Edith Cowan University
Research Online

Australian Information Warfare and Security Conference

Security Research Institute Conferences

2006

Conceptual Modelling: Choosing a Critical Infrastructure Modelling Methodology

Graeme Pye
Deakin University

Matthew J. Warren
Deakin University

Originally published in the Proceedings of 7th Australian Information Warfare and Security Conference, Edith Cowan University, Perth Western Australia, 4th - 5th December, 2006.
This Conference Proceeding is posted at Research Online.
http://ro.ecu.edu.au/isw/16

Conceptual Modelling: Choosing a Critical Infrastructure Modelling Methodology

Graeme Pye and Matthew J. Warren

School of Information Systems,
Faculty of Business and Law,
Deakin University,
Geelong, Victoria, Australia, 3217

graeme@deakin.edu.au and mwarren@deakin.edu.au

Abstract

This paper reports on further research undertaken regarding systems modelling as applied to critical infrastructure systems and networks and builds upon the initial modelling research of Pye and Warren (2006a). We discuss system characteristics, inter-relationships, dynamics and modelling of similar systems and why modelling of a critical infrastructure is important. In overview we compare four modelling methods and techniques previously used to model similar systems and discuss their potential transference to model critical infrastructure systems, before selecting the most promising and suitable for modelling critical infrastructure systems for further research.

Keywords

Critical infrastructure, dependency, interdependency and modelling.

INTRODUCTION

The nature of critical infrastructure systems and their interconnection display the characteristics of highly structured, complex and highly interconnected networks that also have the added issues of dependency and interdependency relationships that necessarily exist between infrastructures to facilitate the supply of services. This is particularly prevalent when considering the energy sector, where the continuity of the supply of electricity for example, is crucial to many other sectors of critical infrastructure for ongoing provision of services to the community at large (Scott 2005).

However, critical infrastructures are vulnerable and can be damaged, destroyed or disrupted by breakdowns, negligence, natural disasters, accidents, cyber incidents, illegal criminal activity and malicious damage to name a few, and for this reason the continuity of supply must be protected against such hazards, threats, vulnerabilities and risks. Therefore the aim of government policy and by association that of infrastructure owners and operators, is to ensure continued supply availability through identifying and implementing improved protective safeguards and analysis in response to the identified threats and risks posed (Scott 2005).

The focus of this paper is that in order to address, analyse and determine system vulnerabilities effectively. It is apparent that such system analysis requires the initial modelling of the system, possibly at a number of scalable levels of infrastructure that not only mimic normal operation, but also enable the modelling of prognosticative outcomes, as a consequence of deviations from normal functionality whether they are internally or externally based influences or a combination thereof.

At the outset this paper will focus on establishing the characteristics of a system, discuss systems thinking before proceeding to discuss the characteristics of critical infrastructure systems and how this relates to systems and systems thinking. The next aspect will focus on the rationale behind the modelling of such systems and the issues surrounding the modelling of critical infrastructures together with identifying the functional and relational dynamics at play internally and externally to the system/s. Finally a brief assessment of the potential value offered by various security system modelling and simulation development products will be undertaken to determine which is potentially best suited to the modelling and development of computer simulations that best mimic critical infrastructure function. This critique should also include the potential not only to model normal critical infrastructure operations, but also model artificial deviations from the norm so that identification and testing of security risks and their possible adverse ramifications can be undertaken and determined prior to physical implementation into the particular critical infrastructure system.

WHAT IS A SYSTEM?

The perception of what constitutes a system evokes different meanings and conceptual visualisations to different individuals, depending on their interpretation of the system characteristics and the physical or inferential complexity of the components that may interact together to form the basis of a functional system representation. Such systems can take the form of biological, ecological, social, mechanical and natural (e.g. the solar system) that assist in performing routine functions. Furthermore systems can be comprised of sub-systems, for instance our work can consist of a number a sub-systems relating particularly to human, economic, technical, legal and social systems that can act individually, be influential or interact with each other (Maani & Cavana 2000).

In seeking a general understanding of what commonalities indicate a system we can characterise that a system is a collection of smaller parts that cooperate with one another to function as a whole. Of course a system is not only the sum of its parts, but is also a representation of its interactions and furthermore a system can also associate its own parts to itself and thereby become part of an even larger system (Maani & Cavana 2000).

