Bridging the Air Gap: An Information Assurance Perspective

Christopher John Richardson

BEng CEng MIfL QTS

Bridging the Air Gap is a Ministry of Defence (MoD) sponsored research into the assurance of Cross Domain Solutions(CDS); to discover and examine the possible impact and exposure implications of establishing, operating and managing highly classified systems that are operationally required to multilaterally, multilevel interface with lower classified domains, coalition networks and possibly the Internet. Information Assurance (IA) is the key to trusting, maintaining and developing Defence Cyber Operations and Information Exploitation capabilities. MoD's Network Enabled Capability (NEC) has intrinsic and often complex interdependencies, information interactions and knowledge transactions which can be chaotic, unsafe, insecure and untrusted. To comprehend, structure, make safe, secure and risk manage the NEC's enterprise architecture, its integrity and dependability requires educated IA practitioners and an assured, cultured aware user community.

Ministry of Defence
Defence College of CIS
Blandford Forum

27 August 2012

Copyright

Published by the Defence College of Communications and Information Systems

Disclaimer

This report has been written by Christopher John Richardson, MoD sponsored Research Engineer on the EPSRC Engineering Doctorate Degree Course, University of Southampton, 2007– 2012. This particular paper is a redacted version of the original UK Restricted Thesis.

The views expressed in this thesis, together with any recommendations, are those of the author and not necessarily those of the Defence College of Communication and Information Systems or any of its staff. This report therefore has no official standing as a Ministry of Defence document and must not be quoted as such. Further, such views should not be considered as constituting an official endorsement of factual accuracy, opinion, conclusion or recommendation of the UK Ministry of Defence or any other department of Her Britannic Majesty's Government of the United Kingdom.

EPSRC

Engineering and Physical Sciences
Research Council

UNIVERSITY OF
Southampton

Degree of Doctor of Philosophy in Engineering

Title:

Bridging the Air Gap: An Information Assurance Perspective

Research Student:	Christopher John Richardson **Email:** cjr1x07@soton.ac.uk
Research Group/School:	Electronics and Computer Science
Sponsor:	Ministry of Defence
Industrial Mentors:	Mr Adrian Price and Mr Nigel Rich
Academic Supervisor:	Dr. Peter R. Wilson

DEFENCE COLLEGE of
COMMUNICATIONS & INFORMATION SYSTEMS

Research Engineer

Christopher John Richardson
Research Engineer
School of Electronics and Computer Science
University of Southampton
Southampton
SO17 1BJ

Telephone: 01202 966670
Email: cjrichardson@bournemouth.ac.uk

Industrial Sponsor

Adrian Price
Head of Information Security Policy
Directorate of Defence Security
Ministry of Defence
Whitehall
London SW1A 2HB

Telephone: 020 7218 3746
Email: Adrian.price895@mod.uk

Industrial Supervisor

Nigel Rich
Head of Department
ICT Faculty, Old School Building
Defence College of Communications and Information Systems
Blandford Forum
Dorset DT11 8RH

Telephone: 01258 482272
Email: nrich@bournemouth.ac.uk

Academic Supervisor

Dr Peter R. Wilson
School of Electronics and Computer Science
University of Southampton
Southampton SO17 1BJ

Telephone: 023 8059 4162
Email: prw@ecs.soton.ac.uk

Thesis Abstract

Name of university	UNIVERSITY OF SOUTHAMPTON
Abstract	ABSTRACT
Name of Faculty	DEPT OF ELECTRONICS & COMPUTER SCIENCE
Discipline	INFORMATION ASSURANCE & SECURITY
Degree for which thesis is submitted	DOCTOR OF PHILOSOPHY IN ENGINEERING (EngD)
Title of thesis	BRIDGING THE GAP: AN INFORMATION ASSURANCE PERSPECTIVE
Full name of author	by CHRISTOPHER JOHN RICHARDSON

The military has 5 domains of operations: Land, Sea, Air, Space and now Cyber. This 5th Domain is a heterogeneous network (of networks) of Communication and Information Systems (CIS) which were designed and accredited to meet Netcentric capability requirements; to be robust, secure and functional to the organisation's needs. Those needs have changed. In the globalised economy and across the Battlespace, organisations now need to share information. Keeping our secrets, secret has been the watchwords of Information Security and the accreditation process; whilst sharing them securely across coalition, geo-physically dispersed networks has become the cyber security dilemma.

The diversity of Advanced Persistent Threats, the contagion of Cyber Power and insecurity of coalition Interoperability has generated a plethora of vulnerabilities to the Cyber Domain. Necessity (fiscal and time-constraints) has created security gaps in deployed CIS architectures through their interconnections. This federated environment for superior decision making and shared situational awareness requires that Bridging the (new capability) Gaps needs to be more than just improving security (Confidentiality, Integrity and Availability) mechanisms to the technical system interfaces. The solution needs a new approach to creating and understanding a trusted, social-technical CIS environment and how these (sensitive) information assets should be managed, stored and transmitted.

Information Assurance (IA) offers a cohesive architecture for coalition system (of systems) interoperability; the identification of strategies, skills and business processes required for effective information operations, management and exploitation. IA provides trusted, risk managed social-technical (Enterprise) infrastructures which are safe, resilient, dependable and secure. This thesis redefines IA architecture and creates models that recognise the integrated, complex issues within technical to organisational interoperability and the assurance that the right information is delivered to the right people at the right time in a trustworthy environment and identifies the need for IA practitioners and a necessary IA education for all Cyber Warriors.

Academic Thesis: Declaration of Authorship

I, **Christopher John Richardson**, declare that this thesis and the work presented in it are my own and has been generated by me as the result of my own original research.

Bridging the Air Gap:

An Information Assurance Perspective

I confirm that:

1. This work was done wholly or mainly while in candidature for a research degree at this University;

2. Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated;

3. Where I have consulted the published work of others, this is always clearly attributed;

4. Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work;

5. I have acknowledged all main sources of help;

6. Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself;

7. Either none of this work has been published before submission, or parts of this work have been published as:

Richardson, C. J. (2007). Security: a necessary compromise? *NATO Conference, Bletchley Park, 26 June 2007.* Telindus.

Richardson, C. J. (2008). Bridging an IA Capability Gap. *Realising Network Enabled Capability (RNEC'08), NECTICE, Leeds, UK, 13 October 2008.* NECTISE Loughbourgh University.

Richardson, C. J. (2009). A Holistic Approach to Effective Information Assurance Education. *Military Information Assurance and Security Symposium, MoD Abbey Wood, 16 April 2009.* Cobham Technical Services.

Richardson, C. J. (2011). Cyberspace: The 5th Domain. *Cyber Security 2011, Brussels, Beliguim, 31 May- 1 June 2011.* IQPC.

Richardson, C. J. (2011). Information Assurance: Holistic and Human Centric. *iGRC TD2 Presentation, Birkbeck, University of London Symposium, 15 December 2011.* Bournemouth University

Richardson, C. J. (2012, June 5). The Assurance of Socio-Technical Enterprise Operations. *MSc Information Assurance Module 2*. London, UK.

Signed:

……………………………………………………………………………………………………..

Date: 4th July 2012

Acknowledgement

*In loving memory of **Shirley Richardson** (May 1937- June 2010), my mother who saw me through my life, but didn't manage to see this Thesis completed.*

This is my opportunity to say Thank You...

My inspiration has always been the challenge of the unknown, finding the limits of my understanding and then pushing the barrier outwards. For that I thank Adrian Price and Dr Stuart Wray for opening the door to Information Security and its Assurance. Both had a totally different but authoritative perspective to this vast, complex domain of knowledge and understanding. I also must thank my colleagues at the Ministry of Defence (MoD) Defence College of Communications and Information Systems (DCCIS) who have supported my work, analysis and evaluations, my line manager and Director, Nigel Rich.

Thanks to my fellow researchers and friends Paul McCreeth and Dr Michael Jones who have shared the pleasures of discovery and hardships of necessary selfishness in the starting and completion of research degrees. A special appreciation to my friend and fellow lecturer Alexander Wilson as his considerable insight to Traffic Engineering and Network Simulation has given balance and some reality to the research. He's an enthusiastic engineer and an innovative artist that has made the impossible, possible.

Furthermore, I thank the support and encouragement from the research scientist at the Defence Science and Technology Agency (DSTL); the project engineers at the Defence Equipment and Support (DE&S); the Directorate of Security and Safety, MoD's Chief

Information Office and The Defence Working Groups that have entertain and listen to my opinions and observations which provoked insights to the complexities of this research; and the National School of Government, in particular the listening and advice from Sharon Wiltshire.

A special thank you to Dr Peter Wilson, my long suffering Academic Supervisor at the University of Southampton whose encouragement and leadership was always been implicit and timely; a wise man who knew the time when to inject and when to leave alone; to Dr Neil Richardson, FESM Assistant Dean and Head of Industry Doctoral Training Centre (IDTC) and his hard working assistant Sally Hawthorne who kept me informed on everything and the staff of the School of Electronics and Computer Science (ECS) at Southampton University, where many have contributed time and giving a helping hand to my work. To the Southampton University's School of Management who broaden my strategic vision and most of the taught elements of the Engineering Doctorate and to the Engineering and Physical Sciences Research Council (EPSRC) and the Ministry of Defence who financially sponsored my thesis and research engineering activities.

My personal thanks go to my family and friends. To my three wonderful children, Helen, Fiona and Alexander whose support and kindness I have needed on many a tiring weekend. To my life-long friend Regina Elliott who open my mind to other alternative interpretations of real and virtual space. Over the past years I have lost many precious moments as thoughts, energies and time were devoted to the pursuit and rigours of this doctorate's academic goal and research. It has been a discovery and an awaking to the constant determinant that Bridging the Air Gap has no foreseeable final resolution and pursuing the goals formulates further, more intricate, problems, however at some point a stake needed to be driven home and a Thesis written.

Contents

CHAPTER 1

CHAPTER 2

CHAPTER 3

CHAPTER 4

CHAPTER 5

Table of Figures

Thesis Tables

ABBREVIATIONS

C^2	Command and Control
C^4II	Command, Control, Communications, Computing, Intelligence and Information
CBM	Command and Battle Management
CDS	Cross-Domain Solution
CIIA	Cyber, Identity and Information Assurance
CII	Critical Information Infrastructure
CIP	Cognitive, Information and Physical
CIPE-V^2R	Cogitation, Information, Physical Environment – Virtual, Visual, Real
CIS	Communication and Information Systems
CNA	Computer Network Attack / Cyber Network Attack
CND	Computer Network Defence / Cyber Network Defence
CNE	Computer Network Exploitation / Cyber Network Exploitation
CNM	Computer Network Management / Cyber Network Management
CNO	Computer Network Operations / Cyber Network Operations
COI	Community of Interest / Communities of Interest
CoNSIS	Coalition Network for Secure Information Sharing
COP	Common Operational Picture
COTS	Commercial off the Shelf
CPNI	Centre for the Protection of National Infrastructure
CSA	Cyber Situational Awareness
DAD	Disclosure, Abuse and Denial
DAIA	Defence Assured Information Architecture
DBSy	Domain Based Security
DCCIS	Defence College for Communication and Information Systems
DCF	Defence Conceptual Frameworks
DCPD	Direct, Collect, Process, Disseminate
DEC	Director of Equipment Capability
DEC(CCII)	DEC Command & Control and Information Infrastructure
DIAN	Defence Information Assurance Notice
DII	Defence Information Infrastructure
DLOD	Defence Line of Development
DMZ	Demilitarized Zone
DoD	(US) Department of Defense
DSA	Defence Security Architecture
DSTL	Defence Science and Technology Laboratory
EBAO	Effects Based Approach to Operations
EEFI	Essential elements of friendly information
ES	Electronic Surveillance
ESII	Enabling Secure Information Infrastructure
GIG	Global Information Grid
GII	Global Information Infrastructure
GOSCC	Global Operations Security and Control Centre
HUMINT	Human Intelligence

I^2	Information and Intelligence
IA	Information Assurance
IER	Information Exchange Requirements
IIS	Internet Information Services
IM	Information Management
INFOSEC	Information Security
IO	Information Operations
IS	Information Services
ISTAR	Intelligence, Surveillance, Target Acquisition and Reconnaissance
ITIL	Information Technology Infrastructure Library
IX	Information Exploitation
JCDX	Joint Cross Domain Exchange
JDP	Joint Doctrine Publication
JP	Joint Publication
JSP	Joint Service Publication
JWICS	Joint Worldwide Intelligence Communications System
JWP	Joint Warfare Publication
KID	Knowledge, Information & Data
KT	Knowledge Transfer
MIB	Management Information Base
MIP	Multilateral Interoperability Programme
MNIS	Multinational Information Sharing
MOD	Ministry of Defence
NEC	Network Enabled Capability
NCW	Network-Centric Warfare
NIDS	Network-based Intrusion Detection System
NII	Network Infrastructure and Integration
NSA	(US) National Security Agency
OODA	Observe, Orient, Decide, and Act
OPSEC	Operations Security
ORAC	Opportunities, Risk Assurance, Architecture and Complexities
PJHQ	Permanent Joint Headquarters
PRIME	Privacy and Identity Management for Europe
RMA	Revolution in Military Affairs
SCADA	Supervisory Control And Data Acquisition
SDM	Superior Decision Making
SFIA	Skills for the Information Age
SIPRNet	Secret Internet Protocol Router Network
SOA	Service Orientated Architecture
STE	Socio-Technical Enterprise
UCDMO	Unified Cross Domain Management Office

CHAPTER 1
Bridging the Gap: An Information Perspective

The responsibility will fall on young officers to build trust across the ranks to improve information sharing. In this age, I don't care how technologically or operationally brilliant you are; if you cannot build trust [across various multiple participants], you might as well go home.

Marine Corps Gen. James N. Mattis
Commander of U.S. Joint Forces Command

In an age, where having accurate and timely Information makes the difference to superior decision making (Khatri & Ng, 2000; Bradley, Pridmore, & Byrd, 2006) and where Cyberspace has transformed how these decisions make immediate, instantaneous impact on the global market place (Coyle, 1999)**,** affecting many communities of interests; it has become imperative to get the right information to the right person at the right time. This imperative makes all the difference as the process of sharing trusted information has far greater influence than mere communication (Katz & Lazarsfeld, 2006).

Getting it right; through a process of gaining trust and managing risks, providing safe and secure information that can flow across resilient and protected systems and where the information assets are both dependable and timely should be, and within this thesis will be argued as the aim and scope of Information Assurance (IA). Through providing some solutions to the problems of interoperability and secure cyber communication, this thesis will redefine the Art and Science of IA.

Moreover, this thesis will provide an argued solution to its fundamental question:-

> ***Can Information Assurance provide sufficient Trust and Risk Reduction to allow information processed, stored and communication within highly sensitive (often critical) networks, with their own discrete security domains (including encryption mechanisms), which are often Air-gapped (physically and electronically isolated) to interact safely and securely, particularly across many interoperable networks and including the possibility of interfacing with the Internet.***

Substantiate the need to better define Information Assurance (making it more distinct and effective than its current scope which is heavily dependent upon its roots within Information Security); innovate an IA Architecture that is based on the developed this thesis goals' of assurance and not just on the dimensions of security; provide an eight dimensional model to better understand the need for tolerance and trust across many different interoperable networks and the maintenance of cross-domain solutions for system (and system of systems) dependability; create a professional framework to direct what IA skills we need today and define the necessary IA education that is needed for the 21st Century Cyber workplace and ultimately argue how we should best employ Information Assurance for Governments, Enterprises and the Military; to use it more effectively and reliably.

Information Assurance has become one of the most important studies in Computer Science, Information Technology and Cyber Knowledge Transfer and probably will have a significant social and cultural impact to our globalised knowledge economy (Drahos & Braithwaite, 2002). Without an assured process between two interconnecting systems, trust can soon diminish, whilst risks will grow and the *need to share* through its layers of interoperability will rapidly fall back to a defensive *need to know* operation and the enterprise cyber operations will once again rely on more critical (inefficient and unresponsive) *stove-piped* networks and their isolating security domains and curtaining policies. An Assured environment is not risk free, but it promotes the interoperability of services and communication channels between communities of interest (COI) whilst actively reducing and managing risk through education, professional best practices, Ignorance Management, Shared Situational Awareness (SSA), controlled Information Exploitation (IX). Information Assurance can provide a comprehensive cyber defence strategy; dependable Information Operations (IO), resilient Infrastructure Architectures and networks and above all, through Business (Enterprise and IA) Architecture, a *Trusted environment*. In the hierarchy of human needs (Maslow, 1943; Huitt, 2007): water, food and shelter, law and order are surely still the most important things to us all; but the transformation toward increasing dependence on Information Technologies (Powell & Dent-Micallef, 1997) and the continuance of digital interconnections, the *network effects*, have these information systems and technologies becoming pervasive and essential to us all. It is the control of this Cyberspace that has become a strategic priority to states and non-state actors. As our Information and its infrastructures have become national assets, they also constitute a tier-1 national security risk that requires appropriate management controls and defences (Cabinet Office, 2011a).

There is an unprecedented reliance on information infrastructure as Governments, Enterprises and the Military find that their transformation to Information driven operations, increased operational transparency and exploitation have generated complex risks and a considerable reduction in their ability to control the information flows. The sense of necessity, comfort, wonder and curiosity within the virtual world is a real paradigm where informed cyber actors and agents have increased their transformation skills as they digitally create, adjust, innovate, exploit, survey, manipulate, subvert or sabotage cyber domains. This poses varied and complex assurance issues to managing Cyberspace.

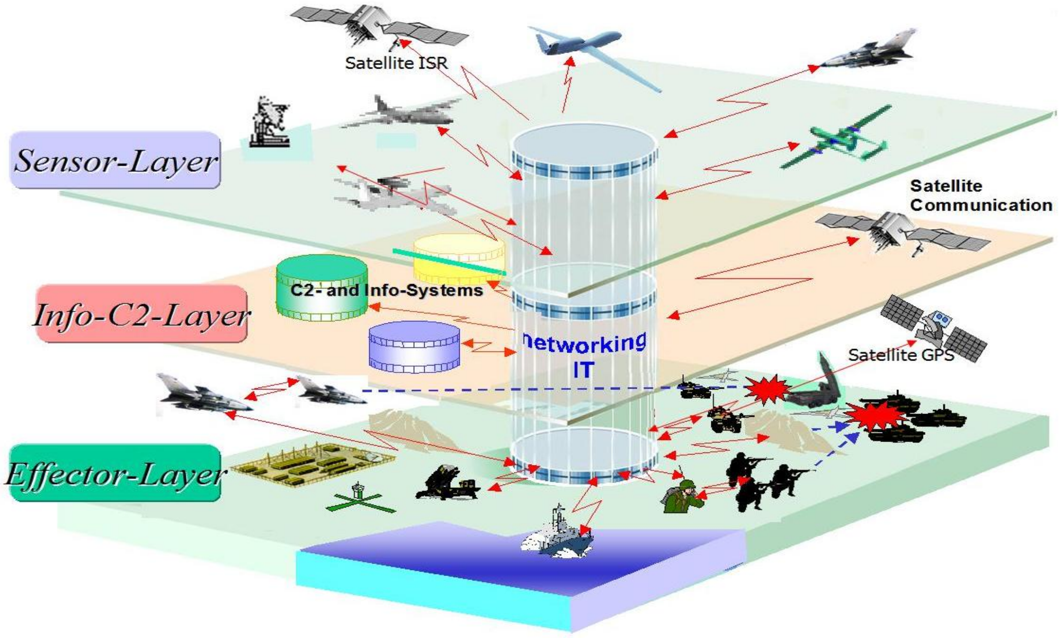


Figure 1: Netcentric Operations and Military Mobility (Benedict, 2011)

Bridging the Gap is a holistic investigation to see whether there might be practical technical or human factor solutions that assures interconnection of highly classified domains to the information rich environment that the Internet offers. Without access to timely and effective use of information our decisions become jaded, inappropriate or suspect. We need our information to be accurate, trusted and not compromised, lost, leaked, disseminated, unauthorised publication or corrupted.

> *"Our reliance on cyberspace stands in stark contrast to the inadequacy of our cyber security,"* **DoD Strategy for Operating in Cyberspace, 2011**

This Ministry of Defence (MoD) sponsored research will determine how we achieve acceptable assurance and limit the risk of establishing, operating and managing a highly classified system interfacing to cross domains and ultimately the Internet. The Network Enabled Capability (NEC) and its ISTARs community has intrinsic, often complex interdependencies, where information interactions and knowledge transactions needs to cross many domains. The NEC doctrine of Information Superiority predicates the need for information security and its assurance to provide accredited, safe, secure, robust and trusted sources. The foundation lies with better networks that provide better information sharing which leads to better decision; actions and effects. The benefit is operation efficiency and superior military capability (MoD, 2011). The military's robust, secure and extensive information domains are not what is generally associated with the ubiquitous, open access Internet and its hosted web-based services but rather a bespoke environment under full control of its owners or coalition partnership. However, it is the mating, mash up and interconnection of any network that needs to be investigated, because the boundary between military computer network operations (CNO) and others have become blurred, removed or created without authority. Recognising that Information and Knowledge in its various forms, media, databases, reports, services, interpretation and usage have become one of the most important assets to our business, but *do we really comprehend this*?

Analysis suggests that the only way to really secure a military system is to isolate it. Disconnect the system from other networks, in particular the Internet and its associated risks to Computer Network Attacks (CNA) and Computer Network Exploitation (CNE) as well as to other elements of the information domain (see figure 3). From a security perspective the Internet is unorganised, chaotic, unsafe, insecure, untrustworthy environment of viruses, worms, exploited vulnerabilities, denial-of-service attacks, cyber power, cybercrime and cyber war but it can also be an assured world of creativity, innovation, commerce and social cohesion.

1.1 A New World

The Council of the European Union (2010) has made Information Assurance one of its 14 main policies and it has become a key component of the US Comprehensive National Cybersecurity Initiative (The US National Security Council, 2008) and the subsequent International Strategy for Cyberspace (The US National Security Council, 2011). This thesis will, in part, need to consider the impact of IA to the cyber environment (Cyberspace) and in particular to current security policies and domain isolation. Through IA, we need to find an effective approach and possible Cross-Domain Solutions (CDS) between the "*Need to Know"* (keeping our secrets safe and available only to a closed authorised community) and the "*Need to Share*" (allowing information to used and accessed by global communities of interest); hence the thesis will demonstrate how, when and most importantly, *why we need to Bridge the Air Gaps*: by developing and employing the need for trust and risk management, education and skilled practitioners, tolerant organised structures with resilient architecture, dependable and safe procedures and appropriate use of security and protective countermeasures: in effect by applying the proposed IA definition, models and frameworks. The Council defines Information Assurance *in the field of communication and information systems is the confidence that such systems will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users. Effective IA shall ensure appropriate levels of confidentiality, integrity, availability, non-repudiation and authenticity. IA shall be based on a risk management process.* This definition derives authority from many similar declarations in national policies (CESG, 2003), Security Taxonomy (Savola, 2007) and IA Glossaries (Committee on National Security Systems, 2010). However, all these IA definitions rest upon the 3 tenets of Information Security: *Confidentiality, Integrity and Availability* (CIA). This thesis will argue that these foundation tenets, the CIA and the 5 other dimensions of security: Non-repudiation, Authentication, Access Control, Privacy and Communication Security (ITU-T X.805, 2005) are themselves only one of 8-Dimensions of Information Assurance (as proposed in Chapter 6) that is required to fully understand, address and assure the holistic issues of cyberspace, its environment, capabilities and culture.

Information in Cyberspace has a complex paradigm; the need for a trusting, dynamic "*Need to Share*" (Alberts D. S., Garstka, Hayes, & Signori, 2001) opposed to the secure but distrusting, restrictive "*The Need to Know*" (Denning, 1976) which is further complicated by anonymity and the "*Need to Hide*" (Buda, Choi, Graveman, & Kubic, 2001). The common operating environment has become a need to protect information across security domains so that Enterprises survive the interoperability of increasing networks of networks and the systems of systems that form the information infrastructures across cyberspace. This environment is expanding, evolving, constantly exploited and is becoming both an economic asset and liability that has been described as a new mindset to security practitioners (Task Force on National Security in the Information Age, 2002).

The intelligence community (G2) has longed deliberated the importance of sharing information and to keeping secrets, secret (Frigns, 2004; Liles & Liles, 2009). Information Services (IS), Knowledge Transfer (KT), Superior Decision Making (SDM) and holistic Shared Situational Awareness (SSA) and Cyber Situational Awareness (CSA) are becoming an ever more important component to businesses, their intelligence communities as well as transformational Government policing and warfighting (Kelly O. L., 2008; Bailey, 2010; Bieniek, 2011). Moreover, the increasing dependencies on cyber governance, assured e-commerce and social computing is making information a critical asset for nations, enterprises and online communities, the military and to individuals. The *Need to Share* (Dawes, Cresswell, & Pardo, 2009) and also the *Need to Belong*[1] (Baumeister & Leary, 1995) requires an assured skilled and educated workforce to manage, maintain and service the cyber environment and the cultures it supports. Within the military (and many enterprises) we need a framework to culturally shift our mindset from 20th Century security practices to cross-domain assurance which will provide a comprehensive, dependable, resilient and trustworthy architecture that is capable and tolerant to withstand and survive the emerging, interoperable, evolving cyber environment. This culture shift, however, presents the Military, as well as Governments and Commercial Enterprises, with a number of complex challenges to solve (Anderson & Rainie, 2010; Sommer & Brown, 2011).

A challenge and another fundamental question raised by this Thesis is: ***How do we provide Assurance when we do not control the asset we want to secure and protect?*** There is a considerable array of threats, attack methods and injected software instruction approaches to our networks and to our information assets (processed, stored or communicated) that provide new challenges every day (McCumber, 1991). Harvard Professor Joseph Nye described this cyberspace security challenge at the

[1] Existing evidence supports (Baumeister & Leary, 1995) the hypothesis that the *need to belong* is an innate, powerful, fundamental, and extremely pervasive motivation to affiliate with others and be socially accepted.

opening of the Munich Security Conference, 2011, where he remarked that: *"The threat is real but national governments had only just now started to tackle the issue*." Cornelia Habig (2011) reported that this further reinforced the need to address complex security and assurance challenges. "*In the EU, but also on the national level, the responsibilities in terms of cybercrime issues are immensely fragmented…Every two seconds, there are new cyber-crime incidents, and every four seconds, there is an attack on the network of the German administration*," was the worrying criticism expressed by German Federal Minister of the Interior; Thomas de Maizière. The conference remarks demonstrated a collective concern of Governments and the Military towards the potential damage that an unpoliced cyberspace could do national and international interests. The threats are real; many of the defences are inadequate.

Coalition Collaboration

Collaboration is defined as: *"The act of working together with others to achieve a goal"* The UK's MoD Comprehensive Approach (Joint Discussion Note 4/05, 2006), its own and NATO's Network Enabled Capability (NEC) and the US Joint Force Command's Effects Based Operational Approach (EBOA) have all proposed the need for an agile, robust interoperable "*Netcentric*" network for Joint Actions and coalition communications. This desire and operational imperative to interconnect modern and legacy systems that allows coalition forces to benefit from extensive and responsive Information Exploitation (IX), Knowledge Transfer and digital encapsulation of the Operational theatre, providing commanders an accurate, trustworthy Cyber picture and Cyber Situational Awareness, "*knowing what's going on"* (Knight, 2001), thereby facilitating Superior Decisions. These doctrines also call for the projection of Cyberpower, conduct of Cyberwar and Information Operations (IO). Whereas, a key UK NEC component[2] is the assurance and protection of its 4 Domains: (1) Networks, (2) Information and (3) People operating in a (4) Joint Actions Environment (MoD, 2005). The US Committee on National Security Systems (CNSS, 2006) defined this Joint Actions' Communication and Information Systems (CIS) environment as a "*Cross-Domain Solution*" (CDS) as "*any information assurance solution that provides the ability to access or transfer information between two or more security domains*."

[2] The MoD's Joint Services Publication (JSP 777) provides a clear expression of what the UK means by NEC in order to engender a much wider and more common understanding of its tenets not only within the UK's Ministry of Defence and Armed Forces, but also across Government, within Defence Industry and Academia, and with allies and coalition partners.

Interoperability has become a key network driver for transforming governments (Cabinet Office, 2005), businesses and other institutions; the use of Cyberspace (its capability) to communicate and securely transact with peers, other enterprises (B2B) and the global audience of active users has far reaching opportunities and development. However, these interacting activities require system availability, resilience, tolerance, dependability, security and above all an ability to create trust. As such the Cross Domain Solution has three main assurance categories:

- The need to allow **Access Solutions**; (allow users to request /pull information resources in multiple multi-lateral and multi-layered domains). Access Control, Authentication and System Integrity
- The need to provide **Cross Domain Transfer Solutions**; (enabling secure and accurate movement, copy, and deletion of information from one domain to another and ensuring system dependability and resilience.)
- To need to have **Accredited Solutions**; (Providing structured, safe, secure and trusted CDS for Information Operations and Exploitation).

