, demonstrating how it can strategically affect shareholder value, and support the development of mental models to frame wider cyber security operations.

5. Provides a framework in Chapter 6 with experimental results described in Chapter 8 that addresses Question 4 - *How can we increase the efficacy of the serious games to deliver the change in risk perceptions?*, that provides a progressive, cost-effective establishment and maintenance of situational awareness and skills proficiency through cyber range and table-top exercises that incorporate the scenarios played out in the strategic serious game environment.

6. Introduces a novel CDX structure in Section 7.5.2, with experimental results in Sections 8.5 and 8.9 to maximise training value to participants and further address

Question 4 - *How can we increase the efficacy of the serious games to deliver the change in risk perceptions?*

Chapter 10

Further Work

Contents

10.1 Introduction

This thesis has explored the use of experiential learning through serious games to progressively build a set of shared mental models that describe the nature of an adversary and establish enterprise situational awareness. This is underpinned by a set of coping strategies to identify attractive targets for advanced threat actors and assess their future courses of action.

The possible directions of research that emerge from a consideration of this thesis are divided into two categories:

1. Directly related themes
2. Broader research areas

The *directly related themes* in Section 10.2 proposes future scope to address topics that have arisen from a review of the research results and limitations. *Broader research areas* in Section 10.3 considers the potential wider perspectives of further work that arise from the techniques proposed in this thesis.

10.2 Directly Related Themes

10.2.1 Theme Generalisability

The themes described in this thesis developed as a result of the analysis of feedback from experiments, and was used to successfully assess the effectiveness of the CDX described in Section 8.11. As discussed in Section 9.6, the logistics and complexity of coordinating personnel and cyber ranges limited the number of experiments that could be realistically undertaken during this research. The results, therefore, only reflect the comprehension of the research sample. Further analysis is required to confirm the wider generalisability of the results.

10.2.2 Development Areas for Incident Response

Table 9.1 shows that three of the ten development areas for IR, as proposed by Tetrick et al. (2016) [187], are not fully addressed in the shared mental models proposed in this research. Whilst *'Continuous education in incident response'* can in some part be related to the progressive collective training framework described in Chapter 6 and used during the experiments described in this thesis, *'Sustainable attention management and focus over time'* and *'methods of performance evaluation'* were beyond the scope of this programme. Further research is required to integrate these areas within the framework.

10.2.3 ICS-CDTP Support Tooling

The use of the CARVER matrix and the Diamond Model within the ICS-CDTP, whilst demonstrated to be effective, was resource-intensive. Tools are required to support the initial development of these models, as well incorporate safety information where available, to make effective use of the data during a cyber attack.

10.3 Broader Research Areas

10.3.1 Driving Cyber Security Cultural Change Within Organisations

As discussed in Section 3.6, the majority of educational programmes within the cyber security domain have been awareness campaigns which have achieved mixed results [108, 109, 110]. In instances where training has delivered an immediate increase in understanding, it has been demonstrated that this does not necessarily reflect the long-term perspective of the audience [20]. This has an impact on peoples' adherence to organisational security policies [108].

Coventry et al. (2014) [108] analysed the factors that contributed to employees not following cyber security policies, citing poor threat perception, incorrect or incomplete mental models, and no clear link between security decisions and consequences as significant [108].

Whilst literature describes the advantages of developing appropriate mental models to support cyber security understanding [273, 274, 18] no detail of the content of the models has been observed. This thesis has demonstrated that multi-player serious games can aid in the formation and solidification of mental models in the minds of participants. This, however, requires the metal models to be well-defined and their characteristics understood.

The scope of the mental models described in this thesis has been focused on enterprise-level situational awareness to address the APT threat to ICS organisations. Future research is recommended to focus on the development of mental models to address the factors described by Coventry at al. (2014) for more general users, in a configurable serious gaming environment that is representative of the real-world situations personnel may face, describing the consequences of their actions in a game economy they are familiar with.

10.3.2 Integrating Gaming Techniques to Improve Cyber Threat Intelligence Assessment

ICS operators, and businesses more generally, face a dynamic threat landscape with evolving capabilities increasingly available to antagonists. Cyber threat intelligence analysis is a discipline that integrates established techniques with the cyber domain [275]. In a rapidly changing threat environment, intelligence analysts must analyse reported information and assess its potential impact on the networks, systems and processes they protect. Strategic intelligence assessment involves a number of stakeholders [276] and can be delayed by extended analysis and review cycles, or be assessed by analysts without a detailed knowledge of the impact of antagonistic activities. This affects either its timeliness or its accuracy.

Serious gaming can engage a community of participants to consider the possible courses of action and impact that antagonistic activities may cause. Such gaming techniques offer potential opportunities to provide a framework for stakeholders from diverse parts of an organisation to come together to assess intelligence reports and determine possible strategic impact in a reduced timeframe.

Structured game frameworks that integrate the operations of an organisation, integrated into the intelligence cycle, may offer an efficient means to consider the wider implications of threat reports. Further work in this area is recommended to determine its effectiveness.

10.3.3 Driving Architecture Improvements Through Design Red Team Methods

Techniques such as attack trees [88] model a potential antagonists progression through a network to a specified target node. The Diamond Model of Intrusion Analysis [190] proposes an extended alternative to this method that supports an analysis of competing hypotheses [277] and attacker potential courses of action. Such attackers can be represented by Red Teams in post-implementation penetration tests or cyber defence exercises, but they are rarely adopted at the design stage of an enterprise to determine how an antagonist might exploit the architecture. If used, such techniques do not form part of a formal and repeatable assessment of security design coherence in enterprise approaches such as TOGAF [278] and SABSA [279].

The ICS-CDTP, described in Section 5, proposes a triage method to consider the impact of loss or degradation of key systems and processes to an ICS operator, based on an understanding of the deployed architecture. It is feasible that similar techniques could be adopted at the design stage of an enterprise architecture to consider antagonistic courses of action directed at critical systems to drive cyber security improvements. For research in this area to be credible, the output should be a formal design stage, following a defined, repeatable process that integrates an understanding of the strategic cyber risks affecting an organisation into a threat-centric view of the architecture.

Chapter 11

Summary Conclusions

Contents

11.1 Introduction

In this, the closing chapter of the thesis, we summarise the conclusions of the research, restate the contribution, and reiterate the proposed further work that results from this analysis to date.

11.2 Summary Conclusions

In response to the research questions posed in Section 1.4, this thesis concludes that:

1. A progressive training programme that incrementally delivers realistic scenarios based on real-world threat actor characteristics is the key factor that influences the development of the mental models described in this research to provide cyber situational awareness.

2. The adoption of coping strategies that support the identification of attractive ICS targets for antagonists, and frames the development of defensive and incident response strategies that can be rehearsed prior to a cyber attack, increases enterprise situational awareness.

3. Participants of serious games that use realistic scenarios were observed to demonstrate a significant shift in risk perceptions and situational awareness, moving from initial high-level, non-specific threat commentary, to focused strategic descriptions that described adversary intent and impact, and the need for intelligence to adequately maintain an understanding of the threat landscape.

4. The efficacy of serious games is increased through providing *agency* to the participants to influence a realistic scenario through meaningful decision-making and coping strategies, underpinned by iterations of gameplay that provide periods of reflection based on imagery that solidifies acquired understanding in the minds of the participants, to promote the formation of mental models that can be subsequently tested in a crawl-walk-run model.

5. Following participation in serious games, participants have been observed to demonstrate increased situational awareness, perceiving information elements in a scenario, comprehending their consequences and likely intent, and projecting future antagonistic courses of actions that were used to shape proactive defensive activities to mitigate cyber attacks.

6. It has been demonstrated that participants of serious games, if provided with the necessary formalised coping strategies, including role definitions, communication and information flows, and operating procedures, are able to develop shared mental models and use the generalisation of this understanding to allow them to assess the immediate and longer-term impacts of adaptive cyber attacks.

11.3 Contribution

The research described in this thesis is novel in that it combines and extends concepts found in risk assessment, intrusion detection, education and exercising, with safety and process models that are known within the operations of many ICS facilities.

1. The progressive collective training framework provides an educational construct that incrementally develops the content of the five mental models necessary for situational awareness and incident response.

2. The qualitative analysis derived from the experiment results of this research characterises a set of themes that shapes the nature of experiential learning within a serious gaming environment.

3. The coping strategies described in this thesis provide a focus on the identification and defence of critical ICS equipment from malicious manipulation, allowing ICS operators to actively identify and attempt to thwart malicious attacks based on an incident response *'playbook'* developed from analyses of antagonistic intent.

4. The SCIPS serious game delivers an environment that allows participants to experience the simulated impact of a cyber attack on an ICS enterprise, demonstrating how it can strategically affect shareholder value, and support the development of mental models to frame wider cyber security operations.

5. The progressive collective training framework provides a structure for the progressive, cost-effective establishment and maintenance of situational awareness and skills proficiency through cyber range and table-top exercises that incorporate the scenarios played out in the strategic serious game environment.

6. The novel CDX format derived in this research focuses the efforts of the Red and White teams to deliver learning outcomes focused on the identified needs of the Blue Team training audience.

11.4 Further Work

This thesis, whilst delivering a coherent set of results and conclusions from the research undertaken, also highlights six areas for further analysis.

1. The themes developed from the qualitative analysis should be used to assess further cyber exercises to ascertain their wider generalisability beyond the samples used in this research.

2. Methods are required to determine how to sustain attention management and focus over time during an incident response, as well as defining methods for evaluating the performance of incident response teams beyond the themes defined in this thesis.

3. Software applications to support the use of the CARVER matrix and Diamond Model would be beneficial to reduce the intensity of resources required to develop and maintain these analytical tools.

4. Consider the promotion of cyber security cultural change by developing broader mental models to address general IT users, supported by real-world scenarios in a serious gaming environment to underpin experiential learning for participants.

5. Integrate gaming techniques to improve cyber threat intelligence assessment, providing a framework for stakeholders from diverse parts of an organisation to come together to assess intelligence reports and determine possible strategic impact in a reduced timeframe.

6. Drive cyber security improvements to enterprise architectures by introducing formal Red Team analyses of antagonistic courses of actions at the design stage to determine how an attacker might exploit the technology estate and operational processes.

Appendix A

Theme Elaboration

Contents

A.1 Introduction

This appendix elaborates on the themes developed from the experimental results described in Sections 8.5, 8.8, and 8.10 of the main body of this thesis. It provides a richer description of the themes, using further narratives from interviews and questionnaires.

A.2 Pre-Exercise Questionnaire, April 2017

Questionnaires were completed at the start of the week-long experiment at DMU in April 2017 that comprised SCIPS and a CDX. The responses established the baseline of understanding of the experiment participants. Of the 26 participants, 11 described themselves as having high technical competency, 12 as medium, with three as low. This described general technical competency and was not necessarily cyber specific. The particpants had a range of cyber exercise experiences; comprising nine participants with no prior experience of cyber exercises, seven participants with experience of one prior cyber exercise, ten participants with prior experience of more than one cyber exercise.

The pre-exercise questionnaire asked seven questions:

1. Describe your technical background.
2. Describe your experience with industrial control systems.
3. Describe your experiences of being on a Blue Team in the past, and the levels of learning achieved.
4. In your opinion, how effective have these past exercises been, and why?
5. What do you perceive as essential to maintain situational awareness in a network defence scenario, and why?
6. How would you characterise the threat and nature of a capable network attack adversary?
7. If it were under your control, what measures would you put in place to address the threat?

A total of 26 questionnaires were received. These identified three key themes; *'adversary understanding'*, *'defensive operations'*, and *'defensive planning'*.

A.2.1 Adversary Understanding

The adversary understanding theme focused on the intent of the adversary, and the attack methods employed. A total of 22 sources and 22 references were identified.

Attack Intent

This sub-theme discussed the intent of the antagonist. It was characterised by broad, general statements that focused on generic actors, as opposed to those who would specifically target ICS. Adversaries were stereotyped as:

> *"A person who is trying to gain information from an organisation for profit or malicious use. This can be gained initially through social engineering to target a weak point in an organisation"*

Attack Methods

The attack methods sub-theme concentrated on the nature of the network intrusion:

> *"An individual or group that have conducted extensive research and reconnaissance, and the ability to target very specific points of network successfully – all whilst creating minimal disturbance (to avoid detection). Leave no trace, but leave open the route for future attacks. Has the use of, and access to, high-end software/hardware and extensive knowledge of how to use it"*

> *"Able to move quietly, using existing network capabilities or configuration issues to move laterally and escalate privileges. 2. Ability to maintain persistence, using volatile memory and injection. 3. Has a defined motive – a reason to get in and be determined to stay there. 4. Can conduct reconnaissance quietly so the network boundary penetration is not discovered"*

A.2.2 Defensive Operations

This theme focused on cyber defence operations, and almost exclusively discussed the need for establishing and maintaining SA when responding to a complex incident. It cited 25 sources and 25 references.

Situational Awareness

The sub-theme of defensive operations concentrated on the establishment and maintenance of situational awareness during a network intrusion:

> *"For a Team Leader situational awareness is maintained by constantly receiving updates from the various sub-teams and integrate with intelligence and known methodologies"*

> *"Good leadership. Communication and all informed awareness. A good network monitoring tool, the ability of the team not to be drawn into one element disregarding others. A solid understanding of 'normal' network activity and quick recognition of any incidents or events that are abnormal. Without all of these things, any team would never achieve full situational awareness"*

A.2.3 Defensive Planning

The defensive planning theme focused on pre-incident activities and concentrated on two sub-themes; *'preparatory actions'* and *'security architecture'*. It was cited in 23 sources, with 23 references.

Preparatory Actions

A focus on the actions an organisation could undertake to prepare itself for a network intrusion incident:

> *"Good system hardening. SIEM/log correlation across all systems. Well-trained incident response team. Regular incident response drills and wash-ups of past incidents. Threat intelligence team in-house"*

> "Boundary protection and management. 2. Centralised logging with appropriate heuristic and manual log sifting mechanisms. 3. Full packet capture at key network points. 4. Network segmentation. 5. Restrict privileges. 6. Timely J2 feed. 7. A dynamic and empowered incident response team"

Security Architecture

The sub-theme described the elements of an overall security architecture that would improve an organisation's security posture:

> *"The basics of cyber security are the best. For example, keeping the systems patched, hardened, users trained and tested on good cyber security hygiene. Defence-in-depth: defender with the right tools and skills to keep ahead of threat actors. Most important is understanding you cannot be able to keep a persistent threat all the time, but focus on being able to detect and track the threat out of your system quickly. Reduce dwell-time (time from compromise to detection). Motto: 'Be breach ready' "*

> *"Baseline: IP and MAC mapping, open port discovery, software identification, process identification, list authorised accounts, list admin/user permissions, list authorised network shares, registry default identification. Harden: firewall passwords, firewall ports, router passwords, password policy, group permissions, tighten control of admin and server accounts, email settings, shutdown null shares, disable IPv6, disable unidentified IP addresses until checked. Monitor: firewall activity, sensor activity, authorised user activity"*

A.3 SCIPS, April 2017

The characterisation of ICS understanding from the 26 participants of the experiment was that 14 were beginners, nine were novices with very limited exposure, and only one had any significant experience in the field. Two participants chose not to answer.

A total of 26 questionnaire responses were received, answering the following eight questions:

1. Before playing that game, what was your understanding of industrial control systems did you have?
2. Before playing the game what was your understanding of the strategic issues surrounding the cyber security of industrial control systems to be a strategic issue?
3. How did the game shape your views regarding the immediate and longer-term impacts of cyber attacks, and their evolution over time?
4. What do you consider to the intent of capable actors attacking ICS?
5. How will this attack likely manifest itself?
6. What information would you need to deal with the attack?
7. How would you obtain this information?
8. If it were in your remit, what would you do to protect ICS from cyber attack?

The four themes that emerged from the questionnaire were *'Adversary Understanding'*, *'Financial Priorities'*, *'Defensive Planning'*, and *'Network Understanding'*. These themes are discussed below.

A.3.1 Adversary Understanding

This was the strongest of the themes, cited in 26 sources, and with 92 references. The theme encapsulated the participants' understanding of the APT actor represented in the SCIPS game. Five related sub-themes to the theme were apparent within the narrative, those of attack *'intent'*, *'impact'*, *'methods'*, *'lifecycle'*, and *'threat intelligence'*.

Attack Intent

Within *intent* there were two dimensions to the consideration of the attacker's intent. Firstly, there was the clear demonstration of cognisance of the strategic dimension of an attack on critical national infrastructure:

> *"To force political change through disruption of public infrastructure"*
>
> *"Ability to manipulate devices according to political or military conditions as part of a wider strategic campaign"*
>
> *"Either corporate espionage or to have a wider political impact"*

Secondly, there was an interrogative aspect of the intent consideration, where the participants reflected on why the attack was occurring:

> *"What are their objectives? Why are they attacking us? Who are they? What are they capable of?"*
>
> *"What is the attacker's goal? Service disruption or data exfiltration?"*

Attack Impact

The intent, however, was intertwined with the *impact* of the attack. Inevitably, the impact reflected the manifestation of the intent:

> *"Loss of control/view and availability of power generation/distribution systems"*
>
> *"It can have a large scale effect on population and countries' ability to function"*
>
> *"to disrupt, damage or destroy ICS which will create panic, distrust in the industry or government, as well as financial impedance"*

Attack Methods

Attack methods described the participants' understanding of the techniques employed by APT actors, and how they would behave in an intrusion on an ICS network:

> "This might involve (living off the land) using tools already available on the targeted network. Such as compromising user without creating new ones. Manipulating malicious traffic to look as normal, such as exfiltration using DNS"
>
> *" 'Silently'... over time. Target vulnerabilities"*

Attack Lifecycle

Game participants reflected on their understanding of the adversary lifecycle, and its efficacy to support the assessment of past, current, and future antagonistic courses of action:

> *"It became apparent, as the game progressed, that the best way to defend was to think where the next attack was going to be. Not just recreating previous attacks"*

> *"you can build up a hypothesis of what and where the attacker has been"*

> *"Placed the threat in a logical framework following the phases of the attack lifecycle"*

> *"Showed the process of an attack and highlighted a longer-term plan is required to maintain a level of security"*

Threat Intelligence

This discussed the exploitation of an understanding of the cyber threat landscape, and its applicability to the network being defended.

> *"Intelligence on the threat actor"*

> *"You can only be effective with the collection of relevant, accurate, and up to date information about the threat"*

> *"Participate in an ICS cyber intelligence programme in order to ensure defensive activity is driven by relevant intelligence"*

A.3.2 Network Understanding

The need to understand a network and its associated systems, as a prerequisite for cyber defence, emerged as a strong theme, with 23 sources and 57 references. The questionnaire respondents described this theme in two forms; *'network baselining'* and *'network monitoring data'*.

Network Baselining

The sub-theme focused on creating a foundational understanding of recognised assets, traffic flows, and behaviours, against which anomalies could be assessed:

> *"Network baseline and information flows. Network ingress/egress points. PLC/ICS process flows and critical points. Zone 0-5 boundaries and cross-boundary information flows"*

> *"How your ICS is configured? Normal ICS traffic. What are your vulnerabilities? How do you mitigate them? How do you detect them? What to do next?"*

> *"This attack requires a good understanding of the network, normal activities and simple/minor diversion from normal must be investigated, i.e. a single DNS query to an unusual domain"*

Network Monitoring Data

Network understanding was strongly related to supporting incident response, but the language of this sub-theme focused on the exploitation of information acquired from sensors and logs. It discussed the use of such understanding in the pre-incident planning stage, as well as during a network intrusion:

> *"From the game, I guess understanding your own network, awareness and profiling traffic is vital to dealing with any attack"*

> *"Any info relevant to the attack. What systems were affected? How were the systems attacked?"*

A.3.3 Defensive Planning

The requirement to proactively defend an ICS network, and plan ahead, emerged as a theme that encompassed both *'preparatory actions'*, and the development of a *'security architecture'*. The theme was apparent in 23 sources, with 46 references.

Preparatory Actions

Questionnaire respondents considered the need to plan ahead of a cyber incident, and ensure that appropriate plans were in place to address such a situation:

> *"demonstrated the importance of planning defences in an integrated manner, taking account of the interdependencies of control measures"*

> *"It highlighted the need to strategically plan and adopt a long term approach, as well as taking advantage of short term goals"*

> *"By the time you have to react it is already too late"*

> *"I think early planning does make a big impact on the upcoming incident. So many things we would have done in the earlier stages won't work after certain time because the enemy is already in and implementing those systems is a waste of time and money"*

Security Architecture

As many of the participants playing the game had a technical background, it is unsurprising that a consideration of security architecture was discussed as a pre-incident requirement:

> *"In an ideal world: Secure-by-design architecture"*

> *"Limit access. Separation of the network. Defence in depth"*

> *"Segment IT and OT networks"*

A.3.4 Stakeholder Priorities

The priorities of the leadership within an organisation emerged as a theme, with three sub-themes; *'financial constraints'*, *'return on investment'*, and *'direction of investment'*. The subject was observed in 14 sources, with 22 references.

Financial Constraints

Participants recognised, many for the first time, the financial constraints imposed by the necessity to maintain a viable, profitable business, and the limits this places on cyber security investment:

> *"had not deeply considered financial balancing act required of executives"*

> *"Increased awareness of budget constraints to directors"*

> *"Didn't realise how much of an impact the cost of implementing security defence had on an organisation"*

Return on Investment

In a similar vein, participants started to acknowledge the requirement to demonstrate a return on security investments:

> *"Assess the risk in order to identify the best return on investment for money spent"*

> *"Consider how long each prevention technique will take to deploy and what might be the financial impact on the company"*

Direction of Investment

Some participants acknowledged the value of using adversary understanding to direct investment to mitigate the threats of cyber attack:

> *"Utilising expertise and investing in the right places"*

> *"Spend wisely. Try to predict the worst attack and find a solution for it. Find the vulnerability in the system and think from the attacker's point of view"*

A.4 DMU Range Interviews, April 2017

A series of eight interviews were conducted with seven individuals, all of whom had previous CDX experience. The interviews highlighted seven themes:

1. *'Incident response training'*
2. *'Exercise management'*
3. *'Red team provision'*
4. *'Defensive operations'*
5. *'Threat intelligence'*
6. *'Cyber range quality'*
7. *'Network understanding'*

Throughout this section, the names of the exercises that the interviewees have been obfuscated. This does not detract from the accuracy or understanding of the commentary.

A.4.1 Incident Response Training

The theme of incident response training emerged as the strongest theme from the interviews, with five sources and 69 references. It encompassed the need for *'adversary training realism'*, a *'consistent toolkit'*, time for *'feedback and reflection'*, the need for the provision of a suitable *'learning environment'*, the advantages of *'progressive training'*, and the use of *'table-top exercises'*.

Adversary Training Realism

Interviewees discussed the requirement for adversary understanding to translate into a realistic adversary that incident responders could train against:

> *"We don't really train according to individual adversaries"*
>
> *"we'll go on an exercise and maybe it's a case of them starting off with hacktivists then evolves into an APT in that classic way that is always kind of predictable, rather than having separate training periods where you discuss a threat from X adversary"*
>
> *"or if you had to defend against a particular adversary, what would your priorities be etc?"*

Consistent Toolkit

This sub-theme focused on the need to train as the team would respond in real life, and the requirement to use the tools that they would have access to should an incident occur:

> *"for example, have Cisco firewalls – we never train with Cisco firewalls..., so it's usually PFSense or Vyatta on exercises. So people are tested on different tools to those we need in the real world, and it also increases the number of tools people have to learn, and we already have overload on that"*
>
> *"We got told to take our sensor array, which was based on SourceFire, Endace and Splunk. We turned up three days into the exercise, connected to a network which was already compromised – badly compromised – and then had to try and engineer-in an enterprise solution for a sensor array"*

Training Reflection

Interviewees commented on the requirement for time to reflect on the events that have unfolded within an exercise, to make sense of them, and adjust their behaviours as a consequence:

> *" It gives us an opportunity to go back and look at things like the logs and see when that happened, what it looked like on the sensor. So then, from a sensor perspective, see what it looked like if it happens again, potentially write signatures for it, and stuff like that. And then also, from a Harden perspective, what can we do to remediate against it should they come in? What can we do to remediate to stop that data from being exfilled? What can we put on the firewall, what can we do on the server?"*

> *"having that time to have a brief think in-between the stages of an attack and how you'd defend each stage of that, has been the best learning experience. Especially down a stream where we're not given formal training, so it gives us time to think, maybe do a bit of research in-between the stages"*

Learning Environment

The interviewees commented on the learning environment at DMU, and drew comparisons to previous exercises:

> *"Whereas what we're doing here is conducive to learning, no-one feels individually at threat"*

> *"This is probably very pink and fluffy, but I just wrote down on a piece of paper this morning, part of the value of being here, in civvies, in an environment which is comfortable and conducive to learning"*

> *"I do think you could significantly improve individual's abilities by putting them in a more academic environment; a non-adversarial, mentored environment"*

Progressive Training

The sub-theme of incident response training discussed the need for a programme that included individual training that develops skills through a series of progressively complex scenarios:

> *"I don't think skills is a massive thing. I mean keyboard skills can be taught. The fundamental thing in anything within the cyber domain would be the inquisitive and analytical thinking aspect. More the mental aspects. You could have someone who'd sit and look at a computer screen and look at a Squil output on a Security Onion, for example, and something would flag up and go'that looks bad', and then move onto the next. Then you could have the person that we want, that looks at it and goes 'that doesn't look right, there something about that that I'm not happy with, right, I'm going to look into that, why is this machine talking to that machine?' It's that inquisitive, deep analytical thinking over the base computer skills that, I think, can be taught"*

> *"In an ideal world we would have a persistent range where we could train as individuals, so that by the time you get to a high-level exercise you're not worrying about simple things like the syntax for specific commands, you'd have learnt that in your individual training. But we're kludging all that into one opportunity to be on a range"*

> *"So, in general terms, we have been doing CT1 through to CT5 [collective training levels 1 to 5] in one exercise, so we never get to train as individuals or as a team before [the exercise]. We tend to be doing our individual and team training on a CT4 or CT5 level exercise , so either an international or national exercise, where it's high tempo. Even if you're not being formally validated, there's an understanding that it's a test, and that it's a reflection on the capability or readiness of the team and the individual, which is not ideal because we've not had prior opportunity to iron-out any issues, or even to rehearse or exercise basic things"*

> *"The CT1 all the way up to CT5 methodology still works really well; you train as an individual, your individual skills, but then you do it in your small teams, and then you add that together. Consequently it builds up towards your big validation exercises"*

Table-Top Exercises

In discussing options for incident response training, the applicability of table-top exercises emerged:

> *"I think we could get a huge amount of value out of just table-topping and just taking away all that technical expense issue and just discussing, verbally, how you would deal with issues. It forces us to think, as well. Even in this scenario today, we've got sucked straight into "are the sensors working?", it's always the engineering issues that suck up the first few days or week, or however long, of an exercise. If that was taken away and we were just speaking in theory about how you would recognise and defend against particular kinds of threats it would force us to focus on the theory, and a more rigorous approach, and we could focus on documenting those lessons and putting them into our SOPs, rather than always just going on an exercise and just fighting through, and just trying to keep our heads above water, and then breathing a sigh of relief and going home"*

A.4.2 Exercise Management

All of the interviewees had experience of previous cyber exercises and reflected on the issues they had encountered on these. The resultant theme had five sources, with 63 references. It comprised four sub-themes; *'objectives'*, *'preparation'*, *'realism'*, and *'control'*.