As a consequence of these commonalities we can begin to investigate systems further to develop an appreciation of how the sub-systems and their parts all interact together in order to function collectively as a whole, but for this to eventuate the investigator has to utilise the paradigm of 'systems thinking' *[sic]* to truly appreciate the system as a whole consisting of many parts.

Systems Thinking

Systems' thinking remains an emergent discipline dedicated to understanding the complexity that is intrinsic within all systems, irrespective of size, natural and the influence of change upon the system and regardless of whether it is internally or externally located. As a paradigm, systems' thinking is about describing the dynamics of relationships between the lessor parts within system and also the dynamics of relationships with other associated systems as a whole.

As a consequence, systems' thinking requires the investigator to consider thinking of systems in the following three ways (Maani & Cavana 2000):

- Dynamic thinking is appreciating that the world is not static and that things are changing constantly;
- Operational thinking is the cognitive condition of understanding the physics of operations and how things really work;
- Closed-loop thinking is recognising that cause and effect are not always linear and that the end (effect) can influence the means (cause).

Of course this is not as easy as it may first appear when you consider the implications of larger systems interacting with other large systems and that each in themselves contain numerous sub-systems all interacting within the boundaries of their own system. Additionally, this complexity exacerbates further when considering the influential relationships that can potentially exist between large systems as well as within the sub-systems making up these larger systems too. All this information is at best difficult for humans to comprehend and process in small relatively simple systems, let alone contemplating large complex and multiple systems together. This is where systems modelling can assist us with enhancing and developing a greater appreciation and understanding of the functionality of the focal system/s, their sub-systems and inter-relationships.

Systems Modelling

To analyse and comprehend the functional behaviour of any system, at any level within the system, it is beneficial to our ultimate comprehension that we can initially model it. By modelling the system we can begin to understand the structure of the system, the interconnection between its elements or components, the relational influences and how localised change can affect the whole system and its lower level components over time. Once we can achieve this, then we can begin to manipulate the model to an extent where it becomes possible to potentially measure and predict possible systems behaviour in response to our manipulation based on attempts to imitate the precursor influences that lead to eventual system change (Maani & Cavana 2000).

When we consider the system from the previous perspective, we are essentially modelling a system that exhibits change and thereby the influence of 'cause and effect' *[sic]*. Therefore, this example requires applied system thinking in relation to and consideration of, modelling the dynamic characteristics inherent within the system or external to the system, where a cause (system influence) has a potentially different effect each time on the means of how the system responds, changes or reacts. Hence in this context, the overriding characteristic is that the system is not behaviourally static in reproducing the same repeatable result, but dynamic in the sense that the result can be infinitely variable and thus modelled with this consideration in mind.

Similarly, critical infrastructure systems also exhibit dynamic behaviour and characteristics. Therefore, to model such systems, the focus of this ongoing research, we have to consider the dynamics characterised by the system and how modelling techniques can be applied precisely that represent a theoretical account that is truly representative of the dynamic characteristics inherent in the physical critical infrastructure system and its subsequent behavioural responses.

MODELLING SYSTEMS DYNAMICS

Modelling systems that exhibit dynamic behaviour requires the consideration of a number of issues. In general terms a dynamic system is one where its parts are interrelated in such a manner that a change in part of the system, by consequence affects other parts of the system and therefore the overall system as a whole. Furthermore, not only can the system be functionality influenced by internal changes, it is also susceptible to influence from external changes in environmental factors surrounding the system or other existing systems, via feedback.

Feedback and System Dynamics?

This premise of system dynamics reflects the description provided by the System Dynamics Society (2006) that describes system dynamics as a method of studying and modelling complex response systems that are apparent in any sort of feedback equipped system. Feedback is the situation where via a chain of 'cause and effect'*[sic]*, X influences Y, which in-turn influences X and therefore the study of the link X and Y cannot be undertaken independently, as it is the link between X and Y that predicts how the system will behave. With this in mind, only the study of the whole system as a feedback system will lead to the appropriate systematic conclusions for modelling purposes.

