2014 6th International Conference on Cyber Conflict
P.Brangetto, M.Maybaum, J.Stinissen (Eds.)
2014 © NATO CCD COE Publications, Tallinn

Dynamic Cyber-Incident Response

Kevin Mepham
PhD Research Student,
Defence and Cyber Security Research Group,
Brunel University
London, UK
kevin.mepham@brunel.ac.uk

Panos Louvieris
Defence and Cyber Security Research Group,
Brunel University
London, UK
panos.louvieris@brunel.ac.uk

Gheorghita Ghinea
Defence and Cyber Security Research Group,
Brunel University
London, UK
george.ghinea@brunel.ac.uk

Natalie Clewley
Defence and Cyber Security Research Group,
Brunel University
London, UK
natalie.clewley@brunel.ac.uk

Abstract: Traditional cyber-incident response models have not changed significantly since the early days of the Computer Incident Response with even the most recent incident response life cycle model advocated by the US National Institute of Standards and Technology (Cichonski, Millar, Grance, & Scarfone, 2012) bearing a striking resemblance to the models proposed by early leaders in the field e.g. Carnegie-Mellon University (West-Brown, et al., 2003) and the SANS Institute (Northcutt, 2003). Whilst serving the purpose of producing coherent and effective response plans, these models appear to be created from the perspectives of Computer Security professionals with no referenced academic grounding. They attempt to defend against, halt and recover from a cyber-attack as quickly as possible. However, other actors inside an organisation may have priorities which conflict with these traditional approaches and may ultimately better serve the longer-term goals and objectives of an organisation.

Shortcomings of traditional approaches in cyber-incident response and ideas for a more dynamic approach are discussed including balancing the requirements to defend against an incident with those of gaining more intelligence about an attack or those behind it. To support this, factors are described which have been identified as being relevant to cyber-incident response. These factors were derived from a literature review comprising material from academic and best-practice sources in the computer security, intelligence and command and control fields.

Results of a PhD research survey conducted across military, government and commercial organisations are discussed; this assesses the importance of the aforementioned factors. The surveyed participants include (but were not limited to) respondents from areas such as Intelligence and Operations, as well as the more conventional computer security areas.

Situational awareness and decision-making aspects of incident response are examined as well as other factors such as intelligence value, intelligence gathering, asset value, collaboration and Intelligence Cycle factors.

Keywords: *Cyber Incident Response Active Passive Risk*

1. INTRODUCTION

In recent decades technology has changed rapidly, especially in the Information Technology (IT) area; in a drive for efficiency and cost-saving organisations and governments have become increasingly-dependent upon IT and its supporting infrastructure. In recent years this transformation has also led to an increasing dependence upon the Internet by critical or important infrastructure. However, the other side of the coin is that this evolution has led to an increased exposure to exploitation or compromise by those with hostile intent as traditionally closed networks or systems have become more accessible. Despite this rapidly-evolving environment and associated risks, to all intents and purposes standard computer security incident response models, have remained largely unchanged since the 1990s. Furthermore, much of the research which contributed to the production or revision of these models has been called into question. In a review of 90 works which claimed to employ quantified investigation and analysis of security, it was discovered that the validity of the majority of these works was questionable when used in the perspective of an operational setting (Verendel, 2009).

This research investigates factors which may influence Cyber-Incident Response from the perspective of a wider-affected audience in order to produce a more dynamic and stakeholder-independent Cyber Incident Response model. It attempts to do this by taking into account the strategic and wider priorities of an organisation and also considers intelligence gathering and sharing priorities as part of incident response. Although not yet at an experimental stage in the research, evaluation of the identified factors by international communities from within and outside the core Cyber-Security areas have already confirmed the requirement for changes to the current models. This has been deduced from both discussion and by the statistical analysis of their responses collected as part of a research survey discussed in this paper.

2. RELATED WORK

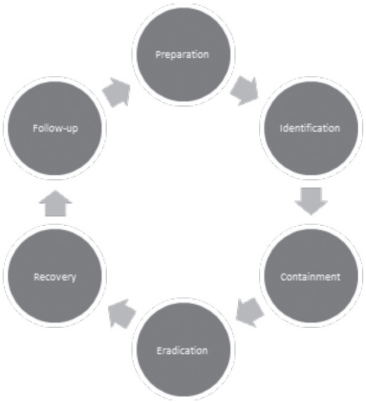
As part of the research, a cross-domain literature review was carried out; this covered not only the core CIS/Cyber Security field but also areas such as Military Intelligence, Command and Control (C2) and Human Factors issues. The aim of this review was to identify significant independent variables defining the problem domain of Cyber Incident Response including parallels from other domains outside of the Cyber Security field. In parallel to the literature review, participation in Multi-National Experiment 7 (MNE7), an experiment intended to capture the important factors related to preservation of access to the Global Commons (air, sea, space and cyber), led to the identification of factors deemed to influence the effectiveness of Cyber Situational Awareness; a key component of effective Cyber Incident Response.