Training Objectives

The subject of exercise objectives was highlighted, as the interviewees had experience unclear objectives in the past, with confusion over the training audience. This led to the perception that Blue Teams were never going to be put in a position where they could adequately defend against Red Teams:

> *"Initially it was quite a hard concept to get used to because on my first one I didn't get that Blue Team's set-up to lose. The network boys always find that the network infrastructure that you're given to defend is always inherently weak"*

> *"I think there's quite often a perception that if you give too much intelligence away, that's helping the Blue Team too much"*

> *"I think there's different types of exercise here. I think with some of the training you genuinely want a bit of Red versus Blue, where Red are following their defined path and you are defending against it"*

> *"So you're put into that environment, yes, the attacks are escalating, but if you're not training toward a defined objective, how do you get there?"*

Exercise Preparation

The *exercise preparation* sub-theme is closely associated with the *consistent toolkit* sub-theme of the *incident response training* theme. Interviewees cited how the preparation of exercises had not considered the requirement for the Blue Team to baseline the network they were defending, or supply the tools necessary for their objectives:

> *"So [EXERCISE] was a case of we turned up about four or five days into it, because of other training commitments, so there was no identify phase – there was not an opportunity to baseline the network, to identify what should be talking to what, and when we asked, that information wasn't there. They didn't know. And yes, there's a degree of that in reality, but not to the point at which that they did it on that exercise. So you can't defend that, because you don't know what you control, you don't know what's there, and then the attacks were just coming in"*

> *"Other exercise points; probably another point would be admin stuff leading up to deploying – there's either not enough information, or we get information too late to act on it. For example, [EXERCISE], it's probably unavoidable because it's international so we're at the behest of our [INTERNATIONAL] partners' decisions, but not only do we not often get to choose and deploy our own tools, we don't even know what tools we're going to have until we get there"*

Exercise Realism

For cyber exercises to be of benefit to incident responders, the interviewees commented on the need for realism in terms of scenario. This included a discussion of which aspects of a network they would realistically be able to change during an incident response:

> *"Not just a broad brush scenario, but a detailed J2 [intelligence] picture. Quite often what we come up against is people thinking that an intelligence picture means just a broad brush scenario, 'oh, you're in whatever country doing whatever thing', what they don't understand is that the J2 picture includes all the technical intelligence"*

> *"So there's always been that unrealistic aspect where we've had to make all these network changes, and engage with these people, that either don't exist in reality or would not give you permission in reality. So it makes you wonder what the point is, because what would you do in the real world?"*

Exercise Control

The control of the exercise by the White Cell emerged as a strong sub-theme, with interviewees highlighting the need for strong management of the exercise to deliver the training objectives:

> *"those skills are deployed during the exercise in a controlled manner, and in a manner that is consistent with the training needs, and with the overall scenario"*

> *"there's a lack of a management layer that understands both the requirements of the training serials and the Blue Teams, the training audience, and has enough knowledge of Red Team activity that they can actually control it"*

> *"There was also a conflict between the Red and Blue teams, in that, who was the training audience? You can't have Red and Blue training at equal pace, because as soon as one gains an advantage over the other, where does that go? The Red Team, by definition, need to get in, but it may take months, well you can't run it - so you need to condense it. So that involves some sort of shortcut somewhere. Well that then steps against the Blue doesn't it? And so it doesn't work, and they were quite naive in thinking that it would all work harmoniously, and that Blue would be able to kick them out, and Red would have to get in again"*

A.4.3 Red Team Provision

The provision of a Red Team for cyber exercises, and their rules of engagement, was an emotive issue for the interviewees. The theme encompassed the *'discipline'* of the

Red Team, their *‘capability’*, and the nature of how they provide *‘feedback’* to the Blue Team. It was cited in four sources, with 33 references.

Red Team Discipline

The sub-theme of Red Team discipline encompassed both the positive and negative aspects of Red Team behaviour, and the requirement for them to play within agreed rules of engagement.

On the positive side, interviewees commented on:

> *“Red Team activity was scripted to match the intelligence function, which means that training audience getting realistic, managed serials”*

> *“Because there was a lot of build-up, we were still quite a new team, that the training objectives that were written were very clear, the attacks were all pre-planned, and at the end of every day there was a shotval [evaluation and reflection period] with the Red Team”*

> “But at least those exercises were controlled from the perspective of the Red Team, in that there was an OPFOR, and they were doing defined things in order to meet a certain scenario”

However, on the negative side, interviewees cited the following experiences:

> *“The Red Team weren’t managed very well, I don’t think. They were almost allowed to go rogue”*

> *“Because there was no-one reigning them in, they weren’t staying within their arcs [agreed limits of responsibility], and were doing things they really shouldn’t be doing. Because there was no control of the Red Team that then meant that they were able to go and do it. Not so much the guy sat at the keyboard’s fault, there was no overarching layer of control to reign people in”*

> *“They lost control of the Red Team pretty early on, and I couldn’t understand why they allowed that to happen. That’s a command and control thing. So they couldn’t control what they were doing, there was no pre-scripted methodology, there were no defined objectives, and there were no hard lines either. There was no ‘once you get on the DC don’t destroy it, but do this to indicate you own it’. There were so many things they could do, but what they were doing was destroying everything, and then, ’oh no, that takes eight hours to rebuild it’ ”*

Red Team Capability

This sub-theme encompassed the capabilities of a Red Team, including their availability, skillset, and agreed attack playbooks:

> *"It would have been helpful to have a persistent OPFOR, or a persistent set of SOPs that applies to OPFOR, which means that there is a catalogue of skillsets for Red Teams, and we can call upon that in a consistent manner, and say that for this exercise we want a Red Team that can do X, Y and Z skills to X, Y and Z level, and then those skills are deployed during the exercise in a controlled manner, and in a manner that is consistent with the training needs, and with the overall scenario"*

> *"At the moment, if we do that ourselves, and we tried it, it's very much 'script kiddy' because we don't concentrate on the same sort of skills. People say 'you're Blue Team you can do Red Team' – I disagree entirely. It's a completely different point of view, I think, in the way you look at your network. A different set of skills really. It absolutely is. I want good network engineers, whereas a good pen tester doesn't actually have to be a good engineer himself. He just needs to know how he can exploit stuff and understand more coding and underlying structures rather than understanding what he needs to make the service work"*

> *"Also, the threat that comes against us is properly defined against real world stuff, so it's not this uncontrolled Red Team penetration-test type stuff, where just because it's possible from one aspect, it doesn't mean is actually going to be deployed. The Americans are quite good at that in the way they get into character for that piece, even down to little fragments of the code modified to make it look like a state actor, and we've not had that level of detail in the UK"*

Red Team Feedback

Interviewees discussed the requirement for the Red Team to provide feedback to the Blue Team, so that the Blue Team had the opportunity to learn from their experiences. In particular, the comments focused on the need for a *shotval*, a military term that describes a period evaluation and reflection period delivered immediately after the end of a day's play on the exercise range. They also commented on the benefit of *Purple Teaming* (a combination of Red and Blue), where the Red Team actually demonstrates their attacks to the Blue Team as part of the feedback process:

> *"We didn't have any shotval wash-up with the Red Team players, so it almost felt like we were sailing into the wind. We didn't know where we were going"*

> *"Because there was a lot of build-up, we were still quite a new team, that the training objectives that were written were very clear, the attacks were all pre-planned, and at the end of every day there was a shotval with the Red Team. That enabled us to see where our strengths were, but also where our weaknesses were, so where we missed things like data being exfilled, but actually we'd spotted reverse-shells and blocked those and caused the Red Team to re-engage another route into the network"*

> *"It enabled us to see, almost to ratify, what we'd done. So the way it worked was we broke down into our individual teams and explained what we saw, what we though happened, how we think something had manifested, and our immediate actions, and then the Red Team would basically talk about what they did, what we'd actually spotted, what we'd blocked. It was almost like having a marking guide there at the end of an exam. Your being put to the test, at the end of the day, and then to not know how well you've done on that test is, well, you've never walked out of an exam and not known whether you'll get the answers at some point"*

> *"But there's also a really good place for the Purple Teaming where the Red Team show you how they do stuff, because their job is to get through with penetration tests, but the way they see the network and the way we see it is very different, and so understanding that just because they've done a certain action doesn't mean we'll see it without looking for it, and the way that could be presented is in an event log, or a single stream of data within a packet capture, that you wouldn't necessarily think of"*

A.4.4 Defensive Operations

The defensive operations theme encapsulated the *'roles and responsibilities'*, *'communications'*, and *'situational awareness'* of the incident response team. It was cited in four sources, with 16 references.

Communications

The ability to maintain effective communications during a network intrusion, where there are multiple concurrent defensive activities in progress, was seen as essential. Interviewees discussed the need for such interaction:

> *"Something we found quite useful in terms of maintaining situational awareness for the whole team outside this [the DMU April 2017 exercise] was having a collaborative chat group within our team, so we'd have our own collaborative working space essentially, which we could use so that any conversations we were having even internally within our own sub-team, as opposed to having them sat immediately next to you, you'd actually type all*

> *that information up – specific things such as IPs, and what you though was occurring, so you'd end up having a log. But also, anyone else in the team who might have been out of the room for five minutes, or notable to listen in, would be able to visibly see that. In that regard, not only would you be able to speak to people, but there would be a log"*

Roles and Responsibilities

Another opinion that emerged was the need for clearly defined roles and responsibilities within an incident response team, and the requirement for effective leadership:

> *"Slimming is down to one word, it's 'leadership'. The breakout of that is by having defined roles in the team, and equally even in small teams of 10 individuals or so, having a defined team leader (TL), but also sub-team leaders, and in front of them, analysts, when something of interest is found that should be immediately flagged-up to the sub-team leader, and in turn, the team leader if it's deemed to be interesting. And the TL probably having an overarching view of that, possibly assisted by a watchkeeper who helps him mark his own homework and keep a record of what's going on"*

Situational Awareness

Underpinning the whole of the Defensive Operations theme was the requirement for situational awareness, and how this was maintained. It included not only the techniques to maintain situational awareness, but also how the layout of the room used by the incident response team affects such cognisance:

> *"Another very useful thing to do is every hour or two, force everyone to have hands-off keyboard and the TL or watchkeeper if necessary, would point at individual respective teams and they would brief quickly what below was going on. Very often we would find that two teams that were working in the same room, suddenly someone would join the dots all of a sudden and realise that actually they were working on the same thing. Arguably, every hour or so, just that five minutes to chance have a chat rather than people going down a certain, specific tasking can be very useful"*

> *"You don't need to overload the team with unnecessary information because there's always going to be a wealth. If you're having an 'around the table' every hour or so, each speaker is giving to the rest of the team exactly what they need to know"*

> *"Not only do we need to maintain our own situational awareness, but we can help others. In that regard, actually having integrated threat intelligence*

> *personnel on the team is very useful, as opposed to just not quite so qualified customers who can potentially ingest that intelligence to a degree, although I would argue less effectively than actually being able to produce it. So actually having credible threat intelligence analysts who can actually look at the work our team is doing, understand out of all the vast array of network activity and information you have, what specific elements will actually be useful to other teams and other members"*

> *"So what we find is there's a couple of factors that will affect how information passes around the team and overall situation awareness. The first one is where everyone's sitting. So if you look at [INTERNATIONAL EXERCISE], everyone will sit facing each other in a circle [open square]. The layout of that room [the room at DMU used for the April 2017 exercise] is all these little islands, and you'll find that the people will naturally drop into the macro problem, they'll start looking at their logs, they'll work on the Splunk server, but they won't talk across each other"*

A.4.5 Adversary Understanding

Within the context of understanding the threat actors that face an organisation, the sub-theme of *'threat intelligence'* was discussed, with four sources and 17 references.

Threat Intelligence

The theme of threat intelligence described the use of threat intelligence as an element of adversary understanding to improve the effectiveness of incident response teams:

> *"Many things affect cyber situational awareness, and I supposed the overarching wording or terminology would be that 'threat intelligence' is absolutely critical to maintaining cyber situational awareness. Not just on your own network, but beyond. Essentially that's the sharing of information"*

> *"So actually having credible threat intelligence analysts who can actually look at the work our team is doing, understand out of all the vast array of network activity and information you have, what specific elements will actually be useful to other teams and other members"*

A.4.6 Cyber Range Quality

The interviews highlighted the dependency of cyber exercises on the quality of the ranges on which they they operate. The theme was cited in four sources, with 12 references. It focused on two distinct sub-themes, those of *'range stability'* and *'range discrimination'*.

Range Stability

The subject of range stability covered the reliability of the cyber range, and minimising the downtime that resulted from a lack of testing or resilience:

> *"Yes, they had some issues with reliability, which seems to a common feature of all cyber exercises. I don't know how we get rid of that"*

> *"it's always the engineering issues that suck up the first few days or week, or however long, of an exercise"*

Range Discrimination

The sub-theme of range discrimination refered to the consequences of using a heavily virtualised architecture, and the inability of the Blue Team to determine whether characteristics of the network were as a result of a network intrusion, or simply a feature of the infrastructure:

> *"the layers of the matrix that you dive into because your virtualised infrastructure and range issues, which are very difficult to get around without spending a lot of money"*

> *"I have done another exercise, and there's always going to be a 'rangeism', there's always going to be something that, you think, well that's unfair or whatever"*

A.4.7 Network Understanding

The defensive analysis theme, in this instance, focused on the *'network terrain analysis'*. It was cited in three sources, with five references.

Network Terrain Analysis

Interviewees highlighted the need to proactively assess the valuable network assets that would be attractive to an attacker:

> *"and that evolves into integrating a genuine Cyber IPE [ICS-CDTP] key terrain analysis"*

> *"Also, having a good network understanding, in terms of the vulnerabilities, the way traffic moves around the network, will help the teams who are remediating to prioritise. There might be specific points on your network that are particularly vulnerable. If you have an understanding of the potential*

> *enemy's intent as well, clearly that helps you identify which parts of the network they're more likely to be targeting, so when you're going through your remediation process in terms of mapping left and right [of the Kill-Chain] and the intent behind the hostile activity, while you might see a random IP on a random box potentially, if it seems indicative of lateral movement, logically, as opposed to trying to look across the whole network to see if they've move around, you can start triaging and prioritising in certain areas that they may be trying to move to next"*

A.5 Post-Exercise Questionnaire, April 2017

Questionnaires were completed at the end of the week-long experiment at DMU in April 2017. It comprised SCIPS and a CDX, and was participated in by the same sample who completed the pre-exercise questionnaire from Section A.2. The responses discussed the participants understanding of ICS, APT actors, and the nature of SCIPS and the CDX.

The post-exercise questionnaire posed 13 questions:

1. Describe your understanding of the key elements of the cyber threat to industrial control systems.
2. Describe your understanding of the tactics, techniques and procedures of a nation-state cyber actor intent on attacking industrial control systems.
3. Describe your role within the Blue Team, and how the behaviours of nation-state actors would influence your activities during an incident response?
4. If you were to deploy to an industrial facility to defend its network from a malicious actor, how would you prioritise the defence of its assets? How would your approach provide protection from an attack?
5. Should any aspects of your standard operating procedures be revised as a result of this exercise, and if so, how?
6. How did the use SCIPS game and the integration of the same attack scenario into the range exercise influence your training?
7. Has the constrained rules of engagement for the Red Team been of benefit you your training, and if so, how?
8. Ignoring any issue with the range, with hindsight, if you were to repeat this exercise again, how would you change your response to the scenario and the attacker?
9. Which areas of this exercise have been of value to the effectiveness of your team?
10. In which areas do you think this exercise has been of value to you personally?

11. Have you identified any training gaps as a result of this week, and if so, what are they?

12. How does this exercise compare to previous cyber exercises you have participated in?

13. How would you suggest we could improve this training programme?

A total of 25 questionnaires were received. These resulted in eight key themes; *'adversary understanding'*, *'defensive operations'*, *'defensive planning'*, *'incident response training'*, *'exercise management'*, *'cyber range quality'*, *'red team provision'*, and *'stakeholder priorities'*.

A.5.1 Adversary Understanding

The adversary understanding theme focused on the *'attack lifecycle'* and the *'attack methods'* employed. A total of 24 sources and 42 references were identified.

Attack Lifecycle

The subject of the adversary lifecycle discussed its efficacy to help predict attack behaviours:

> *"By using the cyber kill chain it will prevent and provide protection as this is how the attacker operates"*

> *"The SCIPS game followed the stages of the exercise very closely, so by understanding what technology was required for each round of the game, we could then understand where to focus our efforts during each stage of the exercise"*

> *" At the different stages of the attack once the Red Team where known to be somewhere on the network – you realise that at each stage after how the consequences would affect the next stage beyond"*

Attack Methods

The sub-theme of attack methods considered the ways and means by which an attack would be executed, and as a consequence, how this understanding would shape defensive actions:

> *"The attacker would have to have done their research and realise the consequences of what they were about to do, so if their intent was to disrupt a nation state's infrastructure, this kind of attack would make sense. If it is*

> *just a 'script-kiddie' type of hacker who was just looking at what they can find 'for kicks' they might not get as far (but may, by chance, due to poor security infrastructure with respect to cyber intelligence)"*

> *"Look for suspicious traffic in ports we cannot close or systems we cannot block e.g. port 80, 53, DMZ (web server, email server)"*

A.5.2 Defensive Operations

The theme of defensive actions was cited in 25 sources with 55 references. It concentrated on four sub-themes; *'command and control'*, *'operational priorities'*, *'communications'*, and *'operating procedures'*.

Command and Control

This focused on the impact of poor leadership during exercise, and incident response in general:

> *"Designated leadership, oftentimes when people were lost/confused/doing their own thing"*

> *"I think I would implement a central command and control team to have overall situational awareness"*

> *" Too many people shouting out identified 'threats' with only a cursory investigation into that incident having being done at that point"*

Operational Priorities

The sub-theme of operational priorities discussed how an incident response team would determine where to focus resources and effort:

> *"Prioritise defence based on commander's mission, critical assets and valuable assets, and likely enemy intent drawn from threat intelligence. Solution may not defend all, but would defend most critical assets"*

> *"Based on a discussion with the business area regarding their critical systems and services, and including the critical network and systems and hardware that support it. Then work outwards from the critical systems towards the network boundary to try and define zones of security thorough segmentation, privilege control, and protection devices"*

> *"Critical business processes would take priority"*

Communications

Questionnaire respondents commented on the need for effective communications between team members:

> *"Communicate more regularly within the different areas of the team"*

> *"Keep responses simple and record them"*

> *"better information flow and logging of activity"*

Operating Procedures

The sub-theme of the requirement for clear, detailed, SOPs to guide incident responders arose:

> *"It would be advisable to have a clear, concise 'threat analysis' SOP, something easy to follow, especially useful to new members of the team"*

> *"We have identified some particular detailed SOP points to amend/create"*

> *"SOPs evolve every time they are used. Points have been added to a number of SOPs during this exercise"*

A.5.3 Defensive Planning

Within the defensive planning theme, four sub-themes emerged; *'preparatory actions'*, *'security architecture'*, *'ICS understanding'*, and *'triage priorities'*. It was cited in 22 sources, with 23 references.

Preparatory Activities

This discussed those activities that would better prepare an organisation for a cyber attack:

> *"We would baseline our systems more thoroughly before attacks commenced"*

> *"A better baselining of assets and having a greater awareness of OS's and applications"*

> *"Patching systems. Set-up firewall logs straight away"*

Security Architecture

A description of the elements of an overall security architecture that would improve an organisation's security posture, and in particular, network segmentation:

> *"Segment the network better to make it harder to get to the ICS"*

> *"Segregate the ICS network from the IT network"*

ICS Understanding

The requirement to accurately understand the nature of ICS was highlighted as a key defensive planning requirement:

> *"There are many threats to ICS, such as external threats (politically motivated, industrial espionage etc.), internal threats (employees with an axe to grind), human error, security challenges, securing ICS networks. Most ICS were built prior to cyber threats existing and therefore not designed with built-in security controls. Goals would be operational disruption, physical damage, theft of intellectual property"*

> *"Systems are old and not everyone understands how they work, so a simple network scan can cause them to fall over. Due to availability being the most important and not all data flows being known, it is hard to implement security rules and procedures."*

> *"With many of the ICS being legacy equipment and unable to be shutdown and restarted, it brings new challenges"*

Triage Priorities

A key element of triage priorities was seen as system availability:

> *"The key element is the availability of the system. This restricts the action that Blue Team can make, providing a unique challenge"*

> *"Threat to availability is more critical for ICS than for standard computer networks. Threat actors include: nation-states, individuals, criminals, political/activist groups (all with varying levels of sophistication). Any of the above may seek to steal data, modify data or deny services from/of ICS"*

A.5.4 Incident Response Training

The theme of incident response training was cited in 16 sources and 21 references. It included the need for a *'learning environment'*, a focus on *'training structure and pace'*, time for *'feedback and reflection'*, and the advantages of *'progressive training'*.

Learning Environment

A clear sub-theme of Incident Response Training was the nature of training environment, and its conduciveness to learning:

> *"Good to work in an academic, non-military environment, as this promotes learning"*
>
> *"All areas have been of value as a lot of us are new and this is a far better way to learn than self-study or non-real-time events"*
>
> *"specific 'arcs of fire' from the Red Team really helped a structured defence strategy, and better understanding"*

Training Structure and Pace

Linked to the nature of the learning environment, the structure and pace of the training emerged as a consistent narrative:

> *"Slow pace of Red Team activity. Being told about the Red Team activity at the end of each stage"*
>
> *"The pace is much better. It allows for a greater learning environment"*
>
> *"The staged approach has allowed a better learning experience"*

Training Reflection

Experiment participants also commented on the feedback and periods of reflection across SCIPS and the CDX:

> *"The visual feedback was brilliant"*
>
> *"non-judgemental, structured learning environment. Sensible pace and regular discussions/debriefs. Collaboration with new individuals and academia enriches our knowledge and understanding"*
>
> *"it has allowed us to look at all stages of the attack cycle. It has also been helpful for improving team cohesiveness and internal information flows"*

Progressive Training

Incident response training reiterated the need for a series of progressively complex scenarios:

> "able to focus in a progressive way on each phase of the attack cycle"

> *"Knowing which phase of the attack we were about to face at each stage, as opposed to a set range window with a small scenario update each day"*

A.5.5 Exercise Management

The management of CDXs emerged as a strong theme, with 25 sources and 75 references. It encompassed *'exercise objectives'* in terms of positive outcomes, and *'exercise duration'*, with a focus on requests to extend the exercise execution window.

Exercise Duration

Exercise participants, whilst apparently enjoying the exercise, felt that greater training benefit could have been achieved if a longer exercising period was adopted:

> *"More time to develop stages and not rush"*

> *" Make it longer so we have more time to learn the range. We could come the week before to help build the range so we understand our network better"*

> *"Longer time period for all (2 weeks would be great)"*

Exercise Objectives

Participants reflected that the exercise had clear training objectives that delivered a positive learning outcome:

> *"This exercise had massive educational value as it enabled Blue Team to have an insight on how some of the Red Team activities would look like"*

> *"this was a very good exercise with much better training value. The exercise was, in my view, Blue Team focused, not just how good the Red Team is. Work and getting a better understanding of each stage of the kill chain enhanced our understanding of the required procedures in security/defending a network"*

> *"Better, as didn't just get 'smashed' by Red Team"*

A.5.6 Cyber Range Quality

Feedback from participants described issues with the range. Their comments continued the two sub-themes; *'range stability'*, *'range discrimination'*, and introduced *'activity visualisation'*. It was cited in 15 sources with 16 references.