Therefore to construct a useful interpretation or model a dynamic system as described requires an analysis of the system to develop a useful understanding of the system situation through elaboration, exploitation and interpretation of a simulation model, which is heavily reliant on the mental interpretation of the developer. Here a useful interpretation refers to a given understanding of the system situation at a given moment together with the perceived mental structure of the whole system (Schaffernicht 2006).

It is these system characteristics and modelling issues that when applied to critical infrastructure systems reflect the similarities of system constructs, components and dynamic behavioural characteristics of critical infrastructure systems. These principles of influential relational characteristics closely reflect the dynamic behaviours of both dependency and interdependency relationships as previously identified by Pye and Warren (2005) in regard to modelling critical infrastructure systems. This was further expanded upon by Pye and Warren (2006a) where the relationships between selected critical infrastructures was modelled to indicate there is a need to supply or exchange services that are crucial to the whole critical infrastructure system's continued normal function.

Critical Infrastructure System Characteristics

According to Australia's national strategy, critical infrastructure is defined as "those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact upon the social or economic well-being of the nation or affect Australia's ability to conduct national defence and ensure national security" (AGD p1 2004a).

Furthermore, by its very structure critical infrastructure systems are interconnected and networked together as necessary for the supply and demand of services to and from each other in varying degrees. It is this structural inter-relationship between critical infrastructure systems and the internal components within them, which characterises critical infrastructure as a dynamic system made up of smaller independent or reliant systems. As a consequence, critical infrastructure systems can be further characterised as dynamic systems because they are highly reliant on each other and by necessity must function together in a cooperative manner so that the system as a whole, can function and supply the services normally expected (Pye & Warren 2006b).

Another intrinsic characteristic of critical infrastructure systems as a whole, is the 'unboundedness' *[sic]* of the component systems that are related or networked together to form a larger functioning system. This is characterised by the distributed nature of local system administrative control that exists without any central governing authority. An unbounded environment cannot be partitioned into a number of finite bounded environments because of the lack of global perspective given to the associated cooperating systems beyond the boundary of their local system, consequently there is a lack of the 'big picture' *[sic]* information represented locally, in regard to feedback from the system as a whole (Ellison *et al* 1999).

From this we can draw the inference that indeed crtical infrastructure sytems do display similar characteristics to that of dynamic systems because they consist of multiple variables with dynamically changing values, dependency relationships existing between and within infrastructure systems and they exhibit network connection charateristics that are subject to both internal or externl change and influences. This necessiatates that in the national interest critical infrastructure systems do need to be modelled as part of the overall security analysis process and assessed to determine points of weakness or areas of vulnerability. The modelling and functional computer simulation of critical infrastrucutre systems is potentially the most appropriate and perhaps cost effective way to manage this process, along with solution development and testing of solution models prior to physical implementation into critical infrastructure systems.

Why Critical Infrastructure Modelling is Important

From a systems dynamics perspective there is a strong logic that offers potential improvements in the analysis, security, functional understanding and strategic management perspectives of critical infrastructure systems that will assist in understanding the performance of the system and variations over time (Warren 2005). Since performance reflects the state of resources or service provision, steering strategies can be developed and tested with system modelling, prior to developing policies, physical implementation and taking security decisions that address variations from normal functionality in the face of unexpected challenges.

With this in mind it is then quite feasible to develop adverse scenarios that could be applied to critical infrastructure models to represent such threats and vulnerabilities that would impinge upon business continuity, incident and consequence management, information system attacks and vulnerabilities, electronic crime, protection of key sites from attack or sabotage, chemical, biological and radiological threats to water and food supplies and the identification and protection of offshore and maritime assets, accident management, cyber incidents to name a few scenarios that could reasonably be developed and applied to models of critical infrastructure (AGD 2004b).

Therefore, by applying modelling techniques to the critical infrastructure systems that everyone takes for granted such as: communication networks; banking; energy; water and food supplies; health services; emergency services and transport networks (DPMC 2004) for example: this provides the opportunity to actually model adverse situations as applied to the critical infrastructure system, without necessarily testing this same adverse scenario situation in the physical realm of the infrastructure itself.