The information assured CDS domain will need to be structured, resilient, dependable, safe, secure, protected, risk managed. Above all we need User Communities to become SMART and capable of pulling cyber resources. According to the US DOD it now requires that Information Operations (IO) be regarded as a military core competency*, “on par with air, ground, maritime, and special operations”* (DoD, 2003, p. 4). *The ability to control the information environment, including interrelated physical, informational, and cognitive dimensions, is now seen as vital to national security* (DoD JP 3-13, 2006) and the Department recognise that Cyberspace is a cognitive dimension, in which *“people think, perceive, visualize, and decide,” that is seen as most important* (DoD JP 3-13, 2006, pp. 1-2). This directive places Information as a Strategic Asset and recent military documentation emphasized the significant need for dependable and interoperable information infrastructures, the net-centricity of military cyberspace as described by Joint Publication 3–13, *Information Operations* and Joint Publication 3–24, *Counterinsurgency Operations* describe that there is: “*The ability to be “persuasive in peace, decisive in war, preeminent in any form of conflict”* (DoD, 2000, p. 1).

Sara King’s (King, 2010) discussion paper “*Military Social Influences in the Global Information Environment*” identified that:- *According to Scales (2006) and* others (Boyd, 2007; Darley, 2007) *this new era of “psycho-cultural battle” - otherwise termed a “war of ideas”* (Murphy, 2010, p. 90) *or a battle for “hearts and minds*” (Claessen, 2007, p. 97) - *is already underway in Iraq and Afghanistan. Modern battle is likely to be more about winning public opinion than about seizing contested geophysical terrain. The modern* *battlefield is likely to be in the information environment.* King's observation that modern wars are more to do with manipulating human factors rather than destruction of assets is an important paradigm for 21st Century Netcentric Warfare. Military Information operations are moving away from the targeting of munitions to the targeting of opinion, thoughts and cultural change. This theme is further explored and analysed with the Human-Computer Interface that have evolved within the layers of interoperability. In particular the developing the *need to share*, allowing participation and collaboration at all levels, educating and training users to exploit assured information, to know where the assets are located and configured, to be able to translate, transform and non-repudiate and to trust the asset in making decisions.

Information Exploitation is essential to future governance in what is now strategically developed the Diplomatic, Intelligence, Information & Interests, Military and Economic (DI^{3}ME) domain. Cyberspace is the DOD's Netcentric domain and it has been described as: *"the extent to which a system or group has at its center the complex connection of people with common interests via communications and computer networks."* Dave Chesebrough, 2006. Although this description places both Information Technology and People as essential elements for the deployment and exploitation of Netcentricity; it doesn't encapsulate the full extent and nature of Cyberspace. Chapters 2 and 3 will develop the Cyber Environment and in particular its creation as the 5th Military Domain of Operations. However, Chesebrough (2006) did further identify 4 components that made the Network domain; these where:

1. *A system of lines or channels that cross or interconnect: a network of railroads.*
2. *A complex, interconnected group or system: an espionage network.*
3. *An extended group of people with similar interests or concerns who interact and remain in informal contact for mutual assistance or support [a social or professional network]*
4. *In Computer Science, a system of computers interconnected by telephone wires or other means in order to share information. Also called [the] net.*

The *Network Effect* of these definitions, when combined, becomes one complex domain which the DoD defines as the Global Information Grid (GIG). The interconnection of theatres of operations, technologies and people formulate the Cross-Domain Problem where deployed systems are required to link digitally to others and the networks need to become interoperable to share data. The Information Exchange creates degrees of complexity as people with common interest interact with technology to create a desired common awareness.

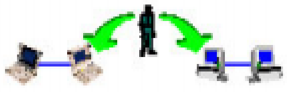
Information Exchange	Levels of Interoperability	Computing Environment
Cross-Domain Sharing **Advanced Collaboration** Interactive COP and event-triggered database replication	**Level-4** **Enterprise** Interactive manipulations Shared data & Applications	
Shared Databases **Sophisticated Collaboration** Common Operational Picture Geospatial imaginary	**Level-3** **Domain** Shared Data, Separate Applications	
Heterogeneous Product Exchange Photo & Videos, digital maps & overlays	**Level-2** **Functional** Minimal common functions Separate data &applications	
Homogeneous Product Exchange FM voice, tactical data links, text files, IM & e-mails	**Level -1** **Connected** Electronic Connection Separate data & applications	
Manual Gateway Impress, Diskettes, tape, hard copy exchange	**Level – 0** **Isolated** Not Connected / Air Gapped	

Figure 2: The LISI Interoperability Maturity Model (2004)

Information Exchange through interoperability within the military (NATO's Network Enhanced Capability and the DoD GIG) has millions of computing devices linked in classified networks becoming ever more reliant on cyberspace for its command and control, logistics, information and intelligence operations, targeting and munitions (Fire) as well as personal management and business operations. Resolving the assurance issues of interoperability has become a major component to finding a cross-domain solution. The goal of military CIS interoperability is to achieve the advance collaboration at the Enterprise Level. This, as Figure 2 illustrates, is the uppermost of DoD's 5 Levels of the Information System Interoperability Maturity Model with its focus on the increasing levels of sophistication between system of systems interoperability.

> *Although technical interoperability is essential, it is not sufficient to ensure effective operations. There must be a suitable focus on procedural and organizational elements, and decision makers at all levels must understand each other's capabilities and constraints. Training and education, experience and exercises, cooperative planning, and skilled liaison at all levels of the joint force will not only overcome the barriers of organizational culture and differing priorities, but will teach members of the joint team to appreciate the full range of Service capabilities available to them.* **(DoD, 2000)**

As quoted, the years of experience in Bosnia, Iraq and Afghanistan has taught the coalition partners; Interoperability between military systems, be them owned by any one nation or federated across communities of interest have generated many complex problems. Interoperability is more than a legacy issue or a technical interface problem, its concerns the harmonisation of organisations, alignment of policies and procedures, cultural changes, federated leadership and an understanding of how system of systems operate and evolve. Cross-Domain Solutions are the application of Information Assurance to the challenges of interoperability. IA has to address the many levels involved in the harmonisation and alignment of Organisation, Systems and Networks, properly define and architect the requirement of the Enterprise, build in system resilience and tolerance to intrusion making the solutions both safe and dependable. The systems have to gracefully decline when under attack and appropriate business continuity and disaster recovery must be prepared and be ready to be deploy at a moment notice. Information Assurance will be required and applied to systems that previously did not interact and often have constraints within their own operations or from the onset with new systems that are designed to interact. This is an important first step; however, there will be systems that as of yet have not been conceived or are required to interoperate, so the IA architecture must anticipate future considerations and be able to cope with uncertainties..

A holistic perspective is that Reality is layered with a virtual world, as illustrated in Figure 3, which now has 5 domains: Land, Sea, Air, Space and Cyber. The cost of doing business in the first 4 domain represent an escalation of equipment costs, training and accessibility, in the 5th domain cost is negligible, *anybody can become a cyber-warrior*. The military 5-layered model(figure 2) is supported by the geographical location (location will be a key component to Access Control, knowing where the user should be is an determining element of authentication) and the physical interconnectivity and interoperability of ubiquitous edge devices. This man-made physical operating environment is constantly changing and needs to be resilient and transnational. We should not consider Cyberspace or the Cyber environment has being virtual or a cloud – Cyberspace exists in physical devices within DNS, Service Orientated Architectures (SOA) and distributive databases forming a local interface to real world of packet routers, telephony and inter-operating networks of networks. Behind these devices are the logical layers that provide software-enabled functions with emergent logical connections and often producing unforeseen outcomes; thereby introducing vulnerabilities, risk and business impact (Castonguay, 2011).

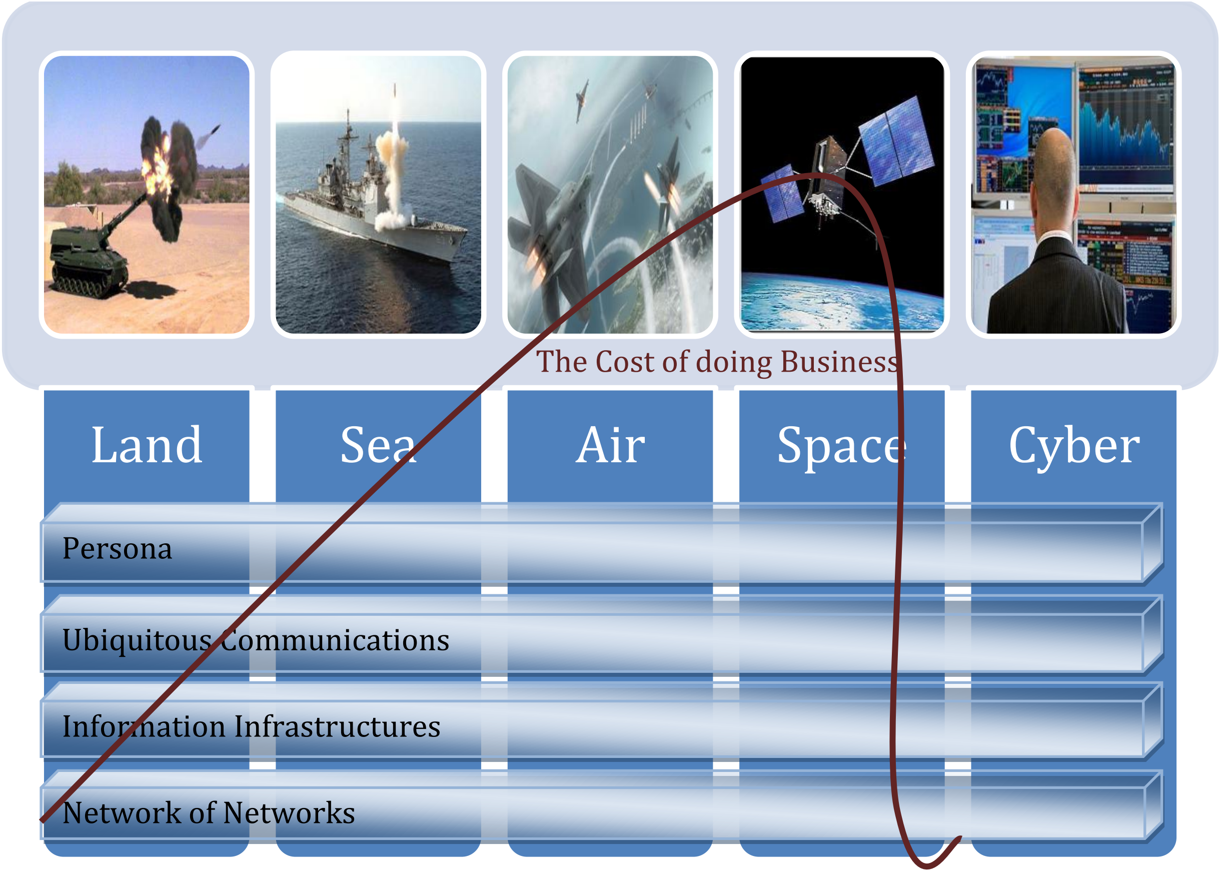

The Cost of doing Business
Land
Sea
Air
Space
Cyber
Persona
Ubiquitous Communications
Information Infrastructures
Network of Networks

Figure 3: The Military Information Lattice (Richardson C. J., 2011)

The MoD's domain security architecture insists through its accreditation process that highly sensitive secure systems remain physically isolated, the Air Gap. Unfortunately, today's enterprises, transformational government departments and the defence environment online communities' sensitive business information is often the same information that needs to be passed beyond the trusted perimeter. We need to extend the trust to cross domains, make our sessions safe and secure; essentially we need to assure our knowledge transfer environment to multiple parties within our communities of interest (COI). Understandingly, Security needs to be positioned strategically in the enterprises. This is a real world issue; the communication paradigm is becoming more dependent upon the safe and secure, processes of virtual machines, their trustworthiness and the availability of information infrastructures being critical to operational success. The development of the Effects Based Approach to Operations (EBAOs), Cyber Situational Awareness (CSA) and NEC domains (Networks, Information and People) is fraught with complexities and an increasing concern for dependable, safe and integral systems that can be defended against orchestrated cyber-attacks. Information Assurance (IA) is the key to trusting, maintaining and developing Defence Communication and Information Systems (CIS) capabilities. Furthermore, Information Assurance research has to also focus on a capability gap in education. Enterprises required us to develop good, educated IA practitioners and change the online user culture to a more assured, cyber-culturally aware environment. To Framework the IA profession will allow continuous specialized training to contextual and conceptualise the ever present risks and demand to assure systems and provide a career structure for practitioners in this important aspect of Engineering and Computer Science. Bridging the professional capability gap of qualifying and sustaining IA practitioners is a real requirement.

Until recently the defensive computer network defence (CND) posture has been the developing a security doctrine to monitor, detect, respond to unauthorized computer activity and attempts to mitigate risk through countermeasures and security devices (Wilson C. , 2006; Stallings, 2006a; CESG, 2006g; MacIntosh, Reid, & Tyler, 2011) using policies and procedures that protected the information by creating compliant, accredited security domains with limited access, restricted user privileges often firewalled behind encryption. These security silos afforded protection through policies & procedures, vetting & restriction of users and the use of IT devices and the security architect traded operability with security producing air gapped networks where often a user had 8 or more DTEs to access 8 different networks (Bethea, 2003). This security technique was exemplified by the McCumber Model in 2004. However, it isn't CND that troubles the minds of strategic planners, moreover the ability to strike back. It is the implacable effects of fear, uncertainty and doubt (FUD) over cyber security that has fuelled this new direction of military cyber offense and the impalpable complexity of cyber activities and the perceived inability to defend that reinforces the military strategic idiom, that the best defence is offense (Mazanec, 2009; Lin, 2009; Hopkins, 2011). Government bodies are clearly at variance, agitated and concerned about the development of cybercrime and unattributed hostile intent vectored through cyberspace. This globally agile, evolving, expansive and exploited cyber domain has little (nearly non-effective) international policing, fewer effective laws and a great deal of anonymity, chaos and inherent systemic risks (Davì, 2010). The threats of cybercrime, cyber terrorism, cyber war inflicting damage and destruction (Cyber Weapons of Mass Destruction) upon indefensible, open networks are attracting diplomatic, political and military responses to militarise cyberspace; to actively develop and build cyber weapons (e.g. Stuxnet, Duqu, botnets, etc), to expand offensive cyber operations to implicitly threaten states and/or to regulate and actively stop malicious cyber threats or face retaliatory consequences. Conceivably, states can build server farms of numerous racked processors running thousands of virtual machines to exploit a "*zero day vulnerability*" which turn infest and herd many millions of devices connected to the internet in order to conduct mass denial of services, generate Zombie launch sites for malware or assumption of control over SCADA and Command & Control (C^2) systems. The Cyber Pearl Harbor scenario, crippling critical information infrastructures, is seen by many (successive US Sec. of Def. John Hamre, 1997; Richard Clarke, 2010 and Leon Panetta 2011) as a very real threat to the State, world economic and social order. In this Cyberpower struggle for allocating scarce funding to offence and defence, IA has to compete against and recognise the very persuasive and militant body who want to build asymmetric cyber weapons to deter (or attack) potential attackers.

The counter argument to 20th Century Deterrence is knowing how to use Information Assurance in the 21st Century. The greater part of the 20th Century was dominated by the threats of war, World Wars and Nuclear Deterrence. Deterrence is *that you possess both the capability and the will to either retaliate or initiate a first pre-emptive strike to thwart an eminent attack* (Powell R. , 1990) and consequently some of today's military thinkers have developed a cyber-strategy to deploy and use offensive cyber weapons as a method of deterring potential cyber assaults and providing a means to retaliate in the 5th Dimension – Cyberspace. Revisiting, Professor Nye's remarks (Habig, 2011), he could have further informed his audience with "*offensive internet weapons have been introduced* as ***a deterrent*** *but the national governments have not quite a clue how to use them."* The use of virtual weapons as a deterrent in a virtual space can have unintentional consequences (Beard, 2009; Sterner E. , 2011) and emergent properties not readily envisaged by the software engineer or by these cyber warriors (Zimet, et al., 2009; Rid & McBurney, 2012). The consequences become more complex as they will affect the many layers of interoperability and wanting to become target selective produces intangibles within an evolving and chaotic network of networks (Schneier B. , 2008; Alperovitch, 2011; Crosston, 2011).

What is required is better Information Assurance, rather than MAD (mutual assured destruction or senseless, foolish, deranged) Cyber Offensive Weapons. The pressing global problem of cyber insecurity and system interoperability is how to develop resilience, trust and dependability to allow interacting information infrastructures and cyber activities to be safe and secure, to have system of systems whose information infrastructures are tolerant (fault and Intrusion tolerant) and risk managed, where the decision making cycle has assured information delivered to the right people.

1.2 The Research Approach

Cyberspace, and the technologies that enable it, allow people of every nationality, race, faith and point of view to communicate, cooperate, and prosper like never before... By its self, the Internet will not usher in a new era of international cooperation. That work is up to us, its beneficiaries. Together, we can work together to build a future for cyberspace that is open, interoperable, secure and reliable. This is the future we seek, and we invite all nations, and peoples, to join us in that effort. President Obama, 2011

Most people working in cyber security recognize that the interconnections and complexities of our economy can have a huge effect on the destructiveness of cyber-attacks. They refer casually to "network effects," "spill over effects" or "knock-on effects." Yet there is little understanding of how such effects actually work, what conditions are necessary to create them, or how to quantify their consequences.

US Cyber Consequences Unit, Dept. of Homeland Security

Purpose

Government classified networks have created in many cases information silos that protect their data sources but fail to inform the greater needs of the communities of interest. The current security given to the UK Government by CESG and its parent organisation GCHQ is that sensitive data (impact level 4 upwards) should be adequately protected using firewalls and other security devices and that networks that are secret and top secret should be isolated. These air gapped networks with their security domains impose very restrictive practices to the movement and communication of information and deny sharing and Information Exploitation. In the world where the timely use information is the asset that needs to be encouraged, the need to share across these domains often outweighs the necessity to keep our information secure. This research aims is to find a balance between protection and availability of information (its information security) and the need to Exploit Information that is also trusted and dependable. This new environment creates the need for trusted cross-domain solutions and the development of Information Assurance offers such a possibility.

As illustrated in figure 4, the research approach follows 6 main themes:

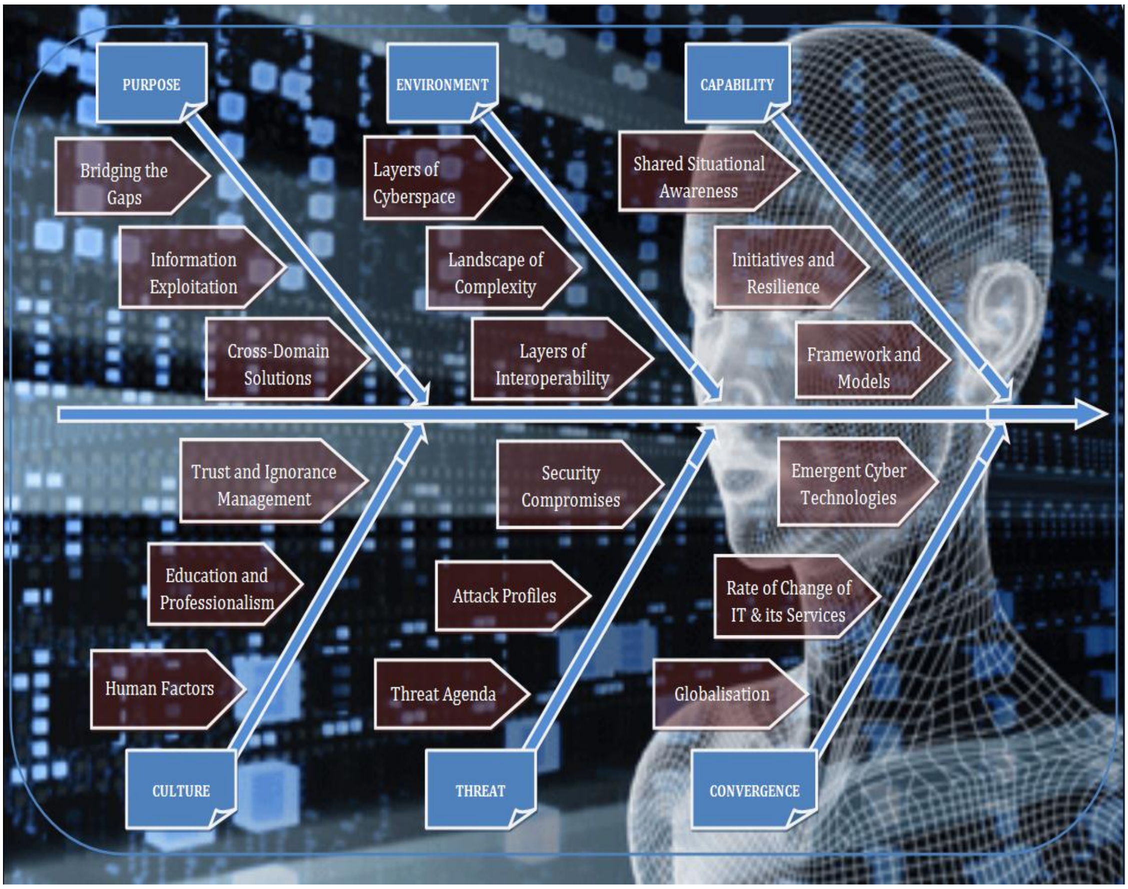


Figure 4: Discovering the Cause and Effects of Bridging the Gaps

In bridging the gap, this thesis addresses the following primary aims:

- To provide an Information Assurance Capability that will facilitate Cross – Domain Solutions. This capability will need a framework that formulates the assurance implications of interoperability within cyberspace, human factors, protection of networks and secure data content, alignment of enterprise architecture, any organisation culture changes, information exploitation, management and service dependability from bridging the air gap between highly classified networks and possible interaction with lower classified networks and the Internet and how it might be done. The investigation will also consider when those bridges might be considered an acceptable risk.

- Establish and develop an information assurance framework and appropriate models to meet operational interoperability requirements; whereby the study shall analysis various contextual and conceptual considerations of aligning and harmonising domain internetworking, thereby offering an assured cross-domain solution to military CIS interoperability

.

- Exploring six main topics within the layered environments and thereby framing the Cyber Landscape through modelling IA concepts. Analysing dependable, resilient convergence of technologies and networks and developing a Cyber-Assured Culture through Education; Promoting Transferable Skills &

Professionalism will provide a new capability for Information Assurance. IA will demonstrate how to provide solutions to system interoperability; operational benefits; operational security and new community learning outcomes.

- Illustrate the value of this research approach to the network-centric security problems of NEC (and the Global Information Environment) and highlighting the real human-centric assurance issues to the various layers, domains and environments of an interoperable Cross-Domain Solution and provide a discussion on how the qualitative experience of this research and individual perceptions can be analysed and developed.
- To identify, formulate and exhibit this approach and model implementation demonstrating it as a worthwhile Doctoral investigation. The thesis will be a successful project managed research programme with achievable, realistic outcomes within well-defined goals and agreed deliverable products.

Engineering Objectives

The four prime Engineering Objectives:

- EO1 - Develop IA Models that will demonstrate a holistic understanding of Information Assurance and Cross Domain Solutions required to bridge: Physical, Virtual and Human Air Gaps. The models shall review a wider context of IA to Interoperability as well as specific analysis to the military context of cyberspace; its strategic, operational and tactical cyber environment.

- EO2 - Determine a contextual framework and model(s) of Information Assurance to provide Enterprise Architecture and strategic cultural change awareness; to make a structured, safe, dependable, secure, protected, risked managed and trusted approach to assure interoperability of networks; the secure continuum of information; increasing trust of people, operations and systems and the reliability of the Cyber picture of the Joint Action environment.

- EO3 - Determine an Architect view of the existing contexts, concepts, logical, system, technologies and management that will formulate a more inclusive Information Assurance Framework to the Cross Domain problem. Conceptually framework and model any assured solutions that illustrates the need for Holistic System Situational Awareness, System Analysis, Engineering, and Simulation to develop core skills for IA Practitioners and a revised Information Assurance Architecture (IA^2).

- EO4 - Provide innovative and original research that will provide sufficient new grounding to Science within the confines of an Engineering Doctoral thesis investigating the problems of bridging air gaps. Demonstrating independent working and the critical awareness of relevant sources, illustrating where appropriate the literature searches, retrieval and synthesis and analysis of findings in relation to the desired aims.

The Culture

The 5-day Research Methods and Implementation course run by Southampton University for first year PhD and EngD students provided an invaluable insight of research mechanisms, methodologies and procedures required for academic rigour and organising the research process. The various readings and assignments over the 2-year taught element of the Engineering Doctorate emphasised the need for qualitative and quantitative research such as Bloom's Taxonomy (see figure 27) and the adaptations of methodologies to suit the particular line of discovery, objective achievements and measurement (Parmet, 2008). Clearly an appropriate research methodology had to be adopted to underpin this Thesis and its intention to provide a genuine contribution to the state of knowledge in Information Security and its Assurance, in particular an assured Bridging of the Air Gap.

An adaptive approach to the research methodology using the herringbone model (see figure 4) was used rather than choosing a specific methodology such as those proposed by Peter Checkland's Soft System Methodology (Checkland, 1981) or Peter Senge's *System Thinking* (Senge P. , 1990; Senge, Kleiner, Roberts, Ross, & Smith, 1994). This might at first make further epistemological complexities to this very complex issue; however the agile use of the herringbone allowed the tailoring of some formalized approaches allowing a greater insight and interpretation of the Hypothesis and helped span a number of key component issues that in themselves where worthy research topics (Connell, Lynch, & Waring, 2000). A Qualitative method evolved during the initial research and examination of current literature, Defence research (DoD, MoD, NATO and DSTL) and current operational difficulties both in Iraq theatre (Op Telic[3]) and Afghanistan theatre (Op Herrick[4]). An examination of the current *State of Art* of Information Assurance and the Interoperability Framework has identified that the current structure of Assurance is both restrictive and intolerant to the problems it needs to define, explore and resolve. The strategic communication and information

[3] **Operation TELIC** is the codename under which all British operations of the 2003 Invasion of Iraq and post invasion peace keeping and redevelopment.

[4] **Operation HERRICK** is the codename under which all British operations in the War in Afghanistan have been conducted since 2002. It consists of the British contribution to the NATO-led International Security Assistance Force (ISAF) and support to the US-led Operation Enduring Freedom (OEF).

flow issues occurring in present operations (2002-2012) within Afghanistan and in particular with the coalition secret network - the Afghanistan Mission Network (AMN) – postulate a new motivation to change the rules for network interoperability.

Finding a cross-domain solution is not just a quest to find an appropriate technological interface to meet the stringent demands of military communication security (Confidentiality, Integrity and Availability) but to change the concept of Information Assurance as a product of security into its own science worthy of the recognition that the UK, the European Commission and the USA has bestowed upon it. By developing a strategic position for IA, this thesis will create a strategic fit that can develop Information Assurance across the organisation as well as developing methods and techniques to deploy technologies that align and harmonise with the military thinking of the layer of interoperability (Khalilzad & White, 1999; Tolk & Muguira, 2003). The current definitions of Information Assurance have not presently evolved sufficiently or conclusively from its roots in Information Security; the time has come for it to do so!

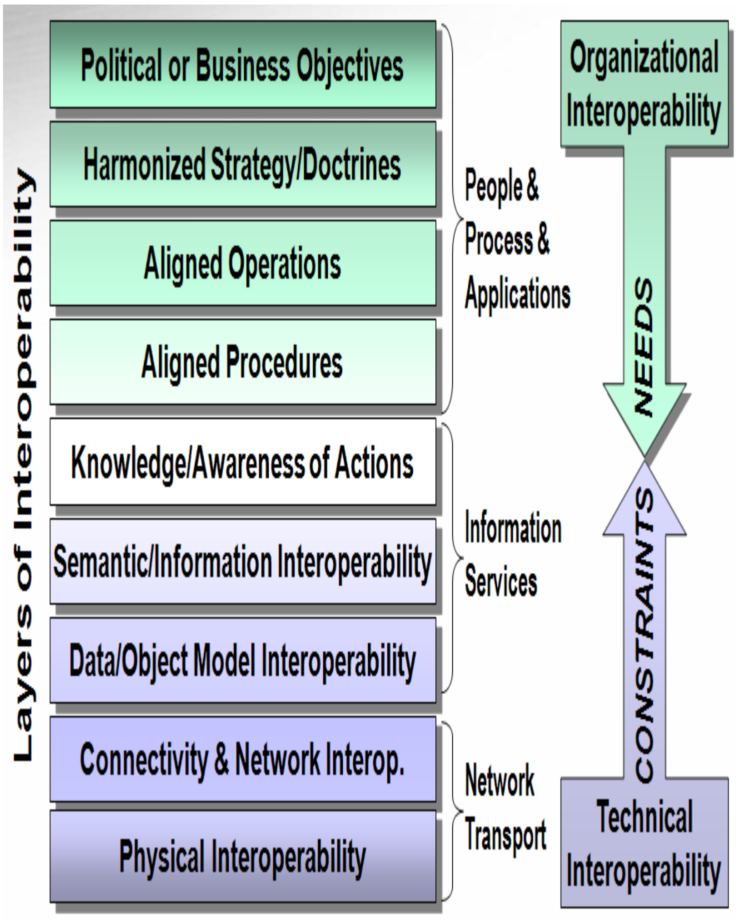

Layers of Interoperability
Political or Business Objectives
Harmonized Strategy/Doctrines
Aligned Operations
Aligned Procedures
Knowledge/Awareness of Actions
Semantic/Information Interoperability
Data/Object Model Interoperability
Connectivity & Network Interop.
Physical Interoperability
People & Process & Applications
Information Services
Network Transport
Organizational Interoperability
NEEDS
CONSTRAINTS
Technical Interoperability

Figure 5: Network Centric Operations Layers of Interoperability (Källqvist, 2008)

Military Commanders using Network Centric Warfare (NCW) and NATO's NEC with their interoperable networks of networks are increasing concerned with networking people, organizations, institutions, services, nations, etc., even though its functionality relies on information delivered via the technical networks (Tolk A. , 2003). NATO's own Reference Model for Interoperability is embedded in its Command & Control Technical Architecture (NC3TA) where it measures the effectiveness through four quality criteria: Data Quality, Information Quality; Knowledge Quality and Awareness Quality.