Range Discrimination

The requirement to understand the nature of the range was reiterated:

> *"Accurate network diagram. Documented configuration"*

> *"Provide us with a network diagram, password sheets and other assorted information prior to attending so we can hit the ground running"*

Range Stability

The comments on rang stability largely referred to period of remediation on the network as a result of a power outage:

> *"ensure the range is completely working without issue, and make it longer so we can cover more training areas"*

> *"Test stability of range more prior to exercise"*

Activity Visualisation

Participants requested the ability to record and replay attack traffic, to allow review and reflection, to aid learning:

> *"watching a video of the screen so the traffic can be matched up might be useful"*

> *"Also, some sort of video replay of what the Red Team have done would be beneficial"*

A.5.7 Red Team Provision

The provision of a Red Team for cyber exercises, their *'discipline'*, frequency of *'feedback'* to the Blue Team, and their *'rules of engagement'* continued in the commentary. The theme was cited in 25 sources, with 37 references.

Red Team Discipline

Feedback from participants focused on the benefits of the discipline of the Red Team on the exercise at DMU, as compared to previous exercises they had experienced:

> *"The exercise was, in my view, Blue Team focused, not just how good the Red Team is"*

> *"Undisciplined Red Team activity (on other exercises) is not only not useful, but actually destructive"*

> *"From experience, cyber exercises seem to be a show-off of how good the Red Team is"*

Red Team Feedback

Participants considered the feedback provided by the Red Team to the Blue Team on the exercise at DMU:

> *"Each phase then concludes with feedback so Blue Team know if their actions had an effect (good or bad)"*

> *"Very good pace, very good feedback from Exercise Lead and Red Team"*

> *"The pace and explanation from the Red Team each day as to which actions they took was very useful"*

Rules of Engagement

The constrained rules of engagement for the Red Team on the DMU exercise were reflected upon by the participants:

> *"Usually the Red Team will go out of scope or advance too quickly for any benefit to be gained. The constrained rules of engagement (ROE) for the Red Team allowed us to gain more from the exercise by understanding more at each phase"*

> *"The constraint of the Red Team was the key component in slowing down the required Blue Team response. This added a level of proactiveness and learning to the activity, rather than being behind the curve and therefore the exercise becoming a purely reactive activity"*

> *"This ensured learning outcomes, rather than just a survival mentality. Splitting the exercise into discrete, identified phases enabled us to focus on understanding particular methodologies, rather than worrying about everything at once, which dilutes training value. Regular wash-ups between phases were also very useful to check understanding before moving on. This controlled exercise has given us more learning value in a week than many less-controlled scenarios over longer periods. Understanding and learning has also improved morale and motivation – the intangible factors which are too often overlooked and which have an important impact on operational effectiveness"*

A.5.8 Stakeholder Priorities

The priorities of the leadership within an organisation again emerged as a theme, this time with two sub-themes; *'financial constraints'* and *'strategic viewpoint'*. The subject was observed in 17 sources, with 17 references.

Strategic Viewpoint

Participants discussed how SCIPS, in particular, shaped their understanding of the strategic issues surrounding cyber security:

> *"The SCIPS game gave a high-level understanding of how security is viewed by COs [commanding officers] and company directors"*

> *"Good baseline for less experienced members on how cyber warfare could occur at a strategic level"*

Financial Priorities

Additionally, participants reflected on the financial constraints that they experienced playing SCIPS:

> *"It helped to see cyber security from the business owner's perspective – why they wouldn't want to spend money, make changes or increase their risk"*

A.6 Incident Response TTX, June 2017

Questionnaires were completed at the end of one-day TTX with 12 participants from the purposeful sample (CPT), that took the scenario from SCIPS and used it to frame the experiment. The intent was to assess the coverage of operating procedures within the team's defensive operations. As such, the responses focused on this theme. A post-TTX questionnaire asked five questions:

1. What is your role in the team?
2. How did the TTX influence your situational awareness and communications within the team?
3. Which of your existing processes require updating as a result of this TTX?
4. How has the TTX changed your comprehension of your team operations?
5. How will you change your individual processes as a result of this TTX?

A total of 12 questionnaires were received.

A.6.1 Defensive Operations

As the TTX focused on operating procedures, it is perhaps unsurprising that the responses focused purely on this theme. It was cited in 12 sources, with 47 references. It encompassed *'communications'*, *'information flow'*, *'roles and responsibilities'*, *'situational awareness'*, and *'operating procedures'*.

Communications

The TTX participants emphasised the need for effective communications:

> *"It has highlighted parts we take for granted that we perceive people should already be aware of – how 'things', 'tasks' are carried out. Also that we need to feed or record all events so they can be correlated for the bigger picture"*

> *"Talking through the process helps to reinforce what needs to be done, and ensures everyone knows what is happening. Communication is key!"*

> *"highlighted the fact that all teams must feed one another to fill the big picture which will allow for full team understanding"*

Information Flow

The TTX highlighted shortcomings in the informations flows around the team:

> *"my comprehension has increased, especially around the gap analysis and information flow"*

> *"Better understanding of sub-team information dependencies"*

> *"It has further solidified the importance of information flows both to and from the J2 [intelligence] cell, to inform actions for all sub-teams and to provide J2 with the information to perform some actual in-house analysis on our own data and incidents"*

Roles and Responsibilities

Questionnaire respondents highlighted an increased understanding of team roles and responsibilities at the end of the TTX:

> *"It has clarified who sits under what team and how they are likely to operate in an operational/exercise environment"*

> *"Within Hunt we have identified that on the initial 'Find and Analyse' phase it would be more effective to work with the Harden team to baseline/enumerate the network to help update/validate the IPE [ICS-CDTP] faster, so we can fully understand our environment quicker, to get on with the Hunt phase"*

> *"how the other teams link into the bigger picture and what they need to do"*

Situational Awareness

SA again emerged as a sub-theme. In particular, the CPT Team Leader and sub-team leads commented on the need to maintain SA:

> *"Has made me think a great deal more as to what the processes should be. I will need to have oversight on all areas, as well as the big picture, and ensure that communications up and down happen regularly to keep an all-informed net"*

> *"While I understand the basic needs of J2 [intelligence] to direct activity, the TTX has helped to really understand the value of J2 during the initial UNDERSTAND phase of a deployment"*

Operating Procedures

As the focus of the TTX was to drive-out the detail of the team's operating procedures, it emerged as a strong sub-theme, and resulted in the scoping of seven new standard operating procedures:

> *"Our SOPs [standard operating procedure] are massively outdated and mostly unfit for purpose -> the new seven consolidated SOPs will be much more appropriate and useful for new teams starting up"*

> *"We knew we had many SOP gaps, and many of them were documented, but this has provided a formalisation of gap analysis, and offered a structure for the leadership to use in order to prioritise future work"*

> *"Several newly identified SOP gaps. Focus more on standardisation and repeatability of processes. Regularly reassess progress in SOP/team development and demand formal acknowledgement of progress and outstanding gaps going forward. Treat situational awareness as a function with SOP in its own right, rather than as a part of other functional areas. More emphasis on developing management (OC) [officer commanding] SOPs"*

> *"Fill-in the many obvious gaps. As a new TL, I would not know my role completely by following the in-place paperwork. The SOPs need looking at, rewritten in a way that someone with limited knowledge and experience can follow"*

A.7 SCIPS - DCO MST Programme, November 2017

The experiment comprised three, one-week training sessions, with each session including playing SCIPS. Thirty-six (36) participants attended over the three weeks, whose experience was characterised as 30 with no ICS knowledge, five novices, and only one with significant ICS understanding.

A total of 36 questionnaire responses were received, answering the following eight questions:

1. Before playing that game, what was your understanding of industrial control systems did you have?
2. How did you articulate the attack activities you identified to your team?
3. How did the game shape your views regarding the immediate and longer-term impacts of cyber attacks, and their evolution over time?
4. What do you consider to the intent of capable actors attacking ICS?
5. How will this attack likely manifest itself?
6. What information would you need to deal with the attack?
7. How would you obtain this information?
8. If it were in your remit, what would you do to protect ICS from cyber attack?

Four themes emerged from the responses; *'adversary understanding'*, *'defensive planning'*, *'network understanding'*, and *'stakeholder priorities'*.

A.7.1 Adversary Understanding

This was again the strongest of the themes, cited in 35 sources, and with 118 references. The theme encapsulated the participants understanding of the APT actor represented in the SCIPS game. Seven related sub-themes to the theme were apparent within the theme, those of attack *'intent'*, *'impact'*, *'methods'*, *'lifecycle'*, *'courses of action'*, *'capability'*, and *'threat intelligence'*.

Attack Intent

The *intent* theme discussed the strategic goals of the antagonist, including how this intent may be intended to apply wider political pressure by an asymmetric adversary:

> *"Intent was to cause instability to the country via the means of power loss and media backlash"*

> *"Political coercion on the bigger scale, however, also a show of force from a below-peer potential enemy"*

> *"To disrupt UK infrastructure to apply political pressure to remove the UK from operating in the area"*

Attack Impact

The *impact* of the attack reflected the manifestation of the antagonists actions in the SCIPS game, specifically the impact on electric power generation:

> *"Physical loss of power eventually"*

> *"It made me more aware of how an attack can snowball over time"*

> *"Attack the things required to produce electricity"*

Attack Methods

Attack methods described the participants' understanding of the techniques employed by APT actors, and how they would behave in an intrusion into an ICS network. They included the initial attack vector through to lateral movement and wider impact, linking this sub-theme strongly to the adversary lifecycle:

> *"First find information about your network, find weaknesses, then expose them to penetrate deeper and gain more control"*

> *"Worked out spearphishing would be a large risk factor"*

> *"Dropping malware onto the computer and branching out using peer-to-peer connections"*

Attack Lifecycle

This sub-theme reviewed the game participants use of the adversary lifecycle and Purdue Model to assess the attacker's progress through a network:

> *"It showed the linear way in which attacks progress"*
>
> *"By traversing through the levels of the model, as well as the adversary lifecycle analysis"*
>
> *"In terms of the Purdue Model and attack chain position"*

Adversary Courses of Action

The assessment of the possible *courses of action* an adversary could pursue whilst on an ICS network is inherently linked to the use of the adversary lifecycle. However, this sub-theme emerged as a distinct element within overall adversary understanding:

> *"Trying to figure out where the attacker was and trying to plan. What to do next to prevent the attacker from damaging the network and infrastructure"*
>
> *"To plan several steps ahead to try and prevent incidents"*
>
> *"The game makes you think a lot more about what the hackers have access to currently and where they are likely to go next"*

Adversary Capability

In discussing the capability of the adversary, the experiment participants differentiated between intent and capability:

> *"The level of attacking team (previous experience, attributed attacks etc.)"*
>
> *"A full understanding of the triad of capability (skill set), intent (on network and ground effect), and ground (network)"*
>
> *"Just because they have the capability doesn't prove malicious intent"*

Threat Intelligence

This sub-theme discussed the exploitation of using intelligence to shape network defence activities.

> *"Intelligence feeds, news, social media"*
>
> "Receiving intelligence on enemy"

A.7.2 Defensive Planning

Defensive planning, in this instance, focused on *'defensive triage priorities'*, *'preparatory activities'*, and *'security architecture'*. It was observed in 32 sources, with 57 references.

Triage Priorities

The participants of the SCIPS game highlighted the need to assess the network under defence to determine the likely targets of interest to the attacker:

> *"Prioritise what is immediately needed and what can wait"*
>
> *"Prioritisation of system defences is important, but the need for immediate defence is imperative"*
>
> *"It brings to bear the meaning of prioritisation and the long-term impact of triaging based on the services that are more important in relation to the posed risks"*

Preparatory Activities

The pre-incident preparatory process emerged as a sub-theme of the defensive planning theme:

> *"Mitigation is better than reaction"*
>
> *"Understand that there are limits to what you can do and you'll probably be successful in some areas, so put procedures in place to deal with that"*

Security Architecture

Participants of the SCIPS game highlighted the need for a robust security architecture as an sub-theme of the overall defensive planning process:

> *"Ring fence our assets and capabilities with layer of security"*
>
> *"Harden external/internal borders. Segregate ICS/OT levels. Deploy robust IDS/AV. Implement effective reporting procedures"*
>
> *"Defence-in-depth"*

A.7.3 Network Understanding

Understanding the network being defended, emerged with 22 sources and 43 references. The questionnaire respondents predominately focused on *'network baselining'* and *'network monitoring data'*.

Network Baselining

This sub-theme focused on creating a foundational understanding of recognised assets, traffic flows, and behaviours, against which anomalies could be assessed:

> *"Accurate information about network and full vulnerability scan of systems"*

> *"[with] hindsight the order in which we implemented the defence was wrong. Highlighted the need for a full understanding of the network processes and functions"*

> *"Knowledge of the network would be vital"*

Network Monitoring Data

Network understanding was related to the exploitation of information acquired from sensors and logs, in the minds of the participants:

> *"You would have to monitor the networks and look for traces left behind"*

> *"Source and destinations in order to determine where they are and what box they are operating from"*

A.7.4 Stakeholder Priorities

The implications and constraints of an organisation's expenditure on cyber security emerged as a theme, with 12 sources, and 12 references in the Financial Constraints sub-theme:

Financial Constraints

> *"It gave a deeper understanding how money is a large aspect of cyber defence"*

> *"Shaped towards CEO stakeholders, and how they are impacted monetarily"*

> *"Balance of spending money due to the reflection on shares / business partners"*

A.8 TTX - DCO MST Programme, November 2017

The experiment comprised the same period as the Section A.7, with three, one-week training sessions. Each session including an incident response TTX that simulated the first three days of a major incident. Two additional participants joined the TTX after the SCIPS game had been played, increasing the overall number to 38

A total of 38 questionnaire responses were received, answering the following five questions:

1. What is your role in the team?
2. How did the TTX influence your situational awareness and communications within the team?
3. Which of your existing processes require updating as a result of this TTX?
4. How has the TTX changed your comprehension of your team operations?
5. How will you change your individual processes as a result of this TTX?

Four themes emerged from the responses; *'adversary understanding'*, *'defensive operations'*, *'network understanding'*, *'defensive planning'*.

A.8.1 Adversary Understanding

Understanding the adversary again emerged as a theme, with 13 sources and 17 references. It encompassed *'attack intent'* and *'attack lifecycle'*.

Attack Intent

Attack intent focused on considering what the antagonist was trying to achieve, rather than simply reacting to observed network activities:

> *"Focusing more on the intent rather than getting sucked into the initial findings"*

> *"developed my understanding of the importance of situational awareness and especially the need to understand the intent of the adversary"*

Attack Lifecycle

The use of adversary lifecycle modelling allowed the participants to think about the attacker's next steps:

> *"think what would the attacker do next to prevent a further attack"*

> *"Be less reactive, but predict what the adversary will do next. Take into consideration CARVER matrix"*

A.8.2 Defensive Operations

Defensive operations was the strongest theme in the responses received from the participants, with 38 sources and 118 references, covering *'communications'*, *'information flows'*, *'roles and responsibilities'*, *'situational awareness'*, and *'operating procedures'*.

Communications

The communications between members of the team emerged as a facet of defensive operations:

> *"Highlighted the importance of passing information around the team"*
>
> *"It highlighted the importance of communication and that to be aware of what each team is doing will mean as a whole you can work together better"*
>
> *"It has taught me how to liaise with the other roles in my team in order to be more efficient"*

Information Flows

The participants were advised to adopt the role of Blue Terrain Manager within their team structure, to manage activities on the network and prevent 'blue on blue' incidents caused by a lack of coordination. This control of information flow highlighted how team interaction could be improved:

> *"Helped me understand to communicate the information to the BTM [Blue Terrain Manager] to keep team operations smooth"*
>
> *"One task may involve more than one team, and using BTM to control our actions correctly, rather than going and disabling the immediate threat to investigate"*
>
> *"How to think when enemy activity has happened, the processes to escalate the information to the BTM and then the way of thinking of what the attacker would do next"*

Roles and Responsibilities

The exercise emphasised the definition of clear role descriptions within the team:

> *"TTX has highlighted the individual roles and responsibilities of each member. Also it has contextualised the training to the degree that all members of the team feel more confident going into the [next] exercise"*

> *"It allowed me to understand the different job roles and what initial on day one what we will be doing"*

> *"Extremely useful to discuss in the open how each team operates, as well as specifically clarifying exactly what is expected of us"*

Situational Awareness

As the TTX progressed, the participants became far more aware of the need for maintaining SA:

> *"It worked very well confirming all topics covered as well as tying it all in together, giving a better understanding of the situational awareness and where that SA information comes from"*

> *"TTX has greatly opened up my situational awareness and understanding for what to look for, and more importantly act upon. Communication within the team is vital and this exercise has definitely highlighted it to me"*

> *"vastly improved my knowledge of cyber and has introduced many new concepts which will now feed directly into my situational awareness and improve my overall ability as a Team Leader"*

> *"Visual situational awareness is always better"*

Operating Procedures

One of the key outcomes of the TTX was to highlight the need for standard operating procedures:

> *"It has highlighted areas of weakness in procedures"*

> *"I hadn't fully developed a set of processes due to no previous experience before. However, the TTX helped me start to form a clear picture of my own processes that I will follow"*

> *"Written SOPs with team input. Develop SOPs that visually illustrate network and events and enable clear passage of information to the team. Ensure during briefs that I ask each team for their input or suggestions"*

> *"The TTX was one of the most useful exercises this week and allowed me to pull together the techniques and tools learnt and place them in the appropriate point of the SOPs. It gave me a good overview of how the team members fit together and highlighted the interchangeable nature of skill sets"*

A.8.3 Network Understanding

The exercise participants acknowledged that an understanding of the network they were defending was critical to their ability to respond to incidents. The theme was cited in 20 sources with 29 references.

Network Terrain Analysis

The questionnaire respondents focused on network terrain analysis in particular:

> *"By categorising the network and its importance"*

> *"creating an audit to see changes in the future rather than relying on my memory or looking for something that doesn't look right"*

A.8.4 Defensive Planning

The participants cited defensive planning in 14 sources, with 19 references. They focused on the need to triage network assets in order to plan defensive activities.

Triage Priorities

The TTX participants made strong use of the CARVER matrix and the Purdue Model:

> *"Coupling my understanding of the Purdue Model along with CARVER, I will now be able to tailor my individual processes to reflect the prioritisation of tasks to support the Team leader and BTM's [Blue Terrain Manager's] strategy"*

> *"Yes, priorities and incident response. Certain systems need to be hardened before other, although they sit further inside the network. Not going and wiping the threat immediately, but studying and tracing the threat and where it might move to next"*

> *"Priorities – my priorities do not fully align to the team, so we need to sit down as a team and use the CARVER system"*

Appendix B

August 2017 CDX Results

Contents

B.1 Introduction

As a follow-on training activity from the exercise described in Section 7.5.4, and to test the emerging SOPs emerging from the TTX described in Section 7.5.5, 16 members of the sample attended a four-day CDX designed to further build their mental models of *APT Attack Behaviours*, *Team Understanding*, and *Team Interaction.* The CDX involved the Blue Team repeatedly defending the Domain Controllers in the network described in Figure 7.6, from the same attack. The intent was that the Blue Team would start to identify the attack behaviour in their sensors and logs, and with progressive use of covert techniques using a crawl-walk-run approach, the CPT would improve their understanding of how an APT takes control of a Domain Controller, and what such activities look like when interpreted via sensors and logs.

The results described below highlight the key network events by Red and Blue Teams during the CDX. They are contextualised in Section 8.9 of the main body of this thesis. Text in **bold** highlights intrusion detection activity by the Blue Team.

B.2 Key Network Events

Ref.	Date	Time	Description
1	30/08/17	0900	START DAY
2	30/08/17	0959	Initial beacon (reverse HTTPS) dropped to WIN7-2 (172.16.2.10) talking to core-upgrade.co.uk (122.129.50.43) and injected into process 964
3	30/08/17	1000	Malicious WMI events created on WIN7-2 (172.16.2.10)

4	30/08/17	1007	Mimikatz deployed on WIN7-2 (172.16.2.10)
5	30/08/17	1007	Initial SMB connection from WIN7-2 (172.16.2.10) to WIN7-3 (172.16.2.12) established
6	30/08/17	1007	Mimikatz deployed on WIN7-3 (172.16.2.12)
7	30/08/17	1023	Initial beacon (reverse HTTP) dropped on SHAREPOINT (172.16.1.40) talking to core-upgrade.co.uk (122.129.50.43) by WIN7-3 (172.16.2.12) via Service Control Manager
8	30/08/17	1025	Malicious WMI events created on SHAREPOINT (172.16.1.40)
9	30/08/17	1034	Mimikatz deployed on SHAREPOINT (172.16.1.40)
10	30/08/17	1039	SHAREPOINT (172.16.1.40) scanned ports 139,445 on 172.16.1.10
11	30/08/17	1042	Initial beacon (reverse HTTP) dropped on DC1 (172.16.1.10) talking to core-upgrade.co.uk (122.129.50.43) by SHAREPOINT (172.16.1.40) via Service Control Manager
12	30/08/17	1044	Initial beacon (reverse HTTP) dropped on DC1 (172.16.1.10) talking to core-upgrade.co.uk (122.129.50.43) by WIN7-2 (172.16.2.10) via Service Control Manager
13	30/08/17	1046	Initial beacon (reverse HTTPS) dropped to DC1 (172.16.1.10) talking to core-upgrade.co.uk (122.129.50.43) and injected into process 1568
14	30/08/17	1047	Mimikatz deployed on DC1 (172.16.1.10)
15	**30/08/17**	**1118**	**Review and modification of GPO on the DC.**
16	30/08/17	1153	Initial beacon (reverse HTTP) dropped on DC1 (172.16.1.10) talking to core-upgrade.co.uk (122.129.50.43) by WIN7-3 (172.16.2.12) via Service Control Manager
17	30/08/17	1155	Malicious WMI events created on DC1 (172.16.1.10)
18	**30/08/17**	**1200**	**Client WIN7-3 (172.16.2.12) established SMB communications to DC1 (172.16.1.10) and SHAREPOINT (172.16.1.40). Initiating events: 7, 16. Time to detection: 1hr 37 mins (from event 7).**
19	30/08/17	1204	Initial oci.dll upload to SHAREPOINT (172.16.1.40) and timestomped with cmd.exe attributes
20	30/08/17	1206	DC1 (172.16.1.10) scanned ports 139,445 on 172.16.1.11
21	30/08/17	1211	Initial beacon (reverse HTTP) dropped on DC2 (172.16.1.11) talking to core-upgrade.co.uk (122.129.50.43) by DC1 (172.16.1.10) via Service Control Manager
22	30/08/17	1243	DC2 (172.16.1.11) scanned ports 139,445,3389 on 172.16.1.20
23	30/08/17	1246	DC2 (172.16.1.11) scanned ports 139,445 on 172.16.9.0/24
24	30/08/17	1249	Mimikatz deployed on DC2 (172.16.1.11)

25	**30/08/17**	**1305**	**SMB connections identified between DC1 (172.16.1.10) and SHAREPOINT (172.16.1.40) connecting to WIN7-3 (172.16.2.12) via SMB port 445, then connection between WIN7-3 (172.16.2.12) and WIN7-2 (172.16.2.10), also via SMB. WIN7-2 (172.16.2.10) observed to be communicating with 122.129.50.43:80 (core-upgrade.co.uk). External IP blocked on firewall. Initiating events: 5, 7, 11, 16. Time to detection: 2hrs 58 mins (from event 5).**
26	**30/08/17**	**1500**	**Communication detected from DC2 (172.16.1.11) to 122.129.50.43:80 (core-upgrade.co.uk). Initiating event: 21. Time to detection: 2hrs 49 mins (from event 21).**
27	30/08/17	1530	FINISH DAY
28	31/08/17	0900	START DAY
29	**31/08/17**	**1000**	**Hardening activity to ensure all client firewalls are active, clients have blocked ports 445 and 139. Review of GPO (Group Policy Objects) to protect domain controller (DC).**
30	**31/08/17**	**1000**	**Connection from DC1 (172.16.1.10) to external IP 5.154.128.20:443 (butterblue.com) identified via Bro logs. NOTE: buttlerblue.com identified as a result of spurious Red Team activity.**
31	**31/08/17**	**1008**	**Connection detected from clients 172.16.2.10 and 172.16.2.12 to 122.129.50.60:80 (powerman.fr). NOTE: powerman.fr identified as a result of spurious Red Team activity.**
32	**31/08/17**	**1023**	**Process Beacon out to 122.129.50.60:80 (core-upgrade.co.uk) from WIN7-2 (172.16.2.10). NOTE: DNS resolution for core-upgrade.co.uk changed by Red Team. Process beacon still active on WIN7-2 (172.16.2.10).**
33	**31/08/17**	**1100**	**Malware identified on DC1 (172.16.1.10): msf.exe md5 083b5ed3e33f3d89bcc4cd49b1ab20e.**
34	31/08/17	1206	Initial beacon (reverse HTTP) dropped to WIN7-5 (172.16.2.14) talking to powerman.fr (122.129.50.70)
35	31/08/17	1208	Mimikatz deployed on WIN7-5 (172.16.2.14)
36	31/08/17	1209	Initial beacon (reverse HTTP) dropped on WIN7-4 (172.16.2.13) talking to powerman.fr (122.129.50.70) by WIN7-5 (172.16.2.14) via Service Control Manager
37	31/08/17	1213	Initial beacon (reverse HTTPS) dropped to WIN7-1 (172.16.2.20) talking to butterblue.com (5.154.128.74) and injected into process 1080