A. Literature Review

The literature review was approached from two perspectives. The first was a practitioner's perspective looking at the best-practice documents from Cyber Security and associated fields. The second was the academic perspective where research was already busy identifying gaps and shortcomings within the field. Both of these perspectives were then drawn together to identify a consolidated list of the existing factors influencing Cyber Incident Response as well as missing factors which could be utilized in future models. These perspectives and factors are described in the subsequent paragraphs.

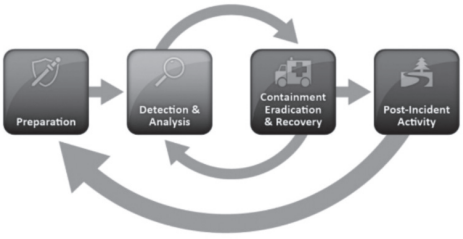
Traditional cyber incident response, even from the early days of widespread computer use, tended to take an approach of detecting an incident and then trying to halt, contain or mitigate it followed by a recovery phase to restore normal operation. Post-incident analysis was then used to identify potential improvements to the infrastructure and processes (if necessary). This approach is best illustrated utilising the SANS Institute Model (Northcutt, 2003) which added more detail to the cycle in 2003 (Figure 1).

FIGURE 1 - SANS INSTITUTE INCIDENT RESPONSE CYCLE 2003 (NORTHCUTT, 2003)



Although some evolution has taken place, even the most recent iterations of the best-practice processes still broadly cover the same issues, for example the latest guidance (Cichonski, Millar, Grance, & Scarfone, 2012) published by NIST (Figure 2), establishes the incident response process as an inner circle with "lessons learned" (post-incident activity) providing the feedback to improve the infrastructure and processes (preparation).

FIGURE 2 - NIST SPECIAL PUBLICATION 800-61 INCIDENT HANDLING PROCESS (CICHONSKI, MILLAR, GRANCE, & SCARFONE, 2012)



This perspective is also echoed in international standards, for example the international Information Security Management standard ISO27001 advocates the Deming Cycle (Calder & Watkins, 2008). This standard advises that Information Security (and consequently Cyber-Security) can be divided into the phases of Plan, Do, Check and Act. Within the live incident response environment this is reduced to the "Do", deploy the sensors and implement planned measures; "Check", look for incidents by monitoring the information sources that have been deployed; Act, respond to detected incidents or identified shortcomings. Outside of this shortened cycle the planning takes place to improve the longer term protection of the information and infrastructure. However, all of these cycles are based around the core tenets of preserving the Confidentiality, Integrity and Availability of these protected assets. Whilst understandable from a Cyber Defence perspective, there are also other communities impacted by Cyber Incidents.

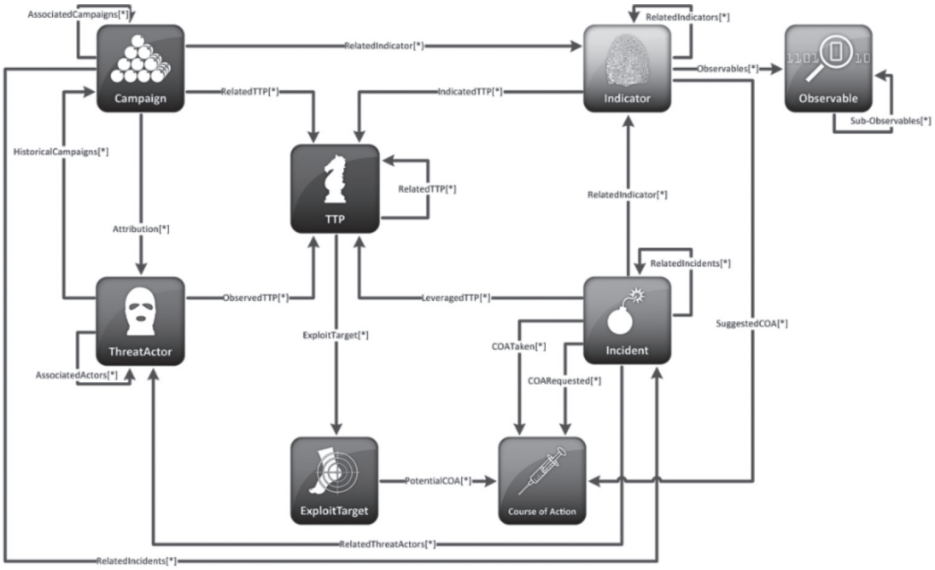
Looking at cyber incidents from a Military/Business Intelligence perspective, the Intelligence Cycle lens can be applied. The Intelligence Cycle (MoD, UK, 2011) has some similarities to the traditional Incident Response cycles (commonly having the phases Planning and Direction, Collection, Analysis or Processing and Dissemination), however, there are also some contrasts. Intelligence work by its nature is designed to gather information about potential adversaries as well as understanding this in the context of own and partner capabilities and objectives; as Sun Tzu (Tzu, 2011) is reputed to have stated "know the enemy and know yourself, in a hundred battles you will never be in peril". This emphasis on "knowledge of the enemy" puts the Intelligence community at odds with the Cyber-Defence community as Intelligence gathering is not a natural partner of preserving Confidentiality. However, this is not an insurmountable problem providing that the priorities can be put in context as will be discussed later.