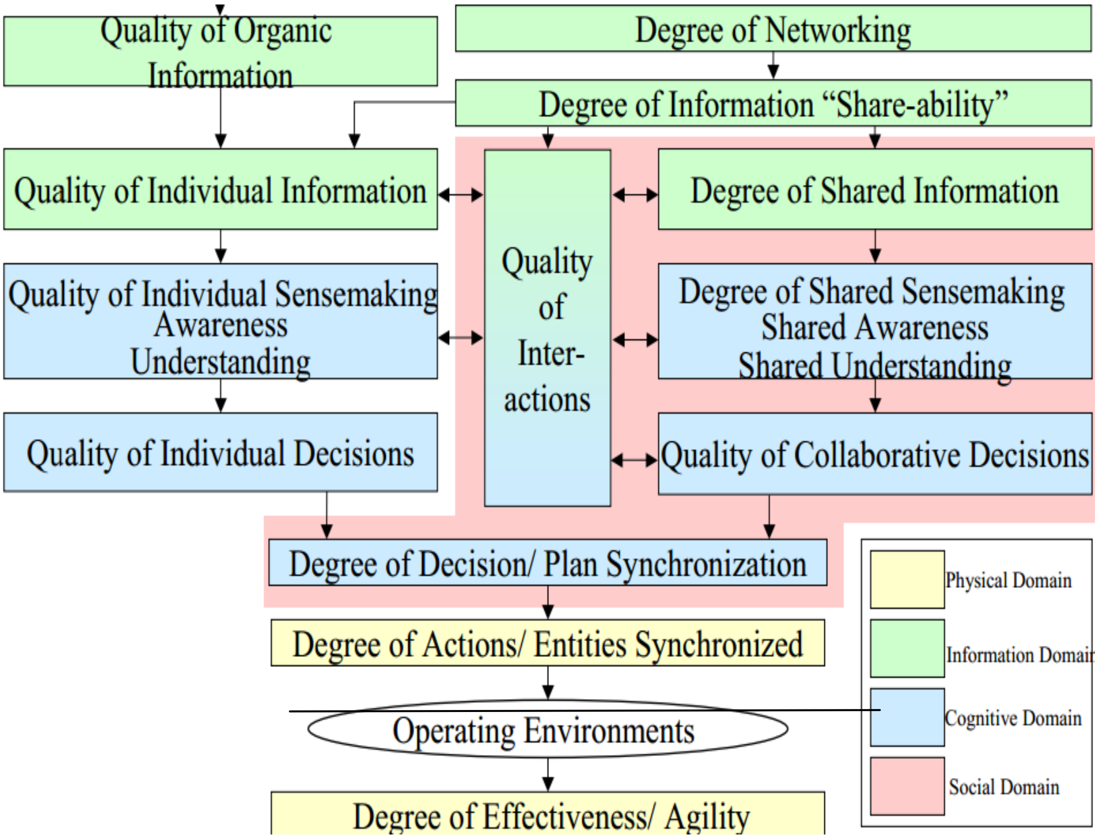

Quality of Organic Information
Degree of Networking
Degree of Information "Share-ability"
Quality of Individual Information
Quality of Inter-actions
Degree of Shared Information
Quality of Individual Sensemaking Awareness Understanding
Degree of Shared Sensemaking Shared Awareness Shared Understanding
Quality of Individual Decisions
Quality of Collaborative Decisions
Degree of Decision/ Plan Synchronization
Degree of Actions/ Entities Synchronized
Operating Environments
Degree of Effectiveness/ Agility
Physical Domain
Information Domain
Cognitive Domain
Social Domain

Figure 6: Network Centric Warfare Metric Framework (Tolk, 2003)

The Quality of these Information Services (Knowledge/Awareness of Actions; Semantic/Information Interoperability and Data/Object Model Interoperability) measures the performance of using the data, information and knowledge for the operation to improve the results, mission effectiveness and overall system/operation agility. It is the degrees of organic information and how it was shared that provides the quality of coalition awareness and decisions. Information Assurance has to deliver this quality across the layers of interoperability. Further investigation of the current literature (Classified and Unclassified) and the necessary qualitative research formulated the need to pragmatically model the situational awareness of the complex issues involved and to determine the quality of interactions as illustrated in Figure 6. To quantify the nature of the security issues formulate and contain the degree of Information "*Share-ability*", their semantic complexities and interrelationships requires a detailed and yet broad understanding of these issues, engineering constraints, common criteria evaluation and the development of Information as an asset in the Revolution of Military Affairs (RMA) and net-centric operations.

Creating a holistic assurance picture using pragmatic modelling and adapting qualitative and interpretive methods have enabled a systematic convergence of this study's research. The plethora of changes in Computer Science, Information Technology (IT), Communication and Information Systems (CIS) has transformed and will probably continue to transform military operations as well as of those of Government and Enterprises. The benefits of these changes can be exploited by our operational agility, the sharing and exploitation of information providing the communities of interest (COI) a Shared Situational Awareness (SSA). However, with urgent operational requests from military theatres and the needs of information to cross security domains of many networks has produced a plethora of potential vulnerabilities, risk and emergent properties that are often overlooked, unrecognised or negated for operational necessities.

The Transformational Government Agenda (Cabinet Office, 2005) outlines the need for a culture change to the development, dependability and deployment of UK Communication and Information Systems. This new agenda requires Government systems to become secure, robust and interoperable. As such, the new Enterprise System Architecture needs to articulate, describe and frame the coalition network of networks that supports an interoperable System of Systems infrastructure that is inclusive of information services, management, and its assurance as well as being tolerant to incidents. Within the MoD this has been recognised as the capability relationship between deployed traditional defence information (legacy) systems and procured modern information technologies that should transform defences Systems into an inclusive interoperable environment of Network Enabled Capability (MoD, 2006) of Information Technology (IT), Information Services (IS) Information Management (IM), Information Exploitation (IX) and their Information Assurance. Traditional Military CIS combat platforms and system acquisitions have very high costs, extremely long lead times (Committee of Public Accounts, 2011) but are developed ruggedised, hardened, secured, and tested to ensure the highest level of performance, confidentiality, integrity and availability; thereby meeting compliance and accreditation standards for Information Security (MoD, 2010).

Military systems are proprietary and communicate securely with little effect on performance but their development processes does require considerable configuration management and documentation processes that are maintained throughout the system life cycle. The system security compliance is captured in the Risk Management and Accreditation Document Set (RMADS). As military systems became more software intensive in computing devices, infrastructure and communications, procurement and integration have incurred increased costs to meet legal and regulatory demands designed to ensure openness and fiscal responsibility. Moreover, their system complexity, operational and environment requirements to meet mission-critical battlefield requirements of high reliability; ease of maintenance and built-in safety systems require much more than quality assurance (Perlo-Freeman, Cooper, Ismail, Sköns, & Solmirano, 2011). However, the lack appropriate Information Assurance methodologies in their design and ineffective maintenance of the RMADS especially when compared with more mature, hardware-intensive engineering (e.g. avionic systems, network rail, air traffic control systems) and development processes have caused considerable system life cost uplifts and urgent operational re-engineering resulting in a number reviews of MOD Asset Management (MOD, 2007; Dunn & Moore, 2011; Committee of Public Accounts, 2011)

The Cross Domain Solution generates risk, fear, uncertainty and doubts across many high-level data custodians who explicitly believe that authorities want the data protected as offered by accredited security domain, air gapped from other networks; not allowing for interoperability across different secured information infrastructure domains. There is little trust, assurance or appropriate risk appetite in the system engineering, traffic engineering, system compliance and accreditation. However, they recognise the demand for more Social computer engineering investigations, risk management, security operational capability and extending practitioners' knowledge to allow for improved interoperability of classified systems within the UK; with MoD's systems; inter-HMG departments; with coalition partners; with NATO; with Non-Government Organisations (NGO's); in particular with highly classified cyber domains such as Secret, Top Secret and above. NEC Interoperability itself has produced a layer effect upon network centric operations as illustrated earlier in Figure 4. These layers direct Information Assurance to align the organisational and technical interoperability across each layer and thereby establishing a coherent and inclusive framework that addresses the layer interfaces. In defining these interfaces, it is crucial to note that the information asset is not regarded as integral to the physical technical infrastructure nor tightly coupled to applications. The direction of this research is therefore to contextualise the concepts, doctrine, policies, technologies, procedures and education that may allow converging organisational and technical interoperability of classified military networks and Information Infrastructures in both multi-level (vertical) and multi-lateral (horizontal) operations providing cross domain solutions to different classified security (Physical and Logical) domains; thereby Bridging the Air Gaps.

Thesis Hypothesis

"Can Information Assurance provide sufficient Trust and Risk Reduction to allow information processed, stored and communication within highly sensitive (often critical) networks, with their own discrete security domains (including encryption mechanisms), which are often Air-gapped (physically and electronically isolated) to interact safely and securely, particularly across many interoperable networks and including the possibility of interfacing with the Internet."

The hypothesis is that a controlled, obeisance, human-centric information assurance framework stacked on a trusted, robust, data train can provide a secure, cross-domain knowledge transfer environment thereby removing the need for network and other air gaps. That such a assured framework can encapsulate the Human-Computer / Human-Cyber Interfaces as information flows (Processed, Stored and Transmitted) across the five layers of Cyberspace (EO1 and EO2). Such an Assured Environment has to provide a safe, secure, accurate operation and be sensitive to the situational awareness of decision makers and operational commanders as well as the security of this country's secrets. Moreover, it has to satisfy security and protection policies of the Information Assets across the complexities of Information and Knowledge exchange and inform the holistic nature of this assured cyber environment to its communities of interests by educated assurance practitioners (EO3 and EO4). The assured capabilities of the Net-Centric environment require more effort to context-dependent research and modelling IA inferences and impact. The interpretive perspective and quantitative methods of Enterprise Architecture (EA) can provide better understanding towards cyber-orientated 21st Century Defence Information Architecture, its Systems Engineering, Assurance and Human Factors. A special sub-set of EA could be Information Assurance Architecture (IA^2) which will need to provide an appropriate infrastructure for cyber-domains to support single service, purple, NATO and coalition operations and missions and any NGO corresponding actions within a contextual references (who, when, why, etc.). Furthermore is has to be based on the information exchange (flows) requirements of the mission. The architecture should be a layered approach to existing and future systems where classified data is structured, processed safely and securely in trusted domains to provide appropriate knowledge transfer and understanding to enable the NEC Benefits Chain and Cyber Situational Awareness. The Research Direction of this Assurance Community and its CDS has begun to move away from technological solutions to managerial and organizational issues through Qualitative Research methodologies (Kaplan & Maxwell, 1994; Kaplan, Truex, Wastell, Wood-Harper, & DeGross, 2004).

The Threat

"Over the last decade the threat to national security and prosperity from cyber-attacks has increased exponentially. Over the decades ahead this trend is likely to continue to increase in scale and sophistication, with enormous implications for the nature of modern conflict. We need to be prepared as a country to meet this growing challenge, building on the advanced capabilities we already have," **Strategic Defence and Security Review, 2010**

The Ministry of Defence through its Strategic Defence and Security Review, (MoD, 2010) its Comprehensive Approach Doctrine, JDN 4/05 (MoD, 2006); Information Strategy (MoD, 2009) and its Network Enabled Capability, JSP 777 (MoD, 2006) has identified that it needs to protect, integrate, manage and exploit its information structures to enable commanders to make proportionate and appropriate superior decision through shared situational awareness. At present policies, regulations and accreditation prohibit certain network operations and electronic data transfer from multiple secure domains, thereby reducing interoperability and limiting information away from *task-orientated communities of interest that exploit collaborative processes in a single Information Domain* (MoD, 2005).

The Government wants and needs to: *"Close the gap between the requirements of a modern digital economy and the rapidly growing risks associated with cyber space...* that MOD will become *significantly more focussed* (to its) *approach to cyber, by ensuring the resilience of our vital networks and by placing cyber at the heart of defence operations, doctrine and training. We* (HMG) *will also work to develop, test and validate the use of cyber capabilities as a potentially more effective and affordable way of achieving our national security objectives; address shortcomings in the critical cyber infrastructure upon which the UK as a whole depends, both to tackle immediate weaknesses in security and to ensure that we maintain access to a trusted industrial base,"* Strategic Defence and Security Review, 2010

At present, the Ministry of Defence does not have a coherent Cyber Security Architecture and no Information Assurance Architecture underpinning its systems of systems approach and tolerant operations. Possible NATO and DoD IA[2] are aligned to security mechanisms and accreditation rather than system operability, dependability and intrusion tolerance. The current MoD Communications and Information Infrastructures have been built up in an ad-hoc manner through the acquisition and deployment of individual systems, each establishing its own security domain through the accreditation and the *purple spotting* technical approval system to join tactical, operational, enterprise and strategic networks. The ISTARs platforms and future Defence Communication and Information Infrastructures must address the needs of technical and operational requirements for better decision making through shared situational awareness with an exploitive information domain that can maintain the assurance of the right information to the right people, at the right time. Many military systems are highly secretive in purpose, design, capabilities, operations and deployment. The economic, expansive, evolutionary and sometimes explosive convergence and accessibility to quantity and quality of data, information and knowledge transfer to the user and potential threat actors is creating a transparent, vulnerable world at an alarming rate to Governments and their Defence Departments. This globalised transparency[5] of open access; open source is counter intuitive to accredited structured, safe, secure and trusted systems.

This study wasn't going to be easy; a positive outcome of the research has a high operational impact on the future conduct of Operational Exploitation of Information and Knowledge crossing many classified security domains[6] (Campen, Dearth, & Goodden, 1996; Hughes, 2002; Pollock, 2002; Fenz & Ekelhart, 2009). How and where can the Air Gap be bridged is a current operational necessity for information exploitation across coalition networks. However, the hypothesis of Bridging the Air Gap is currently in direct conflict with a number of key Defence Communication Doctrine, Policies and Security Procedures. No Government Communication and Information System (CIS) can be operated without prior Accreditation (CESG, 2005; Cabinet Office, 2010b; MoD, 2010) The UK's Technical Authority for Information Assurance; the Government's Communications Headquarters (GCHQ) is amendment that the Air Gap is both necessary and enforceable by accreditation. This provides a stark, negative barrier to the hypothesis. The contrast of secure, accredited military systems is the often quoted insecure and unsafe commercial off-the-shelf (COTS) information systems.

[5] Transparency can seriously degrade several principles of war, most significantly mass, manoeuvre, and surprise; e.g. it can provide a threat actor near-real time, accurate battlespace visibility of a State's military posture at both the strategic and theatre levels.

[6] Defence uses network with a different security domain and security classification in isolated closed user groups and network topology. All Top Secret networks are built and securely maintained separately from other networks, e.g.: JOCs, SLI, NIPRNet, SIPRNet are all independent and isolated networks (Air Gapped).

Security is often easily financially offset by these COTS which have been developed, marketed, and upgraded within a 2-year life cycle (Al-Kuwaiti, Kyriakopoulos, & Hussein, 2009; Anderson & Rainie, 2010). These systems are often not ruggedised, nor robust enough for tactical military operations, with some COTS exhibiting too great a risk than those which would be acceptable for used by public safety or national security organizations. The economic security challenge today (Paquet & Saxe, 2005) is to produce agile, robust COTS systems that are responsive to the Enterprise whilst being secure, and seen to be secure, to satisfy regulations, policies, laws (in particular those concerning data protection and privacy) and accurate reporting (Akdeniz, Walker, & Wall, 2000; Allor, 2007; Colwill, 2010). The Enterprises' profit-and-loss statements are the bedrock of commercial decisions on information system life cycle designs (Hanseth, 2002; Howard & Lipner, 2005). Getting the "*Greatest Bang for the Buck*" with just-in-time component delivery, acceptance of degraded system performance, reduced operational response rates, and increased repair times are considered financially acceptable if the equipment will do the job. Software (and to a lesser extended firmware and some hardware) have been rushed through factory testing or untested beta version released are launched on unsuspecting customers and field testing is forced actual operational environments and consequently user enterprise bottom lines.

In the recent past, it was common practice for COTS systems been shipped under licence, without access to source code? These flawed software or implementation operational glitches were either corrected with software patches or left in the field until new software version was developed (Schneier B. , 2008). Furthermore, it is quite common to find that same code was *third party* developed, often with an overseas sub-contractor, with minimal documentation, flow charts or configuration management (Furnell & Thomson, 2009). Consequently, security is often seen as a bolt-on extra by Enterprises and high assurance software the exclusive reserve for military and some government projects willing to pay a premium. Table 1 illustrates some of the current security issues in the marketplace.

The introduction and adoption by industry of new technologies such as wireless, voice over Internet protocol (VOIP), and radio frequency identification devices (RFID) are rapid, with little design concern for security and privacy. Introduction of this technology in the commercial market is based on user acceptability, legal consequences, and bottom-line cost analysis, not on considerations of information safety, potential loss of life, or national security policy.

Security Issues	System Security non-compliance
Security hinders operation	Agile operations, working flexibility, collaboration and mobility provide opportunities but increased risks and exposure with little understanding of Assurance and Risk Management.
Communication channel are diverse, their security products are obsolete.	The main problems across new media channels and devices include data leakage, archive failures, spam, malware and policy non-compliance.
Inter-enterprise collaboration is not working because of security barriers	The need for greater collaboration is a top business, government and defence priority, interoperability is restricted by security domain architectures.
Poor Security Maintenance and Policies are not enforced	Many enterprises rely on unsupported tools to conduct business and there is increasing user inability to find expertise to solve issues.
Incomplete or immature protection services and security mechanisms	Organizations generally rely on stovepipe solutions that monitor one or two information channels whilst their communication strategies use multiple media channels.
External threats are perceived to be the greatest impact on business	Business impact and consequential continuity planning is more exposed to system vulnerabilities, insider user faults and social engineering. Most systems are intolerant to intruders and malicious users.
Data protection is a legal compliance issue.	A Enterprise security focus has been on protecting organizations against malicious and inappropriate content rather than data protection

Table 1: Security issues and non-compliance

In spite of these potential problems with commercial systems, their advantages—rapid deployment of state-of-the-art technology, consequent higher performance and far lower cost (higher volume cost reductions)—make them extremely attractive. Thus, over the past decade, Defence Acquisition Reform has been focused on developing processes to achieve both the high-performance and low-cost benefits that come from using commercial technology while still assuming the necessary mission objectives of high reliability, rugged environmental capability, and particularly security through compliance and accreditation.

The challenge for the transformed, assured military is to use information technologies to build a highly adaptive, high performance, and interoperable system infrastructure that is resilient, degrades slowly under attack, and reconstitutes itself in a secure mode while under attack. To accomplish this challenge, this transformed military needs a better understanding of the life cycle vulnerabilities of information technologies. At the same time, as strategies for defence in the post-modern era are developed, consideration must be given to changing warfare system requirements to meet changing enemy threat scenarios so we understand how new threats affect system designs and vulnerabilities. As communication channels multiply, organizations are still relying on the same old methodologies and stovepipe solutions to secure communications. The resulting in either stymied mobility and collaboration or insecure communication, neither of which is acceptable to the MoD. Enterprises wanting to increase collaboration but keep Information content under control have had to take a step back to address a wider communication challenge: these organizations need to continue confronting the imminent CDS problems and ensure that today's security technology choices don't complicate the assurance of tomorrow's communications. Making decisions based on the information to hand has been a matter of professional judgement. Are the sources known, is the information believed to be accurate and dependable, is it timely or dated, is it complete and do we trust it? The elements of Fear, Uncertainty and Doubt (FUD) will manifest unless we do something about it! Information Assurance (IA) is both a Science and an Art of removing the FUD contagion by managing the risks and providing a high degree of trust.

An important issue was to remove the desire to analyse the content and usage of classified material in the operational theatre, to accept that there is a clear and present need to bridge the air gaps. This restricted the research qualitative rather than quantitative analysis of sensitive aspects of information management and exploitation in the military environment. By not dwelling on topical, actual but highly sensitive problems, has limited the research to generalist issues and the overall problems for cross domain solutions, the directed research was to more contextual modelling (Strang & Linnhoff-Popien, 2004; Bettini, et al., 2010) than construction of a final engineered system or product. Researching Communication and Information Systems has moved away from technological to managerial and organizational issues through qualitative research methodologies (Kaplan & Maxwell, 1994; Kaplan, Truex, Wastell, Wood-Harper, & DeGross, 2004). The interpretive perspective and quantitative method provides context-dependent research into the holistic problems of Information Assurance and Bridging the Air Gap.

The Need to Know Principle

The protection and security of Data, Information and Knowledge across the Internet, its services and multiple domains, telecommunication networks, inter-connecting corporate and government intra-networks, institutional networks, social networks and military communication and information systems has been examined, reviewed, articulated, sponsored and exploited by many different scholars, strategists, military doctrines, business analysts and security practitioners. Long before 1911 the security principle of "*The Need to Know*" was a key component to keeping secrets, secret and those in "*The Know*" perceived to have gained more power, emotional *Contempt* (Ekman, 1999) over those that were not (Hollander & Offerman, 1990). The introduction of the UK's Official Secrets Act, 1911 was a legal mechanism that reinforced morals of trust and loyalty through secrecy (Williams D. G., 1969). The principle component of this legislation was the moral promise (*honour* and *trust*) from employees not to divulge information or intelligence without express permission from appropriate authorities (Frank & Eisen, 1982). The moral authority (Haidt & Joseph, 2007) underpins the principle of the "*Need to Know*" in military and intelligence operations. This principle is pivotal on the idea that military personnel are only told what is necessary, what they *need* to know and thereby what level of trust (Lewicki & Wiethof, 2006a) was bestowed upon them to carry out their task. If they are subsequently captured or for some reason (the *fear* to) betray the operation, they are unable to divulge any other operational orders or secrets; willingly or unwillingly. Essentially, Nations, Governments, Departments and Operations need to keep its secrets, secret and are emotionally in *fear* of having these secrets exposed (Liebeskind, 1997; Schneier B. , 2000; Colwill, 2010).

Security of Information was proscribed by many policies and articulated by McCumber's Cube (McCumber, 1991; Price S. M., 2008) and the net-centricity of Information Operations has focused early Assurance doctrines on Computer Network Defence (Rathmell, 2003), physical security devices and technologies, policies, procedures, access control and people vetting to provide protection to the data and information flows (Alberts, Garstka, & Stein, 1999; DoD JP 3-13, 2006; MoD, 2006). However, the Cross-Domain requirements of coalition decision-making and other communities of interest imposes directives for the assurance of Information System Interoperability as well as providing dependable and safe Knowledge Transfer Operations across these numerous systems to create a shared situational awareness (the *Need to Share*) and resilient and secure Information Exploitation. IA has become a strategic issue to the modern enterprise, with purpose and capabilities, defining assured environment and cultural awareness as illustrated in Figure 7.

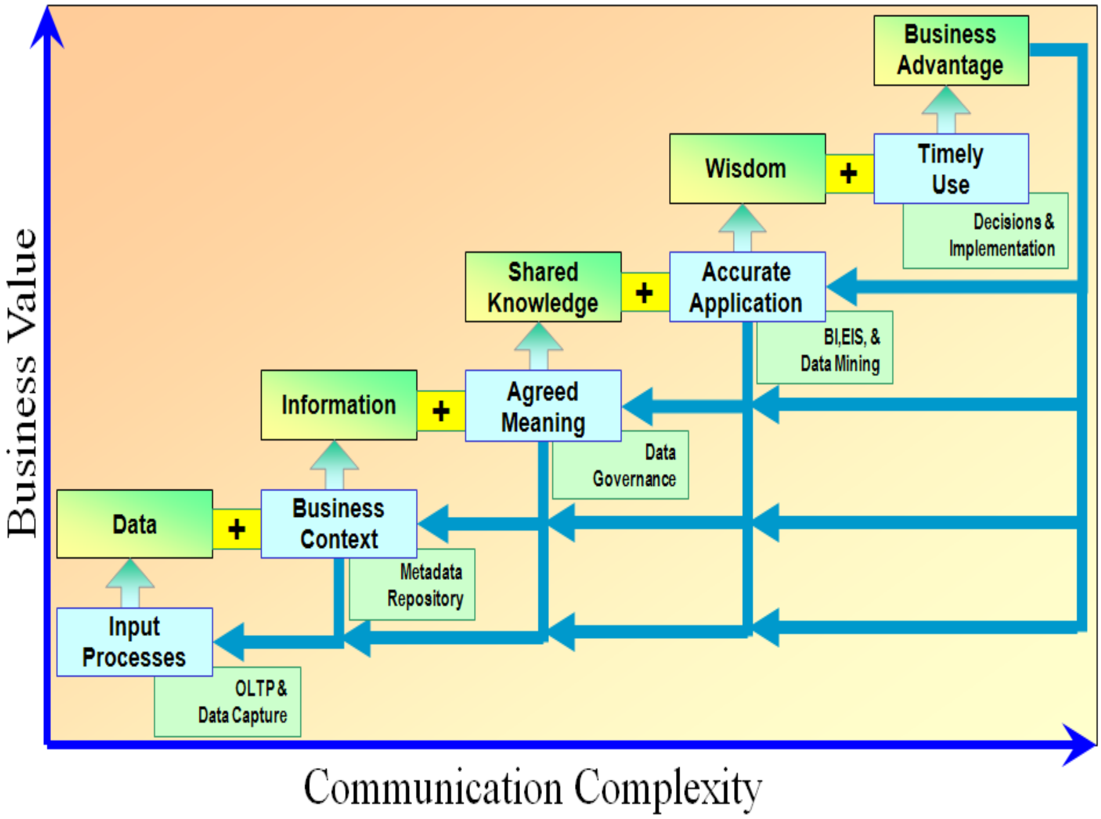


Figure 7: Strategic Asset of Assurance to the Enterprise (Borland, 2008)

This enterprise focus of Information Assurance had many declaring it a State of Mind (Boyce & Jennings, 2002; Stahl, 2005; Borland, 2008) to achieve business values through Enterprise Architecture and conceptual view of security towards net-centricity and increasing complexities of communication networking. IA Architecture (IA^2) has predominantly developed the security domains of Confidentiality, Integrity, Availability, Non-Reputation, Access Control and Authentication (Willett, 2008) and was promulgated without much research in linking IA (and its benefits) with human psychology, education and situational awareness. The Umbrella of Secrecy has help many military operations to succeed, however in a time of instant communications, surveillance, computational analysis and image processing, military activities are often observed and evaluated by opposing forces performing appropriate countermeasures, very quickly. Being aware of this rapid transforming environment, the shared situational awareness of what's going on, and who is performing what task and what agile responses are being played out, the modern field commanders in the Command, Control, Communications, Computing, Intelligence and Information (C^{4}II) Battlespace has become reliant on accurate and timely information, he needs to know!