38	31/08/17	1217	Initial SMB connection from WIN7-5 (172.16.2.14) to WIN7-1 (172.16.2.20) established
39	31/08/17	1217	Initial SMB connection from WIN7-1 (172.16.2.20) to DC1 (172.16.1.10) established
40	31/08/17	1217	Initial beacon (reverse HTTP) dropped on WIN7-9 (172.16.2.18) talking to powerman.fr (122.129.50.70) by WIN7-5 (172.16.2.14) via Service Control Manager
41	31/08/17	1218	Initial beacon (reverse HTTP) dropped on WIN7-8 (172.16.2.17) talking to powerman.fr (122.129.50.70) by WIN7-5 (172.16.2.14) via Service Control Manager
42	31/08/17	1218	Initial beacon (reverse HTTP) dropped on WIN7-7 (172.16.2.16) talking to powerman.fr (122.129.50.70) by WIN7-5 (172.16.2.14) via Service Control Manager
43	31/08/17	1219	Malicious WMI events created on WIN7-1 (172.16.2.20)
44	31/08/17	1219	Malicious WMI events created on WIN7-5 (172.16.2.14)
45	**31/08/17**	**1220**	**Malicious executable HTML file identified (bad.hta) on WIN7-5 (172.16.2.14) communicating with 5.154.128.74, resolved to butterblue.com. Initiating event: 34. Time to detection: 11 mins.**
46	**31/08/17**	**1220**	**122.129.50.70 (powerman.fr) via WIN7-5 (172.16.2.14) identified performing DNS requests to DC1 (172.16.1.10) being routed to 172.16.3.10 (DMZ DNS) to complete lookup to 8.8.4.4 (Google). Initiating event: 34. Time to detection: 11 mins (from event 34).**
47	31/08/17	1220	WIN7-5 (172.16.2.14) scanned ports 445 on 172.16.1.0/24
48	31/08/17	1223	Initial beacon (reverse HTTP) dropped on SHAREPOINT (172.16.1.40) talking to powerman.fr (122.129.50.70) by WIN7-5 (172.16.2.14) via Service Control Manager
49	31/08/17	1224	Mimikatz deployed on SHAREPOINT (172.16.1.40)
50	31/08/17	1224	WIN7-5 (172.16.2.14) scanned ports 445 on 172.16.2.0/24
51	31/08/17	1227	Initial beacon (reverse HTTP) dropped to SHAREPOINT (172.16.1.40) talking to powerman.fr (122.129.50.70) and injected into process 1316
52	31/08/17	1227	Initial beacon (reverse HTTP) dropped on WIN7-10 (172.16.2.11) talking to powerman.fr (122.129.50.70) by WIN7-5 (172.16.2.14) via Service Control Manager
53	31/08/17	1230	Initial beacon (reverse HTTP) dropped to WIN7-10 (172.16.2.11) talking to powerman.fr (122.129.50.70) and injected into process 1156
54	31/08/17	1231	Initial SMB connection from WIN7-10 (172.16.2.11) to SHAREPOINT (172.16.1.40) established

55	31/08/17	1232	Initial beacon (reverse HTTPS) dropped on WIN7-2 (172.16.2.10) talking to butterblue.com (5.154.128.74) by WIN7-1 (172.16.2.20) via Service Control Manager
56	31/08/17	1233	Malicious WMI events created on WIN7-2 (172.16.2.10)
57	31/08/17	1236	Initial beacon (reverse HTTPS) dropped on DC1 (172.16.1.10) talking to butterblue.com (5.154.128.74) and injected into process 3204
58	31/08/17	1237	Initial beacon (reverse HTTP) dropped on DC1 (172.16.1.10) talking to powerman.fr (122.129.50.70) by SHAREPOINT (172.16.1.40) via Service Control Manager
59	31/08/17	1239	Mimikatz deployed on DC1 (172.16.1.10)
60	31/08/17	1239	Initial beacon (reverse HTTP) dropped to DC1 (172.16.1.10) talking to powerman.fr (122.129.50.70) and injected into process 1548
61	31/08/17	1241	Initial SMB connection from SHAREPOINT (172.16.1.40) to DC1 (172.16.1.10) established
62	31/08/17	1242	Malicious WMI events created on DC1 (172.16.1.10)
63	**31/08/17**	**1257**	**WIN7-2 (172.16.2.10) identified communicating with 122.129.50.60:80 (powerman.fr). Initiating event: 55. Time to detection: 25 mins (from event 55).**
64	31/08/17	1311	Malicious WMI events created on DC1 (172.16.1.10)
65	**31/08/17**	**1335**	**SHAREPOINT (172.16.1.40) identified performing HTTP GET requests to 122.129.50.70:8080 (powerman.fr). Potentially malicious files identified as mIOW.html. Initiating event: 49. Time to detection: 1hr 11 min (from event 49).**
66	**31/08/17**	**1346**	**Blocked all traffic from 122.129.50.70 (powerman.fr) to 172.16.0.0/16 on DMZ interface**
67	31/08/17	1349	Initial SMB connection from WIN7-10 (172.16.2.11) to DC1 (172.16.1.10) established
68	31/08/17	1355	Mimikatz deployed on WIN7-10 (172.16.2.11)
69	31/08/17	1355	Initial beacon (reverse HTTP) dropped on SHAREPOINT (172.16.1.40) talking to powerman.fr (122.129.50.70) by WIN7-10 (172.16.2.11) via Service Control Manager
70	31/08/17	1405	Initial beacon (reverse HTTP) dropped on WIN7-3 (172.16.2.12) talking to powerman.fr (122.129.50.70) by WIN7-10 (172.16.2.11) via Service Control Manager
71	31/08/17	1444	SysInternals Suite deleted from DC1 (172.16.1.10)
72	**31/08/17**	**1500**	**Hardened DNS entries on DC01 to sinkhole rogue DNS domains; gameaholic.com, butterblue.com, powerman.fr, and subsequently flushed DNS cache for all clients**
73	31/08/17	1500	Process Hacker deleted from DC1 (172.16.1.10)

74	31/08/17	1515	Initial beacon (reverse HTTP) dropped on DC1 (172.16.1.10) talking to powerman.fr (122.129.50.70) by WIN7-10 (172.16.2.11) via Service Control Manager
75	31/08/17	1515	FINISH DAY
76	01/09/17	0823	Initial beacon (reverse HTTP) dropped on WIN7-5 (172.16.2.14) talking to catchme.com (122.129.50.199) and injected into process 1148
77	01/09/17	0831	Initial beacon (reverse HTTP) dropped on DC1 (172.16.1.10) talking to catchme.com (122.129.50.199) and injected into process 3400
78	01/09/17	0828	Mimikatz deployed on WIN7-5
79	01/09/17	0838	Initial beacon (reverse HTTP) dropped to WIN7-1 (172.16.2.20) talking to catchme.com (122.129.50.199) and injected into process 1080
80	01/09/17	0900	START DAY
81	01/09/17	0900	Initial SMB connection from WIN7-1 (172.16.2.20) to WIN7-5 (172.16.2.14) established
82	01/09/17	0908	Initial SMB connection from WIN7-1 (172.16.2.20) to DC1 (172.16.1.10) established
83	**01/09/17**	**0920**	**Unrecognised traffic between 122.129.50.199:80 (catchme.com) and WIN7-5 (172.16.2.14) identified. Initiating events: 76, 80. Time to detection: 20 mins (from event 80).**
84	01/09/17	0924	Initial oci.dll upload to WIN7-1 (172.16.2.20) and timestomped with cmd.exe attributes
85	01/09/17	0925	Initial oci.dll upload to DC1 (172.16.1.10) and timestomped with cmd.exe attributes
86	01/09/17	0943	Initial SMB connection from WIN7-5 (172.16.2.14) to DC1 (172.16.1.10) established
87	**01/09/17**	**1000**	**SMB traffic between 172.16.2.20 (WIN7-1), 172.16.2.14 (WIN7-5), and DC1 (172.16.1.10) identified and SMB traffic starting to be blocked between user space and DC1. Traffic chain traced from DC1 (172.16.1.10) to WIN7-1 (172.16.2.20) to WIN7-5 (172.16.2.14) to 122.129.50.199:80 (catchme.com). Initiating events: 81, 82. Time to detection: 1 hr (from event 81).**
88	**01/09/17**	**1000**	**Blocked traffic to 122.129.50.199. Added catchme.com to local DNS and resolved to 127.0.0.1 (sinkhole)**
89	01/09/17	1017	Mimikatz deployed on WIN7-1 (172.16.2.20)
90	01/09/17	1125	Data exfiltration from DC1 (172.16.1.10) starts

91	**01/09/17**	**1200**	**Malicious processes on WIN7-5 (172.16.2.14) and WIN7-1 (172.16.2.20) in spooler.exe, rundll32 and SC.exe. Malicious DLL oci.dll injected into a legitimate process identified on DC1. Initiating events: 76, 79, 80, 85. Time to detection: 3hrs (from event 80).**
92	01/09/17	1300	FINISH DAY

Appendix C

December 2017 CDX Results

Contents

C.1 Introduction

Questionnaires were not provided for the attendees of of the exercise described in Section 7.5.8. Instead, observations were made by the author on the performances of the Blue Teams involved. The results of the exercise are summarised in Section 8.11. This appendix is provided to offer further detail to the assessments.

C.2 Assessment and Evaluation Criteria

The exercise was subject to a formalised set of quantitative evaluation metrics defined by the overall exercise White Team, outside of the influence of the author. As such, the assessment performed in this study, wherever possible, fitted within these established evaluation metrics. These overall exercise assessed the Blue Teams against five criteria:

1. Service Availability: A measure of the levels of availability of systems defined as critical by the White Team.
2. Procedures: The adherence of the Blue Teams to procedures defined within the exercise.
3. Red Team Evaluation: A measure, by Red Team, of the levels of defence provided by an individual Blue Team.
4. Mission: An evaluation of Blue Teams' overall cognisance of the changing exercise scenario and its impact on DCO priorities.
5. Out of Game: A measure of altruistic or extra-curricular activities by Blue Teams that benefited the exercise overall.

These measures were gauged by the exercise assessments team, with scores mediated by the White Team to maintain a consistency of scoring throughout the exercise. Each day, a baseline score was assigned to each criteria, then each team's performance was mediated against this to determine how far above or below the standard score their performance was judged to have been.

The assessment of Blue Teams' SA, team structures and information management techniques taught on the DCO MST, described in Section 7.5.7 was undertaken by the author, independently of the White Team assessment of the metrics above. SA was measured using a mediation model in line with the methods used above. It measured three levels of SA (level 1 - 3), plus an overall Team SA. A qualitative measure was used to assess the teams' development of the five mental models defined in Table 6.1.

C.3 Individual Team Performance Analyses

Whilst many working methods are available for DCO teams to operate within, this research focuses on the development of a repeatable model to train incident response within organisations, with interoperable manning and information exchanges. The focus of this assessment is not to measure the overall effectiveness of DCO activities on the network (although this is a factor), but to determine which techniques contribute to an efficient DCO team, and are repeatable. Specifically, it assessed:

- Team SA
- C2
- Information flows
- Understanding of adversary activities and intent

Assessments were based on an average time with each team of 30 minutes per day.

C.4 Technical Skills Self-Assessment Criteria

Figure C.1 illustrates the self-assessed skills of the teams participating in the exercise, using a questionnaire provided by the White Team, as well as presenting the number of participants in each team, which influenced the mean average calculations. No data was recorded for Team 4, who declined to contribute. The intelligence embeds within the team were not asked to contribute to the self-assessment. Members of Teams 5, 7 and 10 arrived late to the exercise and are not reflected in the data.

The author had no input into the assessment criteria, but the results are included as an indicative metric of relative technical competence.

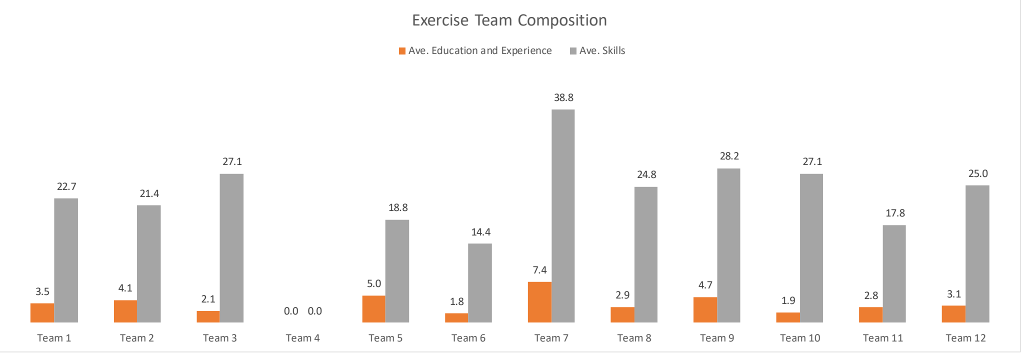


Figure C.1: Self-assessed overall skills of Blue Teams

Teams were asked to assess their formal education in cyber-related subjects, as well as detail their hands-on expertise using a subjective numeric schema. Formal education was recorded using the following values for the presented in Table C.1. It was observed that where exercise participants held more than one degree, they added the values to achieve a score higher than 3. This value was added to a further assessment of whether the exercise attendee had prior experience of cyber exercises. These values are presented in Table C.2.

Education	**Value**
Relevant undergraduate degree or higher	3
Irrelevant undergraduate degree, BTEC qualifications, or similar	2
Other qualifications	1
No qualification	0

Table C.1: Formal education self-assessment guidelines, defined by the exercise White Team, without input from the author.

Exercise participants were further requested to assess their overall individual technical skills, using the criteria in Table C.3. These were aggregated and used to produce a mean value for each team.

Education	Value
Experience of more than two cyber exercises	3
Experience of up to two cyber exercises	2
Experience of one cyber exercise	1
No experience of cyber exercises	0

Table C.2: Prior cyber exercise experience self-assessment guidelines, defined by the exercise White Team, without input from the author.

Technical Skills	Range
Use of established SOPs	0 (no experience) - 10 (significant experience)
Configuration and use of Firewalls and Routers	0 (no experience) - 10 (significant experience)
Configuration and use of Sensors	0 (no experience) - 10 (significant experience)
Configuration and use of Logs	0 (no experience) - 10 (significant experience)
Network and Server Hardening	0 (no experience) - 10 (significant experience)
Incident Response	0 (no experience) - 10 (significant experience)

Table C.3: Individual technical skills self-assessment guidelines, defined by the exercise White Team, without input from the author.

C.4.1 Team 1

Summary Data

Overall Exercise Position: 12th
Manning: 10
DCO MST: The team did not attend the DCO MST.

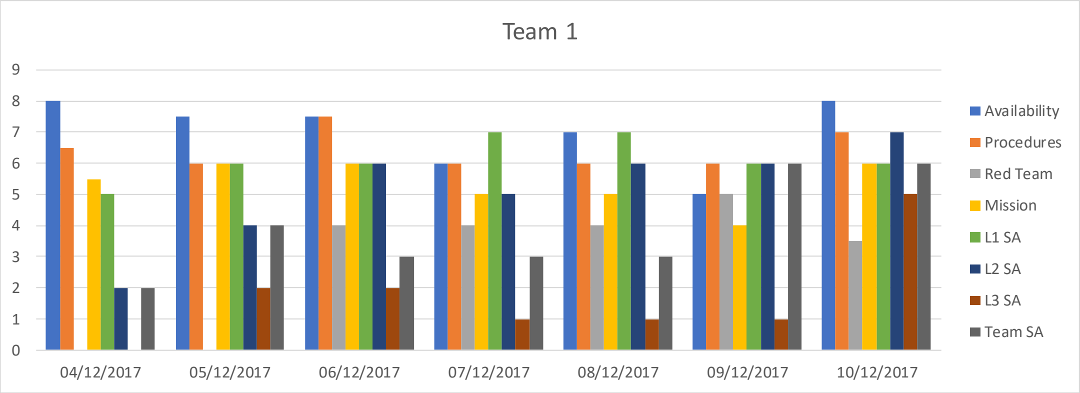


Figure C.2: Team 1 Performance

4 December 2017

Team 1 comprised a mixed team of five individuals from the UK who had not worked together before, and five from an international partner. No members of the team attended the DCO MST. After arrival at the exercise, the team chose adopt a structure similar to that recommended on the training, comprising a Team Leader, a second-in-command (2IC), with the rest of the team forming 1 x Intelligence, 2x Protect, 2x Monitor, 2x Harden. The UK personnel described themselves as having a low level of technical competency, with the international partners exhibiting more experience. The stated plan for Day 1 was to form as a team, map the network, and set-up the SIEM. They did not have any stated plans for any outcomes on the network at 1115hrs. Later they had established a routine, but no details were made available. No means to convey team situational awareness (SA) was observed, and no Intelligence Preparation of the Cyber Environment (IPCE) had been started. They stated their operational cycle included a team meeting at 1130. They sent Requests for Change (RFC) for Kali™ tools and arranged a meeting with the legal team to request RoE to perform counter-operations against Red Team.

In their daily report to White Team they made no forecast of Red Team activities on their network.

5 December 2017

The intent for day 2 was to harden the network segment prioritised by the exercise commander in White Team, and to submit a change to the RoE to allow counter-operations against Red Team activity. The preparation for this was the team's main effort (ME). The request was assessed against mission priorities, and declined.

A task list was visible for the team to track progress against. Network diagrams were being displayed as the network enumeration activities completed. A conversation with the UK team members highlighted that most of the technical effort was being delivered by the international partners, and that the UK team were being mentored as the work progressed. It was apparent during the conversation that the SA resided with the international partner personnel.

The daily report to White Team focused on risks to technical hardening operations, and did not assess likely Red Team actions.

6 December 2017

The team planned to finish hardening and start on their incident response process. An interview with team members highlighted that SA still resided with Canadian personnel. The team had attended the a DCO MST summary training session the evening before and competed a CARVER matrix to articulate priorities within their networks. No forecasts of Red Team activities were made verbally or in their daily report to White

Team.

7 December 2017

Suspected network intrusions were being investigated. No visual aids were used to articulate the state of Red Team intrusions into their network. The plan for the day was to finish their incident response process and consolidate their sensor feeds into Splunk ™. Although the team commented in their daily report to White Team that Red Team activity had increased, they maintained their focus on network hardening. No assessments of Red Team COAs were made.

8 December 2017

The team were observed to recover quickly from a confirmed Read Team intrusion on their network. Interviews with the team highlighted that they acknowledged the need for greater Team SA.

9 December 2017

The team adopted tools and techniques observed in other teams, that were based on the DCO MST. This included overall SA boards and the status' of various Red Team intrusions. An interview with the 2IC highlighted that Team SA, whilst improving, was still low.

10 December 2017

The team demonstrated a continued increase in Team SA, and were using more of the DCO MST tools such as the CARVER matrix in an attempt to integrate a G2 picture into their SOPs.

C.4.2 Team 2

Summary Data

Overall Exercise Position: 8th=
Manning: 9 (plus one intelligence embed)
DCO MST: The majority of the team attended the DCO MST, including the 2IC.

4 December 2017

A subset of the team attended the DCO MST, but were joined by a Team Leader, 2IC, and an intelligence embed, none of whom had any training prior to the exercise and had no previous cyber experience. The team claimed a low level of technical competency.

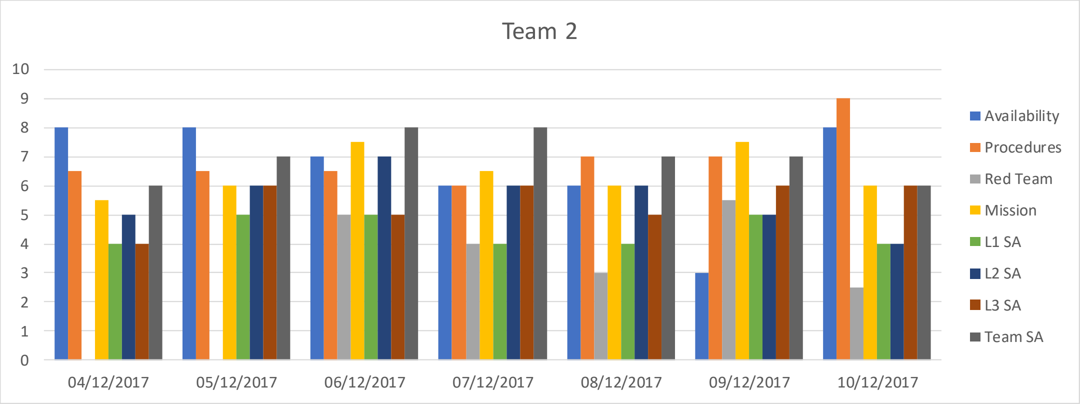


Figure C.3: Team 2 Performance

They comprised 9 personnel in total, and formed into the team structure recommended on the DCO MST (Figure7.7), with a Team Leader, Blue Terrain Manager (BTM), 1 x Intelligence, 2 x Hunt, 2x Monitor, 2x Harden. They had a clear objective stated for Day 1, which was to understand their network. By the end of play they had enumerated and documented two network segments, begun to triage their key terrain using a CARVER matrix, and had started to create a network hardening plan based on their triaged priorities. They maintained an operating cycle that included an hourly heads-up brief to maintain Team SA. The intelligence embed had no cyber experience, and did not attended the MST, so did not understand how to undertake IPCE and fuse this with the Adversary Lifecycle and Diamond Model of Intrusion Analysis. He subsequently attended a summary class that included ICS-CDTP and IPCE at the end of the day that included an explanation of these techniques. The daily report to White Team contained an assessment of forecast Red Team activity on the network, highlighting probable reconnaissance and malware delivery, using the Adversary Lifecycle Model taught on the DCO MST.

5 December 2017

The priorities for Day 2 were to start to harden the networks, perform a vulnerability scan, apply patches and updates, configure sensors, and conduct a CARVER analysis of available systems to triage the key network terrain.

Observation of one of the hourly briefs demonstrated a high level of Team SA and understanding of individual team members' roles and responsibilities. The BTM managed the deconfliction of activities on elements of the networks, with the team making use of the visual representations of the current state of the network and intrusion models to explain the current status of their tasks.

The daily report to White Team contained an assessment of likely Red Team activity on the network.

6 December 2017

The team had completed a CARVER matrix. The plan for the day was to finish hardening and setup their sensors. The team assessed the likely Red Team activity for the day was phishing. The team had a Prioritised Defended Asset List (PDAL) on the wall that articulated their (White Team) commander's priorities. The team had started their network hunt and monitoring activities, focusing on the key network terrain.

An observed hourly brief demonstrated excellent team communications and SA. Two intrusion incidents had been identified and were being investigated. The BTM was maintaining control of team activities, centred around activities on the key network terrain.

7 December 2017

All confirmed intrusions were displayed on the attack model. The team's sensors were active and the BTM had articulated a clear technical plan which included a proactive view of likely Red Team activity. This was reflected in their dailyreport to White Team.

8 December 2017

Splunk™was observed to be installed on all servers and their overall SA picture had improved as a consequence. The team were observed to be recovering from the over-hardening of various devices. They had identified a number of potential Red Team intrusions on their networks and were assessing likely COAs as a consequence.

9 December 2017

While interviewing members of the team it became apparent that individual technical skills was the constraining factor for Team 2. They maintained strong C2, information flows and Team SA, but lacked the abilities to identify sophisticated Red Team intrusions or remediate their consequences. As a result, the team were limited in their ability to defend their networks.

10 December 2017

The team maintained their high levels of Team SA and continued to assess Red Team COAs based on received cyber threat intelligence.

C.4.3 Team 3

Summary Data

Overall Exercise Position: 3rd
Manning: 8
DCO MST: The majority of the team attended the DCO MST, including the Team Leader.

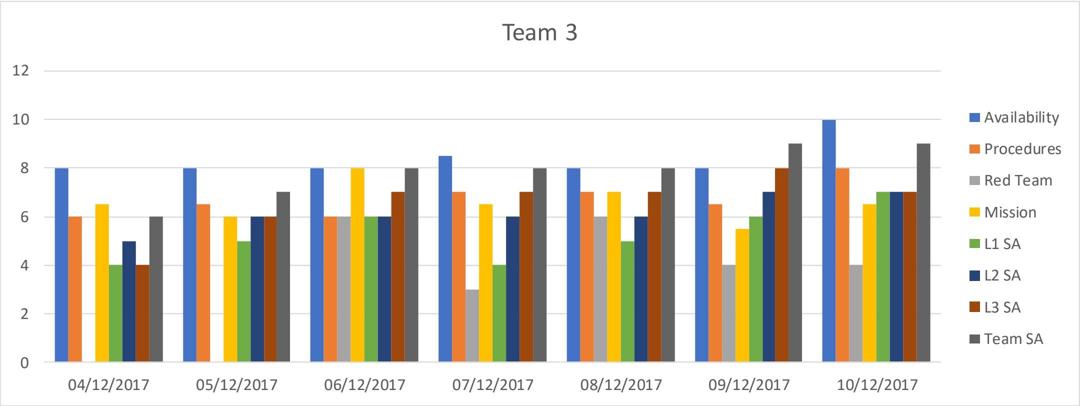


Figure C.4: Team 3 Performance

4 December 2017

The team claimed a low level of technical competency at the DCO MST, which was supplemented by additional individual training to raise their overall understanding of DCO tools. They comprised 8 personnel in total, and formed into the recommended team structure (Figure 7.7), with a Team Leader (also managing threat intelligence), 1x BTM, 2x Hunt, 2x Monitor, 2x Harden. They were not a formed team before the exercise. They had a clear objective stated for Day 1, which was to understand their network. By the end of play they had enumerated an unspecified number network segments and performed a preliminary analysis of their key terrain using a CARVER matrix. They intended to maintain an operational cycle of an hourly heads-up brief to maintain Team SA, but admitted that in practice this had slipped to a two-hourly brief. A Team SA visual aid was observed, displaying the Adversary Lifecycle and Diamond Model analysis frameworks. No IPCE had been undertaken.