In the UK, joint doctrine (MoD, UK, 2011) talks about "Inform", which is defined as "the ability to collect, analyse, manage and exploit information and intelligence to enable information and decision superiority" i.e. this equates to the "Disseminate" of the Intelligence Cycle. In traditional Cyber-Incident Response the collection and analysis is only traditionally carried out up to the point where the incident is thwarted and in the post-incident analysis; at this point the incident has been resolved or averted and there is nothing more to gain in terms of intelligence value (or to disseminate in order to improve infrastructure or intelligence). Combined with the increasing difficulty of maintaining a credible honeynet or honeypot solution (Rowe, 2006); (Wang, Wu, Cunningham, & Zou, 2010) where information has traditionally been gathered to provide Cyber intelligence, this leads to the danger of information starvation for those trying to assess some of the key Cyber Intelligence requirements such as attacker identity, motivation, ultimate target, attack methods, attacking resources, attack goal. The lack of this type of intelligence (especially for novel attacks or unknown attackers) will undoubtedly lead to a reduced ability to defend in the longer term.

With reference to Situational Awareness, this requirement for Cyber-Intelligence is indirectly reinforced by Endsley's model (Endsley, 1995); in this model "Long term memory stores" are seen to inform "expectations". In turn expectations inform the three identified stages of situational awareness: perception, comprehension and projection. This approach infers that without the information (or intelligence) in the long term memory stores the expectations will not be optimally informed, thereby depriving the decision maker of the best situational awareness. This introduces the concept of not only utilising static intelligence but also using this to predict future events to enhance decision-making.

Taking this prediction thread further, as early as 2000, the importance of usable intelligence in a cyber-environment was recognised (Yuill, et al., 2000). In this research a military intelligence type process to enhance the effectiveness of intrusion detection and the subsequent incident response was proposed. At that time, prior to the introduction of the SEI State of the Practice process (Killcrece, Kossakowski, Ruefle, & Zajicek, 2003), Yuill et al considered standard incident-response process to be attack repair, neutralization and containment (ARNC). However, by providing positive identification of the attacker (using part of a proposed technique referred to as Cyber-Intelligence Preparation of the Battlespace (C-IPB)), likely compromised devices (LCDs) could also be identified based on models of the attacker and the infrastructure. This information could then be used to produce two types of estimate for Courses of Action (COA) by the attacker: possible and likely i.e. the notion of predicting cyber-incident progress was proposed. From these estimates, further monitoring could be more targeted and incident-response measures more relevant. The C-IPB process is summarised in four steps: define the battlespace (define the boundaries of the infrastructure), describe the battlespace effects (evaluate the infrastructure and its influence on attack and defence), evaluate the threat (assess attacker capabilities and intent) and determine the threat's COA and infrastructure LCDs. At that time, the cyber-intelligence was broken down into: what the attacker has done (executed action), capabilities, personal traits and intentions. However, whilst the principles remain sound there has been significant development in the types of information that are relevant to capturing threats and attacks such as those described in the Structured Threat Information eXpression (STIX) community-driven standard (Barnum, 2012) maintained by MITRE Corporation. This standard is directly related to another standard maintained by MITRE Corporation, Trusted Automated Exchange of Indicator Information (TAXII) which is designed to allow collaboration between Cyber-entities to exchange threat intelligence.

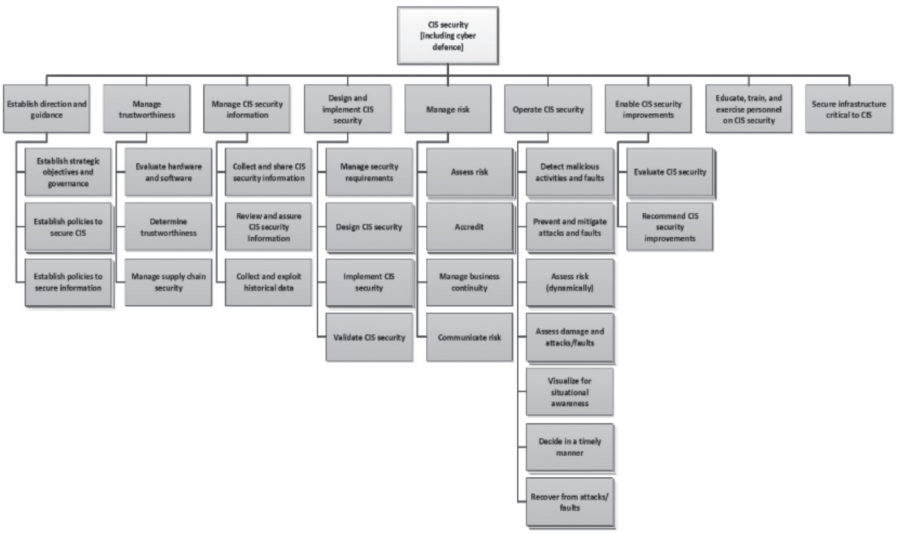
FIGURE 3 - MITRE CORPORATION STRUCTURED THREAT INFORMATION EXPRESSION (STIX) (BARNUM, 2012)



STIX, provides identification of each of the information components illustrated in Figure 3 by a number of variables. Utilising these it attempts to achieve the following four use case goals: analyse cyber threats; specify indicator patterns for cyber threats; manage cyber response threat activities and the sharing of cyber-threat information.

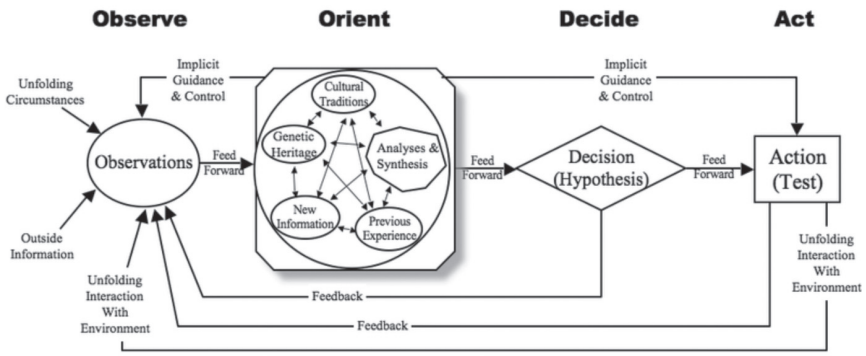
The combination of several elements from the approaches in the previous paragraphs can also be found in a NATO framework document (Hallingstad & Dandurand, 2011) this document (produced with cooperation from several NATO member nations participating in a NATO-led research task group) is summarised in a top-level diagram (Figure 4) which also includes the incident-response processes. This framework was broad enough to cover areas of interest, not only to the Cyber-Defence community but also for senior decision makers and Intelligence community. Whilst explaining the more obvious issues of making sure that the appropriate sensors and trained personnel are in place to allow incidents to be detected, it also covered areas such as ensuring that risks are owned and managed and that trustworthiness of hardware, personnel and partners is addressed. Interestingly, the quandary of whether to stop interesting attacks or to monitor them to gain intelligence is also discussed briefly within the document. Information sharing with regard to CIS security incidents is also identified as a relevant issue in this framework; the importance of this is confirmed by the international work that has taken place in recent years such as Multi-National Experiment 7 – Access to the Global Commons (MNE7), and continues to take place at the moment in the Multinational Capability Development Campaign (MCDC) Cyber Implications for Combined Operational Access (CICOA) 2013-2014.

FIGURE 4 - NC3A CIS SECURITY FRAMEWORK



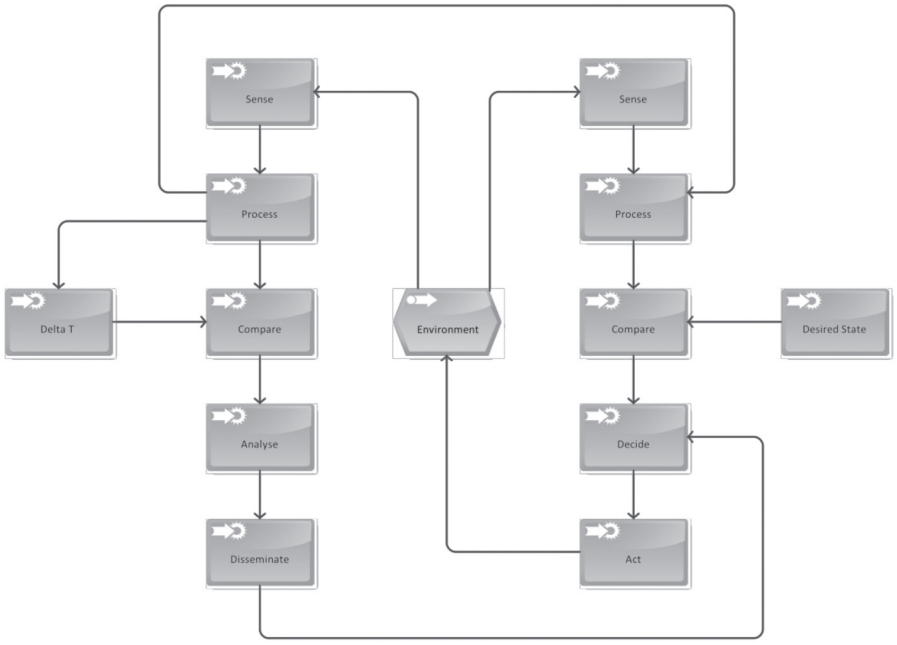
Ultimately, whichever response is chosen to a cyber-incident by the empowered decision-maker, it has to be timely enough to be able to influence the outcome. This is best summarised by the model proposed by Colonel John Boyd USAF (Orr, 1983). The model of Observe (monitor the enemy's actions), Orient (work out possible actions and consequences based on the observations of the enemy and knowledge of your own capabilities), Decide (choose a course of action), Act (carry it out), otherwise known as the OODA loop was designed to describe how to gain superiority in air combat. By completing an OODA loop more quickly than an adversary, the adversary would not be able to react in time to gain air superiority. In Figure 5, this is shown as not only a single uni-directional loop (as illustrated by several interpretations of the model), but also a series of inner feedback loops which influence the observation and consequently orientation, decision-making and subsequent action. Although originally intended to reflect air combat, it has since been recognised that this has wider application for strategy in both military and commercial contexts. This is also pertinent in the context of Cyber-Incident response where, for the advanced attacker, they are often able to respond quickly to any mitigation or actions carried out by the defender. If this response is achieved inside the defending OODA loop they then gain "cyber superiority".

