# A Model to Facilitate Discussions about Cyber Attacks

Jassim Happa[1] and Graham Fairclough[2]

[1] Department of Computer Science, University of Oxford, UK
[2] Department of Politics and International Relations, University of Oxford, UK
jassim.happa@cs.ox.ac.uk, graham.fairclough@balliol.ox.ac.uk

**Abstract.** The evolution of the Internet and digital systems is making it increasingly difficult to understand cyber attacks. Politicians, ethicists, lawyers, business owners and other stakeholders are all affected by them, yet many lack necessary technical background to make correct decisions in dealing with them. Conversely, cyber-security analysts have a better understanding about the technical aspects of cyber attacks, but many do not understand the repercussions of decisions made from their perspective alone. Both contextual (e.g. societal, political, legal, financial, reputational aspects etc.) as well as technical considerations must be taken into account in making decisions that relate to a cyber attack. A plethora of cyber-attack models exist today that aid (to some degree) understanding of attacks. Most of these however focus on delivering insight from a single perspective: technical detail or understanding of human-centric factors. These approaches do not outline how a discussion among expert-domain people of different backgrounds should be conducted to establish a basic situational awareness understanding, from which to make collective decisions. In this paper, we present our efforts towards establishing such a model to enable a collective approach to understanding and discussion of cyber attacks. In turn, decision makers should be able to compensate for their limitations by building a mental map that serves as a basic foundation for understanding an attack. We propose a first version, but believe extensions should be made and acknowledge that testing and assessment in real environments is necessary.

## 1 Introduction

The vocabulary of cyberspace is a much debated topic. The degree to which cyberspace, loosely defined as: the conceptual landscape where people and machines interact, actually exists and the extent to which it can be considered a new threat environment or simply a medium through which there is a means to an end are widely discussed. Several opinions exist, cyberspace can be described as: "*a global commons that has enhanced interaction, information exchange and productivity*" [INSA 2012]; "*an operational domain framed by the use of electrons…to exploit information via interconnected systems and their associated technology*" [Nye 2011], or as Healey in his recent work on cyber conflict defines simply as "*interconnected information technology*" [Healey 2013].

Cyber attack is another conflicted term. Current definitions often fall within two principal categories: *process-driven* or *taxonomy/hierarchical* [Bishop 1995, Cohen 1997, Howard 1998, Lough 2001, Simmons et al. 2009, Hutchins et al. 2011, MITRE]. Being able to precisely define a cyber attack is becoming increasingly difficult.

The technical complexity of systems, the growing variety of exploitable attack vectors and perhaps most importantly the ubiquitous integration of Internet technology into all aspects of our daily lives compounds this problem. This uncertainty is creating a disturbing trend: critical decisions concerning cyber attacks whether it be incident response handling or new policy formulation (as a consequence of cyber attacks) are dependent on a complete understanding of cyber attacks and how they relate to society or organisations. Presently however, such decisions are dealt with by individuals who lack the necessary experience or who approach the issue from a narrow perspective. The failure to adopt a comprehensive approach to the problem is frequently the norm, leading to an incomplete understanding of the attack and a failure to provide an appropriate solution.

A mental model is a person's understanding of a real-world system (such as a cyber attack). Norman [1983] describes mental models as naturally evolving. They change over time as a person learns more about the system, and while they may not be complete or technically accurate, they must be functional. In other words, people must be able to act upon them.

While verbal communication limits our capability to share our own mental model, and erroneous information may be conveyed if attempted, mental models are useful in providing an up-to-date description of the behaviour of a system. However, **mental models are not perfect, and no two maps will be perfectly aligned** because they are developed individually; they are often incomplete and become unstable over time as people forget details; they lack firm boundaries with similar devices and operations becoming confused and they are "unscientific" with people maintaining "superstitious" behave even when it is unnecessary[1].

Even experts from the same domain disagree amongst each other in expert topics, and experts of differing domains are also likely to disagree even when their mental maps are closely aligned. These issues are of particular relevance when understanding the evolving cyber domain. Where people form mental models about "*what a cyber attack is*" and "*what a particular instance of a cyber attack has done*" regardless of any prior experience and background.

Our proposed approach, suggests that by aiming for **a common, shared reference point** will lead to a greater collective understanding of the same problem space, and a better ability to recognise their own gaps in knowledge. Allowing a "common" mental model of the cyber attack to be constructed. One that can be shared by all actors.

[1] For further explanation of the issues surrounding mental models, see Norman [1983].

Figure 1 illustrates the response to a cyber attack decision-making process. Three different mental models of the attack, based upon the actor's role and/or previous experience are integrated to form the basis of "some" common interpretation of the event. This interpretation is then used to construct a decision on the response to the cyber attack. However, this interpretation is likely to lack the degree of detail and shared awareness that is required to produce the necessary level of understanding.