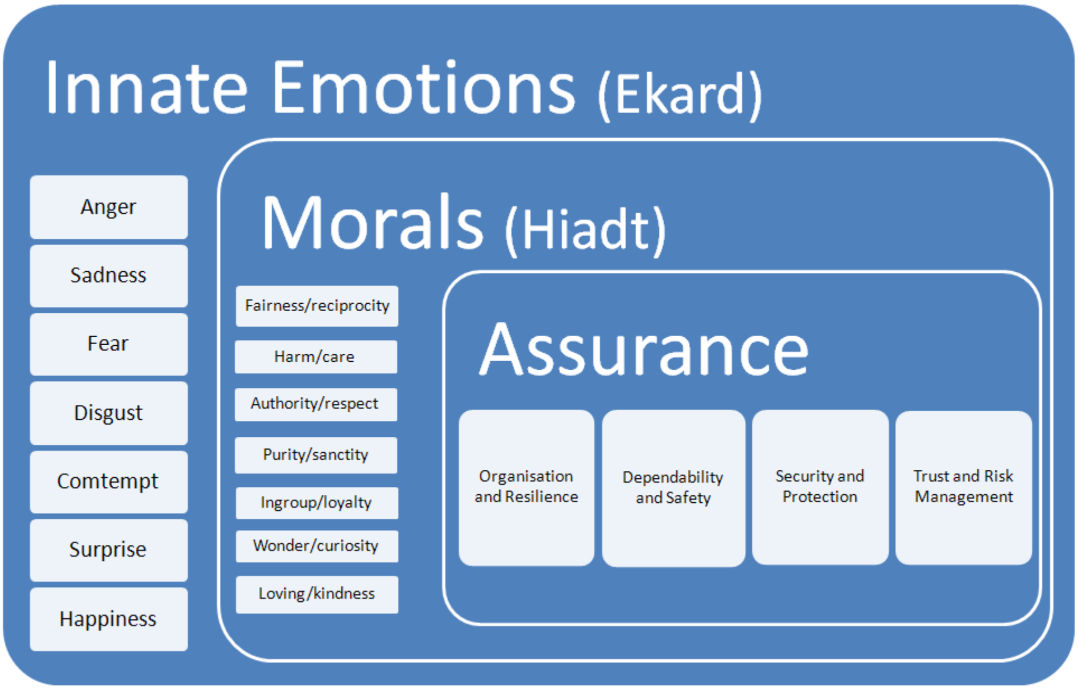


Figure 8: Human Centricity of Information Assurance

This raises the question of identifying and qualifying who needs to know. Furthermore who needs to know what? Conversely, how does a user in need of information "Know whom to ask"? These questions become a complex issue when you have millions of isolated data storages to single systems, and potentially millions of systems interconnected and having to become interoperable. The importance of being able to discover, *knowing who to ask for what* and rationalise the appropriate information could be resolved by semantic tagging or indexing the data structures (Allemang, 2010). However, are these techniques available across the whole interconnected domains? What motivates the interest of communities to move towards information sharing is the desire to improve the decision making process and achieving a shared situational awareness, ensuring all members of the community are aware of the enterprise content that has otherwise been trapped by official denial, power politics, isolation and Air Gaps!. This new direction, as outlined and argued within this thesis, will fundamentally change assurance architecture doctrine and processes away from network defence and security mechanisms towards human factors and its centricity, as illustrated in Figure 8, of education, learning and developing cognitive processes and products that harmonised alignment and interoperability drawn from adaptive unconscious (Wilson T. D., 2002a; Wray, 2011). The research models developed within this thesis integrate and align components of IA against the layering of cyberspace, the layers of interoperability and recent understanding of human psychology (expressed by Ekard and Hiadt) and life-long learning.

Environment

The early 21st Century Cyber World is a many-to-many, globally connected; intrinsically ICT dependent, information rich; culturally diverse, data-to-knowledge transforming environment (Arquilla & Ronfeldt, 2000; Borg, 2005; Lane, Heus, & Mulcahy, 2008; Omand, 2010; Obama, 2011). This virtual space of human thoughts interfacing social-technical networks, vast data processing, capture, store and forwarding cyber domains predicates individualistic empowerment that quantum shift paradigms to open new horizons of statehood; commerce; politics; entertainment and human relationships (Schmidt, 2008; Powell, 2009; Sommer & Brown, 2011).

Where we are beginning to understand the neural networks and complexities of our brain we have created a greater network, bridging human minds through virtual planes (Zohar & Marshall, 1990; Cole, 2005; Krämer, 2008). The geopostion of nations becomes less important as state boundaries are lost in cyberspace (Fisher, 2001; Exon, 2003; Kücklich, 2009), as we socially engineer new communication paths and relationships (Jones & Rafaeli, 2000; Ghosh, 2004; Anderson & Rainie, 2010). The pervasive nature of social-technical internetworking communities (Kolb, 2008) has generated these new horizons in cyberspace; complexities of connectivity; ubiquitous communications; the internet of things; the digital divide; cybercrime; Cyberwar; the realisation of virtualisation and clouds; illusions of reality and new (virtual) freedoms; innovations, digital creations, quantum computing, subterfuge, conflict, privacy, risk and trustworthiness. These composite, conflicting, cognitive domains have become our interconnected, bridged society (Jensen, Danziger, & Venkatesh, 2004; Proctor & Van Zandt, 2008; BIS, 2009).

The Research Engineering to Bridging the Air Gap is a discovery of where to assure the critical infrastructural social technology challenges of trust, trusted and trustworthiness of the real and virtual planes of our societies and the Communication and Information Systems (CIS) we use and in particular establishing a strategic assured military acceptance to cross domain interoperability, robustness and dependability. Cyberspace constitutes a pervasive, ubiquitous, survivable domain that is easily accessible, affordable, exploitative, evolutionary and expansive. It has been defined as: "The *worldwide open IP-enabled network infrastructure for communications, commerce and government*," (Nain, Donaghy, & Goodman, 2008). With the increased Internet usage at homes and businesses there were more asymmetric attacks being generated from malicious users, hackers, script kiddies and criminals (Saydjari, 2004). The US

Defense Advanced Research Projects Agency (DARPA) study (Weaver, Paxson, Staniford, & Cunningham, 2003) categorised in 2003 five worm characteristics (Propagation carriers and distribution mechanisms; target discovery; code activation; payload and attacker motivation) and speculated that future worms could facilitate human surveillance, commercial advantage, the management of distributed malware, terrorist reconnaissance and the cyber-kinetic manipulation of system parameters to SCADA and CII.

Modern electronic warfare is changing asymmetrically (Metz, 2000); changing radically (Richards, 2010); there are revolutions in concepts of running military affairs (Toffler & Toffler, 1980); an evolution of conducting network centric operations (Arquilla & Ronfeldt, In Athena's Camp: Preparing for Conflict in the Information Age, 1997; Alberts, Garstka, & Stein, 1999) doctrines to the conquest of cyberspace (Libicki M. C., 2007) from Cyberspace to Cyberpower (Kuehl, 2009; Starr, 2009) to the formation of USCYBERCOM and lately, formal recognition that there are now five domains of Military, Political and Economic Affairs (Land, Sea, Air, Space and Cyberspace). The Ministry of Defence’s Network Enabled Capability (MoD, 2006; MoD, 2009) and its development from the US Netcentric[7] models has developed intrinsic and often complex transnational interdependencies, involving knowledge transfer, human factors and information interactions across virtual and real planes.

People who have a communication agenda had, before the Internet, communicated their message via a few media channels: an occasional letter to “The Times Editorial”; a placard in a televised march; a stump speech in Hyde Park or a radio broadcast. Even those channels are still prevalent in the UK’s democratic society; there is a considerable movement to blogs, wikis, online forums, IRC’s and social networks (MySpace, Facebook and Twitter) which introduce their topics to a larger, more globalised audience. Now their voice, their thoughts, bias and ideas can have a global impact upon willing and very receptive readers. This pervasive power of communication is widely recognised (Orbe, 1998; Estrin, Culler, Pister, & Sukhatme, 2002; Castells, 2009) and the relative ease of borderless access and anonymity constructs a security dilemma

[77] Netcentric refers to the participation to a continuously evolving, complex community of people, devices. Information and services interconnected by a communications network to optimize resource management and provide superior information on events and conditions needed to empower decision makers. Available at: https://www.ncoic.org/home (accessed 12 August 2010).

(Borg, 2005)that one person could potentially affect an entire nation's security via a cyberspace attack is seen as a *Clear and Present Danger* (Liang & Xiangsui, 2002; Jain, 2005; Harris, 2008; Marks, 2009). The two Chinese Colonels (Liang & Xiangsui, 2002) advocated the idea that a less-capable foe can employ asymmetry warfare principles to take on a military superior opponent. This aligns with Sun Tzu's view that Stealth, Deception and Indirect attacks should be used to overcome a stronger opponent in battle. The US Department of Defense (DoD) Directive[8] leverage their net-centric capabilities with a technical cyberspace framework called the Global Information Grid (GIG) incorporating an IP-based infrastructure linking sensor, surveillance and reconnaissance (SSR) systems; Command and Control (C^2) systems and weapon platforms (fire systems) and associated services necessary to achieve Information Superiority. The DoD vision has six programmes[9] to facilitates the Grid with an agile, robust, interoperable and collaborative command structure where users from Enterprise, the intelligence sector and the armed forces all share knowledge on a secure, dependable and global network that enables superior decision-making, effective operations and network-centric transformation. Consequently, the US doctrine and principles of Network-Centric Warfare (NCW) has modified the doctrines of many military institutions, NATO has adopted NNEC[10] and Australia calls it the Ubiquitous Command and Control (UC^2).

NCW offers a military movement towards cohesive operations; where knowledge transactions, Command & Control (C2) and coalition interoperability provides strategic, operational and tactical Shared Situation Awareness (SSA) and to the planning, execution and assessment of the comprehensive Effects Based Approach to Operations (EBAO) and ultimately to the UK's National Security. The tempo and increased rate of change of operations within societies is a significant characteristic of the Global environment we live and operate in, requiring coalitions, federated collaborative partnerships and multinational user groups to exploit, contain and manage diverse,

[8] Global Information Grid (GIG) Overarching Policy. DoD Directive NUMBER 8100; 19th September 2002.

[9] Four programmes (Joint Tactical Radio Systems (JTRS); Transformational Satellite Communication System (TSAT) deal with communication networks , transportation and delivery of Data, Information and Knowledge, one with enterprise services and final one with Information Assurance.

[10] NATO Network Enabled Capability; http://www.nato.int/cps/en/natolive/topics_54644.htm

geographically dispersed elements of open, loose, closed or classified Government, Military, Commercial, Criminal Investigation and Community operations. The globalisation of political, economic, social-cultural, technological, environment and legal (PESTEL) factors have contributed, manipulated and framed our physical world, but institutions are finding it increasingly difficult to encompass and capture the dynamic, evolutionary, chaotic, turbulent domain of cyberspace (Cerf, 2007). Vested institutional bodies such as the UN; EU; ITU; ETSI; ANSI; police and law enforcement agencies; intergovernmental policymaking bodies; homeland security and other NGOs have been focused on outreach, general education and situational awareness although there are some "*also pursuing global collaboration, harmonization of statutory and regulatory provisions, and the development of incident readiness and response programs*" (Nain, Donaghy, & Goodman, 2008).

Nunes (1995) stated: *"Cyberspace no longer strictly refers to the fictional "matrix" in William Gibson's novel Neuromancer; it has now entered into common speech on and off the Internet as shorthand for this conception of computer networks as a cybernetic space. From a Baudrillardian perspective, this figuration of Internet as a kind of cybernetic terrain works to undermine the symbolic distance between the metaphoric and the real. It abandons "the real" for the hyperreal by presenting an increasingly real simulation of a comprehensive and comprehendible world."* Taking Nunes (1995) to heart; to understand risk and nature of Cyberspace we need to comprehend its transparency. More effort is needed to deconstruct, in conjunction, both the Real and Virtual planes of Cyberspace and its interface to society and individuals (Lessig, 2004). The biomedical reflection of natural science to cyberspace of bugs, virals, worms, Trojans, biometrics, agents, neural networking etc. provide physical views to the materiality of the real world to the virtualisation of cyberspace. The science relates the outlook nature of the Newtonian world as a veneer of day-to-day existence. Science exposes it as a kind of mirage as it establishes and describes the various microscopic and macroscopic realms driven by quantized complex forces. "*It may very well be said that information is the irreducible kernel from which everything else flows, hence the question why nature appears quantized is simply a consequence of the fact that information itself is quantized by necessity*." Zeilinger, 2002. Life sciences paint complexity as an outward simplistic vision of humanity, plants and animals as an evolving, self-generating, self-organising complex system of neural linking, DNA, cellular development and chemical interactions, which are helpfully, hidden from our everyday view. The virtual planes of the Internet, The Global Information Grid and Cyberspace are synonymous to this and its life blood is the mixture of data, information and knowledge. *"Historically, much of fundamental* *physics has been concerned with discovering the fundamental particles of nature and the equations which describe their motions and interactions. It now appears that a different programme may be equally important: to discover the ways that nature allows, and prevents, information to be expressed and manipulated, rather than particles to move."* Steane, 1998.

In effect, these natural science philosophies assert that matter, life, society, cultural creations and the mind are illusions and that we have built cyberspace as a structured mirrored reflection, a virtual illusion with its own complexities. Both the real (physical) and virtual (digital) reality are composed of the same quantized binary bits of information. As Jeremy Levine (Levine, 2010) stated: *"Reality, regardless of its content, is nothing more than the information it communicates*." It is then not so much what visual image that we see, the true reality is "*below the surface and behind the communication*", which consists of underlying physical components, such as atoms, genes, narrative elements and drives, as well as underlying "mechanisms" or rules, which generate the surface structure of reality that are akin to the protocols, standards and domains that have been created to implement the Black and White[11] (Ones and Zeroes) of cyberspace.

Sanes (2008) said "*When we see only the surface, it is said that we are victims of a kind of simulation confusion, taken in by false appearances*." He clarifies this falsehood as that of (1) nature, which trick us because of our limited senses and knowledge; (2) self-deceptions, the unconscious cover-ups that are described as forms of repression or defence and (3) cover-ups, deliberately manipulated appearances and outright lies, such as those attributed to hidden agenda, criminal activities, politics, con artists, and by creation of deceptive simulations, entertainment and magic. The Information Age (Toffler & Toffler, 1980) is reliant on interconnected, robust, interoperable systems of systems, their information infrastructures and connecting communication networks requires more automation, controlling software applications and cyberspace connectivity to manage the increasingly complex interdependencies of the information services and the networks that host them. The very nature of this complexity introduces vulnerabilities and simulation confusions which inflate with our increasing reliance and dependency. The GTISC Professor of Practice, Howard Schmidt (2008) stated: "*Our critical infrastructure systems are fundamentally dependent on the Internet and IP-based technology, and there are*

[11] The Tao Security is an image of Black "Hatted" Hacker and Cracker manipulators and White Knight (security practitioners) countermeasures.

interdependencies between them that our enemies will seek to exploit. Cyber warfare completely evens the playing field as developing nations and large nations with a formidable military presence can both launch equally damaging attacks over the Web."

The need to maintain domain security is also essential to keep conflicts and intrusions to a minimum and access to information on a "*Need to Know*" basis. However, this silo culture but has become obsolete to the desires of exploitation and interoperability that frames the 21st century Information Age and its "*Need to Share*" Culture. In part this thesis conceptualises, contextualises and examines the necessary and highly influential and important gap, and the bridge, between these two cultures. This challenging, and alarming phenomenon of multifaceted risks, insecurities and ignorance needs to be understood, managed and assured. What is acceptable to certain communities may be seen as criminal in others, globalisation has created uncertainty (Cerf, 2007; Heller, 2009) where we are beginning to doubt the effectiveness of security and protection of sensitive, private information assets and where we fear the consequences of being terrorised, criminally exploited or socially subverted:-

In Cyberspace there is a contagion of Fear, Uncertainty and Doubt (FUD).

Richardson, C. J. 2011

However, Cyberspace offers a plethora of opportunities to the individuals, communities, organisations and governments. The ITU (2007) stated that: "*there has been a steady expansion in digital opportunity, both in terms of more widespread access to basic Information and Communication Technologies (ICTs) and the growth in high-speed access to ICTs, on both fixed line and mobile networks. Ever greater numbers of people around the world are enjoying access to the benefits ICTs can bring. Already, the number of people using ICTs around the world has doubled since the WSIS was first proposed in 1998. By the start of 2008, there will be around three billion mobile phones and more than one billion fixed lines around the world*." The Internet World Stats (2010) indicates that "*The Internet has reached 29% of the World's population, some 1,966,514,816 users*." With this increasing online community come associated risks: some risks are obvious, some intrinsic to the complexities of the environment, some are natural and some are manufactured to suit a particular intent. Intentional activity to harm, threaten and exploit vulnerabilities has spurn generations of increasing more sophisticated cyber-warriors, whether legitimated (government sanctioned military, intelligence, business, educational, social-cultural), terrorists, hackers, spies or criminals (EU, 2005). Each has an agenda that might cultivate, educate, deny, subvert, harm or exploit the array of services and assets presented by a cyber-portal (Bynum, 2004; Bishop, Engle, Peiser, Whalen, & Gates, 2008).

"Cybercrime cost the UK economy £27bn a year," **HM Government, 2010**

There are many different types of attack vectors and the security threat to the legitimate users has diverse intent and motivation. Cybercriminals (Schjolberg, 2005; ITU, 2007 and EU, 2008) are committed attackers upon our information assets, having a desire, want and wish to inflict damage, loss, modification, subversion, control, power or other psychological or material reward. They seek to gain advantage, financial benefit, secrets, political hacktivism[12], intellectual property and digital rights by conducting fraud, identity theft, social engineering and launching increasing devious and effective malware. Their malware if often self-propagating, reusable, self-defending, sometimes coordinated, able to use decentralised Command and Control (C2) and is becoming worryingly more intelligent (Ilachinski, 1997; Alberts & Papp, 2001; DCDC, 2010). These viral and malicious software applications, worms and Trojans have morphed rootkits, distributed denial of service attacks, Botnets, Supervisory Control and Data Acquisition (SCADA) specific attack ware (e.g. Stuxnet) and lately the "*Storm*" malware. However, the biggest insidious security risk to any institution is the threat from the "*insider*". The concepts and value of trust (Madsen, 1999; Sandhu, 2000; Day, 2004; Weckert, 2005; Goucher, 2009) is essential to society and in cyberspace it's the keystone to all activities (OECD, 1986; OECD 2002; Jøsang, Keser and Dimitrakos, 2005). An environment that is assured by structure, safety, security, trusted systems and vetted individuals is deemed *trustworthy* (Alexander, Kimmel, & Burke, 2007).

Individuals, employees or contractors with valid user profiles, clearances, logins and passwords operate with frequent, interactivity with the enterprise's Communication and Information Systems (CIS) and consequently can initiate the greatest harm and explicit risk to the security (Confidentiality, Integrity and Availability) and asset of those systems. As figure 34 illustrates, the implicit risk to any organisation is from outside Computer Network Attacks (CNA) but there's greater potential betrayal of a

[12] Hacktivism is the fusion of hacking and activism; politics and technology. More specifically, hacktivism is described as hacking for a political cause. http://www.thehacktivist.com/whatishacktivism.pdf

loyal / trusted insider (denoted by Computer Network Exploitation – CNE); but it is also the ignorance (denoted by Disclosure, Abuse and Denial, - DAD) and non-compliance of the user community (Lapke & Dhillon, 2005; Colwill, 2010). Failures to meet security policies, poor awareness, lack of motivation to protect the assets, laziness, lack of understanding of risk, privacy and sensitivity all contribute and if often overlooked in many security risk assessments (Furnell & Thomson, 2009).

We need mechanisms, doctrines and policies to support the trustworthiness of our Information Assets; Providing tested and compliant solutions, vetting, management and education that help, support and police the user communities, identifying the evolving threats, analyse and assess, defend, patch, recover, repair and control our operational cyber domains. Fundamentally, we all need to understand Assurance and take responsibility of our actions within cyberspace. It's a big ask. To understand cyberspace and the evolving risks needs a national programme of Education, Training and Awareness, a cultural shift from reliance on others to self-reliance and accountability. Users need to take ownership (risk manage) and citizens need to understand that this is a national threat (MoD, 2010).

It is our social nature that we need to gain trust and in doing so we make ourselves more vulnerable (Nikander, 2001). To trust (Minsky, 2003) people, systems or processes takes time, however to lose trusts can take just a moment, and any attempt to regain that lost trust is fraught and inconclusive (Rogers, 1995). Trustworthiness requires us to assure systems, against CNA, CNE and DAD threats, with their user community. Information Assurance (IA) brings trustworthiness to the Enterprise; it allows human trust (Schneider, 1998) to exist in cyberspace and its components and provides a defence-in-depth (May, *et al*, 2006) to Information Operations (CNA, CNE) and Information Insecurity (DAD). It is the key to bridging the communication data train (Protocols, Transmission and Routing), through the information stack (IO/IX; IA, IM; IS & IT) to trusting, maintaining and developing the UK's Defence Information and Knowledge Infrastructures; DEC CCII[13]; Enterprise and joint venture Knowledge Management Transfer (KTM), C^4ISTARS[14] projects; Information Operations (JDP 3-80,

[13] MoD's DEC(CCII) is tasked to deliver optimised, integrated, timely Command and Battle Management (CBM) and Global Information Infrastructure (GII) equipment capabilities that meet UK stakeholder requirements within a coherent, balanced and cost effective investment programme.

[14] Current UK Command, Control, Communications, Computers, Information/Intelligence, Surveillance, Targeting Acquisition and Reconnaissance (C^4ISTAR) programmes are Collaborative System for Air Battlespace Management

2007); Electronic Warfare (EW); Computer Network Operations (CNO); The Global Information Grid (GIG) and Communication Networks capabilities (Rawlinson, 2005 and MODIS, 2009). These various systems are often required to perform seamlessly across multi-functional, federated, lateral, layered and partitioned Information and Communication domains. As we interact with systems and they in turn interact with others networks, the systems of systems become complex with their many interacting components, hierarchical layers and multi-lateral domains. Professor Jensen describes these systems as Complex "*because it is impossible to reduce the overall behaviour of the system to a set of properties characterising the individual components. Interaction is able to produce properties at the collective level that simply are not present when the components are considered individually*," **Moffat, 2003**

Essentially, modern military interoperability and system capability (Alberts and Hayes, 2006) requires bridging the domain air gaps of numerous classified systems within and external to the defence environment. To comprehend, structure, make safe, secure and ensure trustworthiness of these systems of systems, networks of enterprise architecture, information infrastructures with their real-time system orientated processes, applications (SOA) and software serviced engineering (SaaS); their integrity and dependability requires educated IA practitioners and security architects that can work in both the Horizontal[15] and Vertical[16] Domains (Hughes, 2001; Hayat, 2006 and Anderson, 2009).

(CSABM) and NATO's Air Command and Control System (NATO ACCS), the Joint Force Air Component HQ (JFACHQ), the UK's Tactical Air Control Centre (TACC), the Transportable JAPNMS Facility (TJF) and C4ISTAR capabilities being developed for the UK Army's Ground Based Air Defence (GBAD), WATCHKEEPER and Future Rapid Effects System (FRES).

[15] Horizontal Working Security Domain is defined as working between information domains at the same Protective Marking (JSP 440, V3.8, 2010) but with different need to know criteria, e.g. UK SECRET and NATO SECRET.

[16] Vertical Working Security Domain is defined as working between information domains at different Protective Marking (JSP 440, V3.8, 2010), e.g. UK TOP SECRET and UK SECRET.

Capability

The Joint Force will operate in an environment that is increasingly complicated, uncertain, and dynamic. Employment of asymmetric strategies by potential adversaries and the proliferation of advanced weapons and information technologies will create additional stresses on all elements of the force. Future operations will not only require increasing joint integration, but must also better integrate other federal agencies, state organizations, and coalition partners. The current state of human and technical connectivity and interoperability of the Joint Force, and the ability of the Joint Force to exploit that connectivity and interoperability, are inadequate to achieve the levels of operational effectiveness and efficiency necessary for success in the emerging operational environment. **Net-Centric Environment Joint Functional Concept (2005).**

The Joint Functional Concept describes the Net-centric capabilities and attributes of the US Military and Intelligence Communities through a model consisting of three areas:

a) **The Technical Area** (physical aspects such as infrastructure, network connectivity, and environment).

b) **The Information Area** (the environment where information is created, manipulated, and shared); and

c) **The Knowledge Area** (cognitive and social interaction capabilities and attributes required to effectively function in the Net-Centric Environment);

The Net-Centric Environment Joint Functional Concept (NCE JFC) model was developed to examine several important elements of the functional concept and their inter-relations. Appropriate and accurate Information Sharing is created by the NCE JFC through its Knowledge and Technical networking and coupled to the collection force sensors (ISTARS) provides unit and shared situational awareness. General Keith Alexander, the head of DoD's Cyber Command said "*Defense needs a common sharable, operating picture across its networks and to enable real-time response…situational awareness across DOD's networks is now often based on forensics generated after an incident has occurred.*" The NEC benefit chain (MoD, 2006; MoD, 2009) clearly defines that better situational awareness (SA), as illustrated in Figure 9, will allow units to interact, collaborate more effectively and bolster their ability to see and understand in real time what's happening across its networks. Moreover, as: "*they know more about what they need to know, where that information is likely to be found, and with what other* *force elements their capabilities need to combine, and they are interacting and collaborating in a policy, cultural, and technical environment suitable for that interaction,"* (DoD, 2005).

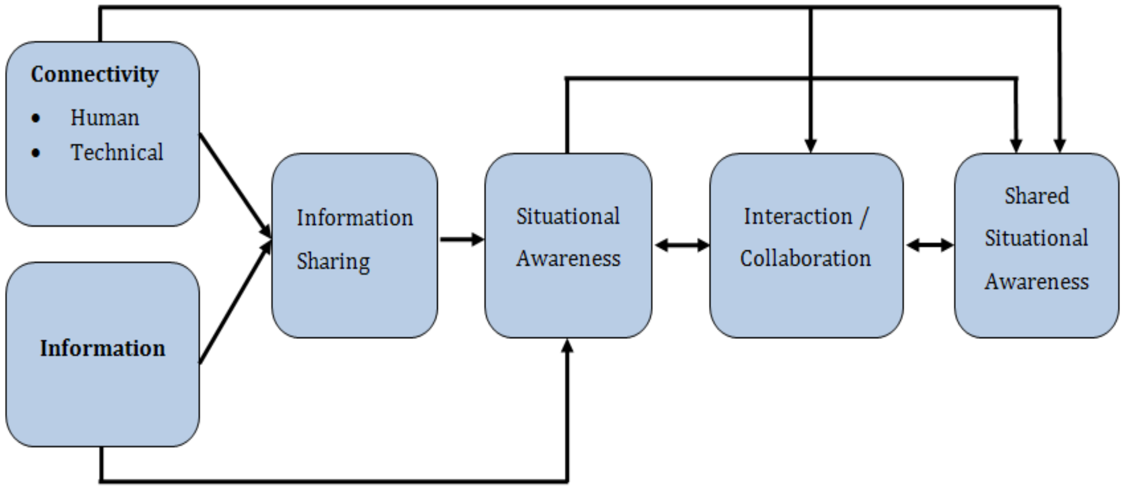


Figure 9: Network and Information Enabled Situational Awareness

The repeatability of this cyclic process further refines the SA, making a more coherent view and deeper cognitive understanding. This will further examine in Chapter 6; The IA Model and in particular modelling the entity relationships between the five Cyber Layers, three Information States and the eight Assurance Components and their attributes. The Net-Centric Environment Joint Functional Concept ultimate end state would be: *"Where there are ubiquitous sensor networks, perfect fusion tools, no restrictions on bandwidth availability and high-resolution, real-time, 3-dimensional visualization, where any collectable information in any force would be available to any force element, and virtual collaboration environments would be indistinguishable in terms of quality from physical "same room" collaborations."* **(Alberts D. S., 2002)**.

> *"In some respects, sharing information is a leap of faith that the recipient will treat the information properly, not abusing the implied trust."*
> **(Crocker, 2007)**

The 4th Annual Unified Cross Domain Management Office (UCDMO) Conference, Boston (2010), theme was "From the Core to the Edge - Information on Demand." Where Net-centricity of military Cyber network capability and information infrastructures, the "Core to the Edge" spanned the Strategic, Operational and Tactical purposes of the NEC: The Global Information Infrastructures (GII), Critical Information Infrastructures (CII), corporate Defence Information Infrastructures (DII) and the Battlespace Information

Infrastructures (BII). The Military cyberspace domain is a networked construct of robust headquarters' environments to the less advantaged, distant reaches of our missions and tactical linkage. Cross Domain capabilities are vital components in today's and tomorrow's information sharing environments (Bailey, 2010). The NEC is an environment of linked sensors, a lattice-work of communications and logistic networks, command and control (C2), intelligence gathering and Fires[17] networks gains dominance.

Within the NEC: "*Warfighters can achieve efficiencies in the full spectrum of operations by sharing information in a common operating environment.* This requires *unity of effort across organizational, national, technical and spatial boundaries as necessary,***"** (Crocker, 2007)**.** Whereas, within the Cross-Domain Solution they are: "*To foster seamless information sharing throughout a diverse user community; across the widest variety of domains.*" (Jamka, 2009)**.**

The UCDMO was initiated by the US DoD CIO and the DNI CIO to develop a roadmap for the community and facilitate the development of a Cross Domain vision that includes all the stakeholders and their stated mission. The Cross-Domain (CD) Community goals are:

- Ensure secure, robust and flexible CD capabilities are available and extensible to share information among a wide range of mission partners;
- Ensure that CD technological developments are timely, responsive and aligned with transformational initiatives;
- Ensure CD investments fill capability gaps, minimize redundant activities, increase efficiency and support the timely migration to the CD Baseline.

[17] In the US Joint Publication 3-09, *Doctrine for Joint Fire Support*, joint fires are "*fires produced during the employment of forces from two or more components in coordinated action toward a common objective*." The military distinguishes between operational and tactical fires: (a) Operational fires are lethal and non-lethal weapon effects that influence enemy operational forces, critical functions, and key facilities to accomplish operational objectives in support of either an operation or a campaign and (b) Tactical fires are lethal or non-lethal weapons effects that achieve tactical objectives in direct support of a major operation.

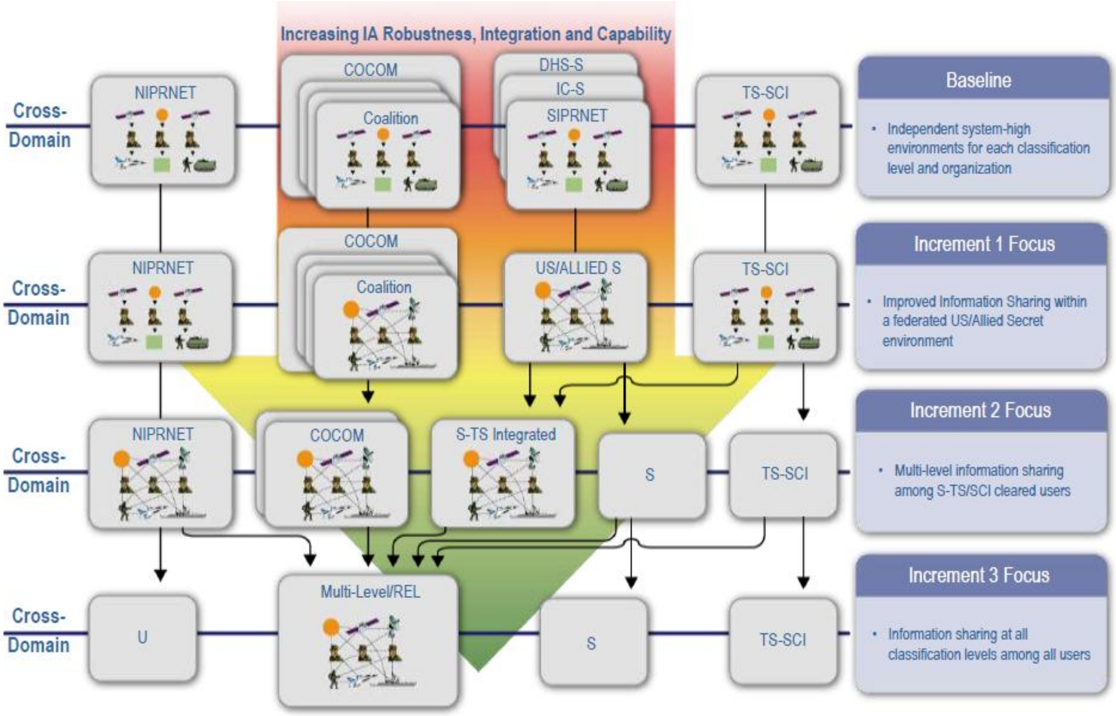

Increasing IA Robustness, Integration and Capability
Cross-Domain
NIPRNET
COCOM
Coalition
DHS-S
IC-S
SIPRNET
TS-SCI
Baseline
Independent system-high environments for each classification level and organization
Cross-Domain
NIPRNET
COCOM
Coalition
US/ALLIED S
TS-SCI
Increment 1 Focus
Improved Information Sharing within a federated US/Allied Secret environment
Cross-Domain
NIPRNET
COCOM
S-TS Integrated
S
TS-SCI
Increment 2 Focus
Multi-level information sharing among S-TS/SCI cleared users
Cross-Domain
U
Multi-Level/REL
S
TS-SCI
Increment 3 Focus
Information sharing at all classification levels among all users

Figure 10: GIG Incremental phased approach for the Information Assurance Component

The evolving, evolutionary nature of Cyberspace, its social-technical development to an increasing function orientated user groups has driven military net-centricity and the importance of information (its acquisition, protection, communication and persuasion). The centrality of Information Operations, articulated by US Joint Force doctrine (DoD, 2000) declared it was the US Military's goal to achieve dominance in the Information domain – Cyberspace. The "*Need to Know*" Security Domain[18] (Hughes, 2002; Farroha, Whitfield, & Farroha, 2009) model has to evolve to the "Need to Share" Cross-Domain Solutions, assuring that information sharing can accommodate real-time information access and transfer between different communities, partners and security domains (Kubic, 2009). The spirit of coalition sharing is the ability to give something and to gain something. CDS long-term strategy is cooperation based on trust enabling reciprocity, getting along with other communities of interest (Kollock & Smith, 1996; Axelrod, 1997; Abraham, 2005).

[18] The Security Domain models provides a means for specifying program state and state transitions, as well as security-related concepts such as subject, information flow, information access, and covert channel vulnerabilities. The model supports formalization of a security policy by providing a framework in which to specify the underlying security properties that represent that policy.

Convergence

"What is inescapably clear, whatever we choose to believe, is that we are altering our infosphere fundamentally...we are adding a whole new stratum of communication to the social system. The emerging Third Wave infosphere makes that of the Second Wave era - dominated by its mass media, the post office, and the telephone - seem hopelessly primitive by contrast. **Toffler & Toffler, 1980**

The Need to Share information has three fundamental enablers that can be identified as follows:

1) Protocol Definition: specifying who can access what information under which conditions and across what boundaries.
2) Protocol Enforcement: ensuring that information dissemination conforms to an agreed IA policy.
3) Protocol Tolerance: ensuring that IA protocols are fault tolerant to the 5 IA pillars, Information Security, Information Dependability, Risk Management, Trust and System Resilience

The State of Art of Information falls into a number of components, a strategic positioning of IA, an operational role of IA and how IA can impact on the Enterprise in both its processes and it ability to create a new culture of trustworthiness. This will be investigated in Chapter 3. Moreover and in part Information Assurance can be seen as an enabler to create organisation change through architecture, policies and education; to better risk manage that change and its on-going operations with skilled practitioners and to create two major paradigms, that of survivability (resilience, dependability and safety) and Cross-Domain Solutions (Security, Protection and Trust Management). For Critical Information Infrastructures there has become a greater need for resilient systems, that are both fault and intruder tolerate, dependable, useable and safe for the operations and its operators. The Cross Domain Solution provides access control; information availability and authority to pull Information from one security domain to another will require Transactional Information Protocols that are derived from a combination of factors including mission, nationality, permissions, vetting and the operational situation. Information systems that support the UK's Network Enabled Capability provide many differing varieties of intrinsic and often complex, interactions, transactions and dependencies. Information is one of the most important assets of our business but do we really comprehend this? Without the timely and effective use of information our decisions become jaded, inappropriate or suspect. We need our information to be accurate, trusted and not compromised, lost, leaked, disseminated, unauthorised publication or corrupted. The NEC doctrine of Information Superiority predicates the need for information security and its assurance, but little has been done to finance a national strategy to bring the skilled individuals (we need) into this new marketplace. How often is it heard in conversations what was perceived as a solution has been discarded because of security, or the lack of it? Or that security has imposed unacceptable additional costs to projects.

Security is deemed to be difficult, intrusive and a necessary evil to protect our information, our assets, from the social engineered, hacked, virus invested, virtual world of cyberspace. There is a culture that doesn't want to understand security; it's too complex; they have no appetite for it, they see it as a horrible medicine to be administered. Often question its values and see no apparent return of investment. Fundamentally, security is a compromise to influences, power and agenda and may be not fit for purpose (one compromise too many). Corporate executives have seen security professional who don't improve the situation as they further complicate or cause a degree of disbelieve when they present doomsday scenarios or forecast future major failings. Then there is a proliferation of guidance, policies and security technologies to understand; the issues of management, architecture, assurance and exploitation; and very little recognition of the skills, knowledge and education that is needed to communicate comprehend and provide necessary assurances. The "*Need to Share*" is the first of many bridges (Richardson C. J., 2008) that this Thesis will argue towards creating a more holistic understandable and interoperable cyberspace that has its infospheres[19], infrastructures. Networks and Operations assured. Building IA bridges across capability gaps in Corporate Strategies, their Information Process and Storage, Communication internetworking and providing a framework to create well educated professionals are all considered to support and develop this new IA science well into the 21st Century.

Building the Bridges across the Capability and Educational Gaps in our knowledge and understanding of Information Assurance and its effectiveness to help solve the complex

[19] R.Z. Sheppard (1971), "Rock Candy", *Time Magazine* first introduced the notion of "Infosphere" as he described: "*In much the way that fish cannot conceptualize water or birds the air, man barely understands his infosphere, that encircling layer of electronic and typographical smog composed of clichés from journalism, entertainment, advertising and government*."

problems of (a) cross-domain security; (b) trusted system interoperability; (c) system survivability and tolerance to faults and intrusion; (d) providing for a better skilled based practitioners and educated cyber warriors; (e) develops the contextual and conceptual science of IA, its architecture (IA^2) and doctrine; and (f) it accomplishes the aforementioned by creating 5 key IA models which are:

1) **Composite Model of Interoperability** (Figure 21, p74)
   This 3-Dimensional model provides the alignment to harmonise business processes within the organisation's social-technical (Enterprise) architecture to the technical-organisational layers of interoperability.

2) **The Assured Cyber Defence Architecture** (Figure 40, p119)
   This provides a coherent overview of IA Architecture as a methodology to provide Cyber Network Defence and a platform for Shared Situational Awareness and Superior Decision Making.

3) **The Information Functional Concept Model** (Figure 47, p133)
   The I-Stack Model provides a contextual overview of the Information flows from the Data Layer to the Knowledge Layer demonstrating the Human-Computer interactive components of Information Exploitation and Information Operations.

4) **The Information Assurance Cuboid Model** (Figure 52, p153)
5) The thesis has structured 8-Dimensions of Information Assurance and these are mapped against the flow of information (Process, Storage and Transit) and the military's layers of Cyberspace (Geographical, Physical, Logical, Persona and Cyber Persona).

6) **The IA Skills Framework** (Figure , p211)
   The skills framework was derived from the UK's National Information Assurance Strategy (Cabinet Office, 2007) to develop the IA profession. It is now incorporated in HMG's Information Assurance Competency Framework and been developed for the National Occupational Standard for Information

CHAPTER 2:

The Assured Position of Information

The risks from Cyberspace *(including the internet, wider telecommunications networks and computer systems) have been identified in the National Security Risk Assessment as a Tier One risk. This means that they are judged to be one of the highest priorities for UK national security over the next five years, taking into accounts both likelihood and impact.*

HMG Fact Sheet 18: Cyber Security, 2011

'I'm not convinced that lack of encryption is the primary problem [of vulnerability to network attack]. The problem with the Internet is that it's meant for communication among non-friends. **Whitfield Diffie, 2010**

Bridging the Air Gap[20] (Bobbitt, 2000; Hurley, 2001; Morabito & Gatchel, 2001; Schou, Kuehl, & Armistead, 2005; Richardson, 2007) encompass social-technical (Enterprise), professional and Educational competencies and capabilities within the organisation and their system (of systems) interconnection to other organisations. Bridging the

[20] In Computer Network Operations the air gap is defined as a type of security where the network infrastructure (domain) is physically secured by keeping it separate and isolated from other domains and the Internet. While this provides security, it also electronically limits access and interoperability of networks (and VPNs) by authorised users and coalition partners.

Domain Gap (linking one secure domain to another) is of operational necessity for system interoperability (the Cross-Domain Solution)as is the Bridging the Competencies Gap within the Information Assurance profession (Richardson, 2008); they are, and have, both military (MoD, 2009) and national requirements (Cabinet Office, 2007). There is a great political urgency as well as military and cultural need for assured Cyber Situational Awareness[21] and the contextual understanding (and individual awareness) of the intrinsic properties of cyberspace (Barbatsis and Fegan, 1999). An important requirement for modern (and in particular military) information infrastructures is meeting its definition as *"a shared, evolving, open, standardized, and heterogeneous installed base"* (Hanseth, 2002) that allows for the interoperability of classified domains and robust connectivity to other coalition partner's information domains. This need to share information across differently configured, classified and owned networks is defining the new cyber landscape and creating a plethora of security and data ownership problems.

The Defense Information Infrastructure ***(DII)"*** *is a shared or interconnected system of computers, communications, data applications, security, people, training, and other support structures serving Department of Defense (DOD) local, national, and worldwide information needs. The defense information infrastructure connects DOD mission support, command and control, and intelligence computers through voice, telecommunications, imagery, video, and multimedia services. It provides information processing and services to subscribers over the Defense Information Systems Network and includes command and control, tactical, intelligence, and commercial communications systems used to transmit DOD information,"* U.S. Department of Defense, Joint Doctrine Division, 2010**.** The military development of Information Infrastructures within its own cyber environment has created many security anomalies, accreditation and compliance problems. The complexity and often insular nature of the military Information Domain has been exacerbated by the need to keep the confidentiality and integrity of information within many different layers of classifications and reader sensitivities, within the military organisation, across departments and ministries and to coalition partners, NGOs and corporate entities. Keeping our secrets, secret has been the watch words of military

[21] Situational Awareness is the field of study concerned with perception of the surroundings and derivative implications critical to decision makers in complex, dynamic areas such as military command and security.

information security, but the need to share our classified information assets have now become an operational necessity. The Information Domain is a three-part concept for information sharing, independent of, and across information systems and security domains that:

1) *identifies information sharing participants as individual members,*
2) *contains shared information objects, and*
3) *provides a security policy that identifies the roles and privileges of the members and the protections required for the information objects.*

CNSS Instruction No. 4009, 2010

CNSS 4009 (3) generates the security need for the integrity of the data structures, dependability & safety of the information and resilience of the systems & services that support the Information flow; equally these interconnecting domains need to be risk managed, secure, protected and above all, trusted.

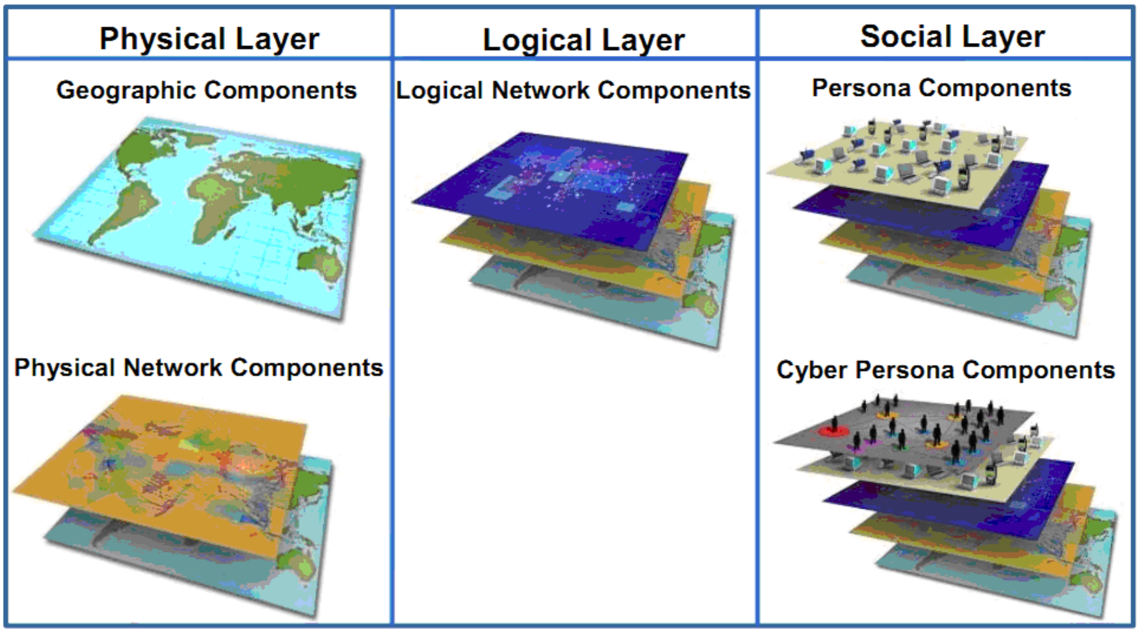


Figure 11: The layers of Cyberspace (US PAM 525-7-8, 2010)

The Social Persona Layers couples human computer interfaces, virtual information infrastructures and virtualised operating environments across multiple security domains. In this human engineered cyber world we have an evolving, expanding and emergent collaborative social-technical and pervasive world of the virtual and real space. Wherein the virtual world we witness avatars representing us, software agents conducting our business, digital signatures authenticating our digital work and digitised imaginary distorting or obfuscating the persona (Powell, 2009).

2.1 The Cyber Landscape: Understanding the Need to Share

The knowledge society requires people who can reach good decisions, cope with new environments and spot new rules—human and physical—as the world changes.

Sir Douglas Hague, *Beyond Universities: A New Republic of the Intellect*, 1991

Intrusion Detection System
TCP
UDP
ICMP
BGP Churn
Update
Withdraw
WEDNESDAY 30 Apr 08
Top Ports - TCP
1 135 DCOM DCE endpoint resolution 21% 10%
2 445 DCOM Microsoft-DS 21% 21%
3 22 SSH Remote Login Protocol 10% 11%
4 139 DCOM NETBIOS Session Service 5%
Top Countries
UNITED STATES 63%
VENEZUELA 21%
TAIWAN 10%
Akamai Internet Intelligence
Prototype Cyber Operations Center
DER, IAW AFI31-204, BAFB SUP 1, PARA 4.2

Figure 12: DARPA's National Cyber Range (Shatchman, 2010)

Composite layered models will allow for future research in determining the utilisation of ethics, standards, governance, policies, procedures and human behaviour across the 9 layers of interoperability. This represents a new approach to understanding the interdependencies of identified attributes, Enterprise Architecture; Skills transfer and Information Assurance. Furthermore investigating the 378 composite model's cuboids will create a new area of research utilising cyber ranges and synthetic system experimentation. Chapter 1 introduced the "*need to share*" information and the CNSS Instruction 4009 (2010) has defined and reinforces these requirements These Information Domain elements requires data and networks structures, in-turn these provide the Information Infrastructure (defined by Pironti, 2006) as *"all of the people, processes, procedures, tools, facilities, and technology which supports the creation, use, transport, storage, and destruction of information"* that has become integral to the DoD's Joint Doctrine (DoD, 2010).

The data networks viva intranets, ad-hoc networks, C2, C^{4}I, ISTARS and SCADA networks have become an organizational form for structuring human activities supported by Information and Communication Technologies and manifestly by the Internet - *a communication pathway for non-friendly activities"* (Diffie, 2010). System capabilities such as IRC (Text Chat), interactive white-boarding, IP Voice, IP Video Teleconferencing (VTC) and instant messaging have rapidly become popular in Information Operations and have proven themselves invaluable to the military; disaster relief agencies and critical infrastructure real-time C2 activities. The use of these technologies goes beyond their original context of social networks (MySpace, Facebook, MSN Live Messenger, etc.) that are associated with online collaboration (Eovito, 2005). *The emergence of social networking technologies and the evolution of digital games have helped shape the new ways in which people are communicating, collaborating, operating, and forming social constructs. In fact, recent research is showing us that these technologies are shaping the way we think, work, and live* (Klopfer, Osterweil, Groff, & Haas, 2009).

Figure 13: Sailing the Cyber Sea (Stavridis & Parker, 2012)

Figure 13 illustrates a military cyber operations room and the rapid evolution and deployment of Cyber Chat in operations across Defence Information Infrastructures. The US Navy's 5th Fleet experienced the rapid deployment of Cyber Chat during Operation "*Iraqi Freedom*" (2003) and the subsequent Operation "*Enduring Freedom"* in Afghanistan where it became extensively used to support of the Navy's interactivity with military intelligence and supporting agencies. Initially, the US 5th Fleet began Operation *Iraqi Freedom* with only one chat server, averaging 300 concurrent users. As the operation intensified, they installed a second server, averaging now 800 concurrent users and later implementing a total of four servers supporting over 2500 concurrent users and they were not unique in evolving, exploiting and expanding its adaptation to Military Cyber Operations (Armistead, 2004; Kuehl, 2009; Bieniek, 2011).

Whilst this synchronous, real-time uplift in ICT capability was essential, its rapid proliferation across the navy became problematical; coalition partners' Computer Network Operations (CNO) found that they could not interoperate with the 5th Fleet chat as they (5th fleet) were using the classified Secret US Only - Secure Internet Protocol Routed Network (SIPRNet). Furthermore, in Operation *Enduring Freedom* a dedicated coalition cross-domain chat solution was provided but many US personnel found "Coalition Chat" distracting or inefficient as they had to collaborate twice; once on SIPRNet and then a second time on the coalition CNO. Consequently, accessibility and the interoperability problems were further compounded with multiple coalition CNOs and other US CNOs trying to deliver the theatre Cyber Situational Awareness to operational commanders with *stove-piped* solutions (Thomas, 2009a).

Engineers, scientists and scholars have addressed the contexts and entropy of computer network operations, the creation of network of networks in a variety of fields, including sociology, informatics, economics, local and national government, criminology and international security and derived many theories around Information (Shannon, 1948; Cover & Thomas, 2006; Gleick, 2011). Some recent academic research is currently investigating and examining the similarities, differences, and connections between network forms of organization across different academic disciplines developing a new topology of inter-group networks and improvements to our understanding of how human behaviour is coordinated through networks (Hejnova, 2010). Furthermore, these network concepts are now underpinned by Enterprise Architecture and system of systems engineering (Yeung, 2002; Laudon & Laudon, 2007; Levine J. , 2010). To provide assurance to these systems requires a detailed look at the complexities and theories that now surround Systems and Informatics. Conceptually, the structure of the Information Domain is now a combination of (a) the creation, communication, transference, storage and deletion of data and (b) the cognitive use and understanding of knowledge and experience, it transference, storage and production of shared situational awareness (McNeal, 2004).

Within the Information Domain we can identify three important components, Information Operations, Information Exploitation and Information Storage. These provide knowledge transfer and intelligent use of information to create the shared situational awareness for commanders and decision-makers. The Assurance of these components provides the trustworthiness of the flow of information, the security of the service provision and the protection of the supporting systems (of systems) as illustrated in figure 14.

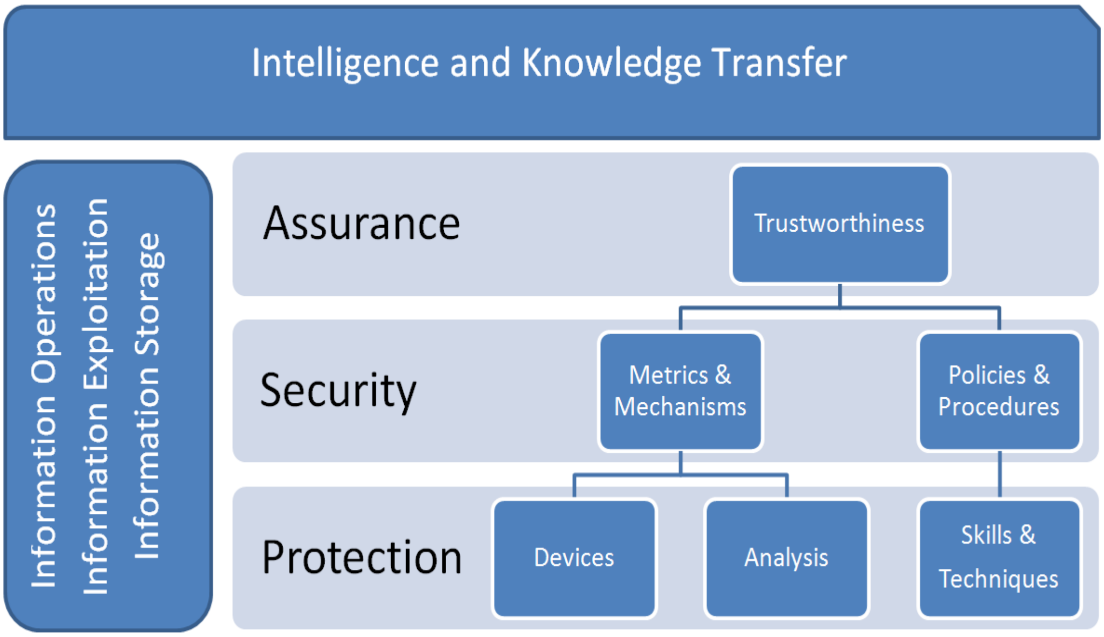
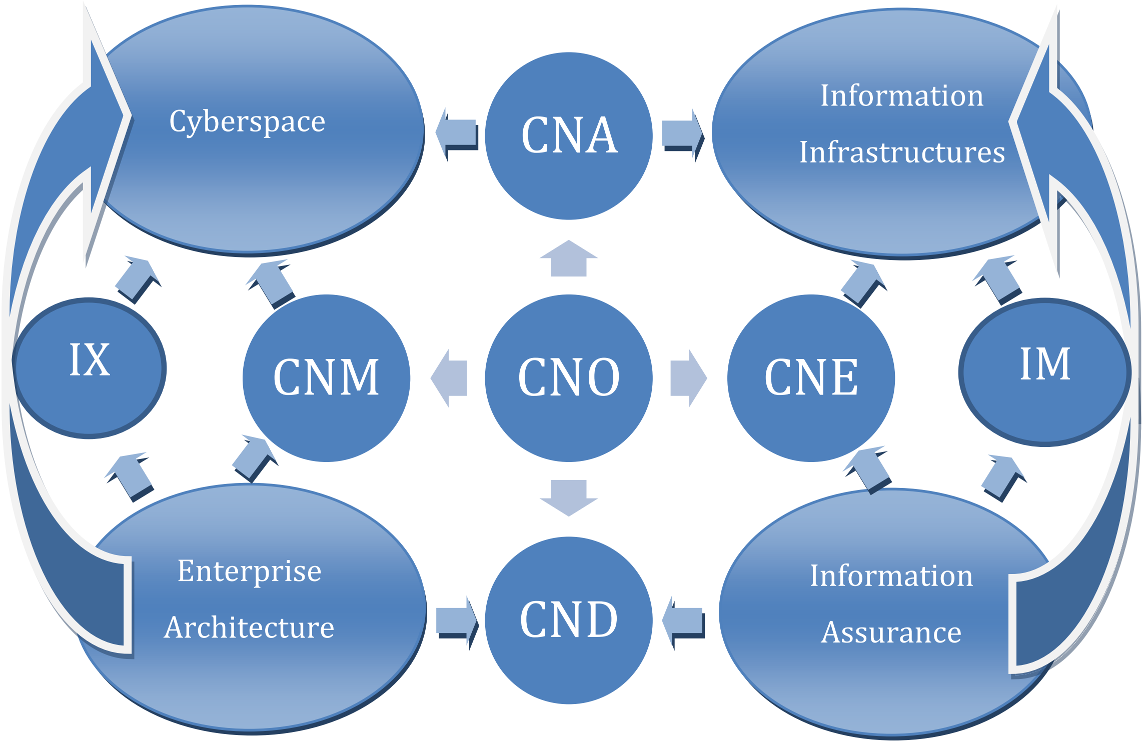


Figure 14: Assurance of Information Operations (Richardson C. J., 2008b)

The intelligence, cognitive and knowledge transfer of this model is expanded, with further details, in Chapter 5 which includes some more essential components of the Information Stack (the I-Stack Model); the flow of information from the data terminals to the Human-Computer Interfaces (HCI); Knowledge Transfer (KT) and the creation of shared awareness. The tier relationship that bridges Assurance, Security and Protection within the Information Domain has become a pervasive process in which we now need to understand the influences each layer affect each other and what their combined effects on business processes and operations are. This causative relationship is further developed (and exploited) with the Information Assurance Model (see chapter 6), as well as part of the computer network operations component of Netcentric system as illustrated in Figure 15. Here, the Information Domain is a virtual, non-physical domain that transverses the other 5 military operation domains (Land, Sea, Air, Space and Cyber) and this concept separates it from the convention of analysing it as just a Cyber Domain (McNeal, 2004; Metz, Garrett, & Hutton, 2006; Halle, 2009).

Information Operations

Information Operations have five core capabilities: (i) Psychological Operations, (ii) Military Deception, (iii) Operational Security, (iv) Electronic Warfare and (v) Computer Network Operations (MoD, 2010c). This thesis examines both Operational Security and a further four principle components of Computer Network Operations: Computer Network Attack (CNA); Computer Network Exploitation (CNE), Computer Network Defence (CND) and Computer Network Management (CNM).



Legend

CNO – Computer Network Operations			
IX	Information Exploitation	IM	Information Management
CNA	Computer Network Attack	CND	Computer Network Defence
CNM	Computer Network Management	CNE	Computer Network Exploitation

Figure 15: Elements of the Information Domain (Richardson C. J., 2009b)

The Enterprise Architecture (DODAF and MODAF) element provides Operational structures and views to the domain; whilst Cyberspace and Information Infrastructures elements bridge the physical communication and data structures to the Cognitive space of Knowledge Management and Situational Awareness. As information is conventionally seen as asset of military power the military community needs to understand the dynamism of these element interactions, within the information domain. Knowing the impact of their interactions is an important step to creating an assured domain. How we shape them, couple them; provide appropriate security metrics that align to the business processes will help provide a more harmonised assured cross-domain solution.