FIGURE 5 - COLONEL JOHN BOYD USAF'S OODA LOOP (ORR, 1983)



A further development of the OODA loop was proposed to describe a Command, Control, Communication and Intelligence (C3I) model (Figure 6) which explicitly includes a simulation/ prediction function (Lawson, 1980).

FIGURE 6 - C3I PROCESS MODEL (LAWSON, 1980)



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

However, in the context of cyber-incident response, the "Desired State" could be replaced with "normal" state to reflect normal infrastructure operation whilst the left-hand side assesses whether the environment is moving away from or towards this state over time. This is a good demonstration of situational awareness; if used in a military decision-making process, the sensors would provide Intelligence information (rather than data) which is then used with expert knowledge or systems to provide a prediction of the future infrastructure state based on monitored behaviour over time.

Ultimately, the literature review confirmed that Cyber-Intelligence is an essential aspect of Cyber-Incident response; modelling of cyber-incidents to provide prediction/projection of the future path of an incident is also important in providing optimal situational awareness and

that different stakeholders impacted by a cyber-incident can have a different perception of the priorities which may not be aligned with organisational goals. When combining these findings with established models from other areas such as the Command and Control and Intelligence areas it can be surmised that further evolution of Cyber Incident Response is necessary to best serve organisational aims.

B. Contribution of MNE7 to this Research

As previously mentioned, the MNE7 Campaign was conducted at the same time that the literature review was carried out. This experiment brought together a rare collection of professionals from governmental, military, commercial and academic areas from both inside and outside the core cyber security areas. Participation in the collaborative cyber-situational awareness track allowed the opinions of an expert community to be gauged and the same community also provided significant feedback on the pilot questionnaire, where the water was being tested with regard to potential gaps in the existing Cyber Incident Response models and processes. However, one of the strongest messages to come across from this community is that everybody can see the benefits of collaborating by sharing incident information, but in practice they are reluctant to do it. Despite this, given trustworthy filtering of information and a mechanism to establish sufficient trust between partners, collaboration can prove invaluable in enhancing situational awareness. In the context of this research, information received from collaboration is viewed as one of many information sources.

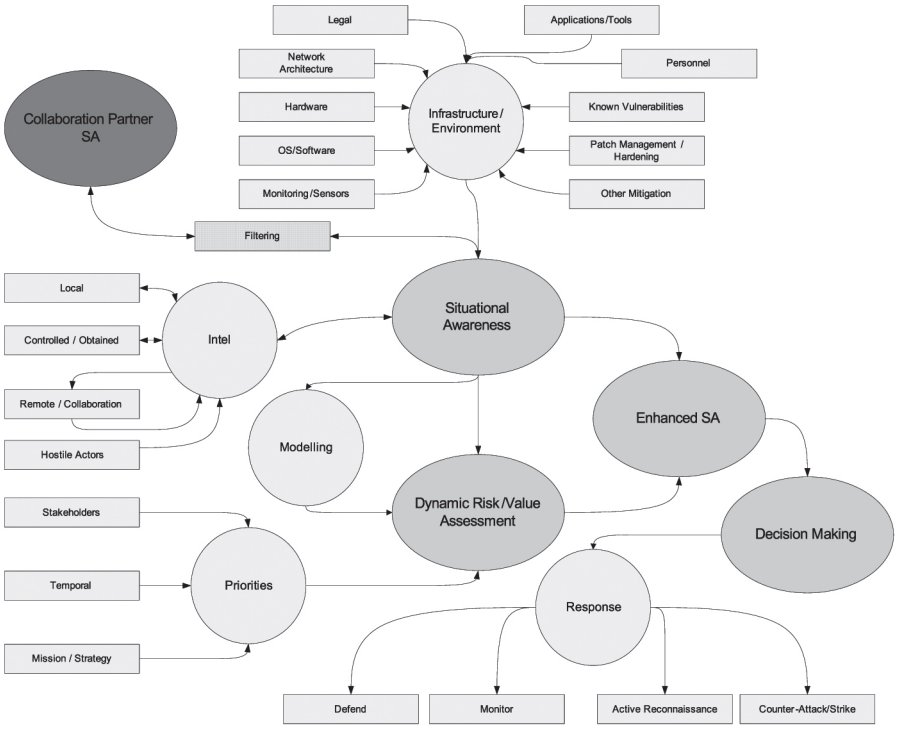
3. METHODOLOGY

A limited pilot survey was carried out with participants from international military, commercial and governmental cyber security communities to evaluate the initially identified variables from the communities and the literature review. Utilising principal component analysis and Varimax rotation (described in more detail later) an initial attempt was made to group some of the identified factors. Whilst not strictly observing the identified grouping, as the results were not statistically significant at that time (due to the sample size) this provided a suitable discussion point within these communities to sharpen the areas of focus for the remaining portion of the literature review and subsequent surveys. However, this focusing of the initial evaluation of these variables, discussions within expert communities and the remainder of the initial literature review led to the production of an initial model which has also been used as a starting point to describe the contribution of cyber to the operational planning process by the technical strand of MCDC-CICOA.

This initial model shown in Figure 7 (which combines process, functions and infrastructure) attempted to describe the interaction between infrastructure and what is described here as static situational awareness i.e. the impact of an incident on the defending environment as it is now, utilising the existing intelligence. This static situational awareness is then used as an input to dynamic risk and value assessment, where, based on the current known situation, modelling of an attack is attempted. This utilises the known vulnerabilities and paths through the infrastructure with the available attack intelligence which is then combined with the assessments by the different stakeholders for that point in time of the value of the threatened assets (recognising that different stakeholders may well place different priorities on the same

asset). The output of this process would be "balance of equities" information to be provided to the key decision maker together with the static situational awareness in order to provide them with enhanced situational awareness. This information would allow them to choose the optimum response in order to meet the organisational goals; examples of these described by the response options (without reference to legal constraints) are to defend the attacked assets via passive means, gather more intelligence about an attack or attacker (via passive means) or use active means to pacify attacker infrastructure or gather more intelligence about the attacker. Referring back to the OODA loop, this whole process needs to be completed before the attacker has a chance to detect and respond to any actions taken by the defenders in order to gain an advantage over the attacker.

FIGURE 7 - INITIAL MODEL



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

7-point Likert scale for each of the assessed variables in order to achieve an appropriate degree of granularity in the results; to date, a combined total of 186 professionals from the identified communities have participated in the survey.

4. RESULTS AND ANALYSIS

From the results to date, there has been a striking difference in opinion between individuals in all communities and their perception of their organisations' opinions. This assessment was confirmed by paired t-tests where all 30 variables were found to have significant results. From the results it appears that individuals across the communities tend to place more importance on the identified factors than their organisations or communities. A good example of this can be seen in the response to Configuration Management (CM) where almost half of the participants assessed that effective CM was essential to provide optimal Cyber-Incident Response (Figure 8) whereas in their communities and organisations just over 10% of the participants (Figure 9) believed that their communities and organisations found CM to be essential. Other notable examples of this phenomenon were reflected in the use of automatic tools for intelligent data reduction, sensors for monitoring at all levels, timeliness and reliability of data and to a lesser extent areas such as environmental conditions that analysts work in.

FIGURE 8 – CONFIGURATION MANAGEMENT: INDIVIDUAL RESPONSE

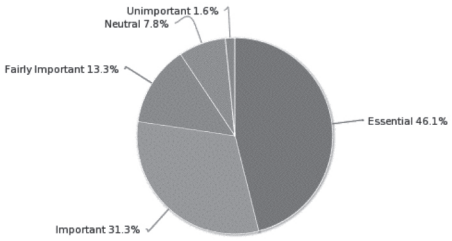
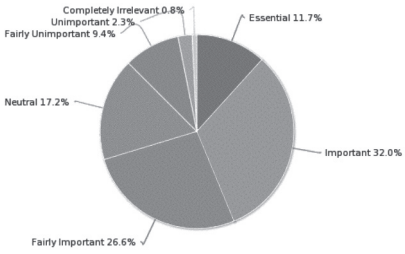


FIGURE 9 – CONFIGURATION MANAGEMENT: ORGANISATION RESPONSE



As expected, there are also significant differences in the importance placed on assigning a value to intelligence regarding the attackers and attacks between the communities. This

is demonstrated below in the contrasting opinions on the importance of placing a value on Intelligence information as part of the Cyber-Incident response process (Figures 10 and 11).

FIGURE 10 - IMPORTANCE OF INTELLIGENCE VALUE: INTELLIGENCE PROFESSIONALS

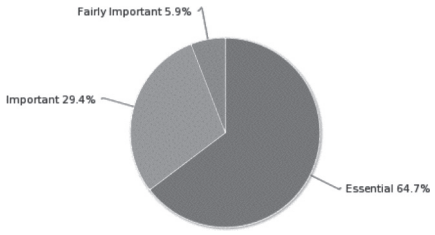
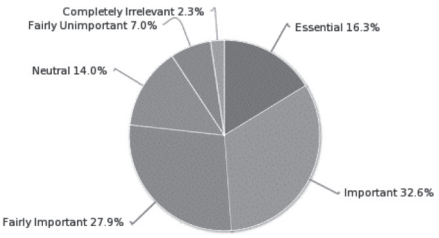


FIGURE 11 - IMPORTANCE OF INTELLIGENCE VALUE: IA/SECURITY PROFESSIONALS



However, some unexpected differences of opinion were also identified across the communities, even relating to the importance of stakeholders being able to assess the value of assets from different perspectives (Figures 12 to 15). In this example, it might be assumed that the CIS/ Engineering communities believe that they already know the priority of the assets that they maintain so it is not essential to have the functional owner's perspective.

FIGURE 12 - IMPORTANCE OF ASSESSING STAKEHOLDER VALUES: IA/SECURITY COMMUNITY

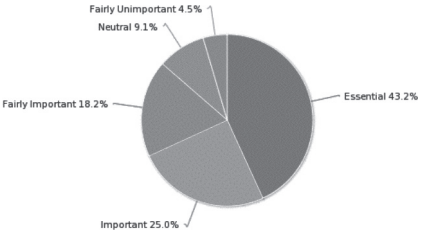


FIGURE 13 - IMPORTANCE OF ASSESSING STAKEHOLDER VALUES: OPERATIONS COMMUNITY

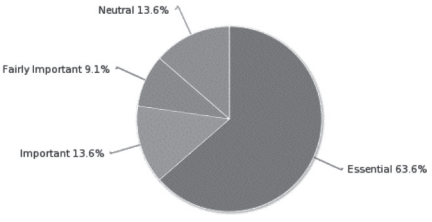


FIGURE 14 - IMPORTANCE OF ASSESSING STAKEHOLDER VALUES: IT/ENGINEERING COMMUNITY

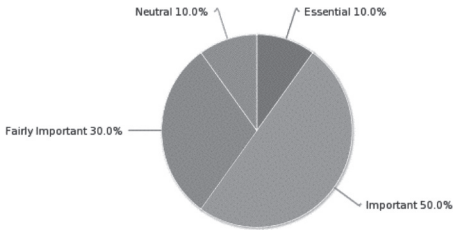
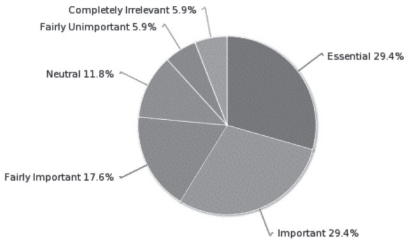


FIGURE 15 - IMPORTANCE OF ASSESSING STAKEHOLDER VALUES: INTELLIGENCE COMMUNITY



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

For the first time (as far as can be determined) factor analysis was carried out to determine key areas of importance in the cyber incident response process. This was achieved by analysing the results obtained from the communities of interest (from the survey) using principal axis factoring and Varimax[1] rotation. This dimension reduction process allows correlated variables to be grouped into common components or factors and those which are orthogonal to them are grouped into separate factors. From the sample size, it is suggested (Hair, Black, Babin, & Anderson, 2014) that a factor loading of more than 0.50 be used in order to achieve power level of 80%. Utilising this process (using the SPSS software package), the following factors were identified from the data sources:

i) Sensors (monitoring of operating system logs, network sensor logs, application logs etc).
ii) Collaboration (both inbound and outbound SA collaboration with trusted partners).
iii) Information Credibility (accuracy, timeliness and reliability of information).

1 Created by Henry F Kaiser in 1958

iv) Incident Discrimination (analyst experience and automated tools to reduce the "noise" of routine events).

TABLE 1- PRINCIPAL COMPONENT ANALYSIS OF INTELLIGENCE SOURCES

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

These variables were then grouped together to create a process that for the purposes of the model will be called Intelligence Gathering. Utilising a series of similar reductions using the same Varimax process, the rest of the variables were grouped together to create a number of functions to form the basis for a new model. These processes then become:

i) Intelligence Gathering: the gathering of information from relevant sources with the appropriate credibility including collaboration information received from partners.
ii) Static Impact Evaluation: the immediate assessment of the relevance of the attack at that point in time given the received intelligence and the known configuration of the infrastructure.
iii) Dynamic Risk and Value Assessment (DRVA): the relative values of the "at risk" assets from the perspectives of different stakeholders combined with their exposed known vulnerabilities and the known attacks. In this function an intelligence value is also calculated for the information that may be gained by responding in an "unconventional" manner. The organisational goals are also taken into account in creating this assessment for both the asset and intelligence values.
iv) Modelling: this is the prediction of the future path of the attacks based on known attack patterns, attackers, exposed vulnerabilities and asset values. Combined with the output of the DRVA this provides the decision maker with optimal enhanced situational awareness.
v) Decision: based on the modelling, the DRVA and the static impact evaluation, the responsible decision maker takes the organisational goals into account before deciding on a course of action. They are provided with a number of response options (which may be reduced by their legal and organisational constraints): these options are:

a. A conventional response, i.e. defend against the attack via conventional means (for example blacklists, IPS, etc).
b. Passive monitoring response, i.e. observe but show no reaction at all to the incident (as though it was undetected) in order to gain intelligence.
c. Active intelligence gathering, i.e. actively reconnoitre the attacking infrastructure by any means possible in order to gain intelligence but without intentionally causing disruption to the attacking infrastructure.
d. Cyber strike, neutralise the attacking infrastructure via any available Cyber means.

5. CONCLUSIONS

By analysing the relevant literature it is concluded that the traditional responses to Cyber-Incidents and the implementation of these models are not meeting the requirements of all communities impacted by them. In order to meet these requirements, not only do responses need to be based on the "balance-of-equities" decision between the priorities of the different stakeholders whose assets are being attacked, they should also take account of the value of intelligence (both local and collaborative) associated with an attack and consider a more flexible suite of response options. The proposed Dynamic Cyber-Incident Response model enables those responsible for cyber-incident response and their key decision-makers to develop a more dynamic set of response procedures within their legal and organisational constraints. That is not to say that if a high-value or critical asset is being attacked that it should necessarily be allowed to fall in order to gain intelligence; however, if a low value asset is being attacked and the attack or attacker is unknown or novel, the organisation might be better served by learning about the attack rather than defending the asset. With this approach, the gained intelligence could well help to defend a higher-value asset in the future.

6. FURTHER WORK

The next stages of this work will be to evaluate the survey data and refine and develop the proposed model. The intention is evaluate the model in a variety of deployment scenarios utilising a purpose-built Cyber Range at the university. The current evaluation criteria for the model are expected to be

i) Assessment of intelligence gains which may be achieved by allowing a predefined set of cyber incidents to continue under observation.
ii) The contribution of DRVA to the situational awareness of the decision-maker and consequent influence on their ability to make the optimal decisions.

REFERENCES:

Barnum, S. (2012). *Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX)*. Online: Mitre Corporation.

Calder, A., & Watkins, S. (2008). *IT Governance: A Manager's Guide to Data Security and ISO27001/ISO 27002*. London and Philidelphia: Kogan Page.

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Special Publication 800-61 Revision 2; Computer Security Incident Handling Guide*. NIST, US Department of Commerce.

Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors: The Journal of the Human Factors and Ergonomics Society, 37*(1), pp. 32-64.

Hallingstad, G., & Dandurand, L. (2011). *CIS Security (including Cyber Defence) Capability Breakdown*. The Hague: NATO Consultation, Command and Control Agency (NC3A).

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2014). *Multivariate Data Analysis - Pearson New International Edition* (7th ed.). Upper Saddle River, New Jersey, US: Pearson.

Killcrece, G., Kossakowski, K.-P., Ruefle, R., & Zajicek, M. (2003). *State of the Practice of Computer Incident Response Teams (CSIRTs)*. Pittsburgh, PA, USA: SEI Carnegie Mellon University.

Lawson, J. S. (1980). Command control as a process. *19th IEEE Conference on Decision and Control including the Symposium on Adaptive Processes* (pp. 1-6). IEEE.

MoD, UK. (2011). *JDP 0-01 British Defence Doctrine.* Shrivenham, UK: MoD Development, Concepts and Doctrine Centre.

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

Northcutt, S. (2003). *Computer Security Incident Handling*. 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.

Rowe, N. C. (2006). Measuring the Effectiveness of Honeypot Counter-Counterdeception. *Proceedings of the 39th Annual Hawaii International Conference on Periodical, System Sciences, 2006*. (pp. 129c-129c). IEEE.

Tzu, S. (2011). *The Art of War (translated by Thomas Cleary)*. Boston and London: Shambala.

Verendel, V. (2009). Quantified Security is a Weak Hypothesis. *Proceedings of the 2009 Workshop on New Security Paradigms* (pp. 37-50). New York, USA: ACM.

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

West-Brown, M. J., Stikvoort, D., Kossakowski, K.-P., Killcrece, G., Ruefle, R., & Zaijicek, M. (2003). *Handbook for Computer Security Incident Response Teams (CSIRTs) 2nd Edition*. Carnegie Mellon University.

Yuill, J., Wu, F., Settle, J., Gong, F., Forno, R., Huang, M., & Asbery, J. (2000). Intrusion-detection for incident-response, using a military battlefield-intelligence process. *Computer Networks*, 671-697.