Only from this necessary level of understanding can the correct decision concerning any reaction to the cyber attack be made. **The failure to move from "some" interpretation of the event to a single, shared level of understanding is a consequence of the lack of a common foundation or reference point from which each of the actors derives their individual mental models.** This point is shown in Figure 1 where a policy maker, a technical analyst and a legal representative formulate a response – the decision. Based upon their own prior knowledge of cyber attacks and considered from their own perspectives loosely combined through "some" interpretation.

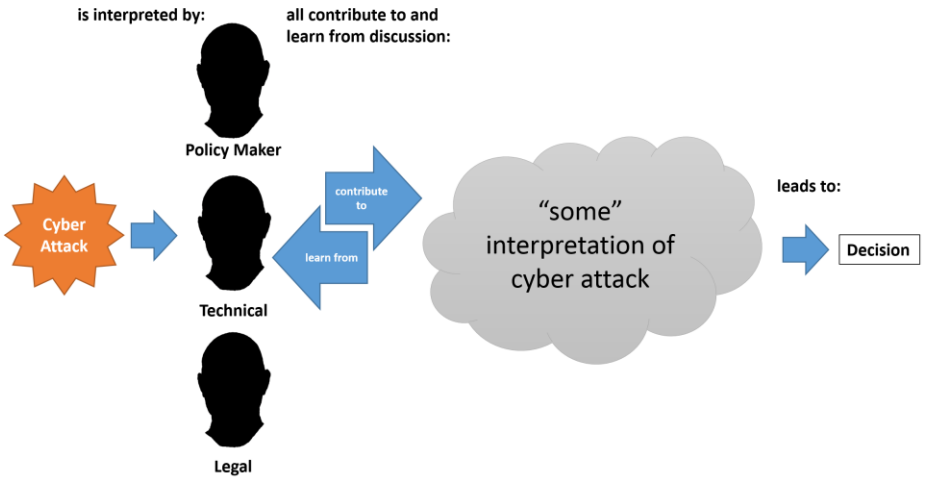


**Fig. 1: The Cyber Attack Decision-Making Process.**

We argue that knowledge gaps occur because of the failure to move from "some" interpretation to the necessary level of understanding required to enable decision makers to take appropriate, compensatory actions i.e. seeking advice from those who do possess the requisite insight to fill in the respective gaps.

Our approach proposes a model that can be used to fill in these knowledge gaps. The outcome being a more appropriate decision. We envisage this transformation as being a weighting problem. For instance, if the decision maker has a non-technical background (e.g. law, business or ethics), more consideration (weight) will be required on the technical aspects during the decision making process to yield a balanced result.

In this chapter, we investigate existing definitions of cyber attacks with in order to understand their characteristics and what the impacts they have upon actors operating in cyberspace today. We use this to propose our model to generate shared understanding of cyber attacks for decision makers. Our approach is a high-level (abstract), inclusive approach that enables decision makers from different backgrounds and roles to form greater understanding of cyber attacks. Our intent is to enable informed decisions on how to response to a cyber attack, which incorporate a number of perspectives to be made. We do not attempt to define concepts such as cyberspace, attacks or defences comprehensively believing such definitions are not necessary for our abstract approach and that adequate literature exists elsewhere.

The remainder of this chapter is as follows: Section 2 lists the related work in modelling cyber attacks. Section 3 outlines our model and how it can be used in relevant environments, while Section 4 presents a discussion about additional applications; how it might be extended for other cyber events. We also discuss means to test and assess the usefulness of our model and potential future work. Finally, in Section 5 we present our conclusion.

## 2 Related Work

The development of new technologies is frequently accompanied by the concurrent exploitation of identified and unidentified concerns within these systems. These weaknesses include design failures, network architecture or software challenges, those that occur during implementation and those that become apparent after adoption. An insider threat may use a tool or exploit social weakness that only becomes apparent after a period of time, while an *Advance Persistent Threat* (APT) may achieve success through agile exploitation of a chain of occurrences. Some of these occurrences exploit technical weaknesses while others exploit flaws in human behaviour.

A large body of cyber security literature identifies a set of core components that constitute a cyber attack. We have framed these in a manner in which we assess most decision makers will be able to understand and make sense of; technology-centric models, social models and cyber situational models. We identify some of the more important models to illustrate existing threats and current academic focus.

### 2.1 Technology-centric Models

Technology-centric models seek to define cyber attacks from the perspective of how an attack operates. These are typically described at a lower (detailed), technical level (e.g. how a piece of malware operates or how a vulnerability can be exploited), and frequently require a high degree of technical knowledge of the system and its constituent parts in order for sense to be made of a cyber attack. These models often remain difficult for decision makers lacking a technical background to comprehend the full implications of a cyber attack and through which to generate the necessary degree of understanding. Examples include:

- Bishop [Bishop 1995]: Bishop presented a taxonomy that expresses attacks in the form of six axes: Nature of a flaw; Time of introduction; Exploitation gain; Effect domain; Minimum number necessary and the source of the identification of the vulnerability.