Inevitably, people confronted with the undertaking of exercising control over dynamic systems, be they business production systems, the economy, global warming and in this case critical infrastructure management for example. They are still required to deal with what Jensen and Berndt (2003) describe as 'dynamic decision issues' *[sic]* that characterise a series of related decisions where invariably the systems/s situation will change both in itself and in the response to the actions taken. Modelling of the dynamics at play within the system enables not only the normal functionality to be observed, but also the functionality of an adverse change and its effect upon the critical infrastructure system as a whole, for without this knowledge owners and operators of the critical infrastructure will remain severely handicapped and ill prepared for whatever may potentially eventuate (Warren 2005).

MODELLING CRITICAL INFRASTRUCTURE SYSTEMS

The effective modelling of critical infrastructure would enable both the government and critical infrastructure owners to analyse, identify and effectively manage and maintain the security, stability and availability of their particular critical infrastructure through the development of solutions and contingencies against unexpected or otherwise challenges to the systems' stability (Pye & Warren 2006a).

Here we will briefly examine four different modelling methods and their potential to address the primary issue of effectively representing the modelling of critical infrastructure systems to critically represent the existing physical nature of the infrastructure system within the modelling scope. Also incorporating its dependency relationships to other associated infrastructures, within the boundaries set by the model developer and whether such modelling techniques as applied justifiably represent the dynamics of the system being modelled and if it is applicable, adaptable or transferable to critical infrastructure modelling.

The EASEL Way

EASEL (Emergent Algorithm Simulation Environment and Language) is a beta version software program designed for the 'simulating, depicting, and gathering information about networks, software agents, and other active entities of the physical, electronic and software worlds, about their interactions, and about their collective global effects' (Fisher p1 1999) of real-world systems upon which the EASEL simulation is modelled.

EASEL is a script language that utilises property-based types to define the various entities (actors) that can be created by the language and its strength lays in its capability to model, depict and model unbounded systems and simulate the complex interactions that take place between the various types of entities within the system being modelled (Redman et al 2005). Additionally, the software is still freely available online for download from the Software Engineering Institute at Carnegie Mellon, but current support and development of the EASEL software itself seems to have lapsed (SEI 2006).

Redman's (2003) research into system survivability noted that the use of EASEL as a simulation development tool had some performance limitations during the design and development of his survivability simulation research project. Principally the software was only available in the Apple Macintosh operating system platform and because the software was still in the 'beta' *[sic]* development, there was a lack of resources to support the developer or instruction to easily produce a simulation using the EASEL software. Therefore, the simulation development was a time consuming process due to 'trial and error' *[sic]* development method used, the lack of support and the taxing resource load imposed by EASEL on the operating system, this made testing and running of the simulations difficult due to the resource demand instability. Likewise, Marasea's (2003) research utilised EASEL to develop a simulation model representing an attack upon the critical infrastructure that was developed and modelled in the EASEL environment, here again Marasea (2003) noted similar design, development, support and operational issues that impinged upon this research project too.

EASEL is not particularly conducive to rapid model development or systems analysis of dynamic and unbounded systems modelled utilising the EASEL environment. This is due in part to the long development lead time necessary to develop a functional simulation and that the user support for EASEL was and remains essentially no-existent. The issue of heavy computer resource use, even in the review of these previously functioning simulations, is still a major issue that more often than not leads to the computer devoting 100% resources to running the EASEL software, to the extent that the simulation program cannot load and run.

EASEL presents one alternative to the question of modelling critical infrastructures, however the time consuming model development and the lack of ongoing development of the EASEL software package itself, has now ceased with no likelihood of resumption in the near future (SEI 2006). Although, there is still a need to model critical infrastructure systems quickly so that important analysis of the system can be undertaken to identify normal operation, vulnerabilities and the effect of adverse incidents upon normal functionality.

Stock and Flow Diagrams

A form a dynamic system modelling that is growing in popularity within business particularly is the Stock and Flow diagram whose notation consists of three of three different types of elements, namely, stocks, flows and information. The three elements together in a diagram graphically represent any dynamic process that may be apparent in any business and therefore can be utilised to establish and study the characteristics of such processes and illustrates the relationship among variables which have the potential to change over time (Kirkwood 2005).