The "*need to share*" tactical information among single services, joint forces, coalition partners, non-government organisation (NGOs) and other agencies is critical to the providing a safe and successful operation. However, this need to share information is often odds with the "Need to Hold" where the sensitivity of the Cognitive, Information and Physical attacks, as illustrated in figure 46, across the Battlespace's electro-magnetic spectrum necessitates accredited heterogeneous channels amongst diverse groups. These tightly regulated channels presents significant operational security challenges often restricting business processes and operational expediency. Bridging the Gaps requires successful negotiation of multilevel, interdependent and sometimes conflicting agencies, their protocols, policies, accreditation and doctrines as well as the interagency aims of governments. This is formally recognised by Joint Forces chain command policies, but often is done more informally between pairs of agencies as cultural and organisational norms. (Suri, et al., 2008; Feltovich, Bradshaw, & Bunch, 2009).

In 1969, NATO constituted the Committee on the Challenges of Modern Society[22] (CCMS), which argued for, and promulgated the introduction of a non-military focus within the Alliance to address increasing social-technical vulnerabilities from sources beyond the traditional security framework and this committee has cooperated with the US Defence Advanced Research Projects Agency[23] (DARPA) to improve multidisciplinary information sharing, cyber security capabilities, crisis management, interdependencies among critical infrastructure and technologies (NATO, 2002).

[22] The Committee provides a unique forum for the sharing of knowledge and experiences on social, health and environmental matters both in the civilian and military sectors among NATO and EAPC Partner countries. The work of the Committee is carried out on a decentralised basis and participation by nations to the pilot studies, projects, workshops and seminars, which are nationally funded, is voluntary.

[23] The DARPA's mission is to maintain the technological superiority of the U.S. military and prevent technological surprise from harming our national security by sponsoring revolutionary, high-payoff research bridging the gap between fundamental discoveries and their military use.

The 9/11 atrocity and the continued increase of the global threat of cyber-terrorism (NATO, 2007), the Estonia and Georgia cyber conflicts and information warfare has transformed the military landscape for NATO and its member nations (NATO, 2008). Their New Strategic Concepts presented at the Lisbon Summit (NATO, 2010) placed cyber security at the forefront of NATO's security challenges and created the new Emerging Security Challenges Division (ESCD) to formulate Cyber Defence Strategies. Within a year, NATO's Defence Ministers had agreed the framework Concept on Cyber Defence (Bieniek, 2011). NATO's CIS is beginning to transform from "stove-piped" silo platform-centric to federated network-centric force structures (Price, Beltz, & McKinnon, 2006).

This transformation has made the reliance of the Information Infrastructures across all 5 domains an operational necessity and a robust cyberspace has become the most prominent in operational planning (Alberts, Garstka, & Stein, 1999; Hobbins, 2005; Bieniek, 2011). US Air force (USAF, 2008) demonstrates the IER creation of 3-Dimensional Computer Network Operations within the physical confines of Cyberspace and the Information Superiority platform provision for offensive capabilities of CNA (Bayles, 2001; Berenger, 2006); and CNE (Armistead, 2004; Krekel, 2009); but also ensure the CND (USN, 2010; CJCSI, 2011) of friendly decision cycles (Burris, 2010); and the military usage of Computer Network Management (CNM), as listed in Table 2, whose management activities include:

Network Management
Incident Management
Problem Management
Change Management
Release Management
Configuration Management

Capacity Management
Availability Management
Service Level Management
Continuity Management
Financial Management
Security Management

Table 2: IO Computer Network Management

The Military gains its Information Superiority in the Information Environment through the use of Intelligence, Surveillance and Reconnaissance to provide sensory data for the Joint Operational Picture (JOP). The Information Operations can use Knowledge, Information and Data (KID) through its Cognitive, Information and Physical (CIP) dimensions to provide Direct and Indirect attack mechanisms (CNA and CNE), derived from its Superior Decision Making processes and the NEC benefit chain (Baber, Stanton, Houghton, & Cassia, 2008), to target the opponent's decision cycle (Alberts, Garstka, & Stein, 1999; Berenger, 2006; Armistead, 2010). This projection of Cyber Power requires the Assured Friendly Information Stack (a defensive posture) to be also able to project an offence posture in all 3 dimensions (Physical, Information and Cognitive) to conduct Information Operations (IO) and C2 functions. This model becomes more complex when the decision loops involves joint force actions across multiple coalition KID-CIP stacks.

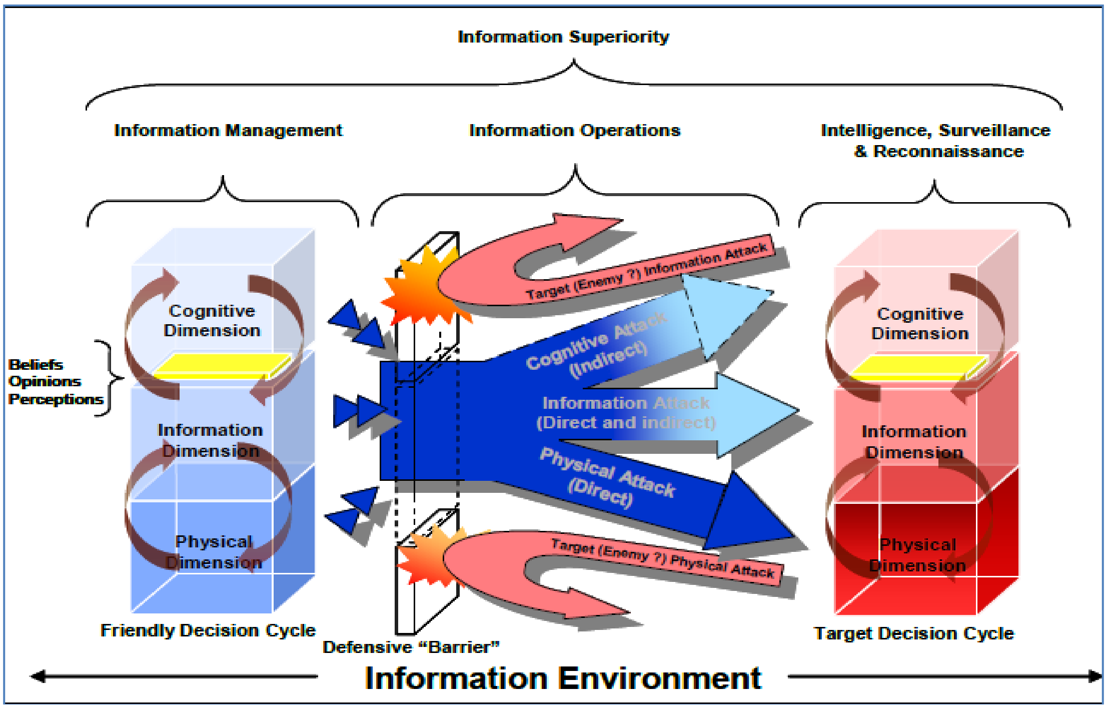


Figure 16: Gaining Information Superiority in the Information Environment (MoD, 2006)

Consider a scenario where the Commander has determined a target and asked for a FIRES (operational use of munitions) response, the FIRES CNO would SMART-pull information from Navy, Air or Army forces' operational management and databases, as illustrated in Figure 17, where there is a need to gather Knowledge, Information and Data on such issues as theatre actors, weapon availability, target acquisition, impact assessment and cost to delivery. In return these forces will need to have target information, timing and a Shared Situational Awareness to order to provide the best solution for the offensive action. As the ISTAR Joint Operational Picture generates new data, all tasked forces will need updates, so these Real-Time processes become Time-Sensitive with a need to be agile, reliable and accurate. The different aspects, actions and actors of the CNO conducting the FIRES are now rarely discrete operations; instead they interact and impact upon each other, generating a complex mesh of KID-CIP effects and events, providing support and being supported. As more targets are generated, these operations will manifest the operational tempo and scheduling. Consequently, as operational resource struggle, complications may ensue within different decision cycles and their respective Information Operations, deployed assets and actors.

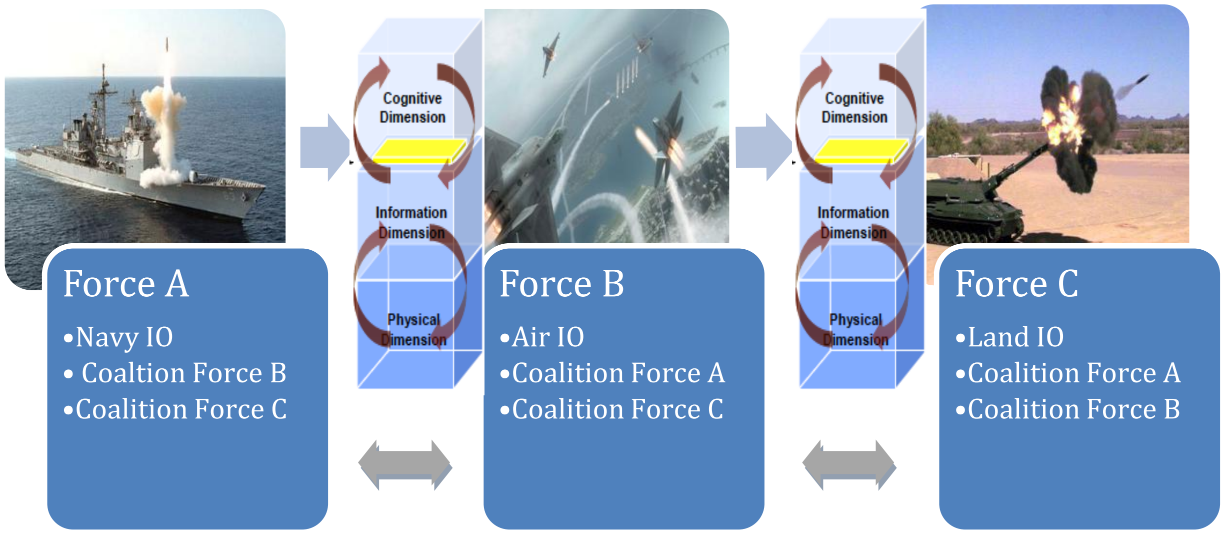


Figure 17: Stacking and interconnecting the KID-CIP loops in a Coalition Network (Richardson, C.J., 2011)

NATO's Network Enabled Capability (NNEC) architects have expressed the importance for military Information Exchange Requirements (IER) in the tactical environment (Tolk, 2001; Mittrick, Richardson, & Kaste, 2008). They recognised that Warfighters must share information across organisational, system and spatial boundaries to achieve operational goals as illustrated in Figure 50. NNEC derives Battlespace Information from critical and highly classified Intelligence, Surveillance, Target Acquisition, and Reconnaissance (ISTAR) systems which are often desperate sourced, macroscopically linking several multi-national battlefield functions together from reconnaissance missions (Aircraft sorties, UAVs, Special Forces, etc.); unmanned sensors (Remote CCTV, Spy Satellites, Electronic Surveillance Devices, etc.); human intelligence networks; the Internet and the Global Positioning System (Tolk, 2003; Dorion & Boury-Brisset, 2005; Tolk & Kunde, 2010).

IER Interoperability is the key attribute for coalition operations, it is not just the physical connectivity between military forces and it's their ability to share information, it's the harmonised contribution to a common operational picture, and building up of shared situational awareness in order to collaborate and produce effective missions (Alberts & Hayes, 2006; Suzić & Yi, 2008).

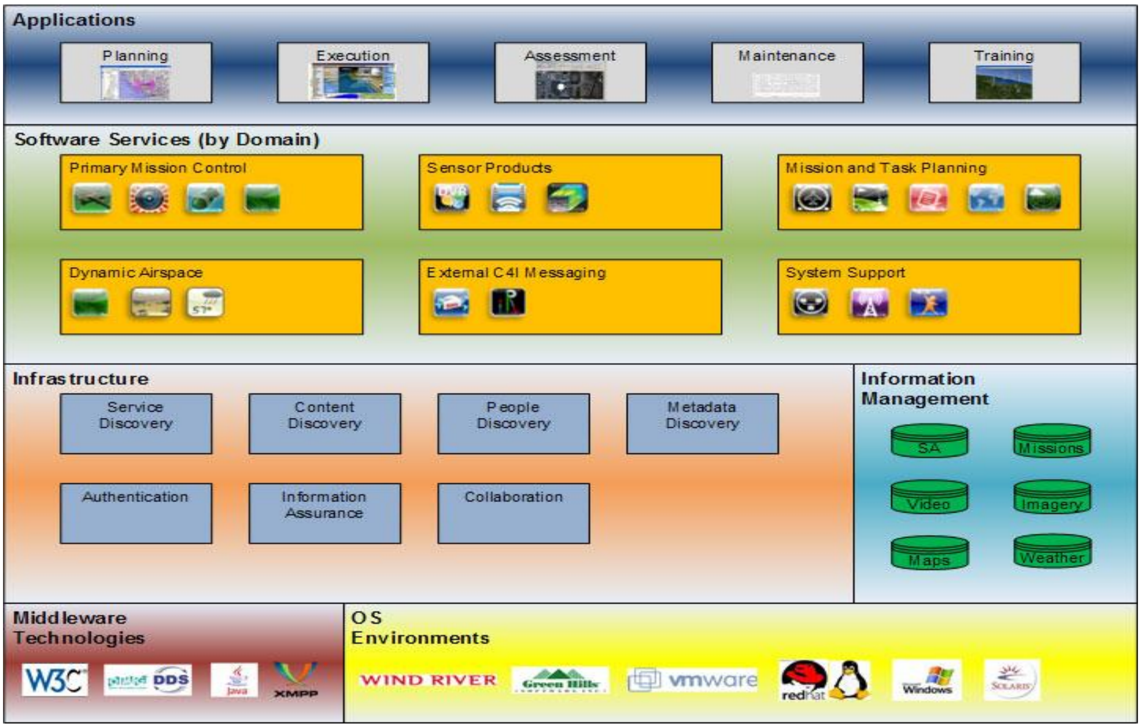


Figure 18: Unmanned Aircraft Systems Control Segment Architecture (DoD, 2010)

This agility (robustness, resilience, responsiveness, flexibility, innovation, and adaptation) is the fundamental component of network centricity and the military adoption and development of cyberspace. However the very nature of an assured, agile, responsive ICT has become the security dilemma. The multiple, rich, multi-user, multi-national orientated Cognitive, Information and Physical dimensions needs to be protected in near real-time for military Intelligence and Information Operations. This time-sensitive, assured cyber environment can be geographically dispersed as a virtually spatial distributed environment which must also allow the transference of routine and classified data in certain, if not most situations.

The military information exchange process is a prime example of the need to exchange technical information which can be "*sensitive but perishable cross the boundaries*" between various domains, e.g. the mission timetable would be highly sensitive until the operation delivers (Army Research Laboratory, 2009). Ideally the message exchanges should be automated such that the messages objects files can flow securely cross boundaries with minimal human intervention; however is important that the Information Exchange supports an appropriate degree of human oversight and intervention. The sharing of Blue Force (Friendly Coalition Forces) tracking data (this information concerns location nature and movement of friendly forces) requires an IER system to precisely identify and tag the type of perishable tactical data that needs to be shared among multiple cooperating organisation such as US forces; UK forces; NGOs, local police, Intelligence communities, enforcement agencies and emergency response units. The known location of friendly forces and non-combatants is critical to avoiding potential fratricide situations and minimising civilian casualties, thus all participating nations are therefore motivated to share such tracking information and are dependent upon its integrity.

Assuring Information Superiority

> *Increasingly, military decision makers have to rely on information provided by other actors within a highly dynamic and distributed Battlespace,"*
>
> (Keller, Carrigan, Atkinson, Clarkson, & Johnson, 2008).

The persistent problem of Blue Force interoperations is that each organisation has regulations governing the kind of data that may be shared, and services offered, with other members. Cross-domain information sharing policy requirements and associated Service Level Agreements (SLAs) can be complex and require rich language (often open to interpretation) to scope many different aspects of the data sets; its modes and channels of communications; service provision as well as context in which the data will be shared. Military organisations are specifically concerned with situations where the inflexibility of IER contracts and insensitive applications of Information Management (IM) policies may endanger life: e.g. when special operations group unexpectedly moves into close proximity of another group; then this normally undisclosed activity may temporary require disclosure to reduce the risk of friendly fire.

The Strategic Positioning of Security Model (Richardson, 2008) describes the Assurance of Information Superiority as the exploitive emergence of tolerant, resilient and trusted Human-Computer inter-exchanging systems and Knowledge Transfer. This secure flow of Knowledge, Information and Data (KID) across platforms has become a key component of modern warfare and the military decision cycle*.* NATO's Network Enabled Capability (NNEC) has irrevocably aligned member nations to coalition interoperability with most activities operating under a single Information Domain (NATO, 2007a) where they identified the need to develop information assurance in NNEC CNO and deduce its implications across coalition environments and was required to improve the *accuracy, timeliness as well as both the spatial and temporal coverage of mission decisions through synergistic employment of sensors, decision makers and effectors within an assured information network* (McIntyre & Flemming, 2001). Assuring the Information flow and services provides the platform for military decision advantage.

Rear Admiral Bill Rowley, USN, (1995) wrote that "*knowledge is the resource of the future - land, natural resources, factories and workers are no longer the measure of a country's wealth because multinational businesses can easily obtain these things anywhere in the world. It is the application of knowledge that now offers the competitive advantage in the world economy. The Knowledge Worker is the true asset because of the knowledge and abilities he or she possesses. In the twenty-first century at least 35 percent of the workforce will be knowledge workers. They must have formal education, possess specific knowledge and skills, have the ability to acquire and apply theoretical and analytical knowledge, and continue to learn throughout their lives. They will work in teams because no one person can know enough to do it all. Because they are the true assets and are highly mobile, companies will work hard to keep them.*" (Rowley, 1995).

The Knowledge workers in the US Director of National Intelligence (DNI) 2015 Vision are clearly those who are mission focussed. The military concepts of Cross Domain Solutions[24] (Kennedy & Soligan, 2010) precipitate an array of Information Assurance risks: *risk of bias and erroneous intelligence, of users' ability to fuse data and ideas into operational concepts, or in adequate assessment of alternative interpretations, of faulty and catastrophic decision-making* (Burgoon, George, Adkins, Kruse, Biros, & Nunamaker, 2007).

[24] Wikipedia describes Cross-Domain Solutions (CDS) as solutions for information assurance that provides the ability to manually or automatically access or transfer between two or more differing security domains. They are integrated systems of hardware and software that enable transfer of information among incompatible security domains or levels of classification. Because modern military, intelligence, and law enforcement operations critically depend on a timely sharing of information, and because of the cost and forethought required for more rigorous approaches, CDS are often considered a "necessary evil". CDS is distinct from the more rigorous approaches, because it supports transfer that would otherwise be precluded by established models of computer/network/data security (e.g. Bell-LaPadula and Clark-Wilson). CDS development, assessment, and deployment are based on risk management. Sharing information with CDS exposes the sharer to greater risk that his secrets may be unintentionally revealed. Available at: http://en.wikipedia.org/wiki/Cross_Domain_Solutions (Accessed 20 March 2011).

The FUD Contagion

> *"The U.S. government, if confronted in a cyber-war today, would not come out on top… If the nation went to war today, in a cyber-war, we would lose. We're the most vulnerable. We're the most connected. We have the most to lose." US Director of Intelligence,* Mike McConnell to the US Senate Committee, Feb 2010

There are real threats, vulnerabilities and Operational Impact with these risks, as they will impose, constrain or damage operations (The FUD Contagion) if CDS implementation is not accompanied by a deeper understanding, training and adopting new tools (such as those envisaged by the next generation of emergency help services to mitigate them. This paradigm shift in the nature of the military enterprises from the "*Need to Know*" (Security Domain) to the "*Need to Share*" (Cross-Domain Solutions) creates OPSEC problems. Increasingly, military and civilian organizations implementing information systems are discovering a greater need for secure, reliable interconnections between existing systems than for systems that provide new capabilities (Vietmeyer, 2004). Recent media articles for command[25] options such as National Cyber-guards, Cyber-militia, Cyber-Police and harking for social Cyber-defence force and more Cyber warriors can be construed as the previous century 3D-mentality and mobilisation that will fail to redress the very real need to control and provide trust in this multi-lateral, multi-layered, multi-dimensional chaos. This new space has opened new opportunities to the way we think, communicate, socialise, emphasise and innovate (ISTAG, 2009). It's a domain of chaos, complexity and evolution of technology and exploitative of human desires, wants and needs (greed, control and power) and where for many users there is Fear, Uncertainty and Doubt (FUD). The many ways that we choose to interacts with globalize instant responses, has both tangible and intangible actors who have their own agenda (Dalal, 2006); where system and infrastructures activities react to our demands (or other controls) and often vary greatly from individuals, enterprises and governments which makes it an impossible place to police, legislate or even place and maintain rudimentary controls. Cyberspace needs to have social trust as an enduring value to the conscious of all its communities, an assurance that is global and empowered by practitioners and users (Collins & Mansell, 2003).

[25] The activation on 1 October 2009 of the US Cyber Command (USCYBERCOM) brought together computer network attack (CNA) and computer network defense (CND) activities of the US DoD Joint Functional Component Command for Network Warfare (JFCC-NW) and the Joint Task Force for Global Network Operations (JTF-GNO) under the USCYBERCOM.

Operational issues through the Cyber operators' lens have become abstract or process orientated as: online game scenarios; e-commerce utilities; web paging; torrents, social networking create their own perceived *realities* and where they might also find new and vibrant virtual realities to distract or augment. The real concepts of war, a declaration to fight an adversary for political, economic or military supremacy, usually involving nation states, population participation and the loss of lives, possessions, prestige, wealth or influence is ingrained in our conscious, but Cyber War doesn't invoked the same FUD feeling within the social conscious, its abstraction obscures its potential devastating effects. The continuing likelihood of inter-state conflict coupled to the increasingly decline of state social cohesion, through Globalisation, suggests a posterity of Information Warfare., Cyber hostilities, malicious viral attacks and an increased global crime wave (Schwartau, 1996a; Boyd C. G., 1999; Anderson K. , 2005; Kierkegaard, 2005; Knapp, 2009). Globally, many people don't realise the true extent of the controls that these virtual (soft) systems have over their lives or the near-future repercussions of these virtual systems that generates and stores vast quantities of data per millisecond; the risk impact of freely evolving knowledge transfers and social networking are engineered to provide empowerment to the individuals who are not aware of its consequences thereby providing possible manipulation or control by individuals, corporations or States: gained, whether legally or not! Realisation and data protection failure becomes media events that expose and sensationalise the impact of malware to critical information infrastructures and the consequential losses that may be exploited and cascaded into a society meltdown.

Cyber-attacks are menacing, but it's the erosion of trust in the digital economy where the true risk lies and the consistent, advance persistent threats may be generating a societal backlash to the digital economy. These governmental, corporate and individual failures further degrade trust and assurance as they focus on intolerances, fear, uncertainty and doubt. The contagion is ignorance and the strategic objective should be to inform communities, provide intelligence and shared situational awareness to combat this ignorance. Experience say this should be expedited, especially by providing more assurance practitioners; to educate CSA as illustrated in Figure 54 (this is further developed in Chapter 7). It is essential, to culturally change our approach; to facilitate enterprise vision and social online responsibilities to assure cyberspace, not to train cyber warriors to war within it, but make everyone a cyber-citizen who wants to embrace security for their own privacy (United Nations, 2004; Bauwens, 2005; Obama, 2009a).

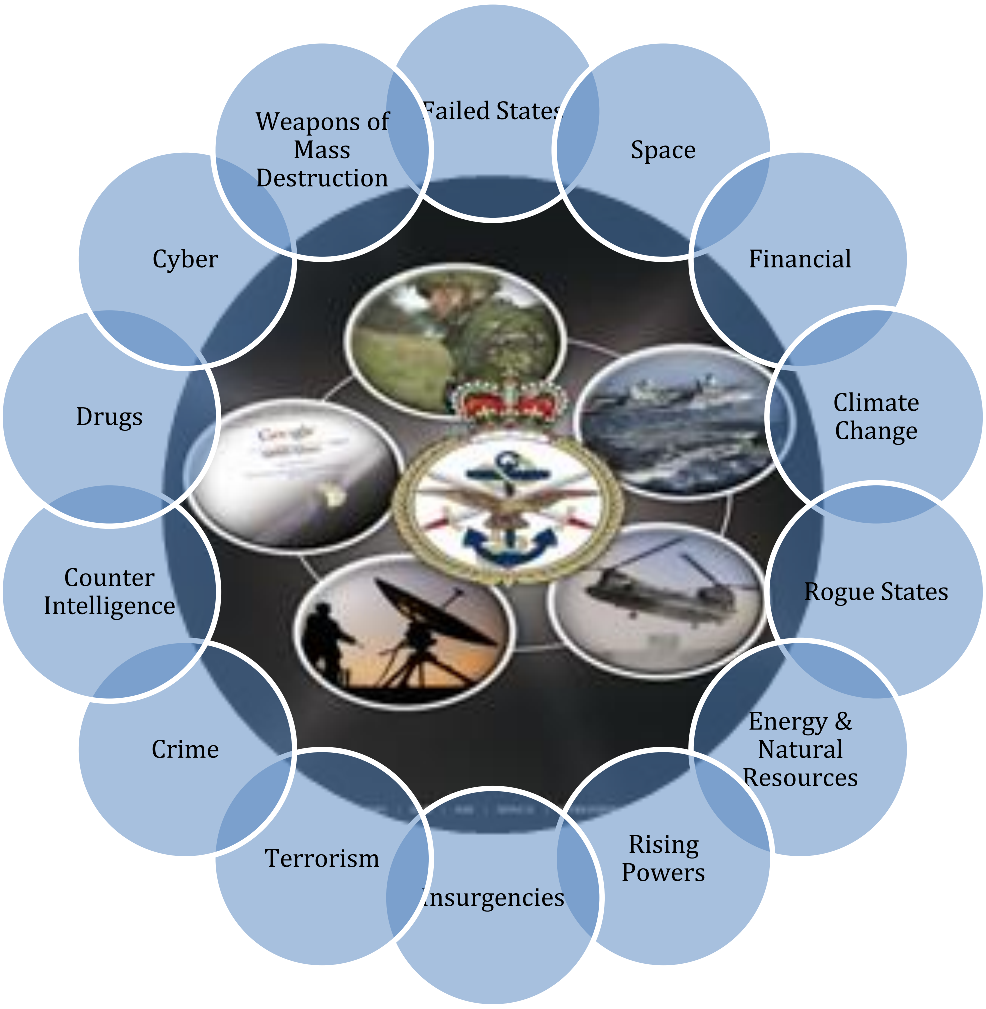


Figure 19: Persistent Threats and Emerging Missions (Richardson, C.J., 2010)

"Over the last 20 years, the Intelligence Community has been challenged to keep pace with rapidly evolving information technology. Although a less-than-agile acquisition and procurement system has been part of the problem, the Intelligence Community is also undermined by its basic approach. If we are to maintain a technology edge, we must adopt an enterprise wide, service-oriented architecture that is interoperable with systems in other federal departments, and can share information with non-traditional partners. A service-oriented architecture provides a proven means to adapt new technologies while responding to changing user needs. By creating "software as a service," this architecture reduces system complexity and deployment risks through a shared development style, uniform standards, and common interfaces. These services will enable a user-defined analytic environment through the use of composite applications – discrete services that can be pulled from a central library and dropped into a user-defined workspace." **(McConnell, 2008)**.

Toffler's (1980) RMA identified how to the conduct military operations in the 21st-century with interoperable, federated coalition networks that would offer military commanders unprecedented capacities for rapid, real-time, global exchange of messages and complex information needed for success in the Battlespace, Information That commercial off-the-shelf (COTS) based CIS and military deployment of Service-

Oriented Architecture (SOA) portends profound changes to CIS Human Computer Inter-exchange with the sheer volume, complexity and speed of information transmission and communication diversity (McConnell, 2008). The Exploitation (IX), Information Superiority and Cyber Situational Awareness (CSA) can be, in turn, exploited and attack from Enemy CIS platforms from many different attack planes as illustrated by Figure 53. However, the Insider threat and CNE causes the most fear and uncertainty to military operations (DoD, 2011).

The complex net-centricity of CDS, to provide assurance and negate FUD has created many emergent properties (Norman & Lucas, 2000) and an unprecedented growth of interdependent, chaotic flows of data, and ever increasing information and knowledge transfers across system boundaries which has been described as Information Overload (Johnson, 2006). This Overload has also permeated a greater lack of understanding of the unintended, as well as intended capabilities (Fink, 2003; Tullao, 2003; Burris, 2010). Furthermore, Enterprise Integration, Net-Centric Information Enterprise and Service Orientated Architecture (SOA) have produced enhanced capabilities of newly adaptive tools and systems which coupled to Cross-Domain Solutions (CDS) pose considerable opportunities as well as accompanying risk.

CDS is further complicated with Protective Marking of Information and their security domains. The Bridging of these domains is an important aspect of the KID Cross-Domain Solution and the speed and effectiveness of interoperable, dependable CNOs will greatly contribute to the overall Information Superiority, providing the commander both freedom of action and force projection. Information Assurance has to create and maintain safe interoperability; structured dependability and security of its enterprise architectures at different business impact levels: ensuring trusted boundaries, accurate and integral information sharing and reliable flows across multi-layered boundaries in dynamic multi-tiered, multi-regional coalition network environments (Phillips, Ting, & Demurjian, 2002). The NNEC Enterprise perspective is of system of systems engineering that requires comprehensive high level assurance to system survivability and intrusion tolerance for wireless networks, tactical networks, ad-hoc networking, network engineering and infrastructure management, as well as the implications of using commercial-off-the-shelf equipment (NATO, 2007b).