- Cohen [Cohen 1997]: Cohen expressed network attacks based on a defined set of properties. These properties view attacks in terms of: Non-orthogonality; Correlation; Hardware Non-specificity; Description; Applicability and Incompleteness. This approach views cyber defence as representing a mirror model.

- Howard [Howard 1998]: Howard's model is process-based, taking into account five stages of an attack: *Attackers, tools, access, results and objectives*. Events that occur in each of the process stages are used to derive understand of the nature of the attack.

- Lough [Lough 2001]: Lough proposed VERDICT: the *Validation Exposure Randomness De-allocation Improper Conditions Taxonomy*. The model specifies four characteristics of network attacks: Improper validation (insufficient validation resulting in unauthorised access); improper exposure (a system or information is improperly exposed to attack); improper randomness: (insufficient randomness results in exposure to attack), improper de-allocation (information is not properly deleted after use and thus can be vulnerable to attack). VERDICT represents a deep technical approach to understanding cyber attacks.

- AVOIDIT [Simmons et al. 2009]: The AVOIDIT methodology is a classification scheme outlining in a tree hierarchy what constitutes a network attack. Its focus is upon: Attack Vector; Operational Impact; Defence, Informational impact and Targets.

- Cyber Killchain [Hutchins et al. 2011]: The Cyber Killchain is another process-based model for describing the stages of a cyber attack. These are Reconnaissance, Weaponization, Delivery, Exploit, Installation, Command & Control, and Act on Objectives.

### 2.2 Social and People-centric Models

Social and people-centric models attempt to understand a cyber attack from a human behavioural perspective. Approaches focus on a wide spectrum of behaviour stretching from the impact of training, identification of non-trustworthy individuals who might represent a cyber-security risk to the discovery of how human behavioural failures can be exploited as part of the cyber-attack process (e.g. phishing). This approach is as technically demanding to the non-human behaviourist as the technical centric frameworks are to non-technicians. Examples include:

- Greitzer et al. [2009] describes an approach to predictive modelling for insider threat mitigation, and continued in 2013 [Greitzer et al 2013] with a paper on methods and metrics for evaluating analytic insider threat tools.

- The Centre for the Protection of National Infrastructure [CPNI] presented guidance to help manage risk of employees' behaviour damaging businesses called *Holistic Management of Employee Risk* (HoMER).

- *Social engineering: The art of human hacking* [Hadnagy 2010] illustrates the methods by which individuals are "persuaded" to conduct actions that result in a negative impact upon them through subsequent loss in cyberspace.

### 2.3 Cyber Situational Awareness and Understanding Models

Cyber situational awareness and understanding models attempt to adopt a high-level, approach to considering cyber attack. Focus is on the environment in which the cyber attack occurs and the resultant impact upon different elements or layers within it. These models are differentiated by the nature of the elements or layers considered. The need for deep technical or behavioural knowledge is of less importance: the aim being to place cyber attacks into context as opposed to define a cause. Examples include:

- The UK Defence and Science Technology Laboratory (DSTL) [2012] showed a layered model for situational awareness in cyberspace. It consists of six layers of interaction: *Social; People; Persona; Information; Network; Real World,* and attacks can exist on any one or more of these layers.

- *NATO Cyber Security Framework Manual* [NATO 2012]. An interdisciplinary approach to its key activities, including: academic research related to the cyber domain from legal, policy, strategic, doctrinal and/or technical perspectives. The Framework supports the NATO Policy on Cyber Defence.

- *Mission Integration Framework* [Booz | Allen | Hamilton] provides a five pillar approach to considering the cyber security problem: Strategy and Policy; Management and Budgeting; Planning and Operations; People and Culture and Technology and Architecture.

- *The Corporate Insider Threat Detection* (CITD) conceptual model presented by Legg et al. [2013] describes a model for detecting insider threats by exploring hypotheses from measurements of the real world. The model suggests that any measurement is likely to fail on its own, but is likely to yield indicators of insider threats using machine learning and visual analytics.

## 3 Core Model to Discuss Cyber Attacks

To understand modern cyber attacks, it is no longer possible to only consider the technological level, but essential to consider all aspects of cyberspace and the threats generated within it. Our model is underpinned by three assumptions, the need to:

1. **consider cyber attacks holistically** – attacks are no longer only technical, and must be treated as such. Some properties will be measurable, but other aspects will be close to impossible to establish (such as attribution or motives).

2. **involve a wide spectrum of stakeholders** when considering a cyber attack – attacks are best understood when stakeholders are able to communicate effectively amongst each other and make a decision collectively. While this may not always be the case, it is nevertheless important to involve all parties.

3. **establish a shared understanding** – as attacks will consist of properties that relate to a variety of different fields (not just technical), it is important to establish a common perspective of what has happened. It is important to identify the knowledge gaps between each expert in order that they can be removed and thus enable better decision-making.