Kirkwood (2005) illustrates in Figure 1 a very simple stock and flow diagram with the three elements Potential Customers, sales and Actual Customers and models the structure of the business process in regard to the rate at which Potential Customers reduces to zero.

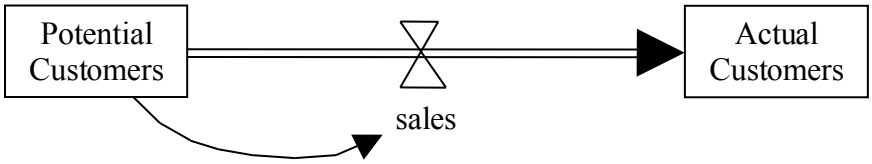

Figure 1 Stock and Flow Diagram

The two different types of variables illustrated inside the rectangles are variables called a stock, level or accumulation. The variable sales is shown next to the 'butterfly valve' or 'bow tie' *[sic]* symbol and this type of variable is known as a flow or rate, thus the two lines through the butterfly valve looks like a pipe with the valve controlling the flow. The premise here is that the graphical depiction represents the flow of Potential Customers towards Actual Customers with the rate of flow controlled by the sales valve; this is the key idea behind the difference between stock and flow. Therefore, a stock represents an accumulation of something and a flow is the movement of something from one stock to another (Kirkwood 2005).

The final element of the Figure 1 diagram is the information link represented as a curved arrow and this notation represents that the value of Potential Customers influencing the value of sales. Additionally, and of equal importance is the lack of an information arrow from Actual Customers to sales, which illustrates that information regarding the value of Actual Customers has no influence over the value of sales (Kirkwood 2005).

Hence the focus of the stock and flow diagram is to investigate the changes and analysis of how the elements and the structure of the process can bring about change and because the focus is on the elements that make up the process (sometimes likened to the components of the system) and how the performance of the process changes over time, this forms the basis for studying the dynamics of a system.

This is only a simple representation within a defined process boundary of a simple process example of a stock and flow and the question remains that this type of modelling may not necessarily be suitable for representing critical infrastructure systems and their relationships. The issue of the scalability potential of stock and flow models can tend to become difficult to interpret due to the diagrams added complexity in depicting the logical interconnection, processes and dependency relationships of critical infrastructure systems. It appears that stock and flow diagrams may be useful to model specific system processes where the boundaries are clearly defined and strictly adhered to, but may not necessarily be well suited to modelling multiple interconnected and large critical infrastructure systems from a security analysis perspective.

Viable Systems Modelling

The Viable System Model (VSM) represents a framework for managing the security of large multi-level organisational information systems as a means of detecting, checking and identifying threats and vulnerabilities as they appear and through local sub-system monitoring that can distinguish between threatening and non-threatening behaviours and adjust the whole system as a consequence (Hutchinson & Warren 2002).

From the research perspective of Hutchinson and Warren (2002), VSM provides a framework to manage the security of and normal function of organisational information systems that are cooperating together as a larger overall information system, to deliver ongoing system security that takes into consideration all levels of the system.

The disruption or destruction of information systems can cause serious loss of service to customers and increasingly information systems are under threat from both internal and external sources and there is a need to establish a robust and dynamic response to protect information assets (Gokhal & Banks 2004). In view of the structure of critical infrastructures and their reliance upon information systems, there is obviously a need to establish ways to protect such systems and VSM may offer benefits here.

However, from the perspective of modelling the activity of a critical infrastructure system with a view to analysing the critical infrastructure system as a whole, its internal system components and the dependency relationships between critical infrastructure systems, VSM may not be applicable due to the sheer scope and size. Therefore, while it may be applicable at the organisational level, the magnitude and scale of modelling critical infrastructure systems across the state or national level would be well beyond VSM's capabilities.

Coloured Petri Nets

As proposed in the research of Pye and Warren (2006a), Petri Nets offer a systematic method of modelling highly interconnected, cooperating networked systems in a scalable manner and is a means of depicting the logical connection based on the physical representation of the critical infrastructure systems modelled.

