12-3-2012

Defence in Depth, Protection in Depth and Security in Depth: A Comparative Analysis Towards a Common Usage Language

Michael Coole
Edith Cowan University, m.coole@ecu.edu.au

Jeff Corkill
Edith Cowan University, j.corkill@ecu.edu.au

Andrew Woodward
Edith Cowan University, a.woodward@ecu.edu.au

DOI: 10.4225/75/57a034ccac5cd
5th Australian Security and Intelligence Conference, Novotel Langley Hotel, Perth, Western Australia, 3rd-5th December, 2012

DEFENCE IN DEPTH, PROTECTION IN DEPTH AND SECURITY IN DEPTH: A COMPARATIVE ANALYSIS TOWARDS A COMMON USAGE LANGUAGE

Michael Coole, Jeff Corkill, Andrew Woodward
SRI - Security Research Institute, Edith Cowan University
Perth, Western Australia
m.coole@ecu.edu.au; j.corkill@ecu.edu.au; a.woodward@ecu.edu.au;

Abstract
A common language with consistency of meaning is a critical step in the evolution of a profession. Whilst the debate as to whether or not security should be considered a profession is ongoing there is no doubt that the wider community of professionals operating in the security domain are working towards achieving recognition of security as a profession. The concepts of defence in depth, protection in depth and security in depth have been used synonymously by different groups across the domain. These concepts represent the very foundation of effective security architecture are hierarchical in nature and have specific meaning. This paper through comparative analysis clearly defines the difference between and establishes the hierarchy such that a common understanding can be achieved.

Keywords
Systems Approach, Defence in Depth, Protection in Depth, Security in Depth, Common Threads, Security Language.

INTRODUCTION

Security, and specifically security as a professional embodiment, has become the subject of many discussions in academic circles. Steering this debate is literature drawn from other domains emphasising that professionals and a profession are defined according to: the status of their agreed body of knowledge, education standards linked to competencies drawn from such bodies of knowledge and the public's confidence as a result of such standards. To date, the security profession is yet to establish a true consensual body of knowledge. In the present discourse attention is being drawn to articulating clear definitions and agreed terminology with the aim of establishing common ground in which the profession can communicate, and standards or professional benchmarks can be established.

This paper presents the argument that a core approach to the protection of assets encompasses a systems approach which draws on conceptualizations such as Defence in Depth, Protection in Depth and Security in Depth. Whilst Nunes-Vaz, Lord & Ciuk (2011) presented their conceptualization of such terms, to date there still exists significant structural variances in both understanding and definition, especially in relation to the fusion between traditional physical and information technology (IT) domains. This paper aims to articulate a functional conceptualization of these terms underpinned by a path modelling approach to physical security towards establishing common understanding and applications in the language used by security professionals, both physical and IT in the protection of assets.

Background

Consistency in security advice is difficult to achieve, given the very concept of security and in particular, security management encompasses a wide spectrum of activities and skills spread across a vast array of contextual concerns (Brooks, 2007, p. 1). This includes conceptions of social contract (Fisher & Green, 2004, pp. 21-23) as they apply to concerns in international relations and internal society functioning accordant with notions of crime prevention (Manunta, 1999, pp. 59-60) which encompasses governments at an international and national level, state level, organisations and individuals. However, as a result of its diversity, security as a profession lacks consensus in definition (Borodzicz & Gibson, 2006, p.182; Manunta, 1999, p. 58). Maslow (1970) considered the very concept of security as one of the more basic human requirements in his hierarchy of needs, encompassing; stability, dependency, protection, freedom from fear, from anxiety and chaos, need for

structure, order, law, limits and strength in the protector, which collectively are defined as "security" (Coole, 2010, p. 10). In contemporary times McCrie (2004, p. 11) points out that no organisation, regardless of context can survive or thrive without adequate security.

The notion of security as a core need is not challenged within the literature. Yet, the diversity described above can result in potentially questionable approaches and advice at a functional level resulting in poorly mitigated risk concerns. In relation to differing definitions of security language, Manunta (1999, p. 57) argued that academia cannot accept the point that a consensual definition of security generally is impossible due to security's diversity, arguing security methodology, decisions, measures and performances have no meaning in the absence of a definition. To this point, Manunta expresses the importance of language within the security profession stating that precise language is essential to convey common meaning and knowledge in all fields of study (1999, p. 57). Such a view point was highlighted by Nunes-Vaz, Lord and Ciuk (2011) in reference to the concept of Security-in-Depth, and Brooks and Corkill (2012) in the area of closed circuit television (CCTV). Drawing on such points, there are common threads or themes within the literature which can lead to more precise articulations of security and therefore consistent approaches to risk mitigation.

The application of Defence in Depth in IT security relies on controls which aim to delay, with very little (or no) implementation of controls aimed at detection or response. As such, organisations are commonly not aware that their perimeter has been breached, nor are they aware that their information and data has been stolen. There are numerous reports and statistics which show that the majority of IT security breaches are reported by a party external to the organisation which has been breached (Mandia, 2011; Verizon, 2012). Recent audits conducted by the office of the auditor general for the State of Western Australia examined State government agencies ability to detect and respond to cyber threat (Murphy, 2011) achieved through a combination of physical and logical access exploitation. Of the 15 agencies' audited, only one was able to quickly detect and respond to the threat posed by the testers. This was due to incorrect application of Defence in Depth at multiple levels. No organisation tested had a defined security policy which detailed how a cyber threat was to be dealt with. Additionally, very few had any kind of security control implemented whose task was to detect that an attack was occurring or had occurred. Consequently because of this lack of ability to detect attacks, they had no driver to instigate a response. Moreover, there was no defined mechanism as to how an organisation should operationally respond, even if it was able to detect an attack.

Whilst security as a concept has been defined in many ways, regardless of context, there exists a desire for an environment where nations, organisations and people are free to act as they would like, accordant with conceptualizations of social contract. However, this is not always the case. There are always threats to such freedoms of action. This leads to the articulation presented by Coole and Brooks (2011, p. 54) that security as a concept, regardless of context should be threat driven and risk based, where protective measures are justified based on context and risk. Such an articulation is supported in the writings of Manunta (1999, p. 58) and Standards Australia HB 167 (2006, p. 3) where Manunta (1999, p. 58) argues convincingly that without a threat to an asset there is no reason for security. This leads to what Coole and Brooks (2011, p. 50) refer to as common professional threads in security. This paper argues that consistent with the available literature these common threads encompass four key points:

1. There exists a threat to a protected asset, real or perceived (Manunta, 1999; HB 167, 2006; O'Shea & Awwad-Rafferty, 2009).
2. There exists a desire on the part of practitioners to protect assets from deliberate and malicious human intervention through a variety of countermeasures (Borodzicz & Gibson, 2006; Coole & Brooks, 2011).
3. Arguably, from a functional perspective the best way to protect an asset is to control access to it.
4. Access is best controlled through a series of measures applied within a systems approach (Underwood, 1984; Fennelly, 1997; Fisher & Green, 2003; Garcia, 2001; Coole & Brooks, 2011) and this would include both physical and logical measures.

In considering such common threads and core themes the Australian Interim Security Professionals Task Force (2008; 2009) proposed that security professionals have a responsibility to ensure that their advice is soundly based in established theory and best practice principles, an approach also supported in Coole and Brooks (2011, pp. 53-54). In order to embrace such a proposition as articulated by Manunta (1999, pp. 57-58) we must ensure the use of common meaning when presenting professional advice towards the protection of assets. The focus of this paper is therefore to stimulate further discussion articulating the functional differences in meaning between

Defence in Depth as a theoretical yet functional approach, Protection in Depth as a best practice principle and Security in Depth as a holistic systems approach to protecting assets.

THE THEORY OF DEFENCE IN DEPTH

Approaches to the protection of assets for security as a domain discipline collectively embraces a consistent strategy towards preventing theft, destruction of facilities, the protection of personnel and information, referred to as Defence in Depth (Smith, 2003, p. 8). Articulated as a security theory (Coole & Brooks, 2011), Defence in Depth is underpinned by core sequential functions including deterrence, or the actual detection, delay, and response (Smith, 2003, p. 8) and recovery (Standards Australia HB 167:2006, p. 3). Smith (2003, p. 8) points out that Defence in Depth in its traditional form has been applied to the protection of assets for centuries, based on the argument that a protected asset should be enclosed by a succession of barriers, to restrict penetration of unauthorised access, towards proving time for an appropriate response (Smith, 2003) and recovery (Standards Australia HB 167: 2006, p. 3). Thus, this paper argues that Defence in Depth is a sound theory, as it is supported theoretically by both Routine Activity and Rational Choice theories from the opportunity paradigm of crime prevention theory.

Routine Activity theory focuses on what Reynald (2011, p. 1) refers to as guardian intensity, where an action will occur if a suitable target is identified, and / or a lack of capable guardian is perceived for a motivated perpetrator (Cohen & Felson, 1979, p. 589), leading to a perception of a low level of difficulty and minimum likelihood of being caught. Within this theoretical explanation for deviance is Rational Choice theory, which considers the decision making processes of a potential rational adversary in selecting whether to attempt to engage in deviant behaviour or not. Rational Choice theory argues that a potential offender focuses on a target according to their perceptions of the chances of being detected, the level of difficulty in achieving their aims (delay) and the chances of being apprehended in relation to their proclivity for violence (response). Where a perceptual cost benefit analysis suggests they have a low chance of being caught and high chance of success a rational choosing adversary will select, if they have access to the necessary resources, to proceed with their desired actions. However, if they perceive that there exists a high level of difficulty and a high chance of being caught they will select not to engage in deviant actions. Thus, accordant with Coole (2010), if security is seen as a whole then the perceived sum of detect, delay and response, as a form of "wholeness" is what drives the deterrence value of a security system. It can therefore be argued that Defence in Depth can be articulated as a security theory as it underpinned by Routine Activity and Rational Choice theories within the opportunity reduction paradigm to articulate a preventative, protective approach within the domain of security.

Defence in Depth is argued to follow a systems approach which according to Garcia (2001) integrates people, procedures and equipment into a barrier system. Such an approach allows for the application of systems thinking which recognizes that individual events (analysis) are part of a pattern of events (synthesis) (Barton & Haslett, 2007, p. 145). That is, in a systems approach, an analysis must precede synthesis where every analysis requires a subsequent synthesis to understand the wholeness of the evaluation (Ritchey, 1991, p. 10). For example, a security door can be considered a subsystem of the building fabric in terms of intruder resistance, here the portal opening is evaluated at the micro level for the material strength of the door itself, the construction of the hinges and their fitting, the use and type of hinge pins, the closing mechanism fitted, the type and quality of the locking mechanism, it's fitting to the door frame to ensure minimum gaps which may serve as a vulnerability and the quality and construction of the frame itself. In addition, sensor technologies may be fitted to aid in detecting attempts to bypass the opening. Each individual security constituent in the opening is evaluated for its design facets and material strength in providing a level of difficulty for an adversary where their effectiveness measures are combined (synthesis) to provide a level of difficulty as a portal measure.

Systems thinking creates a series of subsystems within that security layer's system where Dillon (1983, p. 183) points out that mathematics provides the means of expressing such functional relations to which operational significance (measures of performance) can be attached. Consistent with Dillon's (1983) view, such a physical barrier system's probability of effectiveness was argued by Coole (2010) to be defined accordant with the Estimated Adversary Sequence Interruption (EASI) model which consistent with the principles of General Systems Theory (GST) mathematically defines the relations between the various parts in a Defence in Depth system presenting a mathematical articulation of total system effectiveness. This approach was supported by Garcia (2001, p. 246) and Jang, Kwak, Yoo, Kim & Ki Yoon (2008, p. 748), who highlighted that the integration of people, equipment and procedures can be calculated according with the "systems" success in producing detection, delay and response to the adversary's incursion. In this approach the probability of interruption is calculated from the detection, delay and response variables as a combined system output and neutralization is a probability representing the considered level of effectiveness of the response component

against the systems defined threat. Such quantitative methods are systematic, repeatable, based on objective measures and demonstrate high statistical validity (SAND Report, 2002, p. 11). The input parameters for EASI require:

- Detection, transmission, assessment and communication inputs as probabilities that the total function will be successful; and
- Delay and response inputs as mean and standard deviation time measurements for each element.

EASI is a simple calculation tool which draws on the laws of probability (see Howell, 2008, p. 128) to combine through calculation the quantitative performance measures of the systems constituent subsystems to determine the macro-state of the Physical Protection System (PPS) (Garcia, 2001, p. 252). Thus, accordant with EASI the Defence in Depth system is therefore defined mathematically through Equation 1.

$$P(I) = P(D1) \times P(C1) \times P(R/A1) + \sum_{i=2}^{n} P(R/Ai)\, P(Ci)\, P(Di) \prod_{j=1}^{i-1} (1 - P(Di)) \quad (1)$$

This calculation can be performed from an outward in approach for a single security zone or across multiple zones, but must consider the potential that an insider may seek to move beyond their level of access authorisation to cause harm or remove a protected asset. Accordant with such a scenario, an interruption-neutralization probability is necessary from each zone in high-security contexts, that is, each time somebody can move from one secure area (zone) into another within a protected facility (See Figure 2).

Protection in Depth

The application of security measures or controls is defined by Nunes-Vaz, et al, (2011, p. 375) as a physical, psychological, procedural, technical or other device that performs or contributes to one or more security functions is achieved through the demarcation/ division of physical space; referred to as zones (Williams, 1981, p. 143; Atlas, 2008, p. 35) or rings of protection (Higgins, 1989, p. 229; Coole & Brooks, 2011, p. 54). Such rings are considered in the traditional sense of Protection in Depth, generally referred to as the onion ring model, or layers (Talbot & Jakeman, 2009; Nunes-Vaz, et al, 2011, p. 373; Atlas, 2008, p. 35) and can be conceptually represented through the diagram offered by Fisher and Green (2003, p. 148) and Atlas (2008, p. 35), Figure 1.

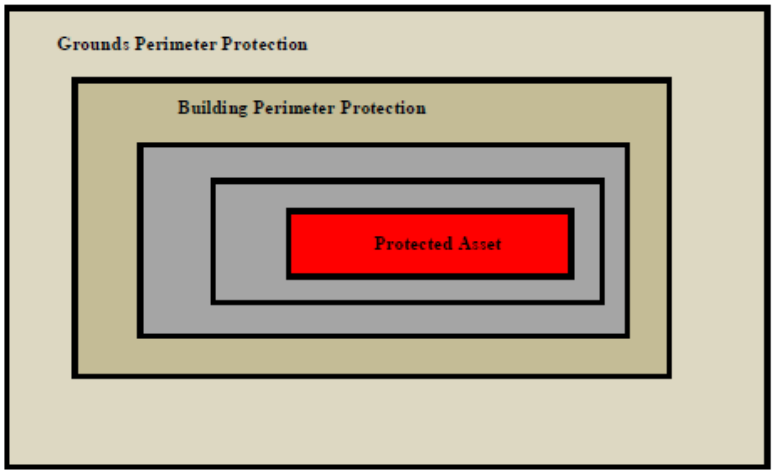

Figure 1 Traditional Onion ring model of Protection in Depth (Fisher and Green, 2003, p. 148).

However, as Coole and Brooks (2011, p. 54) express, Protection in Depth involves a number of distinct measures an adversary must defeat in sequence and considers the avoidance of single point failure in any protection plan. Such an approach potentially incorporates multiple detection constituents, multiple delay measures and multiple response capabilities (Coole & Brooks, 2011, p. 54). It is argued though that such an approach can be implemented for protecting the movement of unauthorised activity across a single security zone, or multiple security zones, where according with potential consequences there is a desire to interrupt and if necessary neutralize an unauthorised attempted incursion across a security zone. Atlas (2008, p. 35) articulates the security zoning principle well, highlighting that some areas in a facility should be completely unrestricted during the hours of designated use. However, within there are controlled or restricted spaces or zones. For a controlled or restricted zone entry is based on valid reasons rather than desire. Atlas (2008, p. 35) points out that the security-zoning concept or onion layers approach is effectively used in many facility designs. In addition, sections within restricted zones may require additional access control authorisations.

Accordant with the zoning principle, Nunes-Vaz, et al, (2011, p. 375) highlights the clear distinction between a security control and a security layer. According to Nunes-Vaz (et al, 2011, p. 375), a security layer refers to the implementation of a set of controls which can potentially stop a defined event from occurring or can entirely eliminate its harmful consequences. Such an articulation lends itself to the application of EASI for each layer in a multi-layered defence. Thus, if security's role is to manage the threats which pose a risk, then accordant with the theory of Defence in Depth there must be a means of detecting, delaying and responding to a security threat at each restricted zone, regardless of context in a systematic approach to security. For example, in the protection of a facility there may be two means of detection and one means of delay coupled into a layer separating one access zone from another. In addition, detection constituents may include intrusion detection technologies and procedural security to detect the unauthorised movement of people across an access zone, or an x-ray machine and an explosive trace technology aimed at detecting contraband moving across a secure zone through a staffed portal. It is therefore argued that Defence in Depth and Protection in Depth are interrelated yet distinct approaches in a holistic security plan. In addition, accordant with the EASI model, there exists a potential requirement to consider the necessity of a high probability of interruption and neutralization at each zone. Therefore, the probability of interruption must be calculated from the detection, delay and response variables as a combined system output for individual zones. Therefore accordant with Adams, et al, (2005, p. 1), it is argued that individual zone effectiveness can be summarized by the equation:

$$P(\text{effectiveness}) = P(\text{interruption}) \times P(\text{neutralization})$$

Security in Depth

As pointed out by Nunes-Vaz, et al, (2011, p. 372) Security in Depth and Defence in Depth are often thought of synonymously. Nevertheless, it is the contention of this paper that they are in fact separate conceptions to a holistic physical security program. Defence in Depth was argued to be a theory which articulates that for security to be effective in controlling access to an asset, area or security zone, there must be a means of detecting, delaying and responding to adversary attempts to gain unauthorised access. And for it to be effective, interruption and neutralization must occur prior to successful zone crossing. However, as with many facilities, this strategy is often required across multiple layers of controls where some trusted insiders may have access to some areas, but not all areas within a protected site. In such a case, access is usually granted based on role and security clearance. Therefore, in separating security zones there must be a means of detecting, delaying and responding to threats of unauthorised access across all zones within a security context and this may include physical and information technology zones. In addition, depending on the risk, it is argued that such separation may include multiple detection constituents, multiple delays and multiple response control measures interrelated as a system for each zone, forming a security layer between zones.

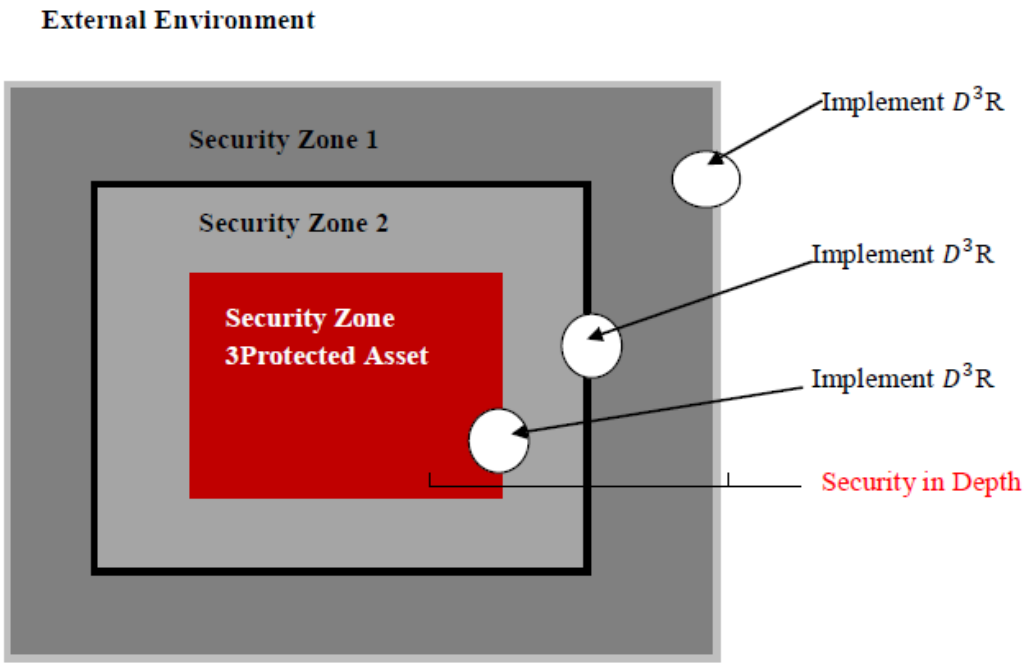

Figure 2 Security in Depth combining Defence in Depth and Protection in Depth to achieve a holistic state of security.

Whilst defence in depth supported by Protection in Depth provides the articulation to secure individual and multiple security zones within a facility, to date they refer to the elements of a physical protection systems (PP). However, contemporary approaches to security and security zoning must also consider the existence of threats, which can be manifested against information technology infrastructures once physical access has been gained within a security zone. As such, conceptions of Security in Depth as a more macro conception of security must embed such concerns into its meaning. Brooks (2011) highlighted the vulnerabilities of modern day building management systems (BMS) to logic based attacks which, once physical access has been gained, can be manifested within a security zone against an asset in a different security zone. Nunes-Vaz, et al, (2011, p. 380) pointed out that security risk may be minimized (with respect to any single threat) by maximizing the effectiveness of any one security layer, where several security functions are entwined to achieve a specific security layer. Based on such logic, the contention is that for a protected asset, Security in Depth for an organisation or facility is the sum of all security layers, physical and logical which stands between an adversary and a protected target and is therefore separate to, rather than synonymous to, Defence in Depth. This contention is highlighted in Figure 2 which depicts the concept of security layers being provided by combining controls measures which contribute to reducing security threat capabilities at that layer through their ability to deter, or detect, delay and respond to attempts of unauthorised access.

The concept of Security in Depth as depicted in this paper is argued to be supported by Nunes-Vaz, et al, (2011, p. 372) when they state that many layers are needed because it is difficult to build the perfect layer, and different layers are more or less effective against different threats. Thus, a holistic approach to security must consider the threats which pose a risk for each articulated layer in a holistic protection plan, where the level of Defence in Depth implemented at each layer and how Protection in Depth at each layer is justified, and how all layers are integrated into a larger holistic system to achieve what can now be considered Security in Depth. Consistent with the work of Talbot and Jakeman (2009), it is argued that such an approach to definition enables the achievement of Security Resilience where Security in Depth is achieved through the implementation of Protection in Depth accordant with the theory of Defence in Depth across all access zones within a protected facility or organisation (Figure 3) where each facility will have many layers or zones of access for both physical and logical measures of access control. In addition, organisational Security in Depth is the sum of all measures across all facilities.

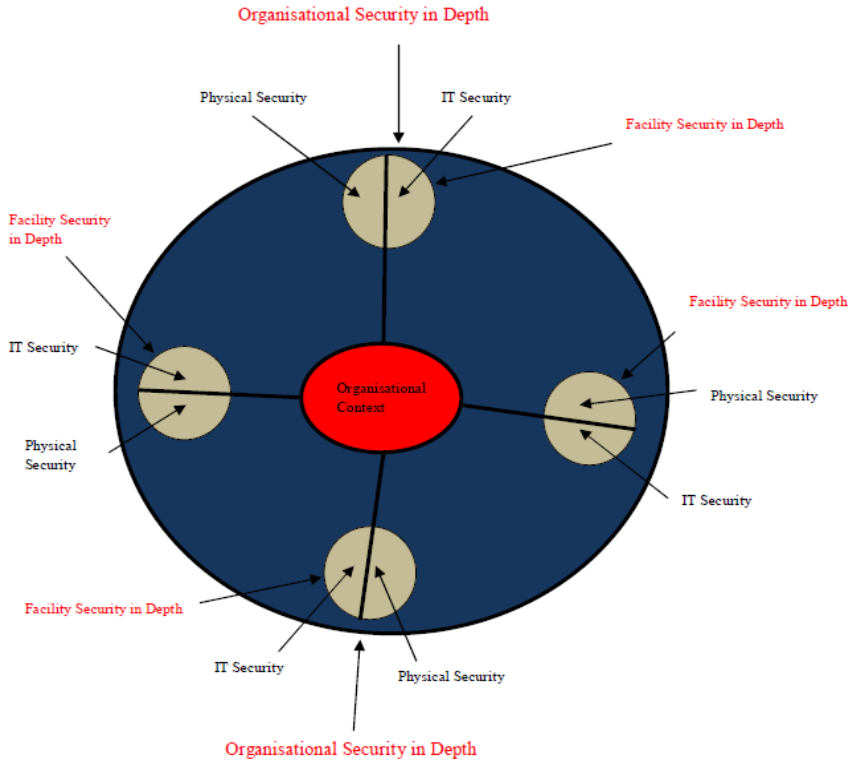

Figure 3 Organisational and facility Security in Depth.

It is argued, therefore, that Defence in Depth is a security theory which presents the argument that to remove opportunities to attack an asset there must in a layered defence, before each security zone is compromised, be a means of detecting, delay and responding to an adversary action. In contrast, Protection in Depth refers the uses of multiple different individual constituents designed to detect, delay and respond to adversary actions which make up a security specific layer separating two different security zones. However, Security in Depth refers to a holistic approach to the protection of assets where based on the threats which pose a risk across an entire organisation or facility different layers and levels of security controls are implemented to ensure access to a protected asset is restricted to those with legitimate access rights. Thus it is argued that Security in Depth can be represented by the formula:

$$\text{Security in Depth} = \text{P(effectiveness)}_1 \times \text{P(effectiveness)}_2 \times \text{P(effectiveness)}_3 \times \text{P(effectiveness)}_4 \quad (3)$$

CONCLUSION

Security as an academic discipline is still young when compared to other disciplines such as sociology, psychology and medicine. Yet as the academic discipline of security develops further, so to must the language and clarity of its definitions. Whilst traditional and often synonymous definitions of security terms have been acceptable to date, as security evolves into higher professional standing, its terms and meanings must also evolve. Otherwise, as pointed out by Manunta (1999), security methodology, decisions, measures and performance will have limited meaning. Thus Defence in Depth is argued to represent the application of Rational Choice theory, Protection in Depth is argued to represent the engineering principle of avoiding single point failure based on defined threat at each zone's layer, and Security in Depth is argued to represent total capable guardianship. Security in Depth refers to a total system view of security incorporating intelligence and, physical and logical measures of security, combined accordant to a threat thesis. Whilst differences in concepts may be subtle, structural differences do exist.

REFERENCES

Adams, D. G., Snell, M. K., Green, M. W., & Pritchard, D. A. (2005). Between detection and neutralization. Proceeding of the 2005 International Carnahan Conference on Security Technology, Institute of Electronic Engineers.

Atlas, R, I. (2008). *21st Century security and CPTED: Designing for critical infrastructure protection and crime prevention*. CRS Press. Boca Raton.

Australian Interim Security Professional's Task Force (2008). Advancing security professionals: Discussion paper. Retrieved from August 2011: http://www.isaca-adelaide.org/pd/Discusion_paper_Future_Security_Professionals_March08.pdf

Barton, J. & Selsky, J. W. (1998). *An Open-Systems Perspective on Urban Ports: An exploratory comparative analysis.* Monash University Faculty of Business & Economics. Working paper series 78/98.

Borodzicz, E., & Gibson, S. D. (2006). Corporate security education: towards meeting the challenge. *Security Journal*, 19, 180-195.

Brooks, D. J. (2007). *Defining security through the presentation of security knowledge categories*. Perth, Western Australia. Edith Cowan University, International centre for Security and Risk Sciences.

Brooks, D. J. (2011). Intelligent buildings: An investigation into current and emerging security vulnerabilities in automated building systems using an applied defeat methodology. Proceedings from the fourth Australian security and intelligence conference. Perth. Western Australia. Retrieved from: http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1013&context=asi

Brooks, D., & Corkill, J. (2012). The many languages of CCTV. *Australian Security Magazine, February/March 2012,* 57-59.

Cohen, L. & Felson, M. (1979). Social change and crime rate trends: a Routine Activity Approach. *American Sociological Review*, 144: 588-608.

Coole, M., P. (2010). The theory of entropic security decay: the gradual degradation in effectiveness of commissioned security systems. A Thesis Submitted to the Faculty of Computing, Health and Science Edith Cowan University. Retrieved from: http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1372&context=theses

Coole, M., P., & Brooks, D., J. (2011). Mapping the organizational relations within physical security's body of knowledge: A management heuristic of sound theory and best practice. Proceedings from the fourth Australian security and intelligence conference. Perth. Western Australia. Retrieved from: http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1013&context=asi
Cyber threats and ongoing efforts to protect the nation, 1-7 (2011)

Dillon, J., A. (1983). Foundations of general systems theory. Intersystem's Publications. California.

Donald, A. S. (1983). *The reflective practitioner: How professionals think in action*. BasicBooks.

Fisher, R. J., & Green, G. (2004). *Introduction to Security* (7th e.d.). Boston: Butterworth- Heinemann.

Fennelly, I. J. (1997). *Effective physical security* (2nd e.d.). Boston: Elsevier Butterworth-Heinemann.

Garcia, M. L. (2001). *The design and evaluation of physical protection systems*. Boston: Butterworth-Heinemann.

Giffiths, M., Brooks, D., Corkill, J. (2011). *Defining the Security Professional: Definition through a body of knowledge*. secau Security Research Centre. Perth.

Higgins, C. E. (1989). *Utility security operations management: for gas, water, electric and nuclear utilities*. Illinois: Charles C Thomas Publisher.

Howell, D, C. (2008). *Fundamental Statistics for the Behavioral Sciences*. Wadsworth. California.

Jang, S, S., Kwak, S, W., Yoo, H., Kim, J., S., & Ki Yoon, W. (2009). Development of a vulnerability assessment code for a physical protection system: Systematic analysis of physical protection effectiveness (SAPE). Nuclear Engineering and Technology. Vol 41 (5).

Mandia, K. (2011). Cyber threats and ongoing efforts to protect the nation. In P. s. c. o. intelligence (Ed.), (pp. 1-7): U.S. House of representatives

Manunta, G. (1999). What is security? *Security Journal*.12, 57-66.

Maslow, A., H. (1970). *Motivation and personality* (2nd end). Harper & Row. New York.

McCrie, R.D. (2004). The history of expertise in security management practice and litigation. *Security Journal* 17 (3): 11-19.

Murphy, C. (2011). Information Systems Audit Report (pp. 1-32).

Nalla, M., & Morash, M. (2002). Assessing the scope of corporate security: Common practices and relationships with other business functions. *Security Journal*. 15, 7-19.

Nunes-Vaz, R,M Lord, S., & Ciuk, J. (2011). A more rigorous framework for security-in-depth. *Journal of Applied Security Research*, 6 (3), 372-393.

O'Shea, L., S, & Rula, A. (2009). Design and security in the built environment. Fairchild Books, INC. New York.

Reynald, D., M. (2011). Factors associated with guardianship of places: Assessing the relative importance of the spatio-physical and sociodemographic contexts in generating opportunities for capable guardianship. *Journal of Research in Crime and Delinquency*, Vol 48 (110).

Ritchey, T. (1991). *On scientific Method- based on a study by Bernard Riemann*. Retrieved Jan 2010 from www.swemorph.com

Smith, C. L. (2003). *Understanding concepts in the defence in depth strategy*, School of Engineering and Mathematics. Edith Cowan University. Australia.

SANS Institute. (2002). A Scalable Systems approach for Critical Infrastructure Security. Retrieved from: http://energy.sandia.gov/wp/wp-content/gallery/uploads/020877.pdf

Standards Australia. (2006). *Security risk management.* Sydney: Standards Australia International Ltd.

Talbot, J., & Jakeman, M. (2009). *Security risk management body of knowledge: (SRMBOK).* New Jersey: John Wiley and Sons.

Underwood, G. (1984). *The security of buildings*. London: Butterworths.

Verizon. (2012). *2012 Data breach investigations report* (pp. 1-92): Verizon Business.