Our model is not intended to provide a solution to cyber attacks or better classify a type of attack. The model's purpose is to facilitate informed discussion among decision makers of different backgrounds, including; ethicists, policy makers, lawyers, cyber security experts and boardroom executives (among others). By identifying aspects of an attack within a framework of relevant categories, each containing relevant sub-categories we believe a better comprehension of a cyber attack can be achieved regardless of prior knowledge and experience.

The model aims to enable stakeholders from a spectrum of backgrounds to communicate about cyber attacks in a manner that is enabled by a common position of understanding. From this common understanding, the most appropriate decisions can be made. Figure 1 showed this in the context of making such decisions within organisations.

Our model has utility in regard to policy-making scenarios, incident response or for educational purposes (more on this in Section 4). We believe a more complete understanding, and ability to make better decisions (as a result) is achieved through the use of abstraction and a common mental map of each category.

At the centre of this approach is our mental model process constructed around the construct of sensemaking. Sensemaking has been described as the process of *"how people make sense out of their experience in the world."* [Duffy 1995]. It has been used widely across a number of disciplines, including informational science [Dervin 1992] and organisational sensemaking [Wieck 1979] but has only been applied to cyber security in more recent years.

By developing an analytics model about network traffic Xiao et al. [2006] extrapolated meaning from activities occurring within the network. Alberts et al. [2002] also discussed the applications of sensemaking for cyber security in net-centric operations within cyberspace in understanding cyber information systems.

Figure 2 illustrates a high-level approach to sensemaking that can be used in making new discoveries and updating a mental model of an attack (adopted from Xiao et al. [2006]). The model is updated as more information about the attack becomes available. Xiao represents only one approach to consider sensemaking, and considerable numbers of work on sensemaking exist, other examples might be to use the sensemaking models proposed by Alberts et al. [2001], Pirolli and Card [2005] or Hutton [2008].

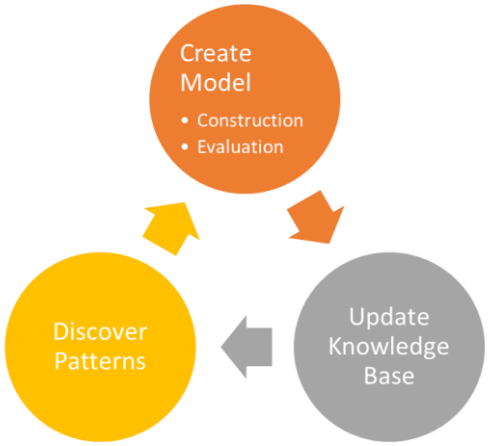


**Fig. 2: Adopted sensemaking model.**

We propose an initial starting point of four core categories: Attributes of Attack; Values of Attack; Impact of Attack and Mitigation of Attack. These reflect the key pillars that underpin our sensemaking of a cyber attack. We do not see these categories as being exclusive, accepting that others might be added depending upon the context of any event and the purpose for which the model is being used. In this sense the model is both expandable and transformative driven by the nature of the cyber attack and the stakeholders who are responsible for subsequent decision-making.

We perceived our model as representing a holistic mental model that is intended to frame the construction of the necessary level of understanding from which appropriate decisions can be made. As new knowledge is obtained through an evaluation process it is incorporated into the mental model. In turn new patterns are discovered, which further aid in its updating. It is our intention to investigate this starting point further and refine our model in the future. Our approach is shown in Figure 3.

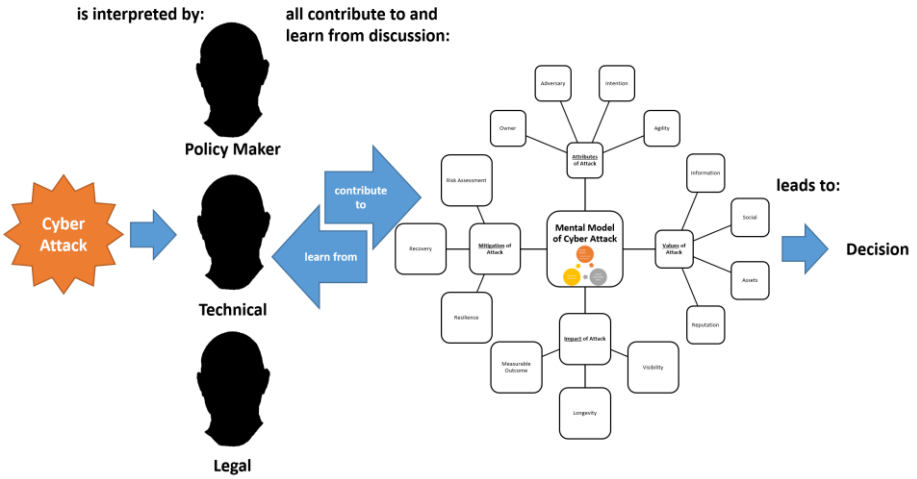


**Fig. 3: The Cyber Attack Decision-Making Process Using Our Model.**

Figure 4 shows an enlarged diagram of our model to understand a cyber attack. Below the four core categories or parent nodes previously identified sit sub-categories that represent activities or factors through which a cyber attack is defined. Xaio's approach can be seen to sit at the centre of this framework, reflecting that the application of sensemaking is a continuous process that builds upon constant evaluation and analysis of all aspects of the cyberspace environment. It is envisaged that the adoption of this approach will allow the identification of any interdependencies existing between the categories. Thus, leading to a more complete understanding of the threat and of those mitigation measures most likely to succeed.

Core categories and their sub-categories present in Figure 4 are defined in the following section. Our concern is with the metadata that describes each of the respective core categories and their supporting sub-categories. Consideration of the measurement used to underpin each of our categories is the subject of separate work outside the scope of this paper.

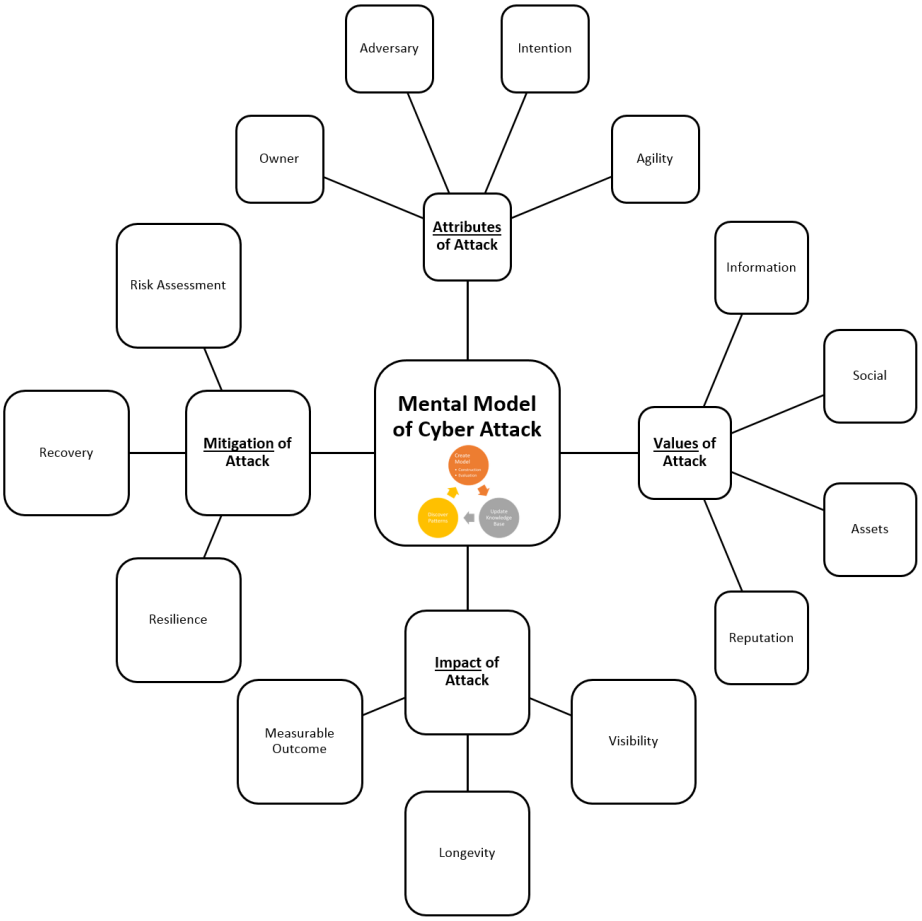


**Fig. 4: Our Cyber Attack Mental Map Model.**

### 3.1 Attributes of Attack

Attributes of the attack describe the context in which the event occurred. Doing so allows the expert actor to place the attack into their own scheme of reference: into their own context. This is important. Context setting provides the platform from which the actor can consider the other three remaining core categories within the model from both their own perspective and in relation to those held by other stakeholders and subsequently make decisions. These values can be described through the application of existing models e.g. Howard or Cohen).

**Owner.** Relates to the owner of the information, asset or capability that is the subject of the attack.

**Adversary**. Relates to the perpetrator of the attack. The Adversary is the entity who is behind the intent of the cyber attack. It should be noted that a separate actor may be responsible for the actual conduct of the attack.

**Intention.** Intent describes the motive for attack. Motives and associated goals may not remain static, changing in response to external drivers or actions undertaken by the Owner of the asset under attack. Subsequently intent may be of short or long duration and may constitute an end in itself or form part of a complex objective. Examples include curiosity/challenge, political, financial, vengeance reasons (see "goals", from Howard's Taxonomy).

**Agility.** We understand agility to be the capacity held by an acto to identify, select and exploit capabilities to achieve a desired intent. We consider all cyber attacks to consist of some form of agility and hence our model goes beyond the traditional, linear, kill-chain approach frequently referred to in the literature.

**Duration**. Reflects a quantitative value that can be measured to capture the length of an attack defined by time. Measurement of duration can be used to define seriousness of the attack or level of intent of the Adversary.

**Dimensions**. This attribute refers to the structure of the attack and is used to inform assessment of complexity and agility e.g. is the attack split into different stages/components. Sufficient knowledge of dimensions might be used as a form of attack profile or "fingerprint".

### 3.2 Values

Values describe the semantic meaning that is generated by the Owner following a cyber attack. These psychological perspectives will influence how the Owner interprets the attack and contextualises it in regard to their wider value system. Values will play an important role in constructing the Owner's "world view" of the event. They will subsequently inform decision making on the nature of any response.

**Information.** Information is the real world meaning behind the data available. In practical terms we can compare this to the data stored on a database. Information can be the values put into systems (digital bits and bytes) or knowledge that is made available from this data, such IP (e.g. blueprints), or HR records at an organisation.

**Social.** Reflects the people aspect of cyber attacks, i.e. whether a cyber attack can have an impact on the social dynamics of people in any way. Will it impact upon they way that they conduct their daily activities or with their relationships with other actors in either the physical world or the cyber domain.

**Assets.** In this sub-category we cover the physical items in the organisation such as physical computers, *Supervisory Control And Data Acquisition* (SCADA) systems etc. that can be affected by cyber attacks.

**Reputation.** The extent to which the outcome of a cyber attack can alter the way other actors perceive the Owner or the entity that they represent. Change is reflected in the impact that occurs in regard to the Owner's achieving their desired intent. While reputational damage is non-tangible it is most frequently reflected in a tangible impact such as loss of revenue.

### 3.3 Impact

Impact describes the consequence of a cyber attack in terms of the victim's ability to achieve their desired intent. Impact can be expressed in tangible or non-tangible terms e.g. online retail fraud or loss of custom through demise in reputation. Form and degree of impact will have considerable influence on the response that is made to a cyber attack. The response may differ in regard of time, allocation of effort and nature i.e. a technical response or a policy response.

**Outcome.** Defines the nature of the impact of the attack. It identifies how and the extent to which the victim can no longer achieve their desired intent. We describe cyber attacks as events in cyberspace that can generate an outcome in the physical world or virtual domain. Outcome may be measurable in tangible or non-tangible terms. A prevented cyber attack is seen as having an unsuccessful outcome.

**Depth.** Depth relates to the duration of an attack in terms of the period existing between its initial consequences being identified and the restoration of the normal, pre-event systems condition. Quantification of Depth can assist in consideration of risk and the choice of appropriate mitigation.

**Visibility.** Defines the extent to which the outcome of the cyber attack is observable, frequently reflected its impact on the victim's intent. This impact might not be visible to all actors who are impacted upon by the attack or visibility may only occur after the adversary's aim has been achieved e.g. State level espionage.

### 3.4 Mitigation

Mitigation represents those actions and capabilities that are available to the target in order to minimise the consequences of a cyber attack. These measures may be protective, existing prior to a hostile event occurring or be responsive, transpiring post event such as recovery software or operational redundancy. Mitigations may take the form of hard measures or soft measures or a combination of the two.

**Recovery.** Recovery reflects the capacity of the Owner to regain pre-event capability post a cyber attack. Recovery can be measured in terms of time and/or use of other capability including manpower and technology. Recovery will be dependent on other attributes including Dimension and Depth.

**Resilience.** Resilience reflects the Owner's ability to deal with the impact of a cyber attack as it is occurring without there being noticeable degradation of capability or asset. Resilience is influenced by Dimension, Depth and Recovery and the existence of prior measures of mitigation.

**Risk.** Represents a formalised process through which the Owner considers the range of potential threats that may exist to their assets or capabilities. Risk Assessment identifies those threats that the Owner can deal with and those which he cannot. This process provides the pivot/bridge between consideration of cyber attack and cyber defence.

# 4 Discussion

## 4.1 Applications of the Model

We have identified a number of other cyber-security challenges that could benefit from the application of our model. The first of these is in regard to cyber defence. Such usage envisages sense making of the same event but from an opposing perspective: a "mirroring" effect. This effect recognises that the attributes of cyber attack have equal relevance when considering their mitigation. In considering cyber defence, the Owner's intent is to fortify his cyber environment in order to protect assets and capabilities from a cyber attack. Achieving this intent requires the establishment of a robust cyber defensive posture founded upon a holistic understanding of the threat that takes consideration of not only the threat but in addition the wider context in which the entity to be defended exists. We see successful cyber defences as being as reliant on the existence of deterrent legal policy, as on strong firewalls and penetrating software based intruder detection systems.

Weick [1988] describes sensemaking in crisis conditions as being particularly difficult, and argues that commitment, capacity, and expectations affect sensemaking. We suspect that in instances where crucial decisions have to happen fast, our model in its form is too comprehensive to be appropriately used. Although, with suitable adaption it can still provide useful structure and guidance to decision makers.

The second area in which we see the model being able to contribute is that of cyber security policy generation. At the strategic level of activity, the establishment of shared situational awareness of the challenges present and the need to consider the perspective of all stakeholders is of equal or perhaps greater importance. The definition and implementation of meaningful cyber-security policy requires that understanding must exist across a wide spectrum, from the creation and enforcement of standards in respect of security measures to the establishment of appropriate authorities that allow Law and Order organisations to operate against potential adversaries proactively. In both of these cases technical input shares the same level of importance as that of a lawyer. We believe that our approach permits consideration of such wide ranging factors through the application of a simple conceptual model.

A third use of the model is in the field of cyber education. In this area, we consider that it has applicability in regard of those involved in the cyber security process, the expert-actors referred to previously and to the education of the users of cyber systems. In this context our model provides a means to identify, dependent upon the past experience and role of the actor those areas where benefit would be gained through the undertaking of education. As such our model provides an informed and targeted approach to education programme design.

Additionally, it provides a structure upon which to build an education programme. One that can be tailored dependent upon a particular subject of interest, with each of the categories being the basis for an individual module in the course timetable. A cyber attack based education programme based upon the graphical representation of our model shown at Figure 2 would consist of at least 14 modules.

### 4.2 Future Work

We do not claim our cyber security mental model framework is complete. We believe that it represents only a first step and it will need continual refinement with experts from a wide variety of backgrounds who can contribute to its development. The first of these is in understanding more fully what are the important categories and sub-categories that must be included when considering a particular cyber security problem. Our illustrative model provides one set that we believe has importance in relation to cyber attack, while recognising that there may be others that also should be present. We would wish to examine in more depth the extent to which we have succeeded in identifying all of the relevant concepts necessary to underpin our model and the validity of the categories from which it is constructed. A second issue concerns the degree to which the categories and sub-categories need to be changed when the focus of the model alters. Is it valid to use the same sets in looking at cyber defence and cyber policy generation? If not, and this would seem the likely answer what new categories might be required and which ones could be removed. In regard to both of these areas we see the need for further analysis of the relevant literature and direct engagement with the cyber security expert community. The latter perhaps, in the long term, providing to be of the most use through the insight that communicating directly should bring.

In order to assess our model it will be necessary to put it in the hands of many different decision makers, obtain their feedback, based on their prior experiences and identify where this model might fit in, if at all. Validating our approach is difficult even in real environments. For laboratory setting, one approach might be to introduce a group of participants to cyber attack scenarios before being introduced to the model, and make decisions, before introducing them to our model and present them with a different scenario in which the model should be used. Another approach to assessment would be to measure how well decisions maker are able to respond to cyber attacks, some with having been introduced to the model, and others not.

A third area of future work is identifying those cyber events that suit the application of the model. In the course of this paper we have discussed a number of instances. Although of these we have only considered that of cyber attack in any detail. This strand of work will focus on identifying other cyber security events that would benefit from our work. Engagement with domain experts particularly as part of testing and assessment process referred to previously represent logical avenues of advance in regard to resolving this concern.

We judge however, that the more pressing area, which requires further work, concerns the identification of appropriate measures for our categories and how these measures can be obtained and validated. In some circumstances this challenge will be relatively easy to overcome while in others gaining a reliable metric may not even prove possible. Tangible values relating to loss of revenue or fall in customer numbers as a consequence of a cyber event against a business enterprise should be accessible as an element of an organisation's routine reporting process. Placing measurable values on the categories of Agility and Visibility are likely present greater difficulty as to some degree their impacts may be non-tangible. Our approach in resolving these types of difficulties will be to consider how such non-tangible values are dealt with in other disciplines including risk assessment and medicine. In the latter case, inference is as a means to make an assessment. The applicability of this approach in respect of our model requires to be determined.

## 5 Conclusion

In this paper we have proposed a conceptual model that we see as enabling a collective approach to understanding, discussion and subsequent decision-making about cyber attacks. The model is underpinned by three assumptions: the **need to consider cyber attacks holistically**, the requirement to **involve a wide spectrum of stakeholders** in considering the cyber-attack problem, and finally, the critical need to **establish a shared understanding**.

The model is constructed from a set categories and sub-categories that reflect the diverse spectrum of factors that must be considered in dealing with a cyber attack. Our choice of assumptions and categories is based upon literature review and engagement with domain-experts. The paper has also examined how the model might be applied more widely in the cyber security field. Consideration has also been given to the future work necessary in the development of our approach.

We do not claim that our approach to considering cyber security attacks and other cyber events is complete. We do however, believe that the approach offers a potential method to establish a common understanding and through that the establishment of an informed start point for collective discussion and decision making.

## References


1. Alberts, D. S., Garstka, J. J., Hayes, R. E., & Signori, D. A. (2001). Understanding information age warfare. Assistant secretary of defense (c3i/command control research program) Washington DC.
2. Bishop, M. (1995). A taxonomy of Unix system and network vulnerabilities. Technical Report CSE-95-10, Department of Computer Science, University of California at Davis.
3. Booz | Allen | Hamilton (2012). Cybersecurity: Mission integration to protect your assets. https://www.boozallen.com/media/file/Cybersecurity-Mission-integration-to-protect-your-assets-fs.pdf. Accessed 08 September 2014.
4. Cohen, F. (1997). "Information system attacks: A preliminary classification scheme", Computers & Security, Elsevier.
5. CPNI, Centre for Protection of National Infrastructure. http://www.cpni.gov.uk/advice/Personnel-security1/homer/ Accessed 07 September 2014.
6. Dervin, B. (1992). From the mind's eye of the user: The sense-making qualitative-quantitative methodology. In Glazier, J. and Powell, R. R. *Qualitative research in information management* (p. 61-84). Englewood, CA: Libraries Unlimited
7. DSTL Centre for Defence Enterprise (CDE) Cyber Situational Awareness Launch Presentation 2012 http://webarchive.nationalarchives.gov.uk/20140410091116/http://www.science.mod.uk/events/event_detail.aspx?eventID=184 Accessed 07 September 2014.
8. Duffy. M. (1995) Sensemaking in Classroom Conversations, Openness in Research: The Tension between Self and Other, I. Maso et al., eds., Van Gorcum, pp. 119-132.
9. Greitzer, F. L., & Ferryman, T. A. (2013). Methods and Metrics for Evaluating Analytic Insider Threat Tools. In Security and Privacy Workshops (SPW), 2013 IEEE (pp. 90-97). IEEE.
10. Greitzer, F. L., Paulson, P., Kangas, L., Edgar, T., Zabriskie, M. M., Franklin, L., & Frincke, D. A. (2009). Predictive modelling for insider threat mitigation. Pacific Northwest National Laboratory, Richland, WA, Tech. Rep. PNNL Technical Report PNNL-60737.
11. Hadnagy, C. (2010). Social engineering: The art of human hacking. John Wiley & Sons.
12. Healey. J. (2013). A Fierce Domain: Conflict in Cyber Space. Cyber Conflict Studies Association. United States.
13. Howard, J. D., & Longstaff, T. A. (1998). A common language for computer security incidents. Sandia National Laboratories.
14. Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Leading Issues in Information Warfare & Security Research, 1, 80.
15. Hutton, R., Klein, G., & Wiggins, S. (2008). Designing for sensemaking: A macrocognitive approach. In Sensemaking Workshop, CHI (Vol. 8).
16. Intelligence National Security Alliance. (2012). Cyber Intelligence: setting the landscape for an emerging discipline. Air & Space Power journal, November/December 2012, Vol.26 Issue 6, p12. United States. http://www.oss-institute.org/storage/documents/Resources/studies/insa_cyber_intelligence_2011.pdf
17. Legg, P., Moffat, N., Nurse, J. R., Happa, J., Agrafiotis, I., Goldsmith, M., & Creese, S. (2013). Towards a conceptual model and reasoning structure for insider threat detection. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 4(4), 20-37.
18. Lough, D. L. (2001). A taxonomy of computer attacks with applications to wireless networks (Doctoral dissertation).
19. MITRE Corporation. Common Attack Pattern Enumeration and Classification (CAPEC). https://capec.mitre.org Accessed 07 September 2014.

20. NATO (2012). NATO Policy on Cyber Defence. NATO Cooperative Cyber Defence Centre of Excellence. https://web.archive.org/web/20120310083820/http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence.pdf Accessed 07 September 2014.
21. NATO. (2012). NATO Cyber Security Framework Manual. NATO Cooperative Cyber Defence Centre of Excellence. https://www.ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf Accessed 07 September 2014.
22. Norman, D. A. (1983). Some observations on mental models. Mental models, 7(112), 7-14.
23. Nye. J. (2011). The Future of power. Public Affairs, Washington, United States.
24. Pirolli, P., & Card, S. (2005). The sensemaking process and leverage points for analyst technology as identified through cognitive task analysis. In Proceedings of international conference on intelligence analysis (Vol. 5, pp. 2-4).
25. Simmons, C., Ellis, C., Shiva, S., Dasgupta, D., & Wu, Q. (2009). AVOIDIT: A cyber attack taxonomy.
26. Weick, K. (1979). *The Social Psychology of Organizing*. New York: McGraw-Hill.
27. Weick, K. E. (1988). Enacted Sensemaking in Crisis Situations. Journal of management studies, 25(4), 305-317.
28. Xiao, L., Gerth, J., & Hanrahan, P. (2006). Enhancing visual analysis of network traffic using a knowledge representation. In Visual Analytics Science And Technology, 2006 IEEE Symposium On (pp. 107-114). IEEE