Furthermore, the Petri Net model also enables an analysis of the physical and operational structure of the critical infrastructure system to be analytically scrutinised, additionally it is a relatively simple task to develop a software simulation of the critical infrastructure system to represent the normal functionality of the system and the normal functional relationships between cooperating critical infrastructures. From this perspective the Petri Net notation would in simple terms represent the following:

- Place - represents a particular infrastructure;
- Transition – is the exchange of services between cooperating infrastructures;
- Arcs – are the connections between infrastructures.

When a critical infrastructure system petri net model is developed and satisfactorily reflects normal functionality, then redeveloped Petri Net models could indicate, incorporate and represent potential threats implemented into a subsequent simulation for response observation. Thus the central focus of this research project is to enable the observation and mapping of the potential impact upon the critical infrastructure system/s targeted and the

associated critical infrastructures via their dependency relationships. From this viewpoint it is potentially possible to identify the likely outcomes of threats and vulnerabilities and simulate potential solution scenarios and responses to such threats and vulnerabilities, in this way testing probable security solutions within the simulated computer environment, before progressing to actual implementation in the physical critical infrastructure system.

Petri Net modelling offer an interesting approach to modelling critical infrastructures that requires deeper investigation, as it takes into consideration the dynamic nature of the systems involved and the dependency relationships that exist between cooperating infrastructures as well as mapping service delivery or failure within the critical infrastructure system model.

MODELLING ASSESSMENT OVERVIEW

Of the four systems modelling methods and applications discussed, they all address the modelling issue from their own perspective and are all potentially beneficial and useable from their specialised perspective for the analysis of security issues relating to critical infrastructure systems, however there is no one single solution. What is required is to choose the best fit modelling methodology or package to enable the effective modelling of critical infrastructures, their dependency relationships, incorporate systems dynamics and enable simulation development for security scenario testing, analysis and solution application.

While, EASEL was specifically designed to model unbounded and dynamic systems it was found that the simulation software was computer resource greedy and unstable, operating system specific (Apple only), still in the software development stage although this has now ceased, along with negligible user support. Perhaps the overriding issue was the extended design and development time needed to develop a model simulation, which means the timeframe required to develop solutions quickly makes EASEL impractical for this task.

Stock and flow diagrams are currently very popular within the field of modelling dynamic systems and processes and while model development is quick, there is no accompanying computer simulation development that is applicable directly from the model. Unfortunately, stock and flow diagrams are not very scalable in a practical sense as the diagrams do become unsuitably complex to be of any real value when dealing with the relationships between multiple processes within a system or representing external system influences. While it is given that there is a need to understand the modelling notation used, it does not necessarily translate well to the layman perspective in regard to understanding the system being modelled, although as shown in Figure 1 it is appropriate for modelling isolated processes for analysis.

VSM represents system modelling from the information security management perspective of an organisation and by it very nature requires close and trusting cooperation between the infrastructures exchanging services and VSM also displays a highly level of complexity that impacts upon the security management coordination required. Unfortunately, the VSM security management framework is not a modelling tool for systems analysis from the critical infrastructure system perspective, although it would have a part to play in the management of systems by the critical infrastructure owners and operators.

Finally, Coloured Petri Nets offer a potential modelling instrument that is scalable and resembles the logical and physical representation of the system very quickly and easily and also has the added benefit of enabling computer generated simulation directly off the initial model, depending on what modelling package you use. Much of petri net modelling research literature relates to process modelling because this form of modelling enables rapid model development and computer simulation development in very short timeframes. This feature would greatly assist in developing and testing solutions that are also easy to manipulate and change, additionally petri net modelling comes from a sound mathematical basis (graph theory) with established rules applicable to petri net modelling. The application of petri net modelling to critical infrastructure systems' modelling was applied in research previously undertaken by Pye and Warren (2005, 2006a) in regard to electricity generation and transmission infrastructures in isolation.

CONCLUSION

This research represents an advancement built upon the previous research undertaken by the authors relating to developing a petri net model representing chosen critical infrastructure systems and the modelling representations of selected parts of the critical infrastructure system in isolation. This research applied petri net modelling to a case study to illustrate the interconnection and physical dependency relationships that exist between associated infrastructures related to electricity generation, transmission and distribution infrastructures (Pye & Warren 2006a).

Although this is an initial comparative analysis undertaken here, there is further and deeper analysis to be undertaken to benchmark the effectiveness and functionality of these modelling packages against a security

benchmarking framework in relation to modelling critical infrastructure. However, at this early stage, petri nets appear to provide the 'best fit' *[sic]* or at least the most potential for transference to modelling critical infrastructure systems as discussed earlier. Although, further research will continue to more deeply test the capability of petri nets as a tool for the effective modelling and computer simulation development of physical critical infrastructure systems. This research will now form the foundation of future doctoral research and is the current focus of deeper ongoing research investigation into the potential to model critical infrastructure systems and networks at the national level and also scale down to lower, local levels.

REFERENCES

AGD (2004a) Critical Infrastructure Protection National Strategy, TISN, URL: http://www.nationalsecurity.gov.au/, Accessed Nov. 2004.

AGD (2004b) Protecting Australia's Critical Infrastructure [Media Release], Attorney-General's Department, URL: http://www.ag.gov.au/, Accessed May 2005.

DPMC (2004) Protecting Australia Against Terrorism, Department of the Prime Minister and Cabinet, URL: http://www.dpmc.gov.au/publications/protecting_australia/docs/protecting_australia.pdf, Accessed Oct 2004.

Ellison R.J. et al (1999) 'Survivability: Protecting Your Critical Systems', IEEE Internet Computing, no. Nov/Dec.

Fisher D.A. (1999) 'Design and Implementation of EASEL. A Language for Simulating Highly Distributed Systems', in MacHack 14, the 14th Annual Conference for Leading Edge Developers, Deerborn, MI, USA.

Gokhale G.B. & Banks D.A. (2004) 'Organisational Information Security: A Viable System Perspective', in 2nd Australian Information Security Management Conference, School of Computing and Information Science, Edith Cowan University, Perth, WA, pp. 178-184.

Jensen E. & Brehmer B. (2003) 'Understanding and Control of a Simple Dynamic System', System Dynamics *Review*, vol.**19**, no.2, pp. 119-137.

Hutchinson W. & Warren M. (2002) 'Information Warfare: Using the viable system model as a framework to attack organisations', *Australian Journal of Information Systems*, vol.**9**, no.2, pp. 67-74.

Kirkwood C.W. (2005) A Modelling Approach, Arizona State University, URL: www.public.asu.edu/~kirkwood/sysdyn/SDIntro/ch-2.pdf, Accessed Oct 2006.

Maani K.E. & Cavana R.Y. (2000) Systems Thinking and Modelling. Understanding Change and Complexity, Prentice Hall, Auckland, NZ.

Marasea P. (2003) Critical Infrastructure Dependencies, Honours thesis, Deakin University.

Pye G. & Warren M.J. (2005) 'Modelling Critical Infrastructure Dependency Relationships', in 6th Australian Information Warfare & Security Conference, School of Information Systems, Deakin University, Geelong, Australia, pp. 149-156.

Pye G. & Warren M.J. (2006a) 'Critical Infrastructure Protection, Modelling and Management: An Australian Commercial Case Study', in 5th European Conference on Information Warfare and Security, Academic Conference Limited (ACL), Helsinki, Finland, pp. 177-190.

Pye G. & Warren M.J. (2006b) 'Security Management: Modelling Critical Infrastructure', *Journal of Information Warfare*, vol.**5**, no.1, pp. 46-61.

Redman J., Warren M., Hutchinson W. (2005) 'System Survivability: A Critical Security Problem', *Information Management and Computer Security*, vol.**13**, no.3, pp. 182-188.

Redman J. (2003) System Survivability, Honours thesis, Deakin University.

Schaffernicht M. (2006) 'Detecting and Monitoring Change in Models', *System Dynamics Review*, vol.**22**, no.1, pp. 73-88.

SEI (2006) Easel, Carnegie Mellon, URL: http://www.sei.cmu.edu/community/easel/, Accessed May 2006.

Scott G. (2005) 'Protecting the Nation', *AUSGEO News*, no.79.

Warren K. (2005) 'Improving Strategic Management with the Fundamental Principles of System Dynamics', *System Dynamics Review*, vol.**21**, no.4, pp. 329-350.

COPYRIGHT

Pye & Warren © 2006. The author/s assign the We-B Centre & Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to the We-B Centre & ECU to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors.