Impact-Focused Cyber Incident Response

Authors: Eur Ing Kevin Mepham, Prof Panos Louvieris, Dr Gheorghita Ghinea

Abstract

Traditional incident response methods, where the standard approaches have been to contain, stop and recover from attacks as quickly as possible, have always represented the best intentions of the Cyber-Defence community. However, if learning about the attacker is one of the interests of the defending organisation, the traditional methods have not necessarily been the most appropriate method of accomplishing this goal.

To evaluate the appropriateness of the standard incident-response methods, several influences on traditional and non-conventional cyber-security were considered by stakeholders potentially affected by cyber-attacks. Their opinions were evaluated to produce conceptual models relating to dynamic asset value, intelligence value and cyber-response decision-making considering a balance of equities. Finally, their responses to a survey were assessed using Structural Equation Modelling which resulted in the production of a high-level model. This model describes a novel Cyber-Incident Response method which uses the potential "effects" and impact (on the mission) of a cyber-attack to determine the most appropriate response method rather than utilising the traditional methods as a standard response.

It is intended that this model be used to drive the creation of cyber-incident response procedures which can be tailored within the legal, political and resource constraints of an organisation.

Introduction

Since the earliest days of formal Computer Emergency Response Teams (Schleris, 1988), traditional Cyber-Incident Response processes have concentrated on responding to cyber threats by triaging attacks until systems can be restored to full functionality as quickly as possible. This can be seen in the evolution from the early descriptions of processes (Wack, 1991), (West-Brown, Stikvoort, & Kossakowski, 1998), (Northcutt, 2003) illustrated by the diagram at Figure 1, to the model from the National Institute of Standards and Technology (NIST) shown at Figure 2 (Cichonski, Millar, Grance, & Scarfone, 2012).

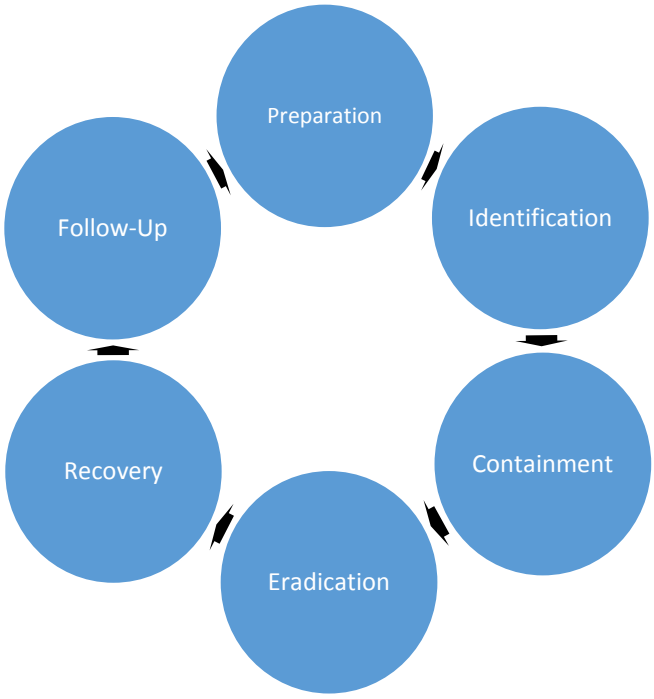


Figure 1 - SANS Institute Incident Response Processes, 2003

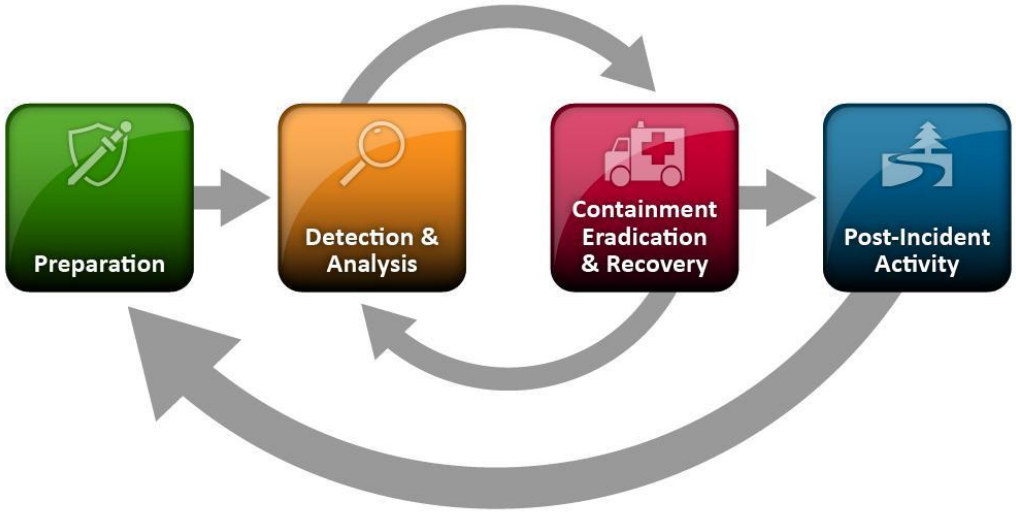


Figure 2 - NIST SP 800-61 Incident Response Life Cycle, 2012

As illustrated in Figure 1 and Figure 2, the priority is placed upon eliminating and recovering from cyber-attacks and, although in the NIST SP 800-61 document an inner cycle of detection and response is created, the processes and decision-making remain largely unchanged. However, despite the unequivocal value of using this revised type of approach for the immediate protection of critical assets and infrastructure, this paper will argue that other types of approaches and other priorities should also be considered when responding to Cyber incidents and will propose a model to accomplish this.

Broader Conflict Domains

Computer warfare, computer terrorism, computer crime and other areas of conflict involving computer and communications networks are commonly grouped into a ubiquitous domain known as "Cyber"; Cyber is often seen to be a unique problem which has no link to other domains of warfare or conflict. However, in the same way that "Air "and later "Space" were added to the battlegrounds of "Land" and "Sea", Cyber is not unique in that many of the concepts which hold true for conventional warfare also apply in the Cyber domain. Multinational Experiment 7[1] (MNE7) recognised the equivalence of Cyber as a domain in its stated intention of "Preserving Access to the Global Commons" where "Maritime, Air, Space and Cyberspace" were defined as the global commons ("Land" was omitted as this belongs to sovereign nations and is therefore not considered to be a "global" commons).

Using this concept of Cyber being "yet another domain" as a starting block, it is then useful to examine some of the principles which are used to understand and excel in the other domains of warfare. The fast-moving decision-making employed in air combat provides the first of the relevant parallels. The renowned Observe, Orient(ate), Decide and Act (OODA) loop conceived by Colonel John Boyd USAF (Orr, 1983) illustrated how pilots need to assess enemy actions in the context of their environment. Based on their perception of what is happening, assessment of the future including possible outcomes of their own actions and the enemy actions, they take a decision and respond. By completing this decision loop faster than an adversary it would be expected that they gain the upper hand in combat. A more comprehensive development of this model can be seen in the area of Situational Awareness (SA), where in Dr Mica Endsley's dynamic decision-making model (shown in Figure 3), the perception (observe), comprehension and projection (orient(ate)) are grouped together to create SA (Endsley, 1995). However, in this model it is

[1] http://www.act.nato.int/mne-7-access-to-the-global-commons

shown that not only the environment, but also task and systems factors, as well as individual factors influence the SA, the decision and the response.