In their daily report to White Cell they assessed the likely Red Team activity anticipated in the next 24-48hrs to focus on phishing campaigns and the establishment of a foothold on the network. This was in line with techniques taught on the DCO MST.

5 December 2017

The Day 2 objectives were to continue with enumerating their networks and start to setup sensors. The team detected two possible network intrusion events and represented these using the Adversary Lifecycle and Diamond models, permitting an assessment of likely next steps by Red Team. Diagrammatic representations of the networks, and associated system availability, were mounted on the surrounding walls, along with clearly marked task priorities.

The daily report to White Team contained an assessment of likely Red Team actions.

6 December 2017

The team had assessed that Red Team were on their networks and as a consequence, had implemented processes to limit the use of administrator credentials in case of key logging being used. The team had also refined their roles and responsibilities, and continued to harden the network. Their priority for the day was to ensure the sensors were properly configured. The Hunt team were still providing additional resources to the harden function.

An observed hourly brief demonstrated that team activities were being shaped by an assessment of likely Red Team activities. These assessments were also reflected in their daily report to White Team.

7 December 2017

Whilst network intrusions were being detected, the team were not being distracted from defending their key network terrain. An assessment of Red Team COAs was made in the daily report to White Team.

8 December 2017

The team had successfully identified a number of Red Team intrusions and were recovering from them. They used this identification to inform a wider assessment of Red Team COAs on their network.

9 December 2017

The team continued to identify and remediate Red Team intrusions, repriortising defences based on changing exercise scenario priorities.

10 December 2017

Strong overall SA based on continuing assessment of Red Team COAs using intrusion behaviours and fusion with cyber threat intelligence reporting.

C.4.4 Team 4

Summary Data

Overall Exercise Position: 5th
Manning: 5 (plus an intelligence embed who joined late in the exercise)
DCO MST: The team did not attend the DCO MST.

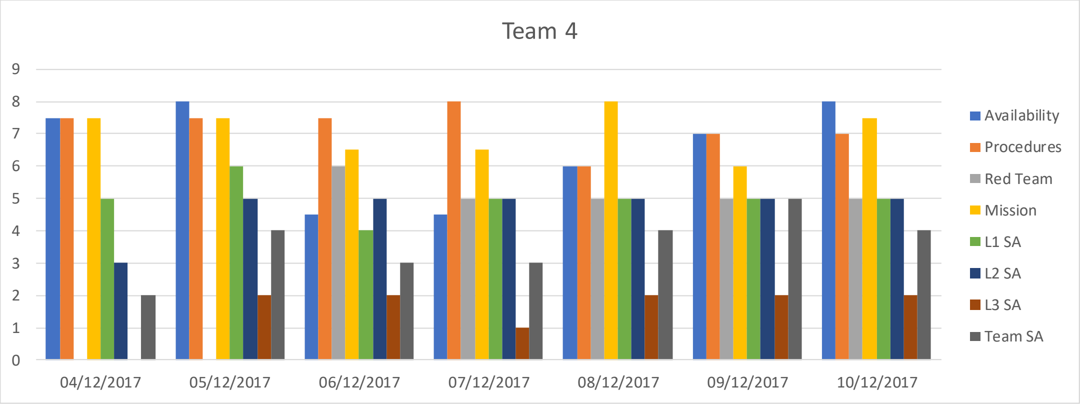


Figure C.5: Team 4 Performance

4 December 2017

The team described themselves as having a mix of cyber technical competencies, from mid- to high-level. They organised themselves based on the networks to be defended, with two personnel assigned to each network segment. They demonstrated a dynamic approach to work; they regularly came together for planning sessions, then broke away to carry-out assigned tasks. They were not a formed team prior to the exercise. They stated their objectives for Day 1 were to understand and baseline their networks. They enumerated the various network segments they were responsible for, followed by running a vulnerability scan that highlighted areas of operating system weaknesses. These vulnerabilities guided their plans to harden their networks in the following days.

The team had no established operational cycle, and displayed no forward assessment of likely Red Team activities on their network during their verbal briefs or daily reports to White Team.

5 December 2017

Enumeration has been completed and the team moved to harden their networks. Once this has been completed the team intend to restructure to follow the Hunt, Monitor, Harden structure taught on the DCO MST. The team culture continued to permeate however, and appeared an effective vehicle for their ways of working. The team were clearly relaxed and working collaboratively. An observation of one of their informal briefs demonstrated good use of cyber threat intelligence reporting and understanding of Red Team techniques. However, no assessment of likely Red Team activities was made in this, or their daily report to White Team.

6 December 2017

The team had produced a map of their networks on a whiteboard as an SA visual aid. They continued to harden their networks and planned to configure their sensors. They believed they had intrusions on their networks. No forecasts of Red Team activity were made.

7 December 2017

Team SA was still being maintained verbally, and the team expressed that they felt they were currently operating reactively. With the addition of an intelligence embed, the team had restructured as 2x Monitor, 2x Server Hardening, 1x Intelligence, 1x floating resource.

A number of intrusion events were detected. All views of risks were expressed technically, with no reference to likely Red Team COAs.

8 December 2017

Various Red Team intrusions had been identified and were being remediated. This was the main effort of the team, with no wider SA beyond this.

9 December 2017

The team were hampered by a lack of sensor coverage that restricted their ability to identify further intrusions. The team dynamic was observed to be positive, and the team were working well together and an understanding of each others' capabilities. However, Team SA remained poor, with isolated pockets of understanding of Red Team intent and likely COAs. No changes to priorities were made based on changes in the exercise scenario.

10 December 2017

The team remained focused on technical detail, with no attempts made to pre-empt Red Team COAs. As such, the team remained purely reactive and focused on hardening as their primary defence mechanism. Team SA remained poor.

C.4.5 Team 5

Summary Data

Overall Exercise Position: 4th
Manning: 7 (plus one intelligence embed)
DCO MST: Part of the team attended the DCO MST, including the Team Leader.

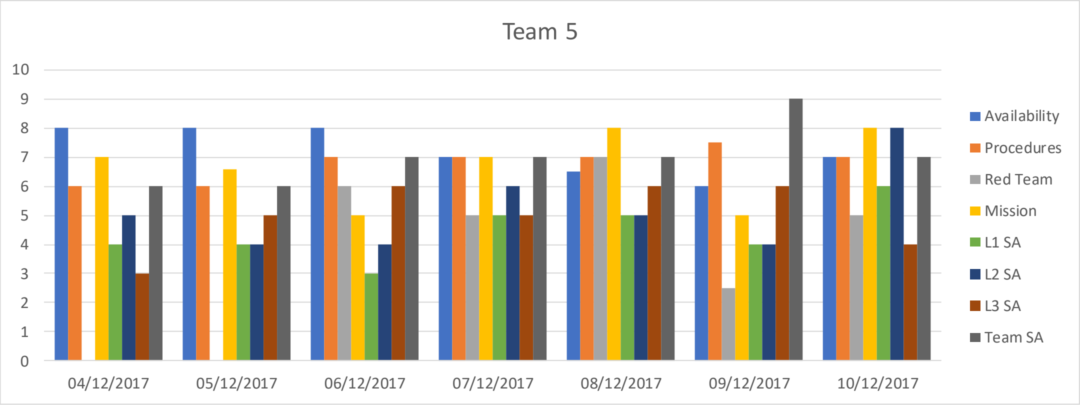


Figure C.6: Team 5 Performance

4 December 2017

The team described themselves as having a low level of cyber competence, and were not a formed unit before the exercise. They aligned themselves to the force structure similar to that taught in the DCO MST (Figure 7.7), providing 1x Team Leader, 1x BTM, 2x Hunt, 2x Monitor and 1x Harden. They integrated an intelligence embed who had not received any training prior to the exercise and had no previous cyber experience. Their intent for Day 1 was to understand their network, in accordance with with the DCO MST. This included enumerating the network segments, auditing user accounts on the Domain Controllers, and inspection of the firewall rulesets. They adopted an operating cycle of hourly briefs to maintain Team SA, and prioritised their immediate actions on the Domain Controllers whilst the network enumeration took place. In their daily report to White Team they provided an assessment of likely activity on their network by Red Team, including phishing and malware delivery within 24 hours, and possibly ransomware within 48-72 hours.

5 December 2017

A CARVER matrix was completed and was used to shape the placement of sensors on the network. They had submitted RFCs to limit user internet access and a PAAL. The team were still attempting to understand their network. Hourly briefs were maintained, and with the delivery of whiteboards the team were able to create a visible network map and task deconfliction register. Their daily report to the White Team contained an assessment of likely Red Team activities.

6 December 2017

The team planned to finish hardening their networks then configure their sensors. The key network terrain was identified. The roles and responsibilities of team members appeared clear in a team brief, and the hourly brief operational cycle was maintained and demonstrated a high level of Team SA. A lack of sensors meant the team could not detect any intrusions. However, their daily report to the White Team displayed a clear view of the Red Team activities they assessed were taking place on their network.

7 December 2017

The team were monitoring their network and hunting for Red Team activity. In line with DCO MST, the team had isolated the ICS on the network. They maintained hourly briefs, using boards to display intrusion activities using the attack model. The team were maintaining a list of priority actions, which were assessed when intrusions were detected, and a risk assessment based on the key network terrain made to determine the priority of the team's response. The team maintained an excellent assessment of risks to continued operations and likely Red Team activities.

8 December 2017

Based on identified intrusions and an assessment of likely Red Team COAs, the team were implementing changes to the router rules to limit Red Team freedom of action on their networks. The team demonstrated an ability to articulate the risks carried by the mission owner as a result of the intrusions. The team had experienced issues with over-hardening caused by limited individual technical skills.

9 December 2017

The team demonstrated excellent Team SA when a junior member of the team was randomly selected by the assessors to brief on the condition of Team 5's networks, the status of the various intrusions, and which team members were working on defined tasks. Subsequent questioning of all team members highlighted the high level of overall Team SA.

10 December 2017

The team maintained their overall Team SA, but were unable to provide a detailed assessment of Red Team probable COAs. They demonstrated limited technical understanding of Red Team intrusion techniques.

C.4.6 Team 6

Summary Data

Overall Exercise Position: 11th
Manning: 8
DCO MST: The majority of the team attended the DCO MST, including the Team Leader.

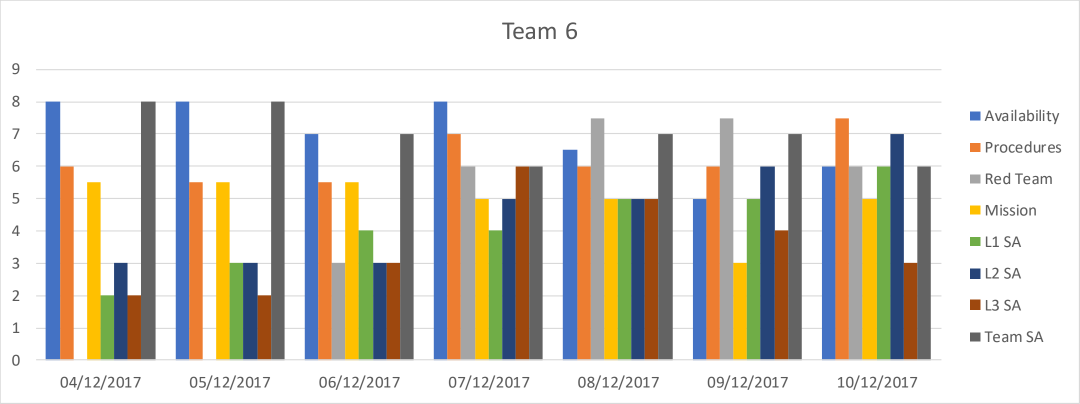


Figure C.7: Team 6 Performance

4 December 2017

The team described themselves as having a very low level of cyber competence, and were not a formed unit before the DCO MST and exercise. They aligned themselves to the structure taught in the DCO MST, providing 1x Team Leader, 1x BTM, 2x Hunt, 2x Monitor and 2x Harden. Their intent for Day 1 was to understand their network, in accordance with the DCO MST. By the end of the day they had established an operational cycle of hourly briefs to maintain Team SA, and had produced a blue terrain deconfliction chart (to prevent blue-on-blue incidents on the network), an attack lifecycle structure in which to model intrusion events on their networks (using the Adversary Lifecycle Model and the Diamond Model of Intrusion Analysis), and had started a preliminary CARVER assessment. They had also sent an RFC outlining their requests for a Pre-Approved Actions List (PAAL) for network changes to the White Team. All of these products and techniques were taught on the DCO MST. Their daily report to the White Team threat analysis focused on issues relating to network hardening, and did not contain a forecast of Red Team activities on their network.

5 December 2017

The team were still attempting to understand their network, with the enumeration process estimated to be 85 percent complete. They assessed their DCs were at risk, and planned to undertake a full IPCE once the enumeration was finished. Hourly briefs were maintained. By the afternoon the enumeration was completed and a network diagram visible. Hardening had started on the DC, with the setup of the sensors in progress.

Their daily report to the White Team contained an assessment of likely Red Team activity on their network.

6 December 2017

The team had completed a CARVER matrix and were hardening their networks. They had submitted RFCs to deploy their sensors in positions based on their CARVER matrix. They maintained an operational cycle including hourly briefs and a deconfliction board to manage their blue terrain.

7 December 2017

As per the DCO MST, the team were prioritising intrusion events against defensive activities on the key network terrain to avoid becoming reactive. They maintained an ongoing assessment of likely Red Team activities.

8 December 2017

The team's focus was on hardening, particularly routers and implementing tighter GPOs. A number of Red Team intrusions were identified and remediation was in progress. An assessment of risks was maintained, but this was purely technical. This was assessed to be as a consequence of individual technical skills and a lack of ability to forecast based on technical indicators.

9 December 2017

The Team SA remained high, but poor individual technical skills continued to limit an assessment of Red Team COAs.

10 December 2017

Overall SA was observed to have reduced as poor individual technical skills continued to limit an assessment of Red Team COAs.

C.4.7 Team 7

Summary Data

Overall Exercise Position: 1st
Manning: 10
DCO MST: Team 7 were the purposeful sample of this research, the CPT. None of the team attended the DCO MST, but elements of their previous training were based on the contents of the DCO MST.

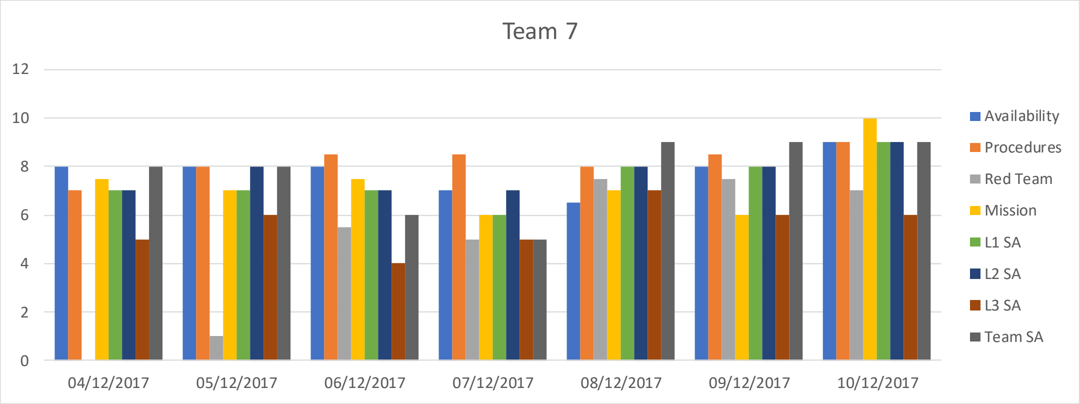


Figure C.8: Team 7 Performance

4 December 2017

Team 7 were the CPT that formed the purposeful sample for this research. They attended the exercise with a relatively high level of training and experience. The team comprised 1x Team Leader, 1xBTM, 3x Monitor, 3x Hunt, 2x Harden and 1x Intelligence. Their SOPs include an operational cycle of hourly briefs, the development of IPCE, a PAAL, and immediate actions for each of the sub-teams within the CPT. Their intent for Day 1 was to understand the networks, produce a baseline IPCE, submit their standard PAAL and RFIs. By the end of the day they had mapped and documented their networks, hardening had commenced, and sensors were being deployed. A preliminary IPCE had been produced and the CPT intelligence operator was assessing possible adversary COAs.

Their daily report to White Team contained no assessment of likely adversary activity, despite this being included in the team's IPCE.

5 December 2017

A network diagram was visible and was shaping the final version of the IPCE. Hardening of the networks had started, along with the submission of a number of RFCs. Sensors had been deployed and the team described themselves as transitioning to 'business as usual'. The team had identified that the operating cycle and blue terrain management was slipping, and so enforced greater control over these aspects of operations.

No assessment of Red Team activity was included in their daily report to White Team.

6 December 2017

The team had one incident under investigation which was being assessed in technical detail for reporting to the exercise intelligence cell and to White Team. Hardening continued, and an ongoing assessment of Red Team activity was maintained in the updated IPCE and CARVER matrix. The team displayed a high level of individual technical skills, with adherence to established SOPs apparent. A deep level of Team SA was observed, with tools such as a network traffic map being used to track Red Team intrusion behaviour.

This level of assessment was not reflected in the daily report to White Team.

7 December 2017

Two further intrusions had been identified, with probable persistence attained and attempts made to compromise the Domain Controller. The impact of these intrusions was not made apparent in the daily report to White Team.

8 December 2017

The team continued to identify and remediate Red Team intrusions. Team SA, C2 and information flows were all identified as well-defined and effective. Full use of the team's established SOPs were apparent.

9 December 2017

Team SA was observed to be excellent, with all details of the statuses of the network segments clearly displayed on visual aid boards, along with individual team member taskings, and an assessment of projected Red Team COAs.

10 December 2017

The team maintained adherence to their established processes and continued their high level of Team SA.

C.4.8 Team 8

Summary Data

Overall Exercise Position: 2nd
Manning: 11
DCO MST: Only one junior member of the team attended the DCO MST.

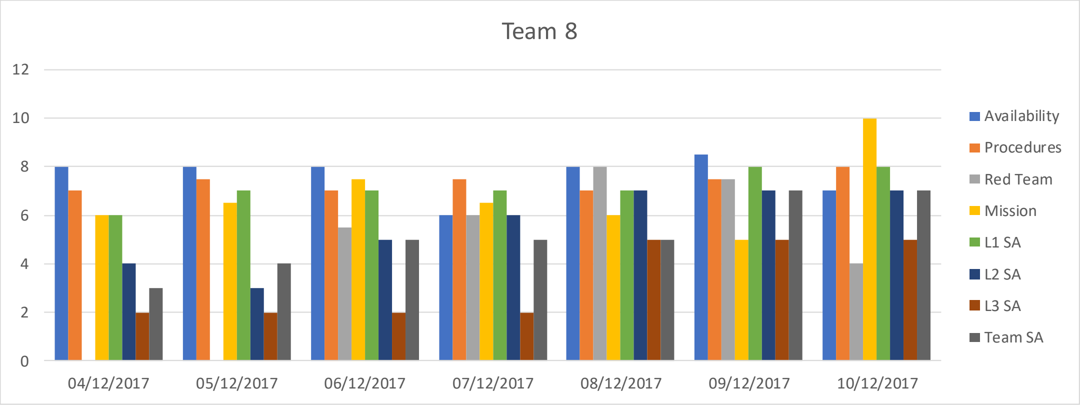


Figure C.9: Team 8 Performance

4 December 2017

The team was not formed prior to the exercise, but comprised a significant element from an established network operations team. They claimed a medium level of technical competence in the cyber domain. The team appeared to adopt the methods of working used by the network operations team and chose not to use any of the DCO MST. Their Day 1 objective was understand their networks, harden, and update the permissions available to users and services via Group Policy Objects (GPO). They had not established a clear operating cycle during the day, other than the external meetings required by the White Team. The team was organised into 1x Team Leader, 1x 2IC, 2x Evaluate and Discover, 4x Harden, 1x Security Onion, and 1x floating resource to be deployed as required. They also integrated an intelligence embed who had not received any training prior to the exercise and had no previous cyber experience. The team did not develop an IPCE or forecast any Red Team activity on their networks.

5 December 2017

Network enumeration was completed, and hardening was in progress. The team maintained informal briefs as required. No forecast of Red Team activities was expressed either verbally or in their daily report to White Team.

6 December 2017

The team's main effort was to apply patches across the networks then, as a secondary activity to finalise the sensor setup for monitoring. The team has re-mapped the network to look for changes, with none identified.

It was apparent from interviews with the team that SA resided with the Team Leader, and team members only retained SA of their own areas.

No assessment of Red Team activity was made verbally or in the daily report to White Team.

7 December 2017

The team had identified possible intrusions and had located malicious files.

8 December 2017

Multiple network intrusions were detected and were being remediated. Some forecasting of Red Team COAs was observed, but only at a superficial level.

9 December 2017

The team remained focused on hardening, but with an improvement in Team SA. Some limited forecasting of Red Team COAs was observed, but lacked technical depth.

10 December 2017

Overall SA was observed to have improved, across levels 1 to 3. Team SA was also observed to have improved, with a greater distribution of understanding across the team, and as a consequence, reduced the potential risks of a single point of failure in the Team Leader.

C.4.9 Team 9

Summary Data

Overall Exercise Position: 8th=
Manning: 4 (plus one intelligence embed)
DCO MST: None of the team attended the DCO MST.

4 December 2017

The team comprised four international partners who described themselves as competent with cyber technologies, although they had not worked together prior to the exercise.

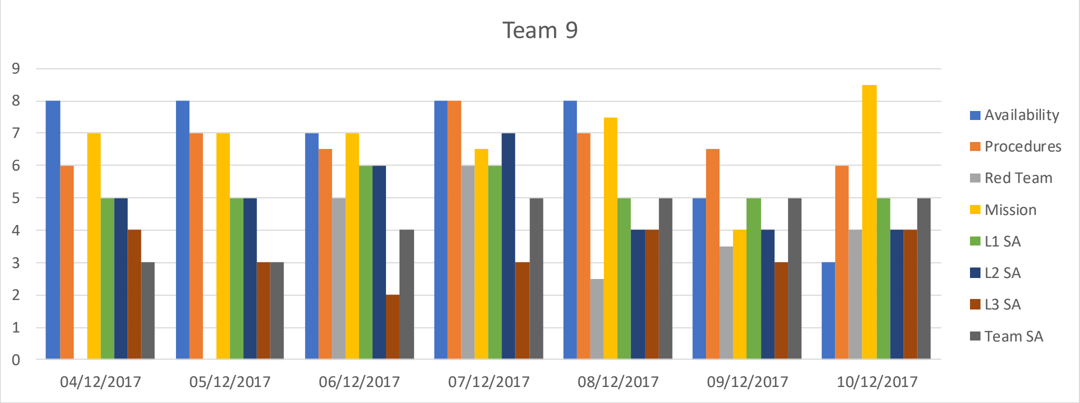


Figure C.10: Team 9 Performance

They also integrated an intelligence embed who had not received any training prior to the exercise and had no previous cyber experience. Their Day 1 priority was to understand their networks, as an initial step in a planned schedule that comprised active defences, passive defences, and the development of a security baseline. No consistent operational cycle was established. The team used informal briefings to communicate priorities. Team members appeared to understand what was required of each of them. The tasks were executed effectively, although no means of displaying information to maintain Team SA were apparent. The team made effective use of the cyber threat intelligence feeds, but did not produce an IPCE. Their daily reports to White Team included an assessment of Red Team likely activity on their networks.

5 December 2017

Network enumeration was still in progress, and hardening planned as the next step. Whilst specific networks had been prioritised, servers within them had not. They maintained informal briefs, with no established operational cycle. No IPCE was created and no visible representations of their networks were apparent. However, they were assessing likely Red Team activities, both verbally and in their daily report to White Team.

6 December 2017

The team had enumerated their networks, but were still waiting for approval on RFCs to deploy sensors. Their plan for the day was to finish drawing their network diagrams and continue hardening.

It was observed that few verbal communications were used by the team.

7 December 2017

The team reported an intrusion. They used Microsoft OneNote™to maintain Team SA, and the details were contained within.

8 December 2017

The team reported an ability to detect intrusions with their sensors finally online and reporting to Splunk™. Hardening continued as the primary means of network defence. Some Red Team intrusions were identified and were in the process of being remediated.

9 December 2017

Interviews with the team highlighted a focus on intrusions, but lacked technical detail. Overall SA was minimal.

10 December 2017

Further interviews with the team highlighted a lack of technical detail on the intrusions detected, resulting in a concern that they had not been fully remediated.

C.4.10 Team 10

Summary Data

Overall Exercise Position: 10th
Manning: 9
DCO MST: Only one member of the team, the Team Leader, attended the DCO MST, but not for the whole course duration.

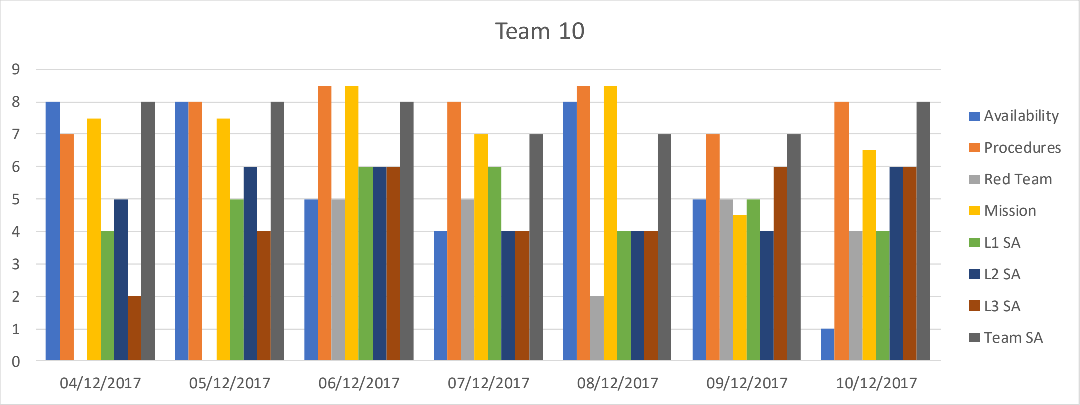


Figure C.11: Team 10 Performance

4 December 2017

The team was not formed prior to the exercise. They claimed a low-to-medium level of cyber competence. The team was structured along the lines of the DCO MST, with 1x Team Leader/BTM, 2x Hunt, 2x Monitor, 2x Harden, 1x Intelligence, with individuals focusing on different network segments to allow concurrent activity. Their intent for Day 1 was to understand their network and to have audited their Domain Controllers. By the end of the day they had established an operational cycle of hourly briefs to maintain Team SA, and an attack lifecycle structure in which to model intrusion events on their networks (using the Adversary Lifecycle Model and the Diamond Model of Intrusion Analysis). The daily report to White Team, however, contained no assessment of likely Red Team activity on the network.

5 December 2017

A CARVER matrix was complete, and the networks were visible on a whiteboard. The team had identified two possible intrusion events, which were displayed on the attack model on the wall. An observed hourly brief highlighted a high level of Team SA and clearly defined roles and responsibilities. However, it appeared that an error in the configuration of the DC had locked users out of the network.

Whilst an assessment of likely Red Team activity was made verbally, it was not reflected in the daily report to White Team.

6 December 2017

The team maintained excellent Team SA with various visual aids and whiteboards in use. No verbal briefing was required to ascertain the status of their networks and the level of intrusions.

The team reported they had locked themselves out of their Domain Controller.

7 December 2017

Further intrusions detected and under investigation. As per the DCO MST, these events were prioritised against activities to defend the key network terrain before allocating resources.

The team maintained an assessment of likely Read Team activities.

8 December 2017

The team were suffering from over-hardening and were locked-out from key systems. Multiple intrusions had been detected and were being remediated. The team maintained an assessment of likely Red Team COAs.

9 December 2017

The team demonstrated excellent Team SA when team member was randomly selected by the exercise assessors to brief on the condition of the team's networks, the status of the various intrusions, and which team members were working on defined tasks. Subsequent questioning of all team members highlighted the high level of overall Team SA.

10 December 2017

The team maintained an overall high level of Team SA, but were observed to be being drawn into responding to incidents too quickly and were starting to become reactive, rather than proactive.

C.4.11 Team 11

Summary Data

Overall Exercise Position: 6th=
Manning: 5
DCO MST: None of the team attended the DCO MST.

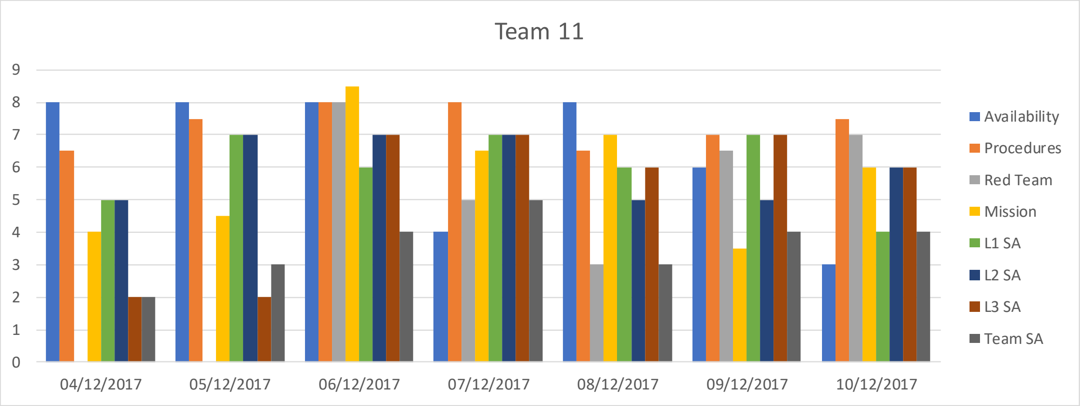


Figure C.12: Team 11 Performance

4 December 2017

The team comprised five personnel. They described their technical competence as low to medium. Given the small size of the team, the Team Leader adopted a flexible structure to allow resources to be deployed as required. The intent for Day 1 was to understand the networks, although resource limitations deprioritised one of the segments. The team used no methods to maintain Team SA and supplied no report to White Team.

5 December 2017

The team had started hardening after enumeration was completed. No network maps or Team SA tools were displayed.

6 December 2017

The team had their sensors active. They maintained an overall task management board to deconflict activities, and were resetting passwords as part of an operational cycle to degrade Red Team activities on the network. The team maintained a focus on hardening. No IPCE had been conducted.

7 December 2017

The team remained focused on further hardening of the network. The team also forecast Red Team progress toward the Domain Controller and detected unusual activity on the server.

8 December 2017

Multiple Red Team intrusions were detected and were in the process of being remediated. Hardening was continuing. Some assessment of Red Team COAs was being undertaken, but limited to specific team members. Overall Team SA remained low.

9 December 2017

It was observed that the team lacked C2 and cohesion, and relied on the Team Leader too much, creating a potential single point of failure. No overall view of the Red Team network intrusions was available and Team SA remained low, despite individual assessments of Red Team COAs demonstrating technical understanding.

10 December 2017

Assessment of Red Team behavioural indicators remains poor within the team, although individual assessments of Red Team COAs continue to demonstrate technical understanding. The relatively small size of the team, along with poor C2 and team understanding was assessed as the root cause.

C.4.12 Team 12

Summary Data

Overall Exercise Position: 6th=
Manning: 8
DCO MST: The majority of the team attended the DCO MST, including the Team Leader.

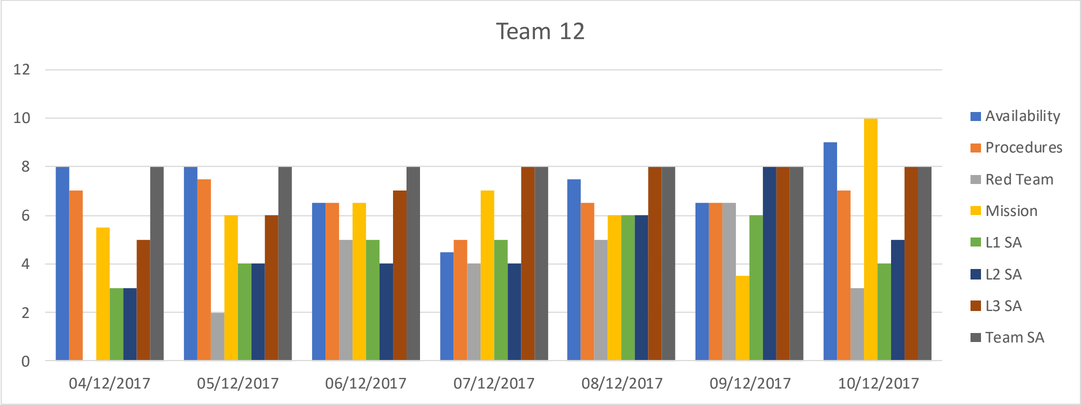


Figure C.13: Team 12 Performance

4 December 2017

The team described themselves as having a low level of cyber competence, and were not a formed unit before the DCO MST and exercise. They aligned themselves to the structure taught in the DCO MST, providing 1x Team Leader, 1x BTM, 2x Hunt, 2x Monitor and 2x Harden. Their intent for Day 1 was to understand their network, in line with DCO MST. By the end of the day they had established an operational cycle of hourly briefs to maintain Team SA, and an attack lifecycle structure in which to model intrusion events on their networks (using the Adversary Lifecycle Model and the Diamond Model of Intrusion Analysis), an external traffic map, and had started a preliminary CARVER assessment. They had also sent an RFC outlining their requests for a Pre-Approved Actions List (PAAL) for network changes to the White Team. All of these products and techniques were taught on the DCO MST.

The daily report to White Team contained an assessment of forecast Red Team activity on the network, highlighting probable malware delivery.

5 December 2017

A CARVER matrix had been completed, and the team had moved on to harden their network. They had submitted an RFC to deploy sensors. Hourly briefs were maintained.

The team maintained a clear assessment of likely Red Team activities, both verbally and in their daily report to White Team.

6 December 2017

The team finished enumerating the networks and had started setting up their sensors. Hardening continued, with a strategy of enforcing the ‘principle of least privilege’ in use. They had identified a potential Red Team implant on the network. The detail of this was maintained on the Team SA boards, and interviews with various team members indicated a deep level of Team SA, and mutual assessments of likely Red Team activities.

7 December 2017

Further intrusions detected and under investigation. As per the DCO MST, these events were prioritised against activities to defend the key network terrain before allocating resources.

The team maintained an assessment of likely Red Team activities.

8 December 2017

The team suffered from over-hardening of firewall configurations and slowed overall defensive actions. Multiple Red Team intrusions were identified and recovered. The team maintained a sound assessment of Red Team COAs and likely actions.

9 December 2017

Further intrusions were detected and remediations were in progress. Overall Team SA remained excellent, with a full understanding of the changing exercise scenario demonstrated.

10 December 2017

The team's SA remained excellent, but the Level 2 assessment continued to suffer from a poor levels of individual technical skills which limited the ability to contextualise the meaning of particular network attack behaviours.

Appendix D

Intelligence Preparation of the Cyber Environment (IPCE)

Contents

D.1 Introduction

The ICS-CDTP has been used to develop the Intelligence Preparation of the Cyber Environment (IPCE) process for the intelligence teams involved in incident response to structure it into their existing processes. IPCE is an embryonic development of Intelligence Preparation of the Environment (IPE) which is the process used for military planning at the tactical level.

D.2 IPCE

IPCE is an approach to modelling contested cyber environments in order to support the achievement of a commander's objectives, determine which areas of network terrain must be defended, and assess adversary COA. It comprises 3 stages:

1. **Battlespace Area Evaluation (BAE):** *Focuses on the effect of the features and constraints the network will have on operations and determines key terrain and adversary attack surfaces.*
2. **Threat Evaluation (TE):** *Characterises how an adversary would move across the network.*

3. **Threat Integration (TI):** *Brings together the features and constraints of the network terrain with adversary scheme of manoeuvre, to determine their probable COA.*

D.2.1 Battlespace Area Evaluation (BAE)

BAE is used to understand the 'battlespace', in this case, the networks on which operations will take place. This incorporate Stages 2 - 'Investigation of Deployed Architecture' and Stage 3 - 'Antagonistic Target Determination' from ICS-CDTP, described in Sections 5.3.2 and 5.3.3, shaped by an understanding of the adversary from Stage 1 - 'Attack Behaviour Modelling' in Section 5.3.1.

D.2.2 Threat Evaluation (TE)

TE considers how an adversary would move across a network to the key terrain defined in BAE. This uses the techniques described in Stage 4 - 'Attack Options Analysis' of ICS-CDTP, described in Section 5.3.4.

D.2.3 Threat Integration (TI)

TI fuses the BAE and TE, producing a Situational Overlay and Named Areas of Interest, that drive the required security monitoring on a network, and provides a framework for the commander's decision-making. It includes elements of Stage 4 - 'Attack Options Analysis', Stage 6 - 'Security Monitoring', and Stage 7 - 'Incident Response Planning', described in Sections 5.3.4, 5.3.6, and 5.3.7 respectively.

Appendix E

Questions from June 2017 TTX

Contents

E.1 Introduction

The following questions, and the associated guideline narrative, were developed for use in the TTX described in Section 7.5.3 and illustrated in Figure 7.5.

E.2 TTX Questions

1. What is the extent of the incident?

1.1.1 Which customers have been affected? The incident response process should include procedures to determine which customer data has been exfiltrated. At worst, the security policy should highlight where customer data is held and describe how access to the data is achieved. For replicas of customer data the policy should describe which subsets of data are held what subset of data is held. Therefore, at worst, they should be able to list the list of potentially impacted customers from this data.

1.1.2 Which staff will undertake the analysis of the extent of the incident? This should be described in the incident response plan.

1.2.1 Does a documented process exist to determine the extent of the incident? Linked to 1.1.1, this should be part of the incident response plan.

1.2.2 Has the process been rehearsed or exercised? Requires documentary of evidence of testing of the incident response plan and evaluation metrics.

1.2.3 How long will it take to determine the extent of the incident? The incident response plan should include manpower resources and allow an evaluation of time required based on potentially impacted systems.

1.3.1 Which sensors, mechanisms or logs will determine the affected systems? Security documentation and network architecture documentation should describe where sensors are located, what they are recording, and where these data are held.

1.3.2 Which data repositories have been affected? Linked to 1.1.1, but looks beyond just customer data. The same guidelines apply as in 1.1.1.

1.4.1 What data has been exfiltrated? Linked to 1.1.1 and 1.3.2, and refers to the entirety of information exfiltrated. The same guidelines apply as in 1.1.1.

1.4.2 What forensic data is available for investigation? 1.3.1 describes the mechanisms for monitoring affected system. This question refers to how long the logs are maintained, whether they are alterable, and whether they support Association of Chief Police Officers of England, Wales & Northern Ireland (**ACPO!**) guidelines. This should be described in the security policy.

1.4.3 Does the published customer information match the data held in corporate repositories? The incident response process should include an assessment of any published customer data to determine whether it is a) accurate, and b) from the repository it has been assessed it was exfiltrated from.

1.5.1 Has any DPA sensitive data been exfiltrated? The security policy should describe where data that is sensitive within the description of the Data Protection Act (DPA) is held. An assessment based on the results of 1.3.2 can determine whether sensitive data has been leaked.

1.5.2 Is there a resulting risk to personal safety, or, of fraud? The incident response plan should include an assessment of impact of the data loss to customers.

2. How will the incident be contained?

2.1.1 Who are the members of the technical incident response team? The incident response plan should identify those personnel who are suitably qualified and experienced to undertake incident response activities, and in which capacity.

2.1.2 What training have the technical incident responders received? Linked to 2.1.1, a training needs analysis should have been conducted to identify skills gaps in the incident response team.

2.2.1 Does a documented incident response containment process exist? The incident response plan should contain processes to contain the incident prior to remediation.

2.2.2 Are critical systems identified, prioritised, and documented, including policies on permissible downtime? The business continuity plan should identify, prioritise and describe critical systems, guidelines for system modification during an incident, and permissible downtime.

2.2.3 What service levels apply during an incident? The business continuity plan should include changes to acceptable service levels during an incident.

2.3.1 Which systems or tools will be used to prevent further data exfiltration? The incident response plan should have guidelines on which systems and tools are authorised to be deployed during an incident.

2.3.2 How will persistent malware be identified across the corporate technology infrastructure? The incident response plan should include processes to identify malware propagation across the enterprise.

2.4.1 How will access to the data repositories be limited during the incident response? The business continuity plan and incident response plan should describe the minimum available service levels for data, including reversionary modes, to ensure further data is not exfiltrated during the containment phase.

2.5.1 To what standards does the incident response process comply? Examples include ISO 22320 - Specifies requirements for incident response. ISO 22399 - Provides generic guidelines that organisations can follow in order to develop their own management system to ensure incident preparedness and operational continuity. ISO 27035 - Details a best practice approach to information security incident management.

3. How will the incident be remediated?

3.1.1 What is the required recovery effort? The incident response plan should contain a view on what size incidents it can resource an incident response team internally, and when external resources are required.

3.1.2 How are technical personnel split across the investigation, containment and remediation functions? The incident response plan should not over-allocate roles to technical personnel.

3.2.1 How does the incident response process guide incident remediation? The incident response plan should include guidelines to assist the responders to contain and remediate the situation.

3.2.2 How does the incident response process determine if the organisation remains vulnerable to the same attack? The incident response plan should include guidelines to ascertain how the attack was achieved, and steps to determine whether the attack paths are still exposed.

3.2.3 How will the affected systems be restored to a known state? The business continuity plan should include approved procedures to restore systems to a known state, and include any cross-system synchronisation activities that are required.

3.3.1 Which tools are available to analyse the logs? The incident response plan should describe how to access the system and network logs, and which tools should be used.

3.3.2 Are stand-by servers and devices available to provide operational continuity whilst affected equipment is investigated? The business continuity plan should describe which stand-by devices are available for which systems and data repositories in order to maintain service levels, particularly if systems need to be taken offline for forensic examination.

3.4.1 What metrics are captured during an incident response to measure the effectiveness of the processes and teams? The incident response plan should include performance metrics and KPI.

3.5.1 How will the remediated systems be assessed for compliance to standards the organisation is required to comply with (e.g. PCI-DSS)? The business continuity plan should describe to which standards systems should be restored to, and where recertification may be required as a consequence.

4. How did the incident occur?

4.1.1 Was the attacker operating remotely, or was it an insider? The incident response plan should investigate how the attack was achieved, this should include not only remote attacks, but the insider threat, and threats from the supply chain.

4.2.1 Does the incident response process include steps to determine methods used to access and compromise the data repository? The incident response plan should include steps to analyse how access to data repositories was achieved.

4.2.2 Does a log retention policy exist? The security policy should state how longs will be retained for, to support forensic analysis of incidents on the network that may have been initiated in the past.

4.3.1 Are the clocks across the corporate technology infrastructure synchronised to provide consistent timestamps for forensic analysis? The security policy should require all clocks to be synchronised to a common time source.

4.4.1 Does the data in logs record querying of corporate data repositories? Access to key critical information assets should be logged. The security policy should state which accesses to the critical data repositories are logged for forensic examination.

4.4.2 Would the data exfiltration show up in any network traffic logs? The security policy should guide the deployment of sensors to identify data exfiltration.

4.5.1 Which external organisations should be informed of the incident? Does the incident response plan specify who needs to be informed about incidents, and in what time timescale?

Bibliography

[1] Adam J Epstein. Thinking strategically about cyber risk. *NACD Directorship Journal, pp. 40(5), 32.*, pages 32–35, 2014.

[2] The White House. Executive order - improving critical infrastructure cybersecurity. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity, February 2013. Accessed 1 July 2018.

[3] Keith Stouffer, Joe Falco, and Karen Scarfone. Guide to industrial control systems (ICS) security. *NIST special publication*, pages 800–82, 2011.

[4] Javier Lopez, Cristina Alcaraz, and Rodrigo Roman. Smart control of operational threats in control substations. *Computers & Security*, 38:14–27, 2013.

[5] Wei Gao and Thomas H Morris. On cyber attacks and signature based intrusion detection for MODBUS based industrial control systems. *Journal of Digital Forensics, Security and Law*, 9(1):37–56, 2014.

[6] Robert Mitchell and Ing-Ray Chen. A survey of intrusion detection techniques for cyber-physical systems. *ACM Computing Surveys (CSUR)*, 46(4):55, 2014.

[7] Thomas Dübendorfer, Arno Wagner, and Bernhard Plattner. An economic damage model for large-scale internet attacks. In *Enabling Technologies: Infrastructure for Collaborative Enterprises, 2004. WET ICE 2004. 13th IEEE International Workshops on*, pages 223–228. IEEE, 2004.

[8] J Mitchell, C Clarke, J Shaffer, J Su, P Chen, S Kuroda, S Smith, and B Savaris. Global industrial automation. *Credit Suisse Equity Research Report (research-doc.credit-suisse.com)*, August 2012.

[9] ICS-CERT. ICS-CERT Year in Review - 2012. https://ics-cert.us-cert.gov/ICS-CERT-Year-Review-2012, Accessed 1 July 2018, 2012.

[10] ICS-CERT. ICS-CERT Monitor November/December 2015. *ICS-CERT Monitor (US Department of Homeland Security)*, January 2016.

[11] Martin Naedele. Addressing IT security for critical control systems. In *40th Annual Hawaii International Conference on System Sciences*. IEEE, 2007.

[12] Paul R Garvey and Susmit H Patel. Analytical frameworks to assess the effectiveness and economic-returns of cybersecurity investments. In *Military Communications Conference (MILCOM), 2014 IEEE*, pages 136–145. IEEE, 2014.

[13] Lloyds and The University of Cambridge Centre for Risk Studies. Business Blackout: The insurance implications of a cyber attack on the US power grid. *Cambridge University Emerging Risk Report - 2015*, 2015.

[14] NERC. High-impact, low-frequency event risk to the north american bulk power system. *A Jointly-Commissioned Summary Report of the North American Electric Reliability Corporation and the U.S. Department of Energy's November 2009 Workshop*, 2010.

[15] Dan McWhorter. APT1: Exposing one of China's cyber espionage units. *Mandiant Corporation*, 2013. https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf, Accessed 1 July 2018.

[16] Costis Toregas and Nicolas Zahn. Insurance for cyber attacks: The issue of setting premiums in context. *George Washington University (Report GW-CSPRI-2014-1)*, 2014.

[17] Christian Biener, Martin Eling, and Jan Hendrik Wirfs. Insurability of cyber risk: An empirical analysis. *The Geneva Papers on Risk and Insurance Issues and Practice*, 40(1):131–158, 2015.

[18] Jim Blythe and L Jean Camp. Implementing mental models. In *Security and privacy workshops (SPW), 2012 IEEE symposium*, pages 86–90. IEEE, 2012.

[19] Anthony D Miyazaki and Ana Fernandez. Consumer perceptions of privacy and security risks for online shopping. *Journal of Consumer affairs*, 35(1):27–44, 2001.

[20] Nicola Davinson and Elizabeth Sillence. It won't happen to me: Promoting secure behaviour among internet users. *Computers in Human Behavior*, 26(6):1739–1747, 2010.

[21] Paul Barford, Marc Dacier, Thomas G Dietterich, Matt Fredrikson, Jon Giffin, Sushil Jajodia, Somesh Jha, Jason Li, Peng Liu, Peng Ning, et al. Cyber SA: Situational awareness for cyber defense. In *Cyber Situational Awareness*, pages 3–13. Springer, 2010.

[22] Jill Jesson, Lydia Matheson, and Fiona M Lacey. *Doing your literature review: Traditional and systematic techniques.* Sage, 2011.

[23] Barbara Kitchenham, Pearl Brereton, Zhi Li, David Budgen, and Andrew Burn. Repeatability of systematic literature reviews. In *Evaluation & Assessment in Software Engineering (EASE 2011), 15th Annual Conference on*, pages 46–55. IET, 2011.

[24] Chris W Johnson, Rob Harkness, and Maria Evangelopoulou. Forensic Attacks Analysis and the Cyber Security of Safety-Critical Industrial Control Systems. In *34th International System Safety Conference, Orlanda, FL, USA, 8-12 Aug 2016,*, 2016.

[25] Chris W Johnson, Maria Evangelopoulou, and Tanya Pavlova. Applying Lessons from Cyber Attacks on Ukrainian Infrastructures to Secure Gateways onto the Industrial Internet of Things. In *Proceedings 35th International System Safety Conference, Albuquerque, NM, USA, 21-25 Aug 2017*, 2017.

[26] Eric D Knapp and Joel Thomas Langill. *Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems.* Syngress, 2014.

[27] Cristina Alcaraz, Gerardo Fernandez, and Fernando Carvajal. Security aspects of SCADA and DCS environments. In *Critical Infrastructure Protection*, pages 120–149. Springer, 2012.

[28] Igor Nai Fovino, Marcelo Masera, Michele Guglielmi, Andrea Carcano, and Alberto Trombetta. Distributed intrusion detection system for SCADA protocols. In *Critical Infrastructure Protection IV*, pages 95–110. Springer, 2010.

[29] Teodor Sommestad, Goran N. Ericsson, and Jakob Nordlander. SCADA system cyber security - a comparison of standards. *Power and Energy Society General Meeting, 2010 IEEE*, 2010.

[30] Brendan Galloway and Gerhard P Hancke. Introduction to industrial control networks. *Communications Surveys & Tutorials, IEEE*, 15(2):860–880, 2013.

[31] Peter Neumann. Communication in industrial automation - what is going on? *Control Engineering Practice 15*, 15(11):1332–1347, 2007.

[32] A Pauna, K Moulinos, M Lakka, J May, and T Tryfonas. Can we learn from scada security incidents? *White Paper, European Union Agency for Network and Information Security (ENISA), Heraklion, Crete, Greece*, 2013.

[33] Matthew Luallen. Breaches on the Rise in Control Systems: A SANS Survey. April 2014. https://ics.sans.org/media/sans-ics-security-survey-2014.pdf, Accessed 1 July 2018.

[34] Bonnie Zhu, Anthony Joseph, and Shankar Sastry. A taxonomy of cyber attacks on SCADA systems. In *Internet of things (iThings/CPSCom), 2011, 4th international conference on cyber, physical and social computing*, pages 380–388. IEEE, 2011.

[35] Theodore J Williams. *A Reference Model for Computer Integrated Manufacturing (CIM): A Description from the Viewpoint of Industrial Automation: Prepared by CIM Reference Model Committee International Purdue Workshop on Industrial Computer Systems.* Instrument Society of America, 1991.

[36] Kelli England Will and E Scott Geller. Increasing the safety of children's vehicle travel: from effective risk communication to behavior change. *Journal of safety research*, 35(3):263–274, 2004.

[37] B Batke and P Didier. The importance of reference architectures in manufacturing networks. In *CIP Networks Conference*, 2007.

[38] Paul Didier, Fernando Macias, James Harstad, Rick Antholine, Scott A Johnston, Sabina Piyevsky, Mark Schillace, Gregory Wilcox, Dan Zaniewski, and S Zuponcic. Converged plantwide Ethernet (CPwE) design and implementation guide. *CISCO Systems and Rockwell Automation*, pages 252–253, 2011.

[39] DHS. Recommended practice: Improving industrial control systems cybersecurity with defense-in-depth strategies. https://ics-cert.us-cert.gov, October 2009. Accessed 1 July 2018.

[40] CockpitCI Consortium. Cybersecurity on SCADA: risk prediction, analysis and reaction tools for critical infrastructures. *European Union Community Research and Development Information Service*, 2011.

[41] DA van de Wouw. Knowledge needed to develop malware to infect and impact industrial control systems. *MSc Thesis, Technische Universiteit Eindhoven*, 2013.

[42] Niv Goldenberg and Avishai Wool. Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems. *International Journal of Critical Infrastructure Protection*, 6(2):63–75, 2013.

[43] Ken Curtis. A DNP3 protocol primer. *DNP User Group*, pages 1–8, 2005. https://www.dnp.org, Accessed 1 July 2018.

[44] Samuel East, Jonathan Butts, Mauricio Papa, and Sujeet Shenoi. A taxonomy of attacks on the DNP3 protocol. In *Critical Infrastructure Protection*, volume 3. Springer, 2009.

[45] E Byres and TJ Burke. Securing Your OPC Classic Control System. https://www.tofinosecurity.com/professional/securing-your-opc-classic-control-system, 2010. Accessed 1 July 2018.

[46] Nicholas B Carr. *Development of a tailored methodology and forensic toolkit for industrial control systems incident response.* PhD thesis, Monterey, California: Naval Postgraduate School, 2014.

[47] E Byres and D Pederson. Understanding OPC and How it is Deployed. ics-cert.us-cert.gov, 2007. Accessed 1 July 2018.

[48] Alan Calder. *Implementing Information Security based on ISO 27001/ISO 27002.* Van Haren, 2011. ISBN:9087535414 9789087535414.

[49] ICS-CERT. ICS-CERT Monitor October, November, December 2013. https://ics-cert.us-cert.gov/monitors/ICS-MM201312, 2013. Accessed 1 July 2018.

[50] E Byres and D Pederson. Hardening Guidelines for OPC Hosts. ics-cert.us-cert.gov, 2007. Accessed 1 July 2018.

[51] Vladimír Modrák. Integration of MES and ERP. *Encyclopedia of Information Science and Technology, Second Edition, IGI Global*, 2009.

[52] Evgeny Lebanidze. Guide to developing a cyber security and risk mitigation plan. *National Rural Electric Cooperative Association*, 2011. https://www.smartgrid.gov/files/CyberSecurityGuideforanElectricCooperativeV11-21.pdf, Accessed 1 July 2018.

[53] Rafael RR Barbosa, Ramin Sadre, and Aiko Pras. Difficulties in modeling SCADA traffic: a comparative analysis. In *Passive and Active Measurement*, pages 126–135. Springer, 2012.

[54] Rafael Ramos Regis Barbosa, Ramin Sadre, and Aiko Pras. Towards periodicity based anomaly detection in SCADA networks. In *Emerging Technologies & Factory Automation (ETFA), 2012 IEEE 17th Conference on*. IEEE Industrial Electronics Society, 2012.

[55] Yi Yang, Keiran McLaughlin, Sakir Sezer, Tim Littler, Eul Gyu Im, Bernardi Pranggono, and HF Wang. Multiattribute SCADA-specific intrusion detection system for power networks. *IEEE Transactions on Power Delivery*, 29(3):1092–1102, 2014.

[56] Dina Hadžiosmanović, Damiano Bolzoni, and Pieter H Hartel. A log mining approach for process monitoring in SCADA. *International Journal of Information Security, Springer*, 11(4):231–251, 2012.

[57] Amit Kleinmann and Avishai Wool. Accurate modeling of the Siemens S7 SCADA protocol for intrusion detection and digital forensic. *Journal of Digital Forensics, Security and Law*, 9(2):37–50, 2014.

[58] Thomas Morris and Kalyan Pavurapu. A retrofit network transaction data logger and intrusion detection system for transmission and distribution substations. In *Power and Energy (PECon), 2010 IEEE International Conference on*, pages 958–963. IEEE, 2010.

[59] ICS-CERT. ICS-CERT Incident Response Summary Report 2009-2011. *ics-cert.us-cert.gov*, 2011. Accessed 1 July 2018.

[60] Adnan Anwar and Abdun Naser Mahmood. Cyber security of smart grid infrastructure. *The State of the Art in Intrusion Prevention and Detection, CRC Press, Taylor & Francis Group, pp. 449-472*, 2014.

[61] Terry Fleury, Himanshu Khurana, and Von Welch. Towards a taxonomy of attacks against energy control systems. In *Critical Infrastructure Protection*, pages 71–85. Springer, 2008.

[62] Bri Rolston. Security Implications of OPC, OLE, DCOM, and RPC in Control Systems. *Idaho National Laboratory Retrieved from http://www.inl.gov/technicalpublications/Documents/3494180.pdf*, 2006.

[63] E Byres and D Pederson. OPC Security White Paper 2 OPC Exposed. https://www.tofinosecurity.com/professional/opc-security-white-paper-2-opc-exposed, 2007. Accessed 1 July 2018.

[64] Iñaki Garitano, Roberto Uribeetxeberria, and Urko Zurutuza. A review of scada anomaly detection systems. In *Soft Computing Models in Industrial and Environmental Applications, 6th International Conference SOCO 2011*, pages 357–366. Springer, 2011.

[65] Otis Alexander, Hagen Lauer, Nicolai Kuntze, and Michael Jager. Enhancing intrusion detection in substation networks. In *2014 ASE BIg Data/Social Com/-Cybersecurity Conference, Stanford University, May 27-31, 2014*. Academy of Science and Engineering, 2014.

[66] Wei Gao, Reaves Bradley Morris, Thomas, and Drew Richey. On SCADA control system command and response injection and intrusion detection. In *Proceedings of 2010 IEEE eCrime Researchers Summit*, 2010.

[67] Robert Koch. Towards next-generation intrusion detection. In *Cyber Conflict (ICCC), 2011 3rd International Conference on*, pages 1–18. IEEE, 2011.

[68] Robert Mitchell and Ray Chen. Behavior-rule based intrusion detection systems for safety critical smart grid applications. *Smart Grid, IEEE Transactions on*, 4(3):1254–1263, 2013.

[69] A Pauna and K Moulinos. Windows of exposure... a real problem for SCADA systems. Technical report, Technical report, ENISA, 2013. https://www.enisa.europa.eu/publications/window-of-exposure-a-real-problem-for-scada-systems, Accessed 1 July 2018.

[70] Thomas Morris, Rayford Vaughn, and Yoginder Dandass. A retrofit network intrusion detection system for MODBUS RTU and ASCII industrial control systems. In *System Science (HICSS), 2012 45th Hawaii International Conference on*, pages 2338–2345. IEEE, 2012.

[71] Ryan Shayto, Brian Porter, Rodrigo Chandia, Mauricio Papa, and Sujeet Shenoi. Assessing the integrity of field devices in modbus networks. In *Critical Infrastructure Protection II*, pages 115–128. Springer, 2008.

[72] Pierre Kobes. Security Levels in ISA-99 / IEC 62443. https://www.scribd.com/document/129590220/ISA-99-Security-Levels-Proposal, 2012. Accessed 1 July 2018.

[73] CPNI. Cyber security assessments of industrial control systems. *CPNI*, 2011. https://www.ccn-cert.cni.es/publico/InfraestructurasCriticaspublico/CPNI-Guia-SCI.pdf, Accessed 1 July 2018.

[74] Stanley Kaplan and B John Garrick. On the quantitative definition of risk. *Risk analysis*, 1(1):11–27, 1981.

[75] Daniel Bernoulli. Exposition of a new theory on the measurement of risk. *Econometrica: Journal of the Econometric Society*, pages 23–36, 1954.

[76] Ted G Lewis. *Critical infrastructure protection in homeland security: defending a networked nation.* John Wiley & Sons, 2014.

[77] Enrico Zio, Piero Baraldi, Roger Flage, et al. *Uncertainty in Risk Assessment: The Representation and Treatment of Uncertainties by Probabilistic and Non-probabilistic Methods.* John Wiley & Sons, 2013.

[78] Norman Fenton and Martin Neil. *Risk assessment and decision analysis with Bayesian networks.* CRC Press, 2012.

[79] National Research Council. *Review of the Department of Homeland Security's Approach to Risk Analysis.* The National Academies Press, 2010.

[80] Donald Rumsfeld. US DoD News Briefing. https://www.youtube.com/watch?v=GiPe1OiKQuk, February 2002. Accessed 1 July 2018.

[81] Lee T Ostrom and Cheryl A Wilhelmsen. *Risk assessment: tools, techniques, and their applications.* John Wiley & Sons, 2012.

[82] George Apostolakis. Probabilistic Risk Assessment (PRA). *Wiley Handbook of Science and Technology for Homeland Security, Volume 1*, 2010.

[83] George E Apostolakis. How useful is quantitative risk assessment? *Risk analysis*, 24(3):515–520, 2004.

[84] Tingting Li and Chris Hankin. Effective defence against zero-day exploits using bayesian networks. In *International Conference on Critical Information Infrastructures Security*, pages 123–136. Springer, 2016.

[85] Kailash C Kapur and Michael Pecht. *Reliability engineering.* John Wiley & Sons, 2014.

[86] Robin L Dillon-Merrill, Gregory S Parnell, and Donald L Buckshaw. Logic trees: Fault, success, attack, event, probability, and decision trees. *Wiley Handbook of Science and Technology for Homeland Security*, 2008.

[87] Ian Sutton. *Process risk and reliability management: operational integrity management.* Gulf Professional Publishing, 2014.

[88] Bruce Schneier. Attack trees. *Dr. Dobbs journal*, 24(12):21–29, 1999.

[89] Oliver Ibe. *Markov processes for stochastic modeling.* Newnes, 2013.

[90] Christopher M Schnaubelt, Eric B Larson, and Matthew E Boyer. *Vulnerability Assessment Method Pocket Guide.* RAND Corporation, 2014.

[91] Anna M Doro-on. *Risk Assessment and Security for Pipelines, Tunnels, and Underground Rail and Transit Operations.* CRC Press, 2014.

[92] Ake J Holmgren, Erik Jenelius, and Jonas Westin. Evaluating strategies for defending electric power networks against antagonistic attacks. *IEEE Transactions on Power Systems*, 22(1):76–84, 2007.

[93] Andrew Fielder, Emmanouil Panaousis, Pasquale Malacaria, Chris Hankin, and Fabrizio Smeraldi. Decision support approaches for cyber security investment. *Decision Support Systems*, 86:13–23, 2016.

[94] Sankardas Roy, Charles Ellis, Sajjan Shiva, Dipankar Dasgupta, Vivek Shandilya, and Qishi Wu. A survey of game theory as applied to network security. In *System Sciences (HICSS), 2010 43rd Hawaii International Conference on*, pages 1–10. IEEE, 2010.

[95] Louis Anthony Tony Cox Jr. Making decisions without trustworthy risk models. *Breakthroughs in Decision Science and Risk Analysis*, page 189, 2015.

[96] Barry Charles Ezell, Steven P Bennett, Detlof Von Winterfeldt, John Sokolowski, and Andrew J Collins. Probabilistic risk analysis and terrorism risk. *Risk Analysis*, 30(4):575–589, 2010.

[97] Thomas S Wallsten and David V Budescu. State of the art encoding subjective probabilities: A psychological and psychometric review. *Management Science*, 29(2):151–173, 1983.

[98] Jason Merrick, Philip Leclerc, Hristo Trenkov, and Robert Olsen. Outthinking the terrorists. *Breakthroughs in Decision Science and Risk Analysis*, page 287, 2015.

[99] Gideon Keren. On the calibration of probability judgments: Some critical comments and alternative perspectives. In *Conference on Subjective Probability, Utility and Decision Making: Overconfidence: Sources, implications, and solutions., Aug, 1995, Jerusalem, Israel.* John Wiley & Sons, 1997.

[100] Steven Hora. Eliciting probabilities from experts. *Advances in decision analysis: From foundations to applications, Cambridge Press*, page 129, 2007.

[101] Handanhal V Ravinder, Don N Kleinmuntz, and James S Dyer. The reliability of subjective probabilities obtained through decomposition. *Management Science*, 34(2):186–199, 1988.

[102] Ronald A Howard. Knowledge maps. *Management science*, 35(8):903–922, 1989.

[103] Teodor Sommestad, Mathias Ekstedt, and Lars Nordstrom. Modeling security of power communication systems using defense graphs and influence diagrams. *IEEE Transactions on Power Delivery*, 24(4):1801–1808, 2009.

[104] D McMorrow. Rare events. Technical report, MITRE Corporation, 2009. https://fas.org/irp/agency/dod/jason/rare.pdf, Accessed 1 July 2018.

[105] Tyson Macaulay and Bryan L Singer. *Cybersecurity for industrial control systems: SCADA, DCS, PLC, HMI, and SIS.* CRC Press, 2011.

[106] Teodor Sommestad and Jonas Hallberg. Cyber security exercises and competitions as a platform for cyber security experiments. In *Nordic Conference on Secure IT Systems*, pages 47–60. Springer, 2012.

[107] Marina Krotofil and Jason Larsen. Rocking the pocket book: Hacking chemical plants. *Black Hat USA*, 2015. https://www.blackhat.com/docs/us-15/materials/us-15-Krotofil-Rocking-The-Pocket-Book-Hacking-Chemical-Plant-For-Competition-And-Extortion-wp.pdf, Accessed 1 July 2018.

[108] Lynne Coventry, Pamela Briggs, John Blythe, and Minh Tran. Using behavioural insights to improve the public's use of cyber security best practices. *UK Government Office for Science*, 2014. https://assets.publishing.service.gov.uk, Accessed 1 July 2018.

[109] Tom van Dijk, Ton Spil, Sanne van der Burg, Ivo Wenzler, and Simon Dalmolen. Present or play: The effect of serious gaming on demonstrated behaviour. *International Journal of Game-Based Learning (IJGBL)*, 5(2):55–69, 2015.

[110] David Gouveia, Duarte Lopes, and Carlos Vaz De Carvalho. Serious gaming for experiential learning. In *2011 Frontiers in Education Conference (FIE)*, pages T2G–1. IEEE, 2011.

[111] David A Kolb. *Experiential learning: Experience as the source of learning and development.* Prentice Hall, 1984.

[112] Michael Zyda. From visual simulation to virtual reality to games. *Computer*, 38(9):25–32, 2005.

[113] David Crookall. Serious games, debriefing, and simulation/gaming as a discipline. *Simulation & gaming*, 41(6):898–920, 2010.

[114] Thomas M Connolly, Elizabeth A Boyle, Ewan MacArthur, Thomas Hainey, and James M Boyle. A systematic literature review of empirical evidence on computer games and serious games. *Computers & Education*, 59(2):661–686, 2012.

[115] Katherine A Wilson, Wendy L Bedwell, Elizabeth H Lazzara, Eduardo Salas, C Shawn Burke, Jamie L Estock, Kara L Orvis, and Curtis Conkey. Relationships

between game attributes and learning outcomes review and research proposals. *Simulation & gaming*, 40(2):217–266, 2009.

[116] Martin Fishbein and Icek Ajzen. Belief, attitude, intention, and behavior: An introduction to theory and research. 1977.

[117] Icek Ajzen. Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior. *Journal of Applied Social Psychology*, 32(4):665–683, 2002.

[118] Kathryn O'Reilly, Sigi Goode, and Dennis Hart. Exploring mobile commerce intention: Evidence from australia. In *2010 10th International Symposium on Communications and Information Technologies*, 2010.

[119] Anthony Caldwell and John McGarvey. Modeling user behaviour in response to cyberthreats. In *Signals and Systems Conference (ISSC 2013), 24th IET Irish*, pages 1–7. IET, 2013.

[120] Dezhi Wu, Paul Benjamin Lowry, and Dongsong Zhang. Patient compliance behavior in a mobile healthcare system: An integration of theories of rational choice and planned behavior. In *System Sciences (HICSS), 2015 48th Hawaii International Conference on*, pages 2976–2984. IEEE, 2015.

[121] Ronald W Rogers. A protection motivation theory of fear appeals and attitude change1. *The journal of psychology*, 91(1):93–114, 1975.

[122] Catherine L Anderson and Ritu Agarwal. Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. *Mis Quarterly*, 34(3):613–643, 2010.

[123] Tapiwa Gundu and Stephen V Flowerday. The enemy within: A behavioural intention model and an information security awareness process. In *2012 Information Security for South Africa*, pages 1–8. IEEE, 2012.

[124] Kim Witte. Putting the fear back into fear appeals: The extended parallel process model. *Communications Monographs*, 59(4):329–349, 1992.

[125] Wolfgang Donsbach. *The concise encyclopedia of communication.* John Wiley & Sons, 2015.

[126] Kim Witte. Fear as motivator, fear as inhibitor: Using the extended parallel process model to explain fear appeal successes and failures. *Handbook of Communication and Emotion Research, Theory, Applications, and Contexts, pages 423-450*, 1998.

[127] Michael D Basil. Effects of social marketing. *The International Encyclopedia of Media Studies*, 2013.

[128] Punam Anand Keller and Lauren Goldberg Block. Increasing the persuasiveness of fear appeals: The effect of arousal and elaboration. *Journal of consumer research*, 22(4):448–459, 1996.

[129] Harry Mills. *Artful persuasion: How to command attention, change minds, and influence people.* AMACOM Div American Mgmt Assn, 2000.

[130] Zack Hiwiller. *Players Making Decisions: Game Design Essentials and the Art of Understanding Your Players.* New Riders, 2015.

[131] Barry Schwartz. The paradox of choice. Ecco New York, 2004.

[132] Brian Burke. *Gamify: How gamification motivates people to do extraordinary things.* Bibliomotion, Inc., 2014.

[133] Lloyd P Rieber. Seriously considering play: Designing interactive learning environments based on the blending of microworlds, simulations, and games. *Educational technology research and development*, 44(2):43–58, 1996.

[134] Susan Weinschenk. *How to get people to do stuff: Master the art and science of persuasion and motivation.* New Riders, 2013.

[135] Michael F Thompson and Cynthia E Irvine. CyberCIEGE scenario design and implementation. In *3GSE*, 2014.

[136] Austin Silva, Jonathan McClain, Theodore Reed, Benjamin Anderson, Kevin Nauer, Robert Abbott, and Chris Forsythe. Factors impacting performance in competitive cyber exercises. In *Proceedings of the Interservice/Interagency Training, Simulation and Education Conference, Orlando FL*, 2014.

[137] Jonathan McClain, Austin Silva, Glory Emmanuel, Benjamin Anderson, Kevin Nauer, Robert Abbott, and Chris Forsythe. Human performance factors in cyber security forensic analysis. *Procedia Manufacturing*, 3:5301–5307, 2015.

[138] Austin Silva, Glory Emmanuel, Jonathan T McClain, Laura Matzen, and Chris Forsythe. Measuring expert and novice performance within computer security incident response teams. In *International Conference on Augmented Cognition*, pages 144–152. Springer, 2015.

[139] Sanjeev Kumar Punia, Anuj Kumar, and Kuldeep Malik. Software development risk management using ooda loop. *Int. Journal of Engineering Research and General Science*, 2(6), 2014.

[140] Richard Kissel. Glossary of key information security terms. *NIST Interagency Reports NIST IR*, 7298(3), 2013.

[141] T Rundmo and AR Hale. Managers' attitudes towards safety and accident prevention. *Safety science*, 41(7):557–574, 2003.

[142] PP Morita and CM Burns. Situation awareness and risk management understanding the notification issues. *Studies in health technology and informatics*, 164:372–376, 2010.

[143] Joel Brynielsson, Ulrik Franke, and Stefan Varga. Cyber situational awareness testing. In *Combatting Cybercrime and Cyberterrorism*, pages 209–233. Springer, 2016.

[144] Eric Cole. *Advanced persistent threat: understanding the danger and how to protect your organization*. Newnes, 2012.

[145] Anne Koskinen-Kannisto et al. Situational awareness concept in a multinational collaboration environment: challenges in the information sharing framework. *Series 1, n: o 31*, 2013.

[146] John C Johnston, Bruce C Leibrecht, Leonard D Holder, Robert S Coffey, and Kathleen A Quinkert. Training for future operations: Digital leaders' transformation insights. Technical report, TRW Systems Fairfax VA, 2003.

[147] Mica R Endsley. Toward a theory of situation awareness in dynamic systems. *Human Factors*, 37(1):32–64, 1995.

[148] Mica R Endsley and DJ Garland. Theoretical underpinnings of situation awareness: A critical review. *Situation awareness analysis and measurement*, pages 3–32, 2000.

[149] John E Mathieu, Tonia S Heffner, Gerald F Goodwin, Eduardo Salas, and Janis A Cannon-Bowers. The influence of shared mental models on team process and performance. *Journal of applied psychology*, 85(2):273, 2000.

[150] Marcus G Dudley, John C Johnston, William S Jones, Christopher P Strauss, and Larry L Meliza. Making the transition from analog to digital warfighting: Changes in unit behavior and knowledge. Technical report, TRW Inc Fairfax VA Systems and Information Technology Group, 2001.

[151] Susannah J Whitney and Armando Vozzo. Recommendations for collective training for the battle management systems (dsto-tr-2685). Technical report, Australian Government Department of Defence, Land Operations Division, 2012.

[152] Brooke B Schaab and Franklin L Moses. Six myths about digital skills training. Technical report, Army Research Institute for the Behavioural and Social Sciences Alexandria, 2001.

[153] John Mathieu, M Travis Maynard, Tammy Rapp, and Lucy Gilson. Team effectiveness 1997-2007: A review of recent advancements and a glimpse into the future. *Journal of management*, 34(3):410–476, 2008.

[154] Richard C Deatz and Charlotte H Campbell. Application of cognitive principles in distributed computer-based training. Technical report, Human Resources Research Organization Alexandria VA, 2001.

[155] Victor-Valeriu Patriciu and Adrian Constantin Furtuna. Guide for designing cyber security exercises. In *Proceedings of the 8th WSEAS International Conference on E-Activities and information security and privacy*, pages 172–177. World Scientific and Engineering Academy and Society (WSEAS), 2009.

[156] BH Kim and C Goodall. Cyber exercise assessment handbook (aos-16-1170). Technical report, The Johns Hopkins University Applied Physics Laboratory, October 2016.

[157] Joel Brynielsson, Ulrik Franke, Muhammad Adnan Tariq, and Stefan Varga. Using cyber defense exercises to obtain additional data for attacker profiling. In *Intelligence and Security Informatics (ISI), 2016 IEEE Conference on*, pages 37–42. IEEE, 2016.

[158] Nina Wilhelmson and Thomas Svensson. *Handbook for planning, running and evaluating information technology and cyber security exercises.* The Swedish National Defence College, 2014.

[159] US Department of Homeland Security. National level exercise 2012: Cyber capabilities tabletop exercise. https://www.fema.gov/media-library/assets/documents/26845, May 2013. Accessed 31/08/2017.

[160] Heide Lukosch, Theo van Ruijven, and Alexander Verbraeck. The participatory design of a simulation training game. In *Proceedings of the winter simulation conference*, page 142. Winter Simulation Conference, 2012.

[161] Jonathan Pike and J Huddleston. Training needs analysis for team and collective training. *BAe Systems*, 2011. https://studylib.net/doc/8826934/training-needs-analysis-for-team-and-collective-training, Accesed 1 July 2018.

[162] ED Weinstein, EF Bates, MV Adler, and KS Gant. Guidance for a large tabletop exercise for a nuclear power plant. Technical report, Nuclear Regulatory Commission, Washington, DC (United States). Office for Analysis and Evaluation of Operational Data; Oak Ridge National Lab., TN (United States), 1995. https://www.osti.gov/servlets/purl/41401, Accessed 1 July 2018.

[163] Jason Kick. Cyber exercise playbook. Technical report, MITRE Corp Bedford MA, 2014. https://www.mitre.org/publications/technical-papers/cyber-exercise-playbook, Accessed 1 July 2018.

[164] Arjan J Lemmers, Bernd Rollesbroich, Timo Hartikainen, and Francisco J Carvajal. Evaluation of collective training in a distributed simulation exercise. Technical report, National Aerospace Lab Amsterdam (Netherlands), 2004. pdfs.semanticscholar.org/2c96/66102bf2138c427a7beabf46d29174543ab3.pdf, Accessed 1 July 2018.

[165] Erik Zipperer, Gerry Klein, Ray Fitzgerald, Henry Kinnison, and Scott E Graham. Training and training technology issues for the objective force warrior. Technical

report, Army Research Institute for the Behavioural and Social Sciences Fort Benning GA, 2003. http://www.dtic.mil/dtic/tr/fulltext/u2/a419873.pdf, Accessed 1 July 2018.

[166] William R Sanders. Collective staff training in a virtual learning environment. Technical report, Army Research Institute for the Behavioural Sciences Alexandria VA, 2002. http://www.au.af.mil/au/awc/awcgate/army/rr1788.pdf, Accessed 1 July 2018.

[167] Arniyati Ahmad, Christopher Johnson, and Timothy Storer. An investigation on organisation cyber resilience. *World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering*, 9(7):1703–1708, 2015.

[168] Steven Fulton, Dino Schweitzer, and Judson Dressler. What are we teaching in cyber competitions? In *Frontiers in Education Conference (FIE), 2012*, pages 1–5. IEEE, 2012.

[169] Eman Alashwali and Hanêne Ben-Abdallah. Design and evaluation of competition-based hacking exercises. In *Global Engineering Education Conference (EDUCON), 2015 IEEE*, pages 998–1007. IEEE, 2015.

[170] Art Conklin. Cyber defense competitions and information security education: An active learning solution for a capstone course. In *System Sciences, 2006. HICSS'06. Proceedings of the 39th Annual Hawaii International Conference on*, volume 9, pages 220b–220b. IEEE, 2006.

[171] Chris Eagle. Computer security competitions: Expanding educational outcomes. *IEEE Security & Privacy*, 11(4):69–71, 2013.

[172] Spyros Makridakis and Michele Hibon. The M3-Competition: results, conclusions and implications. *International journal of forecasting*, 16(4):451–476, 2000.

[173] Akbar Siami Namin, Zenaida Aguirre-Muñoz, and Keith S Jones. Teaching cyber security through competition: An experience report about a participatory training workshop. In *International Conference on Computer Science Education Innovation & Technology (CSEIT). Proceedings*, page 98. Global Science and Technology Forum, 2016.

[174] Raghu Raman, Sherin Sunny, Vipin Pavithran, and Krishnasree Achuthan. Framework for evaluating Capture the Flag (CTF) security competitions. In *Convergence of Technology (I2CT), 2014 International Conference for*, pages 1–5. IEEE, 2014.

[175] Adam Doupé, Manuel Egele, Benjamin Caillat, Gianluca Stringhini, Gorkem Yakin, Ali Zand, Ludovico Cavedon, and Giovanni Vigna. Hit'em where it hurts: a live security exercise on cyber situational awareness. In *Proceedings of the 27th Annual Computer Security Applications Conference*, pages 51–61. ACM, 2011.

[176] Brandon Mauer, William Stackpole, and Daryl Johnson. Developing small team-based cyber security exercises. In *Proceedings of the International Conference on Security and Management (SAM)*, page 1. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2012.

[177] Erik Trickel, Francesco Disperati, Eric Gustafson, Faezeh Kalantari, Mike Mabey, Naveen Tiwari, Yeganeh Safaei, Adam Doupé, and Giovanni Vigna. Shell We Play A Game? CTF-as-a-service for Security Education. In *2017 USENIX Workshop on Advances in Security Education*. USENIX Association, 2017.

[178] Matthew L Berninger. Developing standard exercises and statistics to measure the impact of cyber defenses. *Monterey, California: Naval Postgraduate School*, 2014.

[179] Susan Stevens-Adams, Armida Carbajal, Austin Silva, Kevin Nauer, Benjamin Anderson, Theodore Reed, and Chris Forsythe. Enhanced training for cyber situational awareness. In *International Conference on Augmented Cognition*, pages 90–99. Springer, 2013.

[180] Aunshul Rege, Brian Singer, Nicholas Masceri, and Quinn Heath. Measuring cyber intrusion chains, adaptive adversarial behavior, and group dynamics. In *ICMLG2017 5th International Conference on Management Leadership and Governance*, page 285. Academic Conferences and publishing limited, 2017.

[181] Kathleen A. Lee. CS2SAT: The Control Systems Cyber Security Self-Assessment Tool. Idaho National Laboratory (INL) (No. INL/CON-07-12810), 2008. https://inldigitallibrary.inl.gov/sites/sti/sti/3874554.pdf, Accessed 1 July 2018.

[182] DHS. Recommended practice: Developing an industrial control systems cybersecurity incident response capability. *US Department of Homeland Security*, October 2009. ics-cert.us-cert.gov, Accessed 1 Juluy 2018.

[183] Kyle Wilhoit. ICS, SCADA, and Non-Traditional Incident Response. Trend Micro, 2013. https://digital-forensics.sans.org, Accessed 1 July 2018.

[184] Jungsang Yoon, Stephen Dunlap, Jonathan Butts, Mason Rice, and Benjamin Ramsey. Evaluating the readiness of cyber first responders responsible for critical infrastructure protection. *International Journal of Critical Infrastructure Protection*, 13:19–27, 2016.

[185] Benjamin Aziz, Ali Malik, and Jeyong Jung. Check your blind spot: a new cyber-security metric for measuring incident response readiness. In *International Workshop on Risk Assessment and Risk-driven Testing*, pages 19–33. Springer, 2016.

[186] Deborah Bodeau and Richard Graubart. Intended effects of cyber resiliency techniques on adversary activities. In *Technologies for Homeland Security (HST), 2013 IEEE International Conference on*, pages 7–11. IEEE, 2013.

[187] Tetrick, L., E., Zaccaro, S. J., Dalal, R. S., Steinke, J. A., Repchick, K. M., Hargrove, A. K., Shore, D. B., Winslow, C. J., Chen, T. R., Green, J. P., Bolunmez, B., Tomassetti, A. J., McCausland, T. C., Fletcher, L., Sheng, Z., Schrader, S. W., Gorab, A. K., Niu, Q. & Wang, V. Improving social maturity of cybersecurity incident response teams. Technical report, Fairfax, VA: George Mason University., 2016. http://calctraining2015.weebly.com/the-handbook.html, Accessed 1 July 2018.

[188] Shari L Pfleeger. Improving Cybersecurity Incident Response Team (CSIRT) Skills, Dynamics and Effectiveness. Technical report, Trustees of Dartmouth College Hanover United States, 2017. http://www.dtic.mil/docs/citations/AD1027871, Accessed 1 July 2018.

[189] Peter Eden, Andrew Blyth, Pete Burnap, Yulia Cherdantseva, Kevin Jones, Hugh Soulsby, and Kristan Stoddart. A forensic taxonomy of SCADA systems and approach to incident response. In *Proceedings of the 3rd International Symposium for ICS & SCADA Cyber Security Research*, pages 42–51. British Computer Society, 2015.

[190] Sergio Caltagirone, Andrew Pendergast, and Christopher Betz. The diamond model of intrusion analysis. Technical report, DTIC Document, 2013. http://www.dtic.mil/docs/citations/ADA586960, Accessed 1 July 2018.

[191] Eric M Hutchins, Michael J Cloppert, and Rohan M Amin. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research*, 1:80, 2011.

[192] MJ Assante and RM Lee. The industrial control system cyber kill chain. *SANS Institute*, 2015. https://www.sans.org/reading-room/whitepapers/ICS/paper/36297, Accessed 1 July 2018.

[193] Robert Larkin, Juan Lopez, and Jonathan Butts. Evaluation of traditional security solutions in the SCADA environment. In *Proceedings of the 7th International Conference on Information Warfare and Security*, volume 399. Academic Conferences Limited, 2012.

[194] Scott Dynes. Emergent risks in critical infrastructures. In *Critical Infrastructure Protection II*, pages 3–16. Springer, 2008.

[195] Eric Byres. Using ANSI/ISA-99 standards to improve control system security. The Industrial Ethernet Book, 2014. https://www.tofinosecurity.com/professional/using-ansiisa-99-standards-improve-control-system-security-0, Accessed 1 July 2018.

[196] Allan Cook. MSc Thesis: An Assessment of the Application of Existing IT Security Mechanisms to Industrial Control Systems, Recommendations for Managing

Incident Response, and the Development of a Table-Top Learning Environment. De Montfort University, August 2015.

[197] Joseph Wolfe. The effectiveness of business games in strategic management course work. *Simulation & Gaming*, 28(4):360–376, 1997.

[198] Karl M Kapp. *The gamification of learning and instruction: game-based methods and strategies for training and education.* John Wiley & Sons, 2012.

[199] Glenn Fink, Daniel Best, David Manz, Viatcheslav Popovsky, and Barbara Endicott-Popovsky. Gamification for measuring cyber security situational awareness. In *Foundations of Augmented Cognition*, pages 656–665. Springer, 2013.

[200] K Boopathi, S Sreejith, and A Bithin. Learning cyber security through gamification. *Indian Journal of Science and Technology*, 8(7):642–649, 2015.

[201] ENISA. Trainings for cyber security specialists, https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/operational, 2016. Accessed 25 April 2016.

[202] Emmett J Vaughan and Therese Vaughan. *Fundamentals of risk and insurance, 11th edition.* John Wiley & Sons, 2013.

[203] Michael N Kahn. *Sentiment market analysis.* FTPress Delivers, 2010.

[204] Larry M Wortzel. *The dragon extends its reach: Chinese military power goes global.* Potomac Books, Inc., 2013.

[205] Martin C Libicki. *Cyberdeterrence and cyberwar.* Rand Corporation, 2009.

[206] Justin Menkes. *Executive intelligence.* Harper Collins, 2009.

[207] De Montfort University and CERT-UK. Meeting between De Montfort University and CERT-UK, November 2015.

[208] Robert B Cialdini. *Influence: Science and practice*, volume 4. Pearson Education Boston, 2009.

[209] SCIPS Evaluation Workshop. De Montfort University. 15th May 2015.

[210] SCIPS Evaluation Workshop. Imperial College, London. 29th June 2015.

[211] SCIPS Evaluation Workshop. Queen's University, Belfast. 23rd August 2016.

[212] Ralph Langner. To kill a centrifuge. *Langner Group*, 2013. https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf, Accessed 1 July 2018.

[213] Andrew Nicholson, Stuart Webber, Shaun Dyer, Tanuja Patel, and Helge Janicke. SCADA security in the light of cyber-warfare. *Computers & Security*, 31(4):418–436, 2012.

[214] Yulia Cherdantseva, Pete Burnap, Andrew Blyth, Peter Eden, Kevin Jones, Hugh Soulsby, and Kristan Stoddart. A review of cyber security risk assessment methods for SCADA systems. *computers & security*, 56:1–27, 2016.

[215] Andrew Fielder, Tingting Li, and Chris Hankin. Defense-in-depth vs. critical component defense for industrial control systems. In *4th International Symposium for ICS & SCADA Cyber Security Research 2016 (ICS-CSR 2016)*. BCS Learning & Development Ltd., 2016.

[216] C Velazquez. Detecting and preventing attacks earlier in the kill chain. *SANS Institute*, 2015. https://www.sans.org/reading-room/whitepapers/infosec/paper/36230, Accessed 1 July 2018.

[217] Alexandre C Dimian, Costin S Bildea, and Anton A Kiss. *Integrated design and simulation of chemical processes*, volume 13. Elsevier, 2014.

[218] Sara Taborda, Diego A Muñoz, and Hernan Alvarez. Snowball effect detection and control proposal for its correction. In *Control Applications (CCA), 2016 IEEE Conference on*, pages 1173–1178. IEEE, 2016.

[219] Ralph Langner. *Robust control system networks.* Momentum Press, 2011.

[220] Marina Krotofil and Alexander Isakov. Damn vulnerable chemical process. Black Hat Conference, 2014. https://www.researchgate.net, Accessed 1 July 2018.

[221] Babak Rooholahi and P Lokender Reddy. Concept and application of PID control and implementation of continuous PID Controller in Siemens PLCs. *Indian Journal of Science and Technology*, 8(35):1, 2015.

[222] Turan Gonen. *Electrical Power Transmission System Engineering: Analysis and Design.* CRC Press, 2011.

[223] Christian Brecher, Simon Müller, Thomas Breitbach, and Wolfram Lohse. Viable system model for manufacturing execution systems. *Procedia CIRP*, 7:461–466, 2013.

[224] Rafiullah Khan, Kieran McLaughlin, David Laverty, and Sakir Sezer. STRIDE-based threat modeling for cyber-physical systems. In *Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), 2017 IEEE PES*, pages 1–6. IEEE, 2017.

[225] Riccardo Scandariato, Kim Wuyts, and Wouter Joosen. A descriptive study of Microsoft's threat modeling technique. *Requirements Engineering*, 20(2):163–180, 2015.

[226] Craig S Fleisher and Babette E Bensoussan. *Business and competitive analysis: effective application of new and classic methods.* FT Press, 2015.

[227] Feng Xie, Yong Peng, Wei Zhao, Yang Gao, and Xuefeng Han. Evaluating industrial control devices security: Standards, technologies and challenges. In *IFIP International Conference on Computer Information Systems and Industrial Management*, pages 624–635. Springer, 2014.

[228] Xi Chen and Qi Li. Research on industrial control devices flaw discovery technology. In *International Conference on Advances in Mechanical Engineering and Industrial Informatics (AMEII 2015)*, 2015.

[229] Ali Abbasi and Majid Hashemi. Ghost in the PLC: Designing an undetectable programmable logic controller rootkit via pin control attack. In *Black Hat Europe (pp. 1-35). United Kingdom: Black Hat*. Black Hat, 2016.

[230] Cyber defence exercise, July 2016.

[231] J Vukalović and D Delija. Advanced persistent threats-detection and defense. In *Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2015 38th International Convention on*, pages 1324–1330. IEEE, 2015.

[232] Incident Response Collective Training Workshop, Wiltshire, UK, July 2017.

[233] Lisa M Given. *The Sage encyclopedia of qualitative research methods*. Sage Publications, 2008.

[234] Stephen D Lapan, MaryLynn T Quartaroli, and Frances J Riemer. *Qualitative research: An introduction to methods and designs*, volume 37. John Wiley & Sons, 2011.

[235] Sharan B Merriam and Elizabeth J Tisdell. *Qualitative research: A guide to design and implementation*. John Wiley & Sons, 2015.

[236] John W Creswell. *Qualitative inquiry and research design: Choosing among five traditions*. Sage Publications, Inc, 1998.

[237] Max van Manen. *Phenomenology of Practice: Meaning-Giving Methods in Phenomenological Research and Writing*, volume 13. Left Coast Press, 2014.

[238] Michael Q Patton. *Qualitative Research and Evaluation Methods*. Thousands Oaks, CA: Sage Publications, 4th edition, 2015.

[239] I Sommerville. *Software Engineering, Boston, Massachusetts: Pearson Education*. Inc, 2011.

[240] Helen Sharp, Cleidson deSouza, and Yvonne Dittrich. Using ethnographic methods in software engineering research. In *Proceedings of the 32nd ACM/IEEE International Conference on Software Engineering-Volume 2*, pages 491–492. ACM, 2010.

[241] Robert K Yin. *Case study research: Design and methods*. Sage publications, 2013.

[242] Robert E Stake. *Multiple case study analysis.* Guilford Press, 2013.

[243] Virginia Braun and Victoria Clarke. Using thematic analysis in psychology. *Qualitative research in psychology*, 3(2):77–101, 2006.

[244] Victoria Clarke and Virginia Braun. Thematic analysis. *The Journal of Positive Psychology*, 12(3):297–298, 2017.

[245] David Harper and Andrew R Thompson. *Qualitative research methods in mental health and psychotherapy: A guide for students and practitioners.* John Wiley & Sons, 2011.

[246] Greg Guest, Namey MacQueen, and EE Namey. Introduction to thematic analysis. *Applied thematic analysis*, 12, 2012.

[247] Virginia Braun and Victoria Clarke. *Successful qualitative research: A practical guide for beginners.* Sage, 2013.

[248] Mohammed Ibrahim Alhojailan. Thematic analysis: A critical review of its process and evaluation. *West East Journal of Social Sciences*, 1(1):39–47, 2012.

[249] Emily Namey, Greg Guest, Lucy Thairu, and Laura Johnson. Data reduction techniques for large qualitative data sets. *Handbook for team-based qualitative research*, 2:137–161, 2008.

[250] Richard E Boyatzis. *Transforming qualitative information: Thematic analysis and code development.* Sage, 1998.

[251] Ilker Etikan, Sulaiman Abubakar Musa, and Rukayya Sunusi Alkassim. Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics*, 5(1):1–4, 2016.

[252] Lawrence A Palinkas, Sarah M Horwitz, Carla A Green, Jennifer P Wisdom, Naihua Duan, and Kimberly Hoagwood. Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and Policy in Mental Health and Mental Health Services Research*, 42(5):533–544, 2015.

[253] UK Government. Level 4 Cyber Defence Exercise, February 2017.

[254] De Montfort University. Level 3 Cyber Defence Exercise, April 2017.

[255] UK Critical National Infrastructure Provider. Level 3 Table-Top Exercise, June 2017.

[256] US Government. Level 5 Cyber Defence Exercise, June 2017.

[257] De Montfort University. Level 2 Table-Top Exercise, August 2017.

[258] Lorelli S Nowell, Jill M Norris, Deborah E White, and Nancy J Moules. Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods*, 16(1):1609406917733847, 2017.

[259] Yvonna S Lincoln and Egon G Guba. *Naturalistic inquiry*, volume 75. Sage, 1985.

[260] Egon G Guba and Yvonna S Lincoln. *Fourth generation evaluation*. Sage, 1989.

[261] Sharolyn Converse, JA Cannon-Bowers, and E Salas. Shared mental models in expert team decision making. *Individual and group decision making: Current issues*, 221, 1993.

[262] JJ Koehler and NJ Castellan. *Individual and group decision making*. American Psychological Association., 1993.

[263] Mica R Endsley. Situation awareness global assessment technique (SAGAT). In *Aerospace and Electronics Conference, 1988. NAECON 1988., Proceedings of the IEEE 1988 National*, pages 789–795. IEEE, 1988.

[264] Mica R Endsley. Measurement of situation awareness in dynamic systems. *Human factors*, 37(1):65–84, 1995.

[265] Mica Endsley and William M Jones. Situation awareness information dominance & information warfare. Technical report, Logicon Tehnical Services Inc Dayton OH, 1997. http://www.dtic.mil/dtic/tr/fulltext/u2/a347166.pdf, Accessed 1 July 2018.

[266] Mica R Endsley and W Jones. Situation awareness. *The Oxford handbook of cognitive engineering*, 1:88–108, 2013.

[267] Mica R Endsley. Final reflections: situation awareness models and measures. *Journal of Cognitive Engineering and Decision Making*, 9(1):101–111, 2015.

[268] Mica R Endsley. Situation awareness misconceptions and misunderstandings. *Journal of Cognitive Engineering and Decision Making*, 9(1):4–32, 2015.

[269] Cynthia E Irvine, Michael F Thompson, and Ken Allen. CyberCIEGE: an information assurance teaching tool for training and awareness. Technical report, Naval Postgraduate School Monterey CA, 2005.

[270] Cynthia E Irvine, Michael F Thompson, and Ken Allen. CyberCIEGE: gaming for information assurance. *IEEE Security & Privacy*, 3(3):61–64, 2005.

[271] CE Irvine and MF Thompson. Simulation of PKI-enabled communication for identity management using CyberCIEGE. In *Military Communications Conference MILCOM 2010*, pages 906–911. IEEE, 2010.

[272] Michael Thompson and Cynthia Irvine. Active learning with the CyberCIEGE video game. In *In Federal Information Systems Security Educators' Association Conference (pp. 1-10)*, 2011.

[273] L Jean Camp. Mental models of privacy and security. *IEEE Technology and society magazine*, 28(3), 2009.

[274] Rick Wash and Emilee Rader. Influencing mental models of security: a research agenda. In *Proceedings of the 2011 New Security Paradigms Workshop*, pages 57–66. ACM, 2011.

[275] Scott E Jasper. US cyber threat intelligence sharing frameworks. *International Journal of Intelligence and CounterIntelligence*, 30(1):53–65, 2017.

[276] Don McDowell. *Strategic intelligence: a handbook for practitioners, managers, and users*, volume 5. Scarecrow Press, 2008.

[277] Richards J Heuer. *Psychology of intelligence analysis.* Central Intelligence Agency Centre for the Study of Intelligence, Washington DC, 1999. https://www.cia.gov, Accessed 1 July 2018.

[278] The Open Group. The Open Group Architecture Framework (TOGAF). *The Open Group*, 1, 2009. http://www.opengroup.org/subjectareas/enterprise/togaf, Accessed 1 July 2018.

[279] Jason S Burkett. Business Security Architecture: Weaving Information Security into Your Organization's Enterprise Architecture through SABSA. *Information Security Journal: A Global Perspective*, 21(1):47–54, 2012.

Acronyms

2IC Second-in-command

ACL Access Control Lists

APT Advanced Persistent Threat

BN Bayesian Networks

BTM Blue Terrain Manager

C2 Command and Control

CARVER Criticality, Accessibility, Recuperability, Vulnerability, Effect, Recognisability

CCGT Combined Cycle Gas Turbine

CDX Cyber Defence Exercise

CERT-UK Computer Emergency Response Team - United Kingdom

CIRT Collective Incident Response Training

CNI Critical National Infrastructure

COA Course of Action

CPNI Centre for the Protection of National Infrastructure

CPT Cyber Protection Team

CS2SAT Control Systems Cyber Security Self Assessment Tool

CSIRT Computer Security Incident Response Team

CTI Cyber Threat Intelligence

CV Controlled Variable

CVE Common Vulnerabilities and Exposures

DC Domain Controller

DCO Defensive Cyber Operations

DCO MST Defensive Cyber Operations Mission Specific Training

DCOM Distributed Common Object Model

DCS Distributed Control System

DMU De Montfort University

DMZ De-Militarised Zone

DNP3 Distributed Network Protocol v3

DoD US Department of Defense

DPA Data Protection Act

DPI Deep Packet Inspection

ENISA European Union Agency for Network and Information Security

EPPM Extended Parallel Process Model

ERP Enterprise Resource Planning

ETA Event Tree Analysis

FCE Final Control Element

FMEA Failure Modes and Effects Analysis

FMECA Failure Modes, Effects and Criticality Analysis

FTA Fault Tree Analysis

GPO Group Policy Objects

HAZOP Hazard and Operability

HIDS Host-based Intrusion Detection System

HILF High Impact Low Frequency

HTTP Hypertext Transfer Protocol

HTTPS Hypertext Transfer Protocol Secure

I/O Input/Output

ICMP Internet Control Message Protocol

ICS Industrial Control System

ICS-CERT Industrial Control System Computer Emergency Response Team

ICS-CDTP Industrial Control System Cyber Defence Triage Process

IDS Intrusion Detection System

IEC International Electrotechnical Commission

IED Intelligent Electronic Device

IR Incident Response

ISA International Society for Automation

ISO 22320 ISO 22320:2011 Requirements for incident response

ISO 22399 ISO 22399:2007 Guidelines for incident preparedness and operational continuity management

ISO 27035 ISO 27035:2011 Information security incident management

JASON An independent group of scientists that advises the United States government on matters of science and technology

KPI Key Performance Indicator

LIHF Low Impact High Frequency

ME Main Effort

MEL Main Events List

Modbus Modicon Bus

MSHARPP Mission,Symbolism, History, Accessibility, Recognisability, Population, Proximity

MST Mission Specific Training

mv Manipulated Variable

NERC North American Electric Reliability Corporation

NIDS Network-based Intrusion Detection System

NIST National Institute of Standards and Technology

NRC National Research Council

OODA Observe, Orient, Decide, Act

OPC Open Platform Communications

OT Operational Technology

PAAL Pre-Approved Actions List

PCI-DSS Payment Card Industry Data Security Standard

PDAL Prioritised Defended Asset List

PLC Programmable Logic Controller

PMT Protection Motivation Theory

PRA Probabilistic Risk Assessment

PSA Probabilistic Safety Assessment

PV Process Variable

QRA Quantitative Risk Assessment

RAGAGEP Recognised and Generally Accepted Good Engineering Practice

RFC Request for Change

RFI Request for Information

RLL Relay Ladder Logic

RoE Rules of Engagement

RPC Remote Procedure Call

RTU Remote Terminal Unit

SA Situational Awareness

SCADA Supervisory Control and Data Acquisition

SCIPS Simulated Critical Infrastructure Protection Scenarios

SHPT Microsoft SharePoint Server

SLA Service Level Agreement

SMB Server Message Block

SIEM Security Information and Event Management

STRIDE Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege

SOP Standard Operating Procedures

TCP/IP Transmission Control Protocol / Internet Protocol

TPB Theory of Planned Behaviour

TTP Tactics, Techniques, and Procedures

TTX Table-Top Exercise

UK United Kingdom (of Great Britain and Northern Ireland)

US United States (of America)

USD United States Dollars

VAM Vinyl Acetate Monomer

VM Virtual Machine

VPN Virtual Private Network

WMI Windows Management Instrumentation