2.2 Shared Situational Awareness

> *"While information assurance and information-based security is a difficult problem within any given nation or infrastructure, the additional technological, organizational and cultural dimensions within NATO make implementing NEC security very complex. Nevertheless, progress toward a unified vision for implementing a robust and flexible NEC Security solution is imperative"* NATO, 2007

The contextual Battlespace domains of military operations are land, sea, air and outer space; the 5th Battlespace domain, what Gibson's *Neuromancer* (1984) ichnographically described as Cyberspace has over a very short time created many new dimensions within it (Schoder, 1999; Jog, 2001; Kramer, Starr, Wentz, & Zimet, 2007), as it fuses, exploits and controls the other 4 Battlespaces (Corum, 2009; van den Berg, 2010). That we need holistic initiatives to maintain, explore, expand, expose and control Cyberspace (Alberts D. S., 1997; Armistead, 2004; Alberts & Hayes, 2006; Libicki M. C., 2007) and its many Information Infrastructures that are prevalent, evident and necessary to the National Defence (Cabinet Office, 2009b; MoD, 2010). We also need to define what is Cyberspace and where it differs to the Information Domain, which is pervasive across all 5 Battlespaces (Halle, 2009; Kuehl, 2009).

"In the twenty-first century, the Internet and other interconnected networks (cyberspace) have become critical to human wellbeing and the political independence and territorial integrity of nation states. The danger is that the world has become so interconnected and the risks and threats so sophisticated and pervasive that they have grown exponentially in comparison to the ability to counter them. There is now the capability for nation states or rogue actors to significantly disrupt life and society in all countries; cybercrime and its offspring, cyber conflict, threatens peaceful existence of mankind and the beneficial use of cyberspace." **The World Federation of Scientists, 2009.**

This century has created many new paradigms of human evolution (Schulur 2004; Bauwens 2005 and Arquilla, 2008) as our societies migrate from an Industrial Age to much the herald Information Age (Toffler, 1980); the need to revolutionize our contextual and conceptual thoughts of society evolution and introducing control of this virtual space can still be contextually placed on Maslow's (1943) "*Hierarchy of Needs*" as illustrated in Figure 55. People are curious, innovative and self-actualising in cyberspace but now without much linkage to real citizenship of nation states and its tax[26] gathering agencies (Lukas, 2000; WFS, 2009).

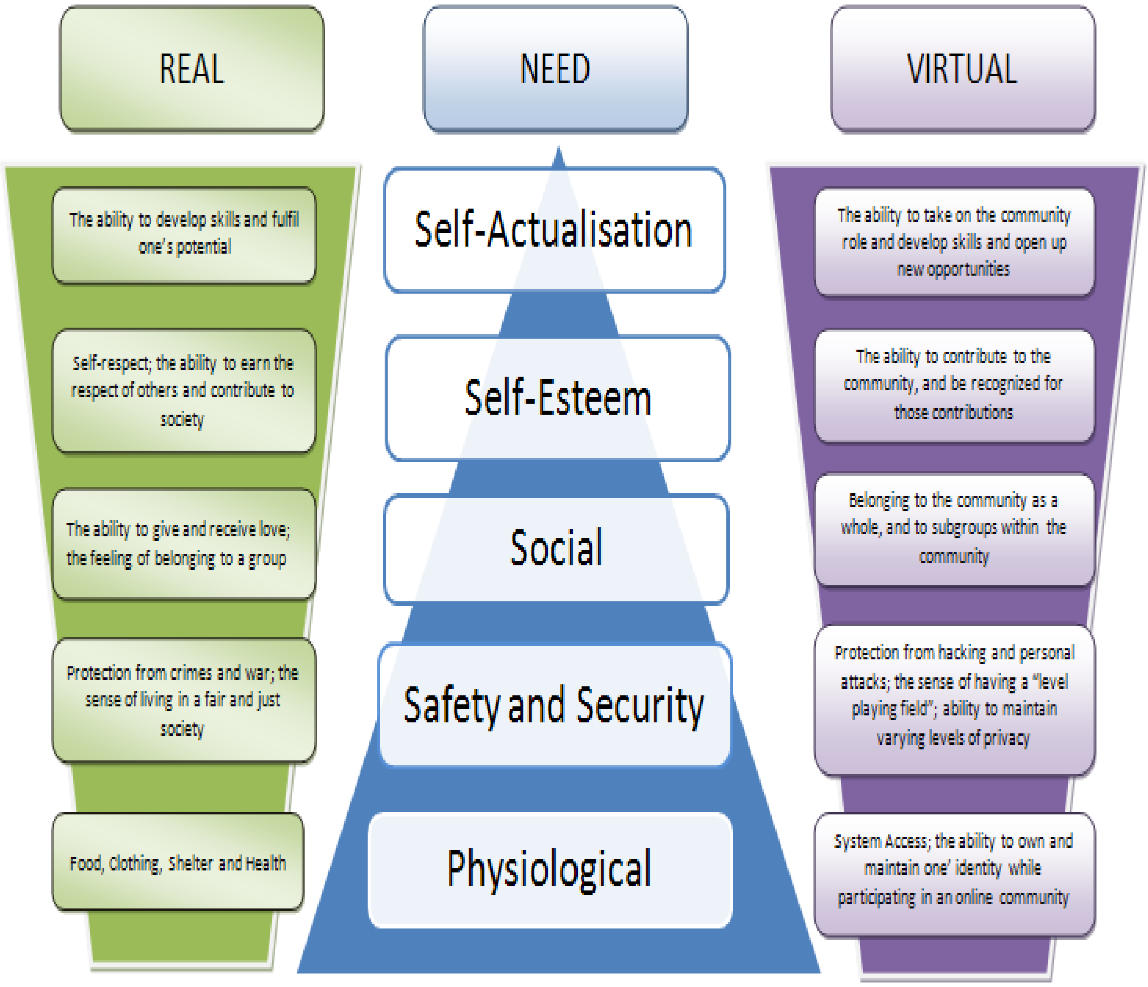

REAL
NEED
VIRTUAL
The ability to develop skills and fulfil one's potential
Self-Actualisation
The ability to take on the community role and develop skills and open up new opportunities
Self-respect; the ability to earn the respect of others and contribute to society
Self-Esteem
The ability to contribute to the community, and be recognized for those contributions
The ability to give and receive love; the feeling of belonging to a group
Social
Belonging to the community as a whole, and to subgroups within the community
Protection from crimes and war; the sense of living in a fair and just society
Safety and Security
Protection from hacking and personal attacks; the sense of having a "level playing field"; ability to maintain varying levels of privacy
Food, Clothing, Shelter and Health
Physiological
System Access; the ability to own and maintain one' identity while participating in an online community

Figure 20 Real and Virtual Communities to Maslow's Hierarchy

[26] According to the US Trade Commission the Internet Economy has become the largest industry in the country who have stated that "*The Internet is inherently susceptible to multiple and discriminatory taxation in a way that commerce conducted in more traditional ways is not.* With approximately 30,000 taxing jurisdictions, compliance becomes a significant obstacle. Double taxation would be inevitable because the borderless nature of the Internet makes taxation very tricky." Address to the ASome Policy Perspectives on the Taxation of Cyberspace, Palo Alto, CA. November 1999.

2.3 Assurance: From Machine to Organisation

Creating an operational picture and shared situational awareness (SSA) of the progression of the operation takes considerable skill, experience, training and supportive tools. The engineering of the processes behind a military Information Operation stems from its initial requirements (IERs) and availability of resources. Field Commander wants to make firm C2 decisions based on all available facts to achieve Battlespace Awareness (as tabulated in Table 4).

Command and Control	Battlespace Awareness
The ability to conduct collaborative, planning, execution, and information sharing among US civil-military agencies and coalition partners from the operational to tactical levels.	The ability to achieve a persistent situational awareness and shared understanding in a joint, multi-agency, and multinational context in order to know the operational environment and the interrelationship among ourselves, our adversaries, and the local population.
The ability to achieve multi-agency coherency of action during planning, coordination, and execution by creating a joint, and combined when necessary, multiagency planning and execution organization empowered to facilitate integrated civil - military operation.	The ability to use an operational net assessment to support stability operations and to reflect that information in the integrated civil-military common relevant operating picture.
The ability to enhance rapid information sharing with coalition members, multiagency players, and non-governmental organizations through information sharing technologies and policies.	The ability to provide persistent intelligence, surveillance and reconnaissance that integrates all intelligence capabilities, including human intelligence assets, into the overall intelligence, surveillance, and reconnaissance architecture.
The ability to field a command and control system with reach back capability and connectivity to facilitate other agency participation.	

Table 3: Stability Operations – Joint Operating Concept Capability (DoD, 2006)

From a CND perspective the Commander must be able to understand the causation of his operations (DIME); to perceive the current situation (situation perception) using his intelligence, recognition, surveillance and reconnaissance capabilities; assess the impact of any attack and tracking; to predict any future attacks and their possible vectors; determine the adversary's behaviour and capabilities; be able to predict plausible future assaults and be acquainted with the quality and trustworthiness of his information flow and the ability of his adversary affecting his OODA loops. For the Commander to achieve Battlespace Awareness he needs perception, comprehension and projection of his assets, capabilities and vulnerabilities and those of his adversary. In order to achieve this, he must manage his assets (Devices, Networks, Systems, Software and Services – Machines) and mould his environment (People, Nationality, Languages and Culture - Organisation). The physical Shared Situational Awareness (SSA) picture is built up from many differently owned, operated and organised (Protocols, Transmission and Presentation) sensory data apparatus, signal processing and interception devices. These ISR system outputs are then synthesised and analysed using appropriate tools which generate the Geo-Physical picture. Intelligence, previous knowledge and other resources apply a logical framework to create a real-time picture. However this interactivity, connectivity and operability of many different types machines and joint force organisations has a recognised flawed, in that there is still a gap between human analytical mental models (intuition, experience and lateral thinking) and the automated capabilities of C^8ISR.

Assuring Layers of Interoperability

In particular, the gap created with the interoperability of systems to other systems and the networking the people and organisations that use them. These layers of interoperability expose assurance issues and explain why the interconnection of physical devices through interface specifications, although an important enabler of system of systems engineering hasn't resolved the social-technical processes and assurance components related to military operations where IO usage of Information and Knowledge Transfer are equally as important as the Geo-Physical Data collected from ISTARs and the interchanging of these information flows to the decision making cycle and creation of the SSA. Creating a quantifiable quality assured SSA requires the harmonisation and alignment of all layers of system interoperability, from the technical issues upwards and the organisational/ enterprise issues downwards.

Assuring Cross-Domain Solutions for multi-layered, multi-functional, multi-national (often geographical disperse) systems of systems is an international task, involving many Enterprises, Government Agencies, Standards Bodies and Academia. The scale of the problem has been recognised (NECSI, 2004; Alberts & Nissen, 2009), as well as identifying many of the key components (from Technologies to Organizational developments) that require research, development and implementation (Morris, Levine, Meyers, Place, & Plakosh, 2004). These Systems of Systems display a number of common characteristics that cause technical and organisational challenges; in that they:

- Operated under different ownership and protocols
- Are decentralised and geographical disperse

- Are heterogeneous with little compliance and configuration management
- Have unknown Scalability and Emergent Properties
- Conform to different IERs and other diverse requirements
- Have dynamic composition with unknown system interactions
- Are in a state of change: continually evolving, expanding and been redeployed
- Are inconsistent in Architecture and Functionality
- Are eroding the Human-Computer Boundaries – complex interactivities and controls
- Are intolerant to system and intrusion failures

The usability of interoperable systems is reliant upon a robust architecture that is coherent (having multiple interdependencies) across the interconnection of Organisations, Services and Networks and supports cross-domain management of the information flows from the physical data networks to Enterprise Knowledge Transfer, Superior Decision Making and creation of a Shared Situational Awareness. International Standards Organisation ISO-14258 (ISO, 1999) has stated that "*Two systems are considered as 'integrated' if there is a detailed standard format for all constituent components.*" Integrating systems has proved to be technically difficult especially the large scale heterogeneous, geographically disperse architectures.

These autonomous systems have become federated with various degrees of coupling. These systems are "*tightly-coupled*" when the network components and services are dependent upon each other's resources (and technically inseparable); whereas the more common "loosely coupled" systems are bridged by communication channels that allows for interoperability of data and services whilst maintaining their own local (often unique) Business Process Operations. The Human-Computer and other technological interfaces between the machines and the organisation is the social hybrid system of a business Enterprise. Where the *Humans (modelled as objects or resources) in the enterprise have a different behaviour (e. g., learning and problem solving) from machines (e.g., acting and reacting) and therefore need a different kind of information* (ISO, 1999). The Enterprises create a dynamic environment undergoing constant stress and change owing to market conditions, operational requirements, fiscal controls, technological advances, service applications and new transferred knowledge.

Many enterprises have devolved power to the individual away from hierarchical organisational structures and C2 chain of command (unlike most military organisations which rely on rank to influence command and control). This distributive control of machine to organisation interactivity has evolved where the communities of interest cooperate, communicate and share in both problem solving and action. This cooperation requires greater cohesion such as building an Enterprise Architecture[27], ISO 15704, (see figure 63), integration of functions and services such creating Service Orientated Architectures, ISO/IEC DTR 30102 and effective management and assurance of Information flows: within the Enterprise and within the interoperability between Enterprises, Operations and Systems.

Maintaining the layers Interoperability transforms the capability of communities of interest to run business processes seamlessly across organizational and technical boundaries. The ISO has defined a framework of 5 different layers of interoperability (as Communities of Interest in their Political Context (the explicit and implicit reasons for cooperation), the alignment of legislative requirements, constraints and reconciliation producing Legal Interoperability; the alignment and harmonisation of organisational interoperability which NATO NEC has formulated in its NATO C3 Technical Architecture (NATO, 2003), the universal understanding of processes, procedures, protocols and language providing Semantic interoperability and the technical interoperability defining the syntax, integration, transmission and interfacing computer network operations and its Information Infrastructures and Cyber networks. These 5 layers achieve Enterprise interoperability by ensuring that the communities understand how *the business processes of different organizations can interconnect; by developing standards to support these business processes efficiently; and by specifying the semantics of messages exchanged between organizations to support these business processes in a scalable way* (Potgieser, 2012). The framework provides a useful standard for these Enterprise Information Exchange Requirements. Interoperability enables coalition IERs and the NEC benefit chain, presenting information in a consistent manner across business boundaries and between systems regardless of technology, application or platform. Aligning the Interoperable attributes provides Enterprises with the ability to process, store and transfer, information across multiple domains, services and technologies.

[27] Enterprise Architecture (EA) is a comprehensive view of an enterprise. EA shows the primary components of an enterprise and depicts how these components interact with or relate to each other. EA typically encompasses an overview of the entire information system in an enterprise; including the software, hardware, and information architectures. In this sense, EA is a meta-architecture. As regards, EA contains different views of an enterprise, including, work, function, process, and information, it is at the highest level in the architecture pyramid (Ostadzadeh & Shams, 2011)

The DoD through its Global Information Grid (GIG) architecture has formulated these attributes (Procedure, Application, Infrastructure and Data) to create cross domain interconnectivity and coalition operability to an unified approach. The DoD's 5-Levels of Information System Interoperability (LISI) model provides a dynamically accommodating meta-level structure. The model reflects the nature of the cross-domain where the relation between technical and operational interoperability is neither proportional nor linear (Chen, Doumeingts, & Vernadat, 2008).

It is possible that two commanders, who share the same command and control facilities, in particular having the same C4ISR system support, make decisions that are contradictive or sub-optimal. It is also possible that two commanders supported by C4ISR systems that are not interoperable on the technical level are fighting very well together. (Tolk & Muguira, 2003). This inability within the Defence realm to provide coherent and optimised cross-domain solutions has cost billions of US dollars and there's a further increase in future expenditure to ensure interoperability brings specific benefits and reducing the plethora of challenges currently beholding the technical and operational perspectives. The military have recognised that their CDS ability to simulate and emulate disparate systems of systems, producing laboratories that create synthetic environments of Red (CNA & CNE), Blue (CNM & CND), White (Digital Analysis and Forensics) and Green (Command and Control) cyber facilities (such the ranges created at DSTL and DCCIS) promote the current *train as you fight* philosophy and improved CDS alignment. The expansion of individual activities to collaborative working environments through System Simulation, Systems-in-the-Loop and Modelling is an important step to understanding real and virtual (as per Figure 20) attributes that effect the layers of interoperability and the Human-Computer Interfaces and how they work within Enterprises. Bournemouth University, its 2018 Strategic Plans incorporates the building of such a cluster of Cyber laboratories that will enables fusion of research, education and practical /kinetic learning to investigate the social-technical impact of CDS to large –scaled systems. The use of standards and enterprise architecture as illustrated in figure 66 provided a Joint Action Concept of the Layers of Coalition Interoperability (LCI) and formulated MoD's Information Strategy linking EA, Skills and IA as the main pillars of its Information Domain (MoD, 2009). The LCI framework defines Enterprise Architecture as adaptive and innovative methodology for interoperability (Smith D. B., 2005) as it identified architectural mechanisms that could accommodate Enterprise changes with minimal impact as it deals with the various layers of semantic interoperability in coalition operations.

The System of Systems Interoperability (SOSI) model developed by Software Engineering Institute at Carnegie Mellon University (Morris, Levine, Meyers, Place, & Plakosh, 2004) had addressed technical and operational interoperability of the DoD and NATO layered models and further progressed the challenges of organizations building and maintaining interoperable systems. SOSI introduces three types of interoperability: (1) Programmatic, interoperability between different program offices. (2) Constructive, interoperability between the organizations that are responsible for the construction (and maintenance) of a system. (3) Operational, interoperability between the systems. Taking the Zachman Enterprise the NCIOC model and the additional SOSI concepts a matrix of the layers of interoperability across a business process can be represented as illustrated in Figure 21.

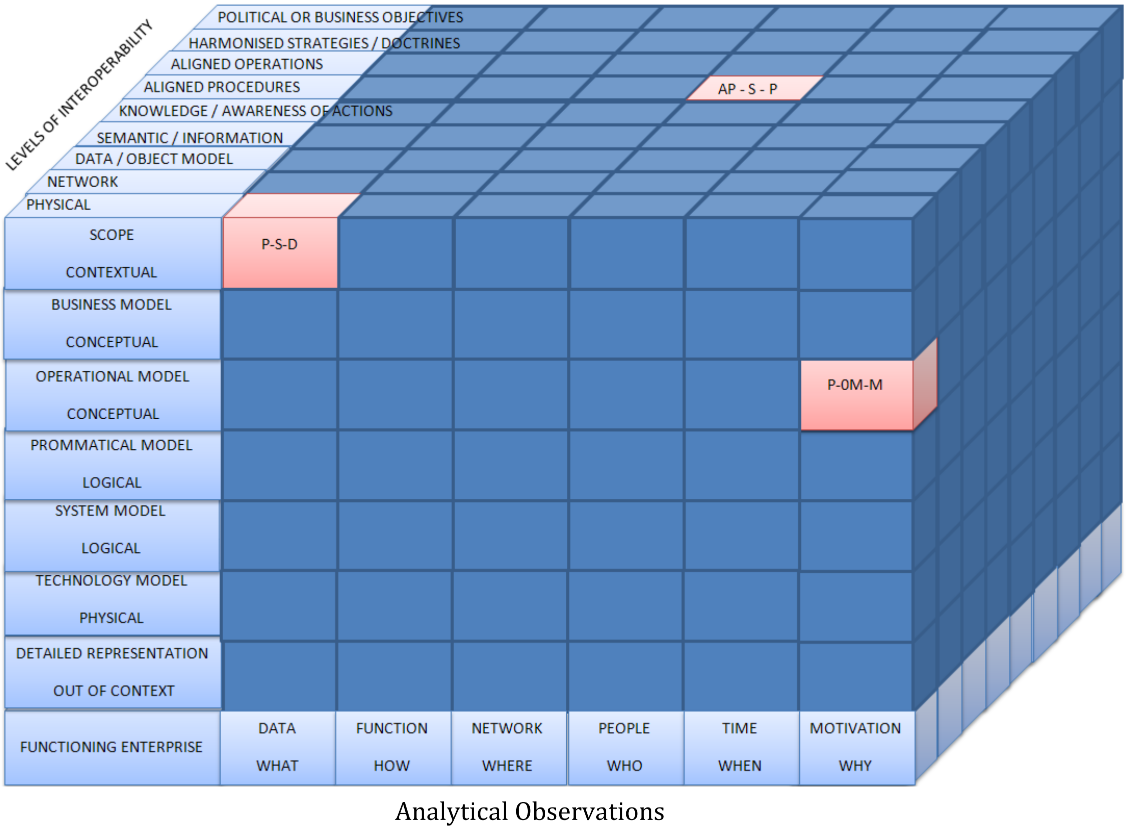


Figure 21: Composite Model of Interoperability (Richardson, C.J., 2010)

The contents of interoperations is represented by the 2-dimensional Enterprise Architectural matrix (abstract × perspective) produced by Zachman. This matrix defines what can take place in various levels of the Enterprise perspectives. The 3rd dimension enables the analyst to capture the structure and type of interoperation from the NCIOC 9-levels. The cross-domain solutions can now be analysed as a Functioning Enterprise within composite cuboids (P-S-D = Physical – Scope- Data, etc.) as highlighted in the above model. There are 378 composite cuboids within the model;

each one can be used to define the contents of Enterprise interoperations. The Alignment and Harmonisation of technical to operational issues is construed from matching each Enterprise's Composite Cuboid to their respective counter-parts within the coalition.

Cyber Network Operations

Conventional architecture has developed Information Operations around Computer Science and the employment of Computer Network Operations. In the 21st Century, Computing is subservient to Cyber (networking of computing devices, routers switches, firewalls and applications). Hence Figure 3 (earlier introduced in Chapter 1, p55) has a new legend:

Legend	Proposed New Convention		
CNO	Cyber Network Operations		
CNA	Cyber Network Attacks	CNE	Cyber Network Exploitation
CNM	Cyber Network Management	CND	Cyber Network Defence
IX	Information Exploitation	IM	Information Management

Cyberspace can be structured by Enterprise Architecture and cyber network manage (CNM) to exploit the Information assets (IX) for the business whilst been designed to reduce vulnerabilities and prevent threats by adopting robust and resilient IA architecture to develop appropriate defences (CND). The Information Assurance policies and practices will manage (IM) the Information Services across the deployed systems and Information Infrastructures. Its trust and risk management will reduce the threats from Cyber-attacks (CNA) and insider exploitation and privacy violations (CNE).)ur systems require new software monitoring tools, more Network Management integration, automated traffic analysis and building greater trust through our Assurance Practitioners working and controlling security mechanisms across other coalition networks. These practitioners (which we need more off) will also require better education and increased transferable skills and this is examined in chapter 4 (Education and Profession).

We need competent, educated professionals to run our systems, secure the information infrastructures; men who understand the complexities of interoperability from a strategic, operational and tactical level, from the technical issues of data interfacing and security devices to the more intricate problems of sensitive information flows and organisational responsibilities. Cross-Domain Solutions needs new initiatives, finance and better strategy to secure Cyberspace as stated in the revised US Comprehensive National Cybersecurity Initiative (CNCI) (Obama, 2010). The CNCI was launched by President George W. Bush in National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/ HSPD-23) in January 2008 and stated that it was a mutually reinforcing initiative:

- ***To establish a front line of defense against today's immediate threats*** *by creating or enhancing shared situational awareness of network vulnerabilities, threats, and events within the Federal Government—and ultimately with state, local, and tribal governments and private sector partners—and the ability to act quickly to reduce our current vulnerabilities and prevent intrusions.*
- ***To defend against the full spectrum of threats*** *by enhancing U.S. counterintelligence capabilities and increasing the security of the supply chain for key information technologies.*
- ***To strengthen the future cyber security environment*** *by expanding cyber education; coordinating and redirecting research and development efforts across the Federal Government; and working to define and develop strategies to deter hostile or malicious activity in cyberspace.*

In 2007 the UK issued its National Information Assurance Strategy (Cabinet Office, 2007) to manage the risk involved in social-technical systems. Information Assurance offers a panacea to the interoperability, providing a new methodology and better way of ensuring safe operations of systems of systems and an its architecture provides an understanding required culturally change our use of information, its processes, storage and its transition from one domain to another .In managing the Enterprise risks, we need to understand the advancement and agility of the threats (as illustrated in the timeline in Figure 22).

The residue of countless scripted attacks, trojans, viruses, worms and the growth of Advanced Persistent Threat Attacks (spear fishing and social engineering) with their various APT attack vectors (advanced evasion techniques - AET**s)** and zero-day attacks (e.g. Flame, Stuxnet and Duqu) At present the cyber-defence countermeasures (firewalls, IDS, Anti-virus, etc.) provide reasonable protection to most attacks, but these systems are also regularly penetrated (externally and internally) and we have to resign ourselves to the likelihood that our systems are compromised and we have intruders (Abadi, 2000; Carr, 2005; Schiller, et al., 2007; Vidanage, 2009; Cabinet Office, 2011).

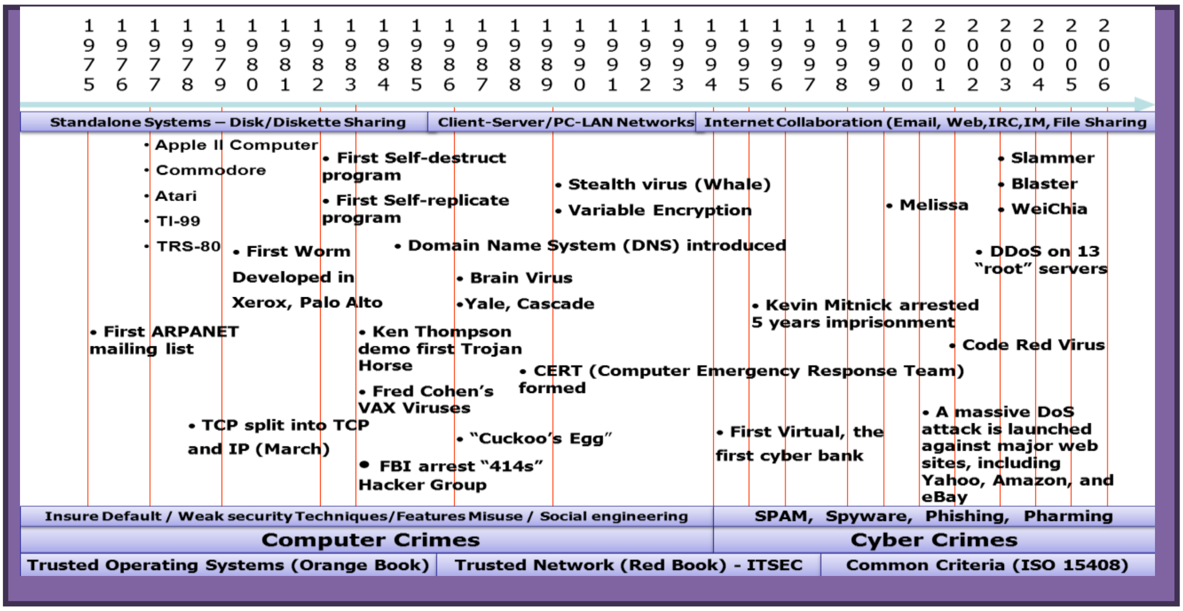

1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
Standalone Systems – Disk/Diskette Sharing
Client-Server/PC-LAN Networks
Internet Collaboration (Email, Web, IRC, IM, File Sharing
• Apple II Computer
• Commodore
• Atari
• TI-99
• TRS-80
• First ARPANET mailing list
• First Worm Developed in Xerox, Palo Alto
• TCP split into TCP and IP (March)
• First Self-destruct program
• First Self-replicate program
• Domain Name System (DNS) introduced
• Ken Thompson demo first Trojan Horse
• Fred Cohen's VAX Viruses
• FBI arrest "414s" Hacker Group
• Brain Virus
•Yale, Cascade
• "Cuckoo's Egg"
• Stealth virus (Whale)
• Variable Encryption
• CERT (Computer Emergency Response Team) formed
• Kevin Mitnick arrested 5 years imprisonment
• First Virtual, the first cyber bank
• Melissa
• A massive DoS attack is launched against major web sites, including Yahoo, Amazon, and eBay
• Code Red Virus
• DDoS on 13 "root" servers
• Slammer
• Blaster
• WeiChia
Insure Default / Weak security Techniques/Features Misuse / Social engineering
SPAM, Spyware, Phishing, Pharming
Computer Crimes
Cyber Crimes
Trusted Operating Systems (Orange Book)
Trusted Network (Red Book) - ITSEC
Common Criteria (ISO 15408)

Figure 22: A timeline of Computing and Cyber Insecurity (Richardson C. J., 2011)

The strategic issues surrounding the need to defend our human-cyber interfaces, the applications and services, the systems, networks and our social-technical infrastructures are investigated. To bridge the capability gap to creating robust and resilient Communication and Information systems requires strategic (international) initiatives to secure cyberspace. These initiatives should include:

- A strategic doctrine for assured Information handling and storage
- The effectively control the DIME usage of Cyber Power
- The provision of trust and risk management across coalition interconnections – cross domain solutions.
- Enhanced operational capabilities to create cyber-shared situational awareness and cyber defence.
- The development of intrusion tolerant and prevention systems
- Targeted funding of Cyber Defence Research and Development
- Creation of an Information Assurance Profession with a Code of Practice
- Provision of IA education and skills training

These initiatives are evolutionary and revolutionary in nature, stemming from the early strategic military thinking of Network Centric Warfare and NATO's Network Enabled Capability (NNEC) and the technical advances in CPU capabilities, communication media, storage & retrieval systems, data (and knowledge) mining, hosted services, mash-ups, architecture and cloud computing allow for increased efficiencies, complexities, emergent capabilities, revolutionising operations and how they are conducted, resourced, financed, generated and expanded. Where processes enhanced with techniques such as SaaS, SOA, Virtualisation, Geospatial identification and Business Intelligence generate emergent behaviours with a plethora of new businesses, Knowledge and Information exploitations. The holistic complexities and risk of interoperability, managing, maintaining, and utilising these unified technologies and system architectures contribute to an increasing chaotic Information Infrastructure of an evolving cyberspace that presents many unpredictable obstacles to effective operations and their assurance as well as exposing gaps in our knowledge and understanding.

"A competency is more than just knowledge and skills. It involves the ability to meet complex demands, by drawing on and mobilising psychosocial resources (including skills and attitudes) in a particular context. For example, the ability to communicate effectively is a competency that may draw on an individual's knowledge of language, practical IT skills and attitudes towards those with whom he or she is communicating," **OECD, 2005.**

With our increasing national dependence of cyber domain operations, the competency of our Cyber Defence Communities, Security Industries and Governing bodies such as the UN's International Telecommunication Union (ITU); US Department of Homeland Defence; European Network and Information Security Agency (ENISA) and the UK's new National Crime Agency (NCA) is both tested and exposed. It is estimated that, worldwide, more than one million people become victims of cybercrime every day (Europa, 2012). These organisations need to demonstrate and provide national (and international) leadership to combat advance persistent threats; attacks; cyber (malicious) network exploitation and the inappropriate use of Cyber Power.

There is nothing more difficult to take in hand, more perilous to conduct, or more uncertain in its success, than to take the lead in the introduction of a new order of things. Because the innovator has for enemies all those who have done well under the old conditions and lukewarm defenders in those who may do well under the new.

Machiavelli, The Prince

Machiavelli understood the apparatus of state power, but do our states understand the uses, consequences and global effectiveness of Cyber Power (see annex 4). The Cyber domain has new and emergent properties that we do not fully understand nor able to produce a satisfactory risk assessment. Consequently these State Actors, Corporate Executives and Academic leaders need to become more agile, engaged, educated and coherent in their resolution to defend the Cyber Information Age and shape their organisations to meet this tier-1 national security risk (Edwards, 2007). These same communities of interest also need to generate greater awareness of how cyber risks are causing fear, uncertainty and doubt (the FUD Contagion, p158) with their citizens, workforce and militaries. The global population requirements for the Cyber Information Age call for (a) better comprehension of cyberspace; (b) greater understanding the consequences of interconnectivity; (c) recognising their own limited knowledge and competencies and (d) have greater access to better information and better education. Furthermore, with 68% of Europeans believing that online personal information has not been kept secure by public bodies as demonstrated in figure 74 and 59% of *EU citizens do not feel very or at all well informed about the risks of cybercrime* and that these needs have become matters of grave concern (European Commission, 2012). This public perception of insecurity and lack of confidence with authorities to provide adequate protection is often exploited by the media *Most EU citizens say they have seen or heard something about cybercrime in the last 12 months (73%), and this is most likely to have been from television,* (European Commission, 2012), as well as more insidious individuals, organisations and state actors.

This EU report also stated that:

> *12% of internet users across the EU have experienced online fraud, and 8% have experienced identity theft. 13% have not been able to access online services because of cyber-attacks. In addition:*
>
> - *More than a third (38%) say they have received a scam email, including 10% who say that this is something that has happened to them often;*
> - *15% of internet users say that they have accidentally encountered material which promotes racial hatred or religious extremism.*
>
> *Internet users express high levels of concern about cyber security:*
>
> - *89% agree that they avoid disclosing personal information online;*
> - *74% agree that the risk of becoming a victim of cybercrime has increased in the past year;*
> - *72% agree that they are concerned that their online personal information is not kept secure by websites;*
> - *66% agree that they are concerned that information is not kept secure by public authorities.*

The majority of internet users in the EU (61%) are concerned about experiencing identity theft. Around half of internet users are concerned about: accidentally discovering child pornography online (51%); online fraud (49%); and scam emails (48%). In addition, 43%

are concerned about not being able to access online services because of cyber-attacks, and 41% are concerned about accidentally encountering material which promotes racial hatred or religious extremism. **(European Commission, 2012).**

Despite widespread media attention and warnings around Flame, Stuxnet, Duqu viruses and other APT attacks; many EU CERT advice organizations relying on Critical Information Infrastructures (CII), supervisory control and data acquisition (SCADA) and other industrial control system (ICS) networks to be vigilant against conventional network threats. These threats pose a far greater threat to Enterprise network security, and include gaps in security infrastructure, social engineering exploits (Insider and other actors), advanced evasion techniques and simple denial of service (DOS) attacks. The social-technical cyber environment is constantly threatened from the growing dangers of cyber-hooliganism, cyber-crime, cyber-terrorism and cyber-war. Corporate Enterprise, especially those that own considerable CIS assets in our Critical Information Infrastructures are beginning to understand that this digital environment facilitates considerable scepticism, insecurity and distrust, particularly at their inability to defend and secure digital assets (Kramer F. D., Starr, Wentz, & Zimet, 2007; Cabinet Office, 2010; Anderson & Rainie, 2010).

The Information Age has created a new paradigm for human competency evolution with the globalisation of societies, communities of interests and enterprises through the medium of the virtual space. The creation of the man-made Cyberspace domain has many opportunities (exploitive and complex) for the UK's and global Economy (enterprise and products), Knowledge Transfer (artificial and real Intelligence, Knowledge, Experience and Wisdom), Social Informatics and Engineering (communities and alternate societies) and Individual Competencies (skills, creation and innovation) generating new ways we can exploit Knowledge, Information and Data (KID) sources within existing systems and the emerging cyberspace with it diverse and expanding applications and services. Four distinct environmental drivers can be identified that propels this paradigm, Expansion, Evolution, Expense and Exploitation.

Our cyber defence communities need to create and provide better strategic understanding of the cyber environment across these networks of networks that: evolve (new technologies, services and applications), expand (interconnections, multiplexing, virtual domains and new deployments), exploit (data mining, business intelligence and knowledge transfer) and expend (financial, technical and human resources). The Cyber Domain needs better Assurance!

Cyber War, Cyber Crime

In understanding the Digital Domain, the thesis methodology identified the Threat Domain (Threat Agenda, Attack Profiles and Security Compromises) as a key avenue of discovery (Figure 24, page 78). Strategically the United Nations have created a Cyber Security Alliance to address the Cyber Threat Agenda. Headquartered in Cyberjaya, Malaysia, The International Multilateral Partnership Against Cyber Threats (IMPACT) agency is administered through the International Telecommunication Union (ITU) and was the first comprehensive global ITU public-private partnership (Governments, Industry and Academia) against cyber threats. IMPACT addresses the ITU's Global Cybersecurity Agenda (GCA) which is the UN's framework for international cooperation to enhance global confidence and security in the information society (ITU, 2008)

"Cyber criminals are an ever present menace in every country connected to the Internet. Organized crime has been on the rise because the Internet has proved a low risk, lucrative business. This is due to the fact that loopholes in national and regional legislation still remain, making it difficult to effectively track down criminals. The main problem is the lack of international harmonization regarding cybercrime legislation. Investigation and prosecution are difficult if the categorization of crimes differs from country to country. Some efforts to address this challenge have been undertaken, and although very valuable, they are still insufficient. The Internet is an international communication tool and consequently, any solution to secure it must be sought at the global level." **(ITU, 2008)**

There are a plethora of attack vectors to our fragile (and some say often defenceless) critical Information infrastructure as illustrated Figure 23. These vectors range from a Cyber Pearl Harbour attack (possible weapon of mass destruction), with total meltdown of systems and societies heading towards anarchy; to Cyber Terrorism (anti-establishment motivated attacks); to organised Cyber Crime and its risk to e-commerce; to the insidious nature of cyber harassment and bullying (destroying confidence and trust in our children): to the simple failures of ignorance and not been aware of the threats within this domain of domains (Colonel Kelley, US Army, 2008). These multi-layered, multilateral, multidimensional domains (Held and McGrew, 2010) are often without boundaries, easily migrating and superimposing on each other, influencing and determining different outcomes which requires complex analysis to find any resolution in this chaos (Vitas, 2001; Gordon, 2007 and Majoris, 2010). The ease of moving from one domain characterised by the lack understanding and the vulnerabilities of a Botnet client; to the risks of all out Cyberwar or some terrorist codifying some catastrophic event is just a mouse click, buts the effects are often global, instant and often ruinous (Lewis, 2002 and Bracken, 2007).

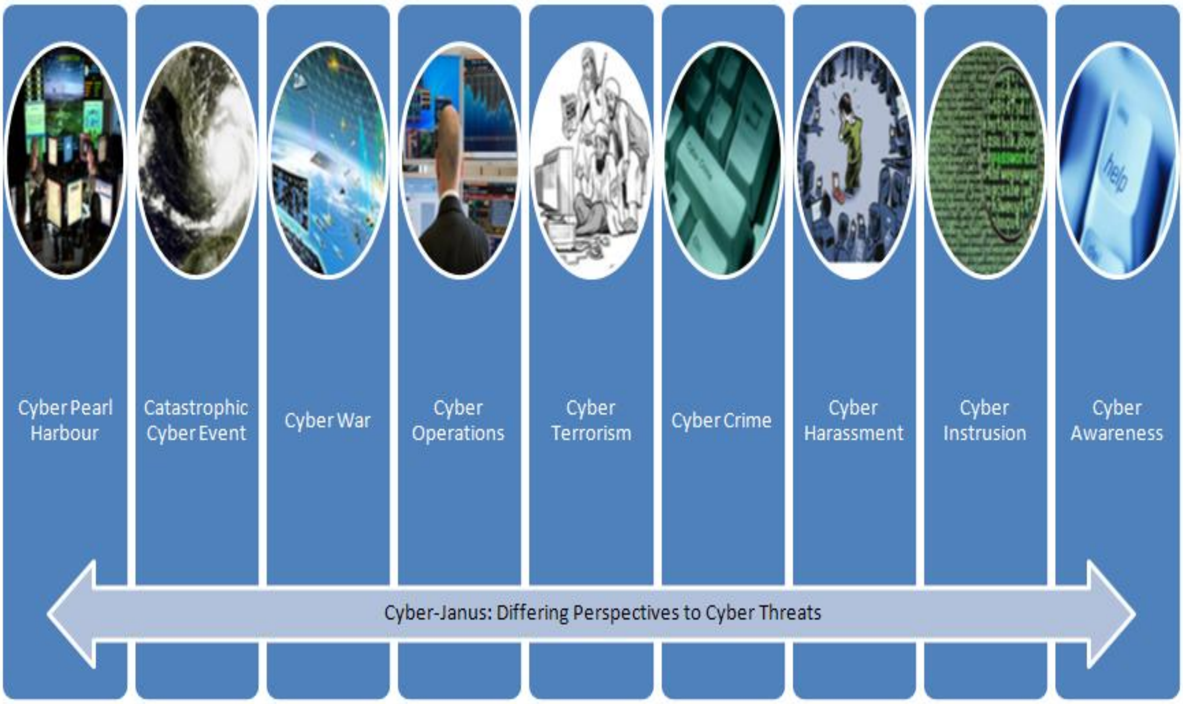


Figure 23: The Plethora of Attack Vectors to Cyberspace (Richardson C. J., 2008b)

Figure 23 provides a framework to understanding the linkages between the different threat profiles. These differences create components of the threat agenda within the Thesis methodology and briefly discussed as follows:

The Cyber Pearl Habor is a State on State Cyber Attack, launched by a hostile state (or a state sponsored organisation) who have the capability to wield a massive debilitating cyber-attack that would effectively paralyze a country and constitutes a Clear and Present Danger that potentially (according to the recent testimonial from US Secretary of Defence, Leon Panetta at the Department of Defense (DOD) budget hearing held by the Senate Appropriations Subcommittee on Defense) *"shutting down financial systems, releasing chemicals from chemical plants, releasing water from dams, shutting down power systems that can affect the very survival of a nation,"* (Mora, 2012).

The Catastrophic Cyber Event is an exploitable national disaster (such as Hurricane Katrina) where people leave their systems unlocked owing to an immediate threat to themselves or their families. A hostile State (or organisation) may then launch a clandestine first strike upon the Critical Information Infrastructure to exacerbate the situation to cause further economic and social damage. The military would also argue that chemical, Biological, Radiological and Nuclear (CBRN) would also cause a Catastrophic Cyber Event. US Senator Whitehouse described the consequences of failure in protecting the US Critical Infrastructure could be catastrophic – "*We all recognize this as a profound threat to this country, to its future, to its economy, to its very being,"* (US Congress, 2012).

The concepts of Cyber War have made considerable impact on DIME strategic thinking. The book *Cyber War* (Clarke & Knake, 2010) defines "cyber warfare" as "*actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption*." The Economist article entitled *Cyberwar: It is time for countries to start talking about arms control on the internet* (2010) describes cyberspace as "*the fifth domain of warfare*," and the US Deputy Secretary of Defense, (Lynn, 2010) had stated that "*as a doctrinal matter, the Pentagon has formally recognized cyberspace as a new domain in warfare... [which] has become just as critical to military operations as land, sea, air, and space.* HMG has developed weapons to counter the cyber threat and "*will strike first to protect itself...We will defend ourselves in every way we can, not only to deflect but to prevent attacks that we know are taking place"* according to the UK's Foreign Secretary William Hague (Dunn T. N., 2011). However, studies are incredulous to the possibility of successful deterrence against cyber-attacks, in particular to the requirements for success: the existence of capability (weapons), the credibility of the threat, and the ability to convey the threatening message to the potential challenger (Lupovici, 2011).

Cyber Operations is about actively (or passively) operating in your adversary's OODA loop (as discussed in Chapter 3, p 149). NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) stated that "*Strategists must be aware that part of every political and military conflict will take place on the internet*" (Geers, 2008) and conducting cyber network operations (CNO) facilitates espionage, cyber network attacks (CNA) and cyber network exploitation (CNE) attacks to disrupt, compromise or undermine the adversary's decision cycles and Information Operations (Alberts & Papp, 2001; Armistead, Information Operations Matters: Best Practices, 2010).

Cyber Terrorism and caused-based hackavist groups have become an increasing international problem as the motivation, expertise, tools and techniques needed for cyber-attacks have become more widely available. "*Darknets, which enable users to share content anonymously, are also likely to become more popular. Cloud computing will enable terrorists to store and distribute material in a more robust way, which can then be* *encrypted and configured to work with smartphones".* Al-Qa'ida has explicitly called for "*cyber*-jihad" and Jonathan Evans, the UK's MI5 Director has stated that the "*Criminals and rival states are using cyber terrorism on an 'industrial scale' to attack Britain's Government and its biggest businesses*, (revealing that) *one company lost £800 Million Sterling as a result of state-sponsored espionage. Terror groups* (such as) *al Qaida will use hacking to steal secrets and damage systems,"* (Robinson M. , 2012)

Cyber motivated by money and the lack of law enforcement "*cybercrime has become more profit-driven* and is shifting *away from Windows-based PCs to other operating systems and platforms, including smart phones, tablet computers and mobile platforms in general,"* (Shinder, 2011) The cost of cybercrime to individuals, corporations, governments and society in general will continue to climb. According to a 2011 study by the UK's Office of Cyber Security and Information Assurance (Holden, 2011), the British economy lost £27 billion pounds sterling attributed to cyber-crime, with most of that being shouldered by UK business.

Cyber Harassment, Cyber Bullying, Cyber-stalking and Cyber Grooming are the most insidious of all the types of cyber-attacks, being highly targeted upon an individual (often people with inexperience and/or mental or physical disabilities) in the workplace, at schools or in the home. Online perpetrators, predators and stalkers often pretend to be children or friends and start online conversations with their victims through social sites. They may try to continue the relationship in personal conversations on mobile phones (sometimes known as whispering), via private chat rooms or produce negative, derogative and harmful images, videos and text across the social sites such as YouTube, Facebook or Instant Messaging channels (Cyber Smart, 2009).

Cyber Intrusion and privacy is about the easy accessibility of data and information held on systems about individuals. There is a lot of information on individuals that can be gleamed / gathered unobtrusively from the Internet which could be used to the individual's disadvantage or for some criminal exploit or social engineering attack. Often seen as passive attacks, these intrusions, ghosting and data mining activities build up considerable intelligence on enterprises, their employees and personal lives.

Cyber Awareness attributes the lack of understanding, poor skills or the ignorance of people operating applications, services and infrastructure devices in cyberspace. Governments need to educate their citizens on the potential harm that cyberspace has, as well as its benefits of social and e-commerce applications. The OECD (2005) identified that a nation can gain a collective return from cyber awareness as illustrated in figure 24.

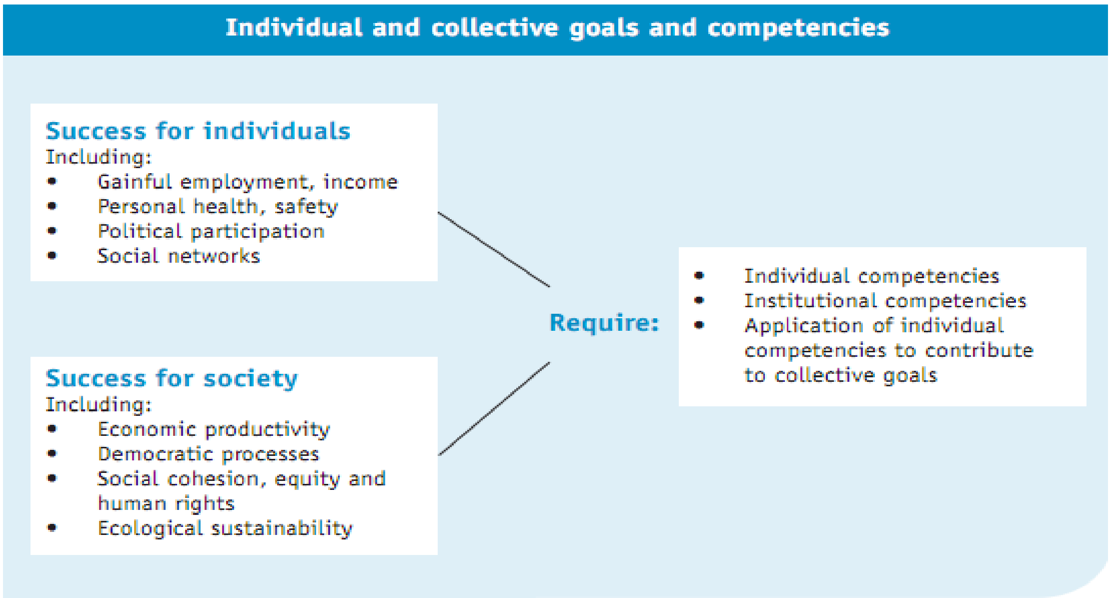

Individual and collective goals and competencies
Success for individuals
Including:
• Gainful employment, income
• Personal health, safety
• Political participation
• Social networks
Success for society
Including:
• Economic productivity
• Democratic processes
• Social cohesion, equity and human rights
• Ecological sustainability
Require:
• Individual competencies
• Institutional competencies
• Application of individual competencies to contribute to collective goals

Figure 24: OECD framework relating individual competencies (OECD, 2005)

Underpinning the attack profile components in figure 23 is the duplicity of benefits/ disbenefits (a benefit becoming an opportunity as well as a threat) to cyberspace that was illustrated by the Cyber-Janus[28] (capturing the nature of Janus) and coupling it to the Black and White Hat communities of cybercrime and prevention. These Black Hat / White Hat communities represents the two main perspective to cyberspace; the first face presenting the ubiquitous nature of cyber-space and how it affects our lives in a positive manner; the sharing environment of our work and workplace; the electronic global commerce and its interconnections of communities and government; and then the second face, the shady and shadow side of spamming, threats, hostilities, malware, crime, terrorism and warfare. That Cyberspace represents information and knowledge systems as strategic national assets and also has become a tier-1 strategic national threat (Cabinet Office, 2010).

[28] Janus of Roman Mythology was the god of doorways and time. Representing him in the 21st Century as Cyber-Janus symbolizes change and transitions, the Good (White) and Evil (Black) within the Cyber Domain, of one condition to another across many virtual domains.

Strategic Direction for Cyberspace

The internet is the digital global community and a coherent international strategy for is use and security is essential. The emerging international landscape can be seen through a European Union (EU) or United Nations (UN) perspective /lens where the physicality and pervasiveness of cyberspace across the world's societies has given this man-made domain considerable depth (Technological, Social, Economic and Psychological) as illustrated by the EU's concepts in Figure 25. Surprisingly the EU study into the future shaping of the Internet (European Commission, 2010) found that Technology wasn't a key driver and although Economic and Social issues had an impact, it was the psychology of trust and at its the core was are the Information Assurance issues of privacy, protection, security and reliability. The United Nations has sought to control the Power of Cyberspace through its own technical authority. The UN's International Telegraph Union (ITU) is the only UN agency with partnerships between government and industry and its activities towards cyber security has been to establish and follow a set of fundamental rules formulated at by the WSIS and the 2006 ITU Plenipotentiary Conference (ITU, 2006).

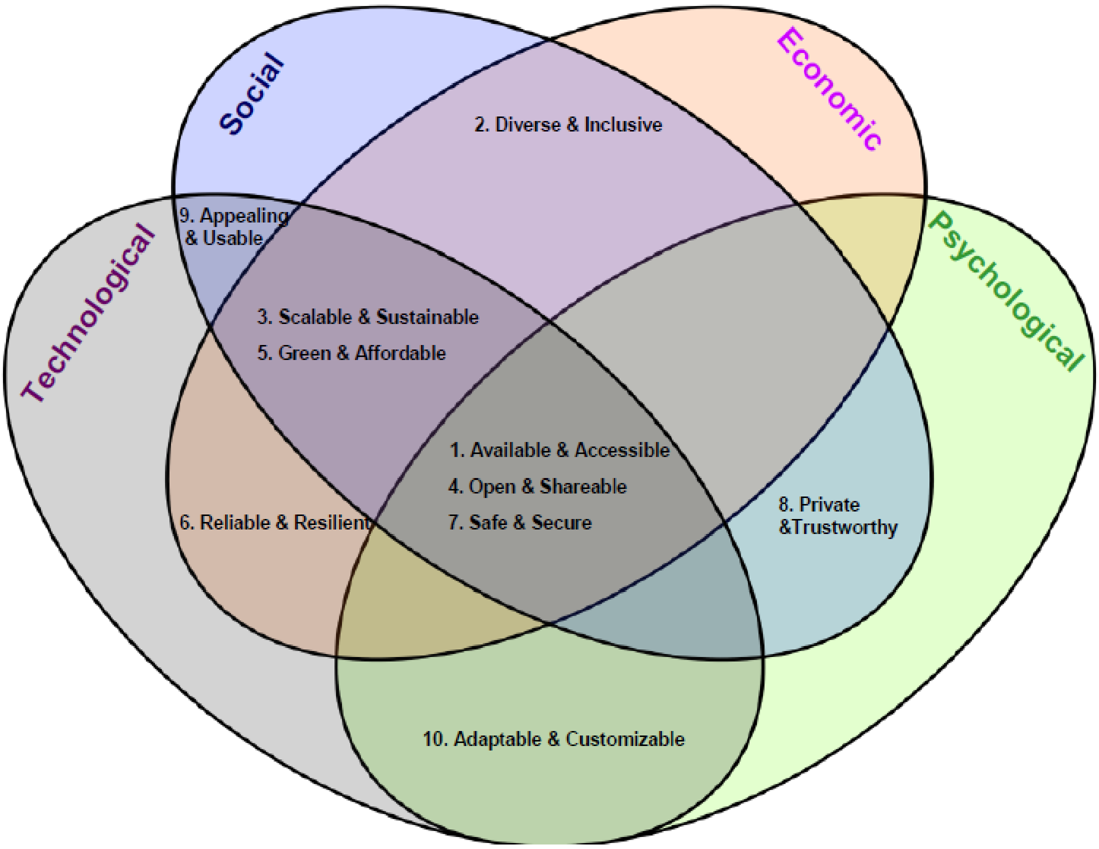


Figure 25: Fundamental principles by overlapping domains (European Commission, 2010)

The ITU was tasked to build confidence and security in the use of Communication and Information Systems, facilitate cooperation among public and private organisations, and to foster education and training initiatives. Global leaders, communities and institutions participating in the WSIS and its own member states representatives further entrusted the ITU to take concrete steps towards curbing the threats and vulnerabilities related to information society resulting in resolution 130. Whereby, the ITU (ITU, 2006) was requested to give high priority to building confidence and security in the use of information and communication technologies, and in Resolution 149 to clarify definitions and terminology relating to building confidence and security in the use of CIS. In order to raise awareness the ITU (ITU-D & ITU-T) has since organised a succession of workshops to establish their framework of cyber security and critical information infrastructure protection and these workshop's purpose were defined as:

- *Identify changes faced by countries and develop frameworks for cyber security and Critical Information infrastructures (CII), share experience and considered the best practices.*

- *Disseminate information on the ITU cyber security work program to assist developing countries and the ITU-D study group question 22/1: securing information and communication networks: Best practices for developing a culture of cyber security.*

- *Disseminate information on unrelated technical security standards activities developing/being developed by standardisation organisations, and in particular related to ITU at-T activities;*

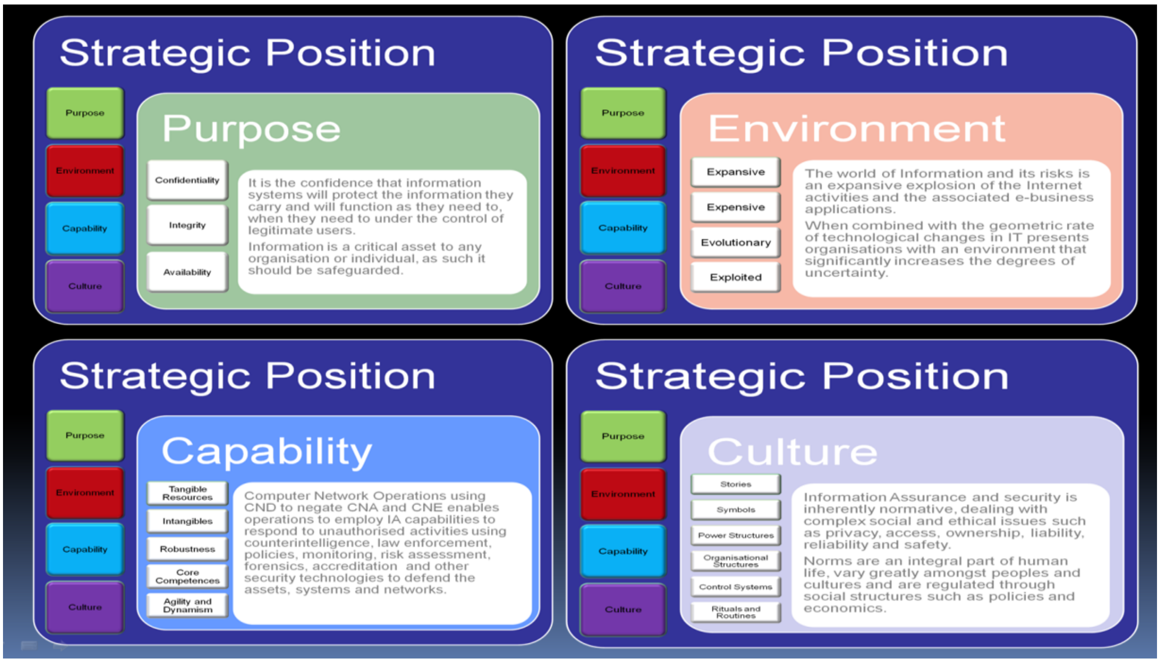
- *And review the roles of various actors (e.g. governments, service providers, academia, city since, etc) in promoting a culture of cyber security.*

(ITU, 2007)

At the national level, the ITU categorises it as a shared responsibility requiring coordinated action related to the prevention, preparation, response, and recovery from incidents on the part of government authorities, the private sector and citizens. At the regional and international level, the ITU has sought cooperation and coordination with relevant partners to formularise and implement national frameworks for cyber security and critical information infrastructure protection through a comprehensive approach