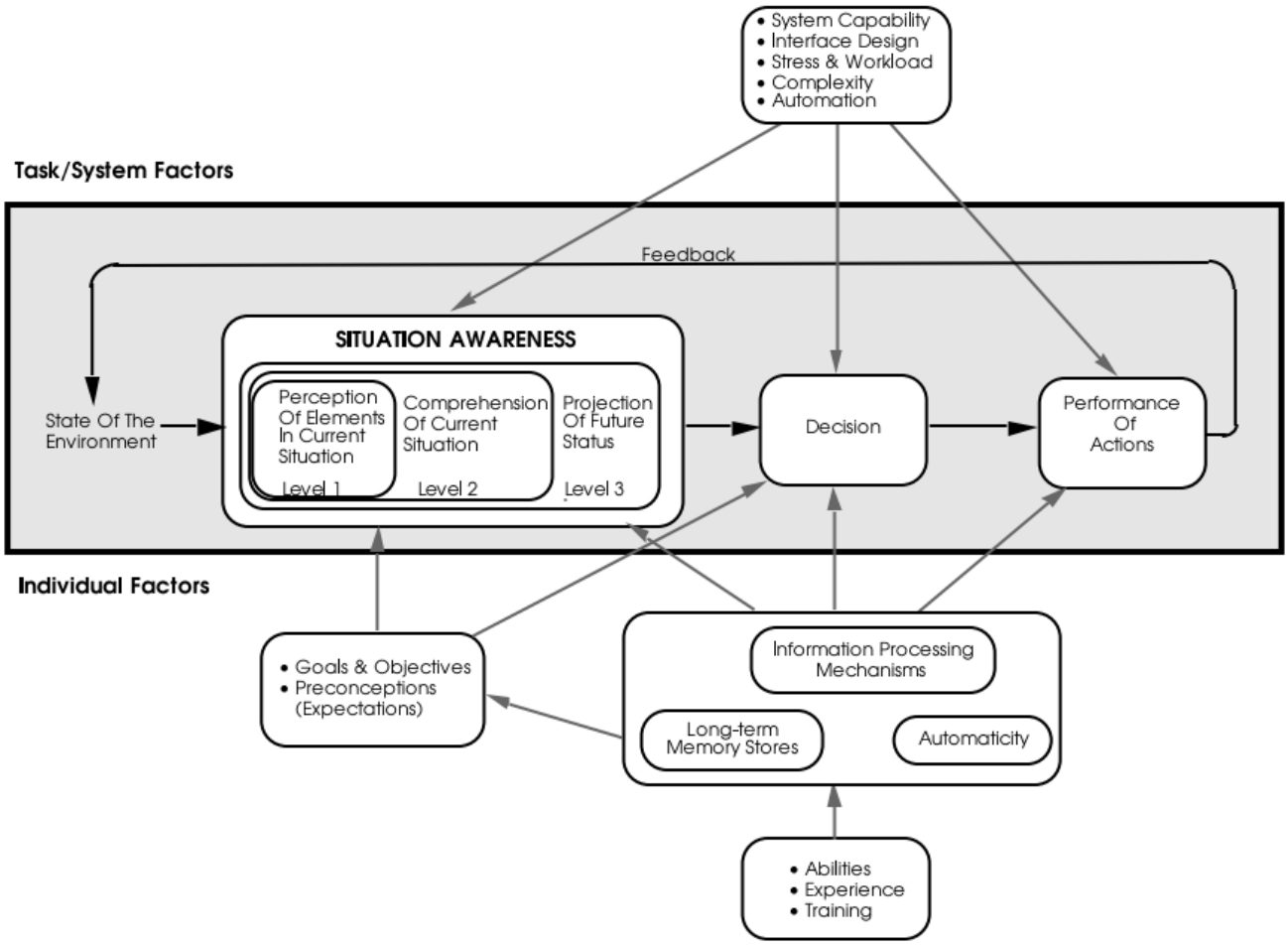
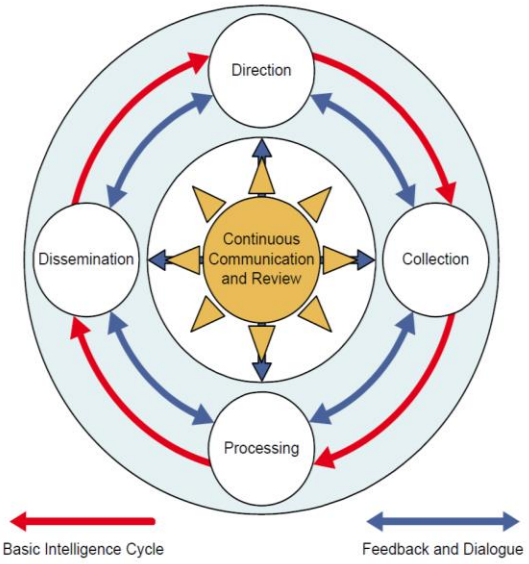


Figure 3 - Model of Situational Awareness in Dynamic Decision-Making

Within this decision-making model, "Goals, Objectives and Preconceptions (Expectations)" are deemed to influence the decision-making and the situational awareness. Looking in particular at the preconceptions and expectations it could be argued that these are formed by existing intelligence (in the military sense of the word). This is also echoed by a much earlier premise reputed to have been promoted by Sun Tzu, "know your enemy and know yourself, in a hundred battles you will never be in peril" (Tzu, 1963), i.e. the knowledge of your own disposition, capabilities and potential actions as well as those of your enemy are a key component of SA and the consequent decision-making.

Having established that Intelligence is a key component of effective combat and, by extension, therefore a key component of an effective Cyber warfare strategy (be it from a defensive perspective as in Cyber-Incident response or from the perspective of Cyber-Offensive operations) it is wise to look at Intelligence doctrine. United Kingdom Intelligence doctrine (Ministry of Defence UK, 2011) describes a cycle of Direction, Collection, Processing and Dissemination as shown in Figure 4.



In Figure 4, one of many similar variants of the Intelligence Cycle, it can be inferred that the disseminated product influences the way that intelligence information is collected. For Cyber, it is certainly true that defence mechanisms and signatures are revised based on previous attacks after post-incident analysis. However, returning to the OODA loop, this process normally occurs outside of the loop after all actions have been carried out and the result has occurred, not inside the loop where an adversary is being actively engaged. From the individual perspectives of Intelligence, Cyber-Defence and SA perspectives and examination of their process cycles it could be anticipated that conflicts arise i.e. the primary aim of cyber-defence is to protect information and assets, the aim of Intelligence to provide the most appropriate information possible and the aim of SA to inform the decision-maker to facilitate optimal decision-making.

Figure 4 - JDP 2-00: The Intelligence Core Functions and the Intelligence Cycle[2]

Cyber Complications

Returning to Figure 3, it can be seen that the importance of Human Factors is emphasised in all areas of SA and decision-making, not only from an environmental perspective where the workload, interface and complexity are reflected not only in the "system factors", but also in the training, experience and ability highlighted in the "individual factors". This is also true for Cyber where not only the discrimination of cyber-attacks from the huge volume of "noise" relating to normal activity becomes a challenge for the analyst but also the representation of cyber-incident and cyber-intelligence information in a format suitable for the decision-makers.

Honeynets and honeypots are designed to monitor would-be cyber attackers in a controlled environment thus providing valuable Intelligence to the defender. However, the more advanced an attacker, the less effective these environments prove to be as it becomes more difficult to maintain a credible environment in the face of a knowledgeable attacker (Wang, Wu, Cunningham, & Zou, 2010). This can be understood by looking at typical characteristics of a workstation in an office; it could be expected that patterns would emerge for updating timestamps on files during normal user activity, equally network activity would also have similar characteristics. If the attacker is looking for these (or other) characteristics and does not see what they are expecting, deeper examination would undoubtedly reveal the presence of this controlled environment. Despite the increasingly advanced open-source and commercial honeynet and honeypot implementations that are available, the attacker and defender are engaged in a continuous game of leapfrog as they surpass each other's technical advances. Combined with the difficulties of creating a realistic environment, the resources to maintain the environment safely and control the access to it appropriately creates a large overhead for any organisation hoping to make effective use of this type of technology.

Collaboration and stakeholder engagement.

In addition to the reviewed literature, participation in international experiments during this research has contributed to understanding of the challenges associated with the Cyber domain. Most notably MNE7 and

[2] JDP 2-00 diagram based on an interpretation of the Intelligence Cycle by Dr Philip Davies from Brunel University.

the successor Multinational Capability Development Campaign – Cyber Implications for Combined Operational Access (MCDC-CICOA) were influential in the development and testing of concepts formed as initial hypotheses by the author.

In MNE7 one of the sub-outcomes investigated Cyber SA (Multinational Experiment 7 Contributing Nations, 2013) and specifically some of the issues related to sharing of information between cyber partners. This culminated in the Limited Objective Experiment (Multinational Experiment 7 Contributing Nations, 2013) which was created in the hub and node structure shown at Figure 5. In this experiment information flow was throttled between the various components and the reliability, accuracy and completeness of the information rated by the participants. The experiment validated the requirement to exchange cyber-related information in order to improve SA and identified that trust between entities was critical in order to allow this exchange.

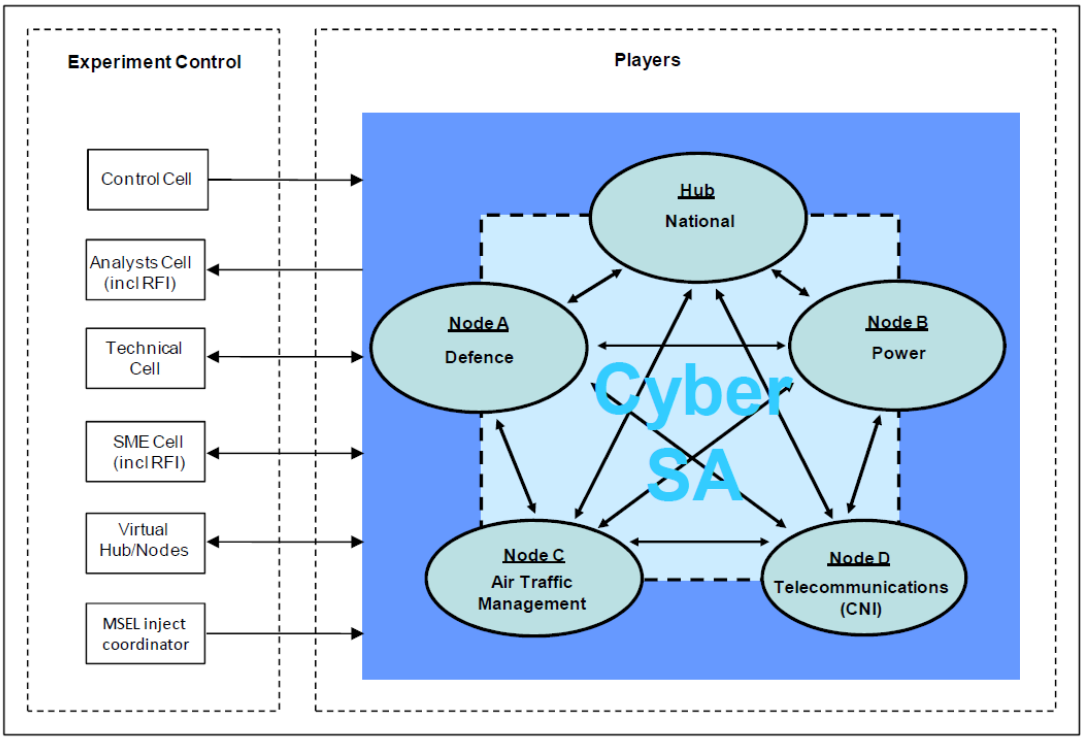


Figure 5 - Hub & Node organisational construct for MNE7 Cyber Situational Awareness LOE[3]

Following on from this experiment, MCDC-CICOA (Multinational Capability Development Campaign Contributing Nations, 2013) tried to build upon this success by bringing cyber into the domains of other stakeholders, in this case the operational community. This Campaign took the North Atlantic Treaty Organization (NATO) Common Operational Planning Directive (COPD), a document developed to deal with operational planning for conventional warfare, and attempted to integrate Cyber planning into the process. It accomplished this through two products:

a. A technical guide (Multinational Capability Development Campaign Contributing Nations, 2014) which described in detail the influence of Cyber (including Intelligence as well as Defence), this also referenced the author's earlier paper presented at the International Conference on Cyber Conflict.

[3] Diagram reproduced from MNE7 Cyber Domain Outcome 3, Cyber SA LOE Report dated 28 Feb 2013

b. A Cyber Handbook to be used in conjunction with the COPD (Multinational Capability Development Campaign Contributing Nations, 2014).

Cyber Factors of Influence

Based on the literature review and discussion with expert communities in the international experiments and security working groups, several topics were identified which were deemed to influence the cyber domain and cyber-incident response in particular. These were also complemented by than 15 years of practical cyber-security experience (in several areas both in military and commercial environments). These proposed influencing factors are shown at Appendix 1 – Cyber Security Variables, but can largely be divided up into Sensors, Human Factors, Targeted Asset Value, Intelligence, Mission Impact and Response.

Hypothesised Concepts

To explain the raison d'être for the inclusion of some of these influential factors, some of the initial hypotheses developed during this research are now described; these are based on the literature review, experience in the field and informal discussions with the expert stakeholders described previously.

Hypothesised Concept - Dynamic Asset Value

An asset has a particular value (not necessarily related to monetary value) to a stakeholder, another stakeholder may have a different value of that asset at any point in time. For example, an incident correlation system may be of high value to a Chief Information Security Officer (CISO), but in the opinion of a Human Resources Director, it may add little value to the organisation. Even the CISO will find that the asset may be more valuable at certain times (for example, during a major incident) than others (for example when the office is closed if it is only monitoring closed networks (i.e. not Internet-facing). In Figure 6 another example is provided where an assumption is made about the relative values of different types of information relating to a military campaign with respect to time. If the information is assessed against its importance to strategic objectives, the following assessments have been made:

a. Strategic plans have a relatively stable value across the lifecycle of a single mission.

b. Mission-related intelligence information will help to inform the mission plans but at some point the intelligence is likely to become less important than the plans (as it is possible that it will inform those undertaking the mission but is less likely to influence the plans the closer to execution that the mission gets).

c. The mission plans are most important immediately prior to mission execution and their importance decays after the mission has executed.

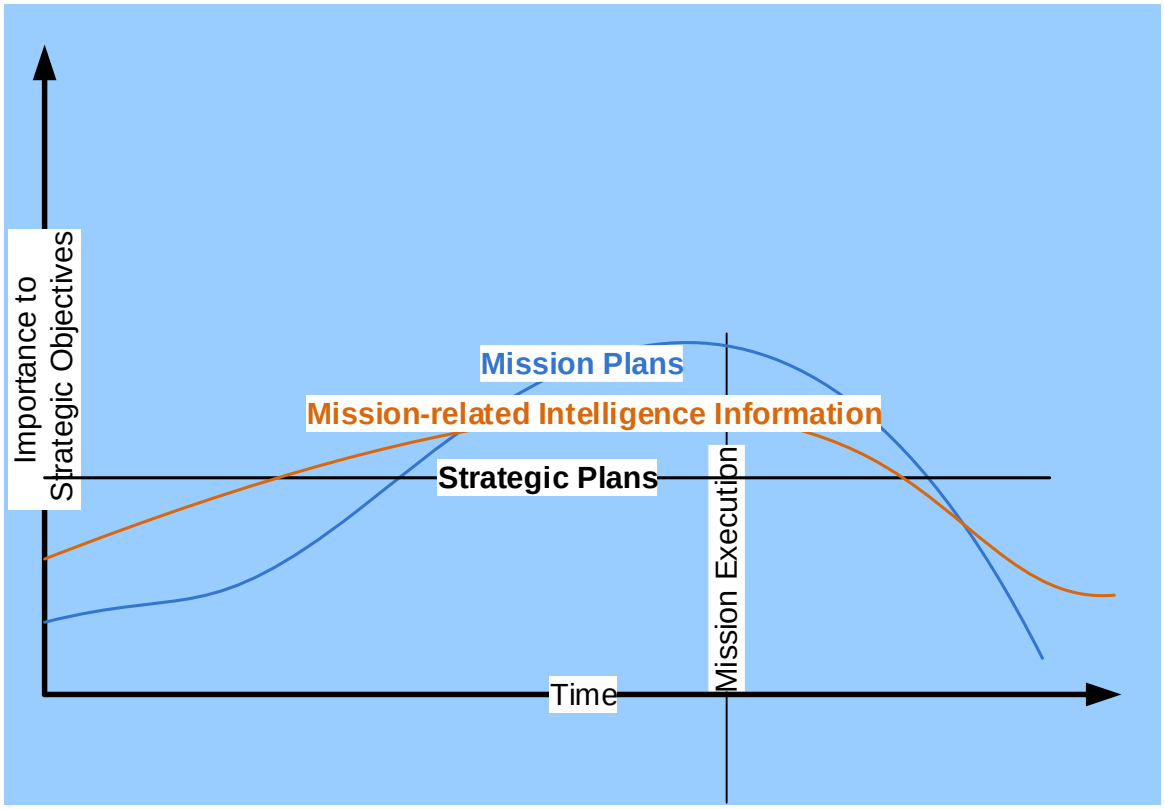


Figure 6 - Dynamic Asset Value

This example highlights, the changing value of an asset, not only to the owner of the asset, but also to key decision-makers who might be trying to balance the interests of many asset owners against organisational priorities and objectives.

Hypothesised Concept - Balance of Equities

The previous example leads onto one particular case which is relevant to Cyber-Incident Response, the case of the Cyber Intelligence community who, during discussions with subject matter experts in the field, often felt short-changed by what they saw as the premature termination of security incidents by the Cyber-Defence community. The particular problem is described by the diagram at Figure 7. This diagram describes an attack from an external network by an adversary which starts at the top of the triangle, at this point, typically, an attack starts with a scan to determine information about the target. This initial probe normally presents very little risk to the targeted infrastructure or assets, however, it also provides very limited information about the attacker. As the attack progresses the risk to the targeted infrastructure or assets increases (this is shown linearly but could equally follow some other pattern as it would be entirely dependent upon the attack and the assets being targeted).

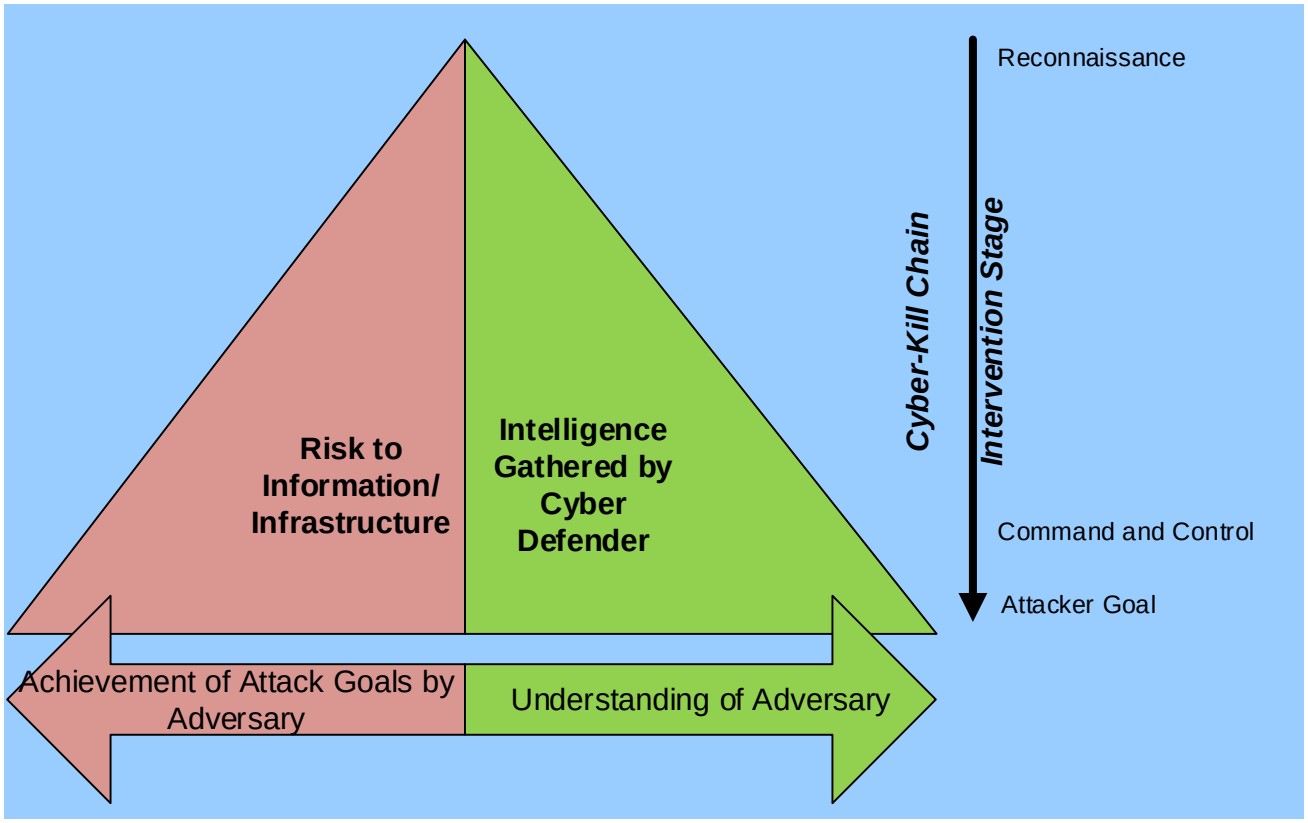


Figure 7- Balance of Equities

In parallel, the intelligence gathered about the attack and/or attacker would also increase (again not necessarily linearly). At each point during the attack, assuming that it has been detected there is a balance to be struck between the value of intelligence that could be gathered by allowing an attack to continue and the potential damage that could be caused to the infrastructure or assets. Using this concept, if a known attacker used a known attack against high-value infrastructure, the potential intelligence to be gained (the right-hand triangle) would be very small, however, the risk to the organisation of allowing the attack to continue would be very large (the left-hand triangle). In this case the decision would be clear, to stop the attack at all costs. However, if a novel attack was detected launched by an unknown attacker the potential intelligence value of gathering information could be very high; if launched against a low value asset the risk to the organisation could be low thereby possibly prompting a decision to allow the attack to continue under close supervision. Using this concept, the defending organisation could be better served than by automatically closing down an attack upon detection in all circumstances.

Survey and Analysis

Utilising the information gathered from the previous sections a list of variables was constructed and a corresponding survey produced. This survey was targeted at not only the Cyber Defence community but also the Operations, Intelligence, and CIS manager communities. From analysis of the results it was intended to determine the most important factors thought to influence Cyber Security in general and Cyber-Incident response in particular. The survey was sent to approximately 1500 potential respondents from many different nations in organisations ranging from military and governmental to commercial and academia. The initial results from 186 respondents (of which 121 completed all survey questions) highlighted significant differences in opinion between the different communities (Mepham, Louvieris, Ghinea, & Clewley, 2014) confirming the initial hypothesised concept, Dynamic Asset Value (Figure 6), that assets are valued by different stakeholders with different priority at different times. By extension of the Dynamic Asset Value concept, the Balance of Equities concept (Figure 7) was also ratified (at least for any instantaneous point during the attack). However, the extension of these concepts to a Cyber-Incident

response model which catered for a mission-impact focus required a more targeted examination of the results for which Structural Equation Modelling (SEM) was chosen.

Structural Equation Modelling (SEM)

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

To describe the survey in more detail in the perspective of the SEM work, the survey rated 30 variables from the perspectives of both an individual and their perspective of how they thought their organisation rated the same variables. This was based on a 7-point Likert scale (as initial feedback from a pilot survey determined that respondents felt too constrained by 5-point responses). By the time that the SEM was commenced, completed surveys from 201 respondents had been received; however, by this point the relevance of their perception of their organisations' responses was not deemed to be relevant to the model development as the individuals were seen to be the domain experts so the results were analysed from the individuals' perspectives. During the initial multiple linear regression in earlier work (Mepham, Louvieris, Ghinea, & Clewley, 2014), the only method of achieving a logical grouping of factors was to split the variables into two logical groups for analysis, Incident Detection and Decision-Making. However, by the time that the SEM was conducted, the additional respondents allowed all variables to be analysed together in the Measurement Model thus providing a more holistic approach. Also reported in this earlier work, most responses appeared to be approximately normally distributed when inspected visually, however, when tested using Kolmogorov- Smirnov tests (Hair Jr, Black, Babin, & Andersen, 2014) the responses were found to be non-normal. Using an alternative assessment method, skewness and kurtosis of less than 1 are generally considered slightly non-normal and values of up to 2.3 are considered to be moderately non-normal (Lei & Lomax, 2009). For the data from this survey, based on this categorisation, the majority of variables fell into the slightly non-normal category with only four variables falling into the moderately non-normal category (network sensors, organisational goal, training and sensor accuracy). However, even with severely non-normal data, in this case defined as having skewness above 0.7 and kurtosis in excess of 3.5, recent work in SEM (Lei & Lomax, 2009) confirmed that for sample sizes of 100 and above, SEM was robust for both the maximum likelihood (ML) and generalised least squares (GLS) methods (typically resulting in significantly less than 10% bias on parameter estimates). Consequently, the data being analysed falls within the range of an acceptably normal distribution for the purposes of this analysis.

Measurement Model

The initial measurement model is shown at Figure 8 and the variables relating to this are described as the Cyber Security Variables (detailed in Appendix 1 – Cyber Security Variables). These variables are considered to either influence the detection of incidents, situational awareness of the decision-maker or to provide a response option for the decision-maker (within organisational constraints).

In this model, each variable has an associated error term and the covariances between the factors are shown as double-ended arrows. Some variables were eliminated from during the exploratory factor analysis phase for falling below a significant factor loading value of 0.4 contributing threshold (Hair Jr, Black, Babin, & Andersen, 2014) whilst others were eliminated for loading on more than one factor

(Appendix 2 – Exploratory Factor Analysis) or for being the only variable loading on a factor. This resulted in the 23 variables which resolved to the identified 8 factors shown in the diagram.

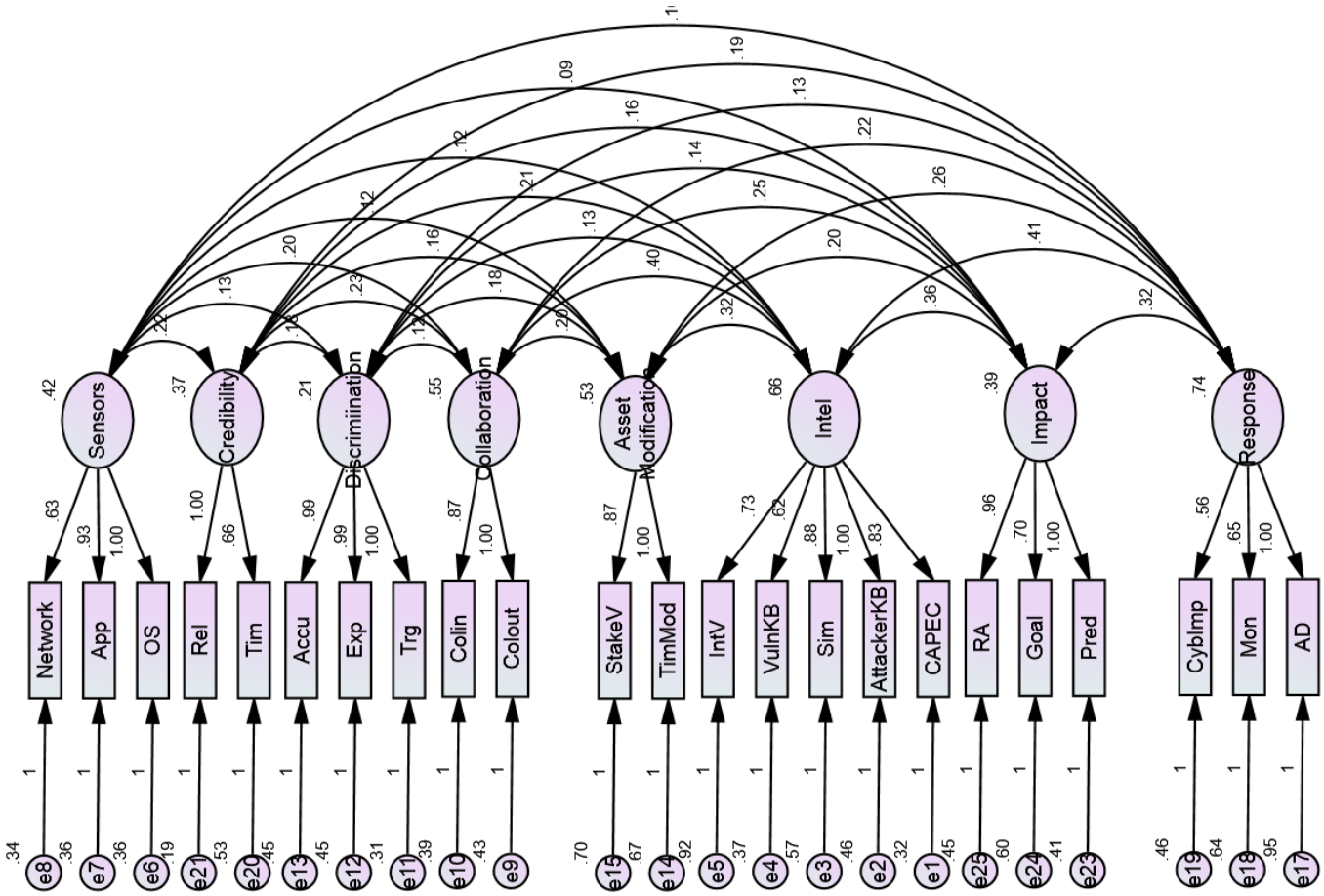


Figure 8 - SEM Measurement Model

The goodness of fit indices associated with the initial SEM model are shown at Table 1. The interpretation of the tests is presented below (an outline of the fit indices with references is described at Appendix 3 – Structural Equation Modelling). The first item of note is the probability test, (based on the χ2 calculation). Although this statistic rejects the model as non-significant, recent academic work (Hooper, Coughlan, & Mullen, 2008) suggests this test is not reliable for large sample sizes or those that deviate from normality. However, the minimum discrepancy between the data and the model divided by the degrees of freedom (CMIN/DF) falls between recommended bounds of 1 and 5 (Wheaton, Muthén, Alwin, & Summers, 1977) which is seen as a better alternative to χ2. Furthermore, it is advised (Lei & Lomax, 2009) that, for sample sizes below 500, the normed fit index (NFI), non-normed fit index (NNFI) and comparative fit index (CFI) are better fit indices than χ2.

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

Abbreviation Key	
CMIN	Minimum discrepancy
CFI	Comparative fit index
DF	Degrees of freedom (DF)
EVCI	Expected cross-validation index
FMIN	Minimum of discrepancy function F
HI90	Upper limit of the 90% confidence interval
IFI	Incremental fit index
LO 90	Lower limit of the 90% confidence interval
MECVI	Modified expected cross-validation index
NFI	Normed fit index
NNFI	Non-normed fit index
P	$\chi 2$ statistic
PCFI	Parsimony comparative fit index
PCLOSE	Test for RMSEA significance
PNFI	Parsimony normed fit index
PRATIO	Parsimony ratio
RFI	Relative Fit Index
RMSEA	Root mean square error of approximation
TLI	

Table 1 –SEM Measurement Model

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

Utilising this evaluated measurement model as a starting point, a hypothesised model is proposed in Figure 9. However, after evaluation of the regression weight divided by the standard error for each of the causal relationships (denoted by Critical Ratio (CR) in the IBM AMOS software package) it was found that the influence of Collaboration on Discrimination was negligible (less than 2 and probability more than 0.05, thus indicating an invalid model) but from a logical perspective a discriminated incident is important information to share with partners and by reversing this relationship it became significant and the CR increased to 4.2.

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

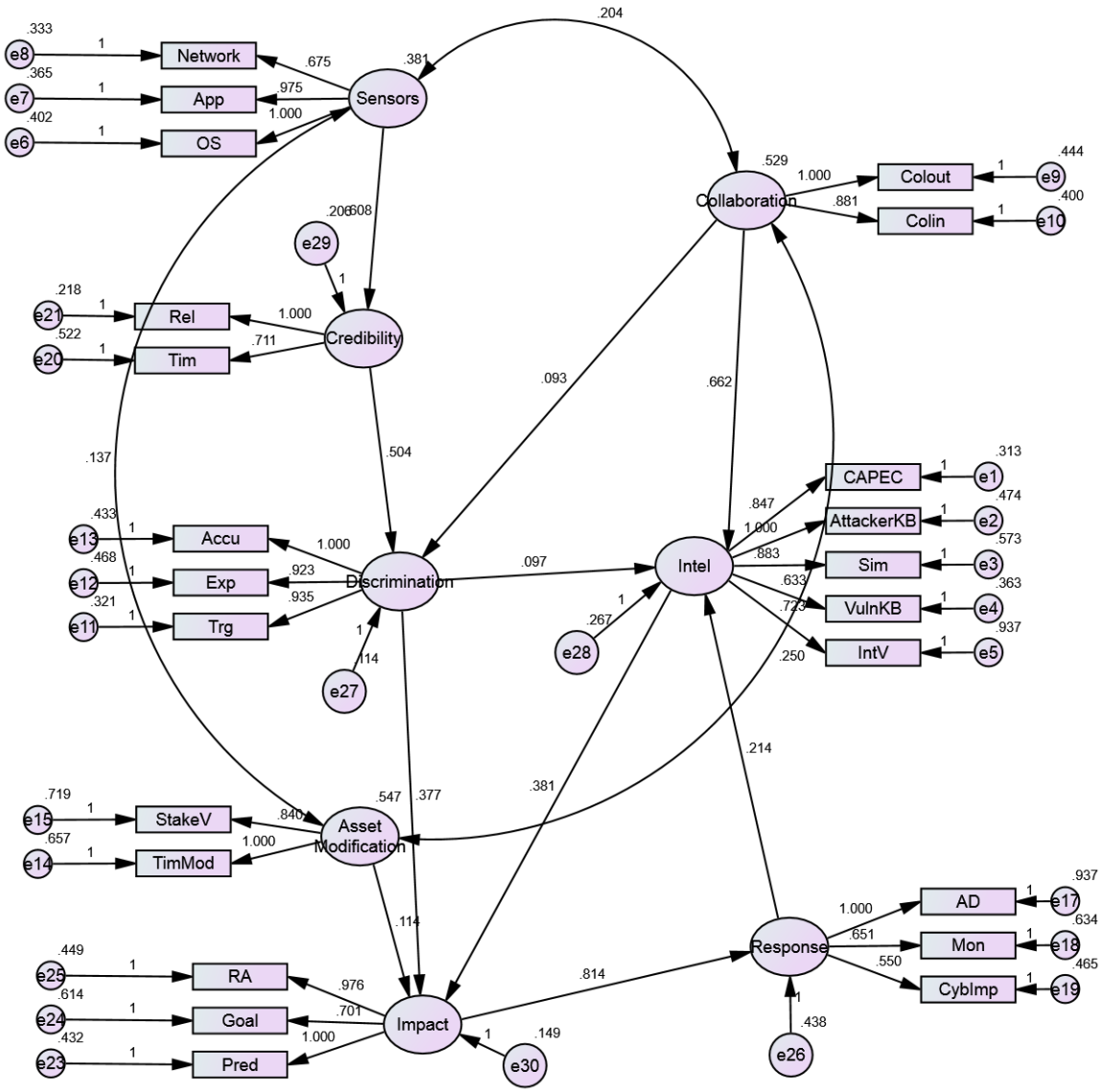


Figure 9- Initial SEM Structural Model

From testing each of the relationships in turn of the initial structural model (Figure 9) in the manner described for the relationship between Collaboration and Discrimination, Asset Modification and Response, and Discrimination and Intel, the final structural model was produced (Figure 10). It is of interest to note that this model development removes the direct covariance relationship between Sensors and Asset Modification and that Collaboration appears to directly influence both Sensors and Asset Modification. From a logical perspective this could be explained by information from collaboration partners highlighting shortcomings in sensor deployment. Equally, in a mission with collaboration partners, targeted assets may have more or less importance to the partners than to the owners of the assets (for example one seaport of many owned by a host nation being used as a single bridgehead by an assistance force from a collaboration partner).

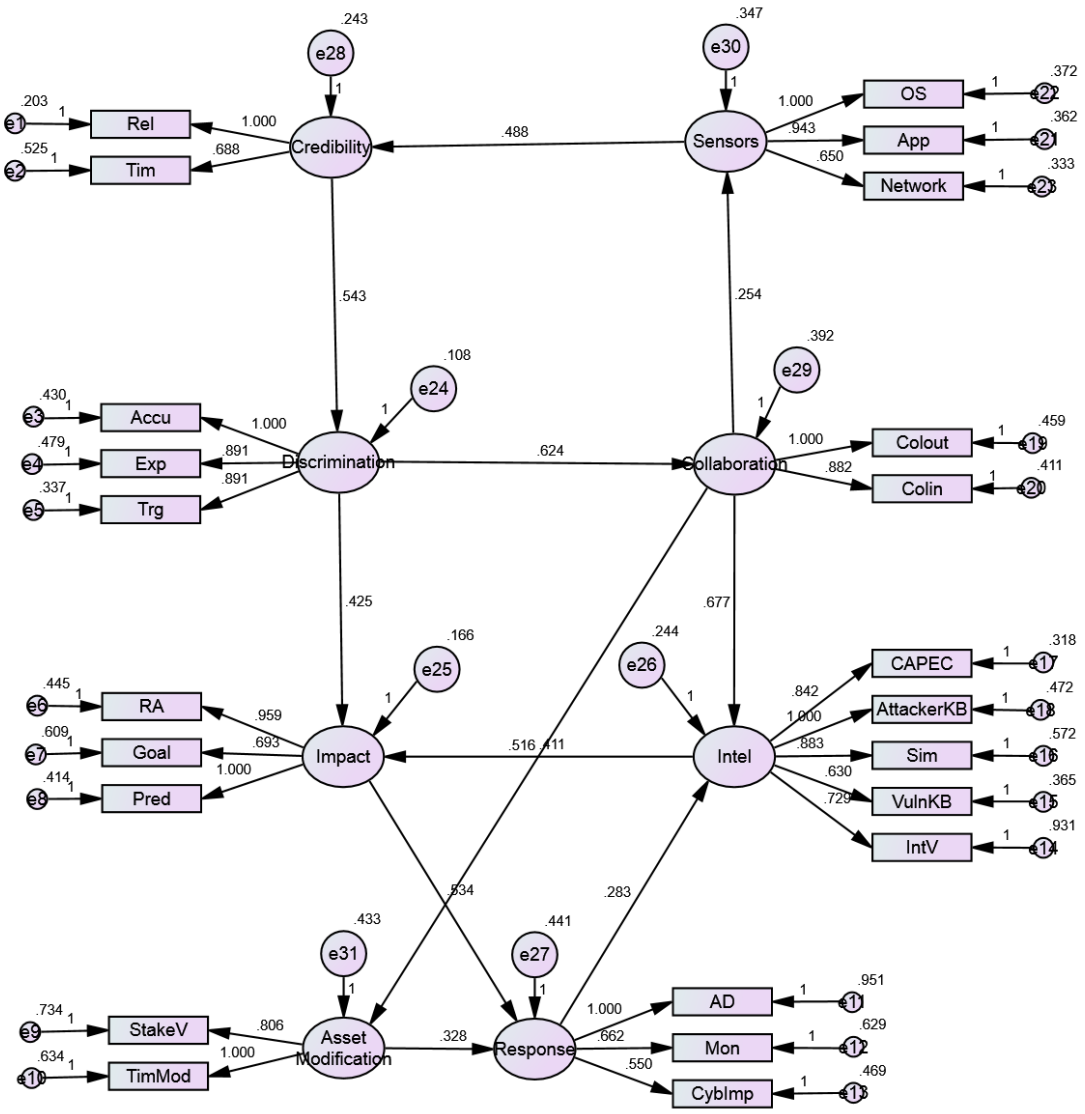


Figure 10- Final SEM Structural Model

However, by analysing the relationships logically, the overlapping stages: incident detection, situational awareness and decision-making, can be seen within the structural model. By redrawing this schematically, the relationship between the factors and interconnecting processes can be seen (Figure 11). In this schematic the three stages can be treated as follows:

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

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

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

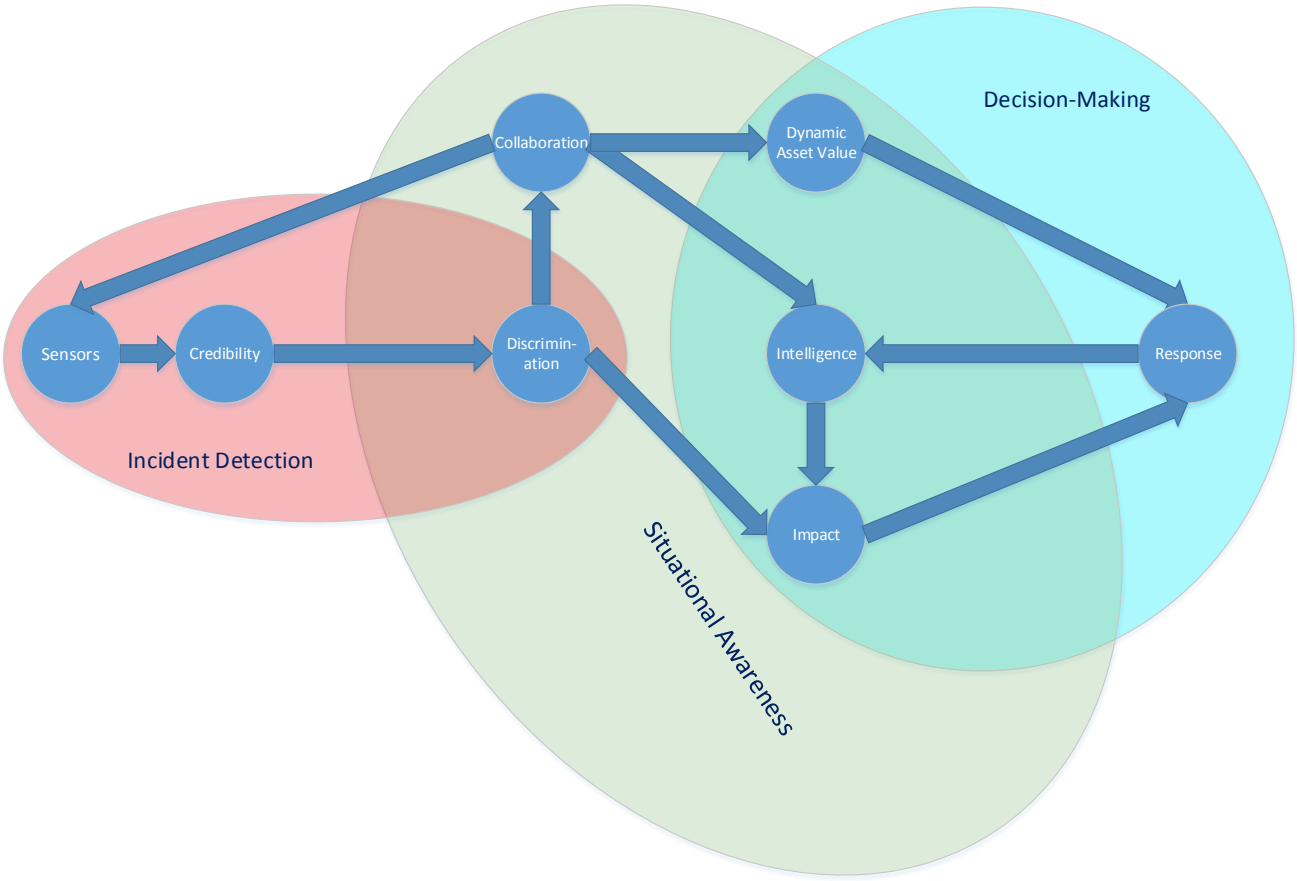


Figure 11-Schematic Impact-Focused Cyber Incident Response

Contrast with Current Models

In contrast with the traditional models, (Figure 1 and Figure 2) where a single loop describes the incident response process (albeit with some additional processes outside the core in the more recent version), the proposed model has separate incident detection and incident response loops. Additionally, through a feed-forward process, the detected incidents are evaluated in terms of the mission impact. Other points of note are that Asset Value is not fixed; this is dependent upon input from collaboration partners (visible in the diagram) as well as the independent variables relating to the stage of the mission and the internal stakeholder assessments.

This model is a significant departure from traditional incident-response models as the impact of the incident on the defending organisation ultimately determines the appropriate response rather than the traditional approach which tended towards "defend at all costs". However, parallels can be drawn with both Endsley's SA model (Figure 3) and the OODA loop as the aim of obtaining an understanding of the complete environment (own, partner, adversary and mission impact) leads to better-informed decision-making.

Practical Implications

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

Future Work

Currently, this model is based on statistical analysis of the personal opinions of professionals directly or indirectly impacted by the way cyber-incident response is carried out. However, in order to assess the practical validity of the model it is intended to assess the effectiveness, efficiency and impact of the decisions made by procedures developed from this model in cyber decision-making. This will be evaluated by means of an experiment conducted on the University's Cyber Range. For this experiment, 8 vignettes are proposed which vary Intelligence Value, Dynamic Asset Value and Mission Impact in low clutter and high clutter environments (i.e. 32 tests will be conducted in all when accounting for a control group that uses traditional response methods for each of the vignettes and clutter conditions). For the purposes of the experiment, no legal constraints will be placed upon the response options to give the decision-maker the options of traditional response, passive intelligence gathering (i.e. non-intervention), active intelligence gathering or cyber offensive operations.

References

Byrne, B. M. (2010). *Structural Equation Modeling with AMOS* (2nd ed.). Ottawa, Ontario, Canada: Routledge.

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer Security Incident Handling Guide (Draft).* Gaithersburg, MD: National Institute of Standards and Technology.

Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 32-64.

Hair Jr, J. F., Black, W. C., Babin, B. J., & Andersen, R. E. (2014). *Multivariate Data Analysis (Pearson New International Edition)* (7th ed.). London, UK: Pearson Education Limited.

Hooper, D., Coughlan, J., & Mullen, M. R. (2008). Structural Equation Modelling: Guidelines for Determining Model Fit. *Electronic Journal of Business Research Methods, 6*(1), 53-60.

Hu, L.-t., & Bentler, P. M. (1999). Cutoff Criteria for Fit Indexes in Covariance Structure Analysis: Conventional Criteria Versus New Alternatives. *Structural Equation Modelling: A Multidisciplinary Journal, 6*(1), 1-55. doi:10.1080/10705519909540118

Lei, M., & Lomax, R. G. (2009). The Effect of Varying Degrees of Nonnormality in Structural Equation Modeling. *Structural Equation Modeling: A Multidisciplinary Structural Equation Modeling, 12*(1), 1-27. doi:10.1207/s15328007sem1201_1

Matsueda, R. L. (2011). *Working Paper no 114: Key Advances in the History Of Structural Equation Modeling.* University of Washington, Center for Statistics and the Social Sciences. Seattle: University of Washington.

Mepham, K. D., Louvieris, P., Ghinea, G., & Clewley, N. (2014). Dynamic Cyber-Incident Response. *6th International Conference on Cyber Conflict* (pp. 121-136). Tallinn, Estonia: NATO CCD COE Publications.

Ministry of Defence UK. (2011). *Joint Doctrine Publication 2-00: Understanding and Intelligence Support to Joint Operations.* Shrivenham, UK: Development, Concepts and Doctrine Centre.

Multinational Capability Development Campaign Contributing Nations. (2013). *Multinational Capability Development Campaign Contributing Nations 2013-2014: Combined Operational Access.* MCDC.

Multinational Capability Development Campaign Contributing Nations. (2014). *Multinational Capability Development Campaign (MCDC) 2013-14 Combined Operational Access Cyber Implications for Combined Operational Access - Handbook for Integrating Cyber Defense into the Operational Planning Process.* MCDC.

Multinational Capability Development Campaign Contributing Nations. (2014). *Multinational Capability Development Campaign (MCDC) 2013-14 Combined Operational Access: Cyber Implications for Combined Operational Access - Guide and Specifications for the Analysis of the Cyber Domain.* MCDC.

Multinational Experiment 7 Contributing Nations. (2013). *MNE7 Access to the Global Commons Concept of Employment - Outcome 3 Cyber Domain: Concept of Employment for Cyber Situational Awareness Within the Global Commons.* MNE7.

Multinational Experiment 7 Contributing Nations. (2013). *Multinational Experiment 7 Cyber Domain Outcome 3 Cyber Situational Awareness: Limited Objective Experiment Report.* MNE7.

Northcutt, S. (2003). *Computer Security Incident Handling.* Bethesda, ML: SANS Institute.

Orr, G. E. (1983). *Combat Operations C3I (Command, Control, Communications, and Intelligence): Fundamentals and Interactions.* Maxwell Air Force Base, Alabama: AIr University - Center for Aerospace Doctrine, Research and Education.

Schleris, W. (1988). *CERT NEWS RELEASE - No 597-88 DARPA Establishes Computer Emergency Response Team.* DARPA.

Tzu, S. (1963). *Sun Tzu: The Art of War (trans Samuel B Griffith).* London: Oxford University Press.

Wack, J. P. (1991). *Establishing a computer security incident response capability (CSIRC).* Gaithersburg, MD; Springfield, VA: National Institute of Standards and Technology.

Wang, P., Wu, L., Cunningham, R., & Zou, C. C. (2010). Honeypot detection in advanced botnet attacks. *International Journal of Information Secuirty*, 30-51.

West-Brown, M. J., Stikvoort, D., & Kossakowski, K.-P. (1998). *Handbook for Computer Security Incident Response Teams (CSIRTs).* Pittsburgh, PA: Carnegie Mellon Software Engineering Institute.

Wheaton, B., Muthén, B., Alwin, D. F., & Summers, G. F. (1977). Assessing Reliability and Stability in Panel Models. In D. R. Heise, *Sociological Methodology* (pp. 83-136). San Francisco: Jossey-Baas.

Appendix 1 – Cyber Security Variables

Abbreviated Name	Name	Description
Hardware	Hardware Monitoring	Sensors deployed to monitor changes at a hardware level
Network	Network Monitoring	Sensors deployed to detect anomalies or signatures in network traffic
OS	OS Monitoring	Sensors (including built-in audit functions) deployed to detect anomalies or signatures in the operating system
App	Application Monitoring	Sensors (including built-in audit functions) deployed to detect anomalies or signatures in the applications on a system
CM	Configuration Management	Awareness of the defended infrastructure including deployment, hardware, software and application versions as well as configuration.
Accu	Accuracy	Accuracy of the information supplied by the sensors e.g. the granularity and accuracy of the timestamps.
Tim	Timeliness	Timeliness of the information provided by the sensors i.e. how soon the information is received after the event e.g. real-time, every 10 minutes, hourly, daily etc.
Rel	Reliability	Reliability of the sensors i.e. the level of confidence that they will always catch and transmit the events that they are configured for also including a long mean time between failure.
Colin	Collaboration Inbound	Cyber information shared by collaboration partners which may be of use to an organisation's cyber security posture.
Colout	Collaboration Inbound	Cyber information shared with collaboration partners from an organisation's own sensors and analysis (in accordance with information exchange agreements)
Auto	Automated Tools	Tools which assist an analyst in filtering and highlighting incidents from raw data.
Trg	Training	Training of cyber analysts
Exp	Experience	Experience of cyber analysts
Env	Environment	Physical environment that analysts work in, i.e. human factors such as monitor size, graphical interfaces, break/shift patterns etc.
AssV	Asset Value	Static value of asset
StakeV	Stakeholder Value	Modification of asset value by stakeholder
ExpVuln	Exposed Vulnerabilities	Known vulnerabilities in own infrastructure.
TimMod	Time Modification	Modification of asset value due to stage of mission cycle, business cycle etc.
VulnKB	Vulnerability Knowledgebase	Knowledgebase of vulnerabilities in general (i.e. not specific to own infrastructure).
AttackerKB	Attacker Knowledgebase	Knowledgebase of known attackers (non-specific to organisation)
CAPEC	CAPEC	Common Attack Pattern Enumeration and Classification. Knowledge base of common attack patterns/techniques and methods for categorising them.
Sim	Simulation	Simulation of possible attack vectors or progression through an organisation's infrastructure
IntV	Intelligence Value	Assigning a value to missing or gained intelligence (to be weighed against asset value).
Goal	Goal	Organisation's goals and objectives
SA	Situational Awareness	Ability to place an incident in context of the environment and potential outcomes.
Pred	Prediction	Credible algorithms to predict an incident's progress and the effect of possible response options (to be used as engine for simulation)
RA	Risk Assessment	Use of robust techniques to provide a standardised approach to risk assessment.
AD	Active Defence	Active defence (including active intelligence gathering and cyber-offensive techniques)
Mon	Passive Monitoring	Use of observation to gain additional intelligence rather than acting to contain or stop incidents i.e. allow incidents to continue unfettered.
CybImp	Importance of Traditional Techniques	Use of standard approaches to cyber security including defence and response mechanisms.

Appendix 2 – Exploratory Factor Analysis

	Factor								
	Intel	Sensors	Impact	Collaboration	Discrimination	Asset Modification	Response	Credibility	Null
CAPEC	.688								
AttackerKB	.652								
Sim	.621								
VulnKB	.533								
IntV	.482								
OS		.728							
App		.652							
Network		.615							
CM		.489			.412				
SA			.681						
Pred			.605						
Goal			.535						
RA			.448						
Colout				.652					
Colin				.582					
Trg					.703				
Exp					.466				
Accu					.403				
TimMod						.609			
StakeV						.549			
Env						.426			
AD							.733		
Mon							.489		
CybImp							.460		
Tim								.678	
Rel								.439	
Hardware		.453							-.499
AssV									.437

Appendix 3 – Structural Equation Modelling: Fit Indices

Fit Index	Acceptable Threshold Levels	Description
Absolute Fit Indices		
Chi-Square χ2	Low χ2 relative to degrees of freedom with an insignificant p value ($p > 0.05$)	Unreliable for large sample sizes and deviations from normality (Hooper, Coughlan, & Mullen, 2008)
Relative χ2 (χ2/df)	2:1 (Tabachnik and Fidell, 2007) 3:1 (Kline, 2005)	Adjusts for sample size.
Root Mean Square Error of Approximation (RMSEA)	Values less than 0.07 (Steiger, 2007)	Has a known distribution. Favours parsimony. Values less than 0.03 represent excellent fit.
GFI (aka Gamma Hat)	Values greater than 0.95 (Hu & Bentler, 1999)	Scaled between 0 and 1, with higher values indicating better model fit. This statistic should be used with caution.
AGFI	Values greater than 0.95	Adjusts the GFI based on the number of parameters in the model. Values can fall outside the 0-1.0 range.
RMR	Good models have small RMR (Tabachnik and Fidell, 2007)	Residual based. The average squared differences between the residuals of the sample covariances and the residuals of the estimated covariances. Unstandardised.
SRMR	SRMR less than 0.08 (Hu and Bentler, 1999)	Standardised version of the RMR. Easier to interpret due to its standardised nature.
Incremental Fit Indices		
IFI (aka BL89)	Values greater than 0.95 (Hu & Bentler, 1999)	Bollen's Fit Index (1989). Non-normed, compensates for the effects of model complexity.
NFI	Values greater than 0.95 (Hu & Bentler, 1999)	Assesses fit relative to a baseline model which assumes no covariances between the observed variables.
NNFI (TLI)	Values greater than 0.95 (Hu & Bentler, 1999)	Non-normed, values can fall outside the 0-1 range. Favours parsimony. Performs well in simulation studies (Sharma et al, 2005; McDonald and Marsh, 1990)
CFI	Values greater than 0.95. (Hu & Bentler, 1999)	Normed, 0-1 range.

Table 2 - Fit Indices and Their Acceptable Thresholds - Note: adapted from (Hooper, Coughlan, & Mullen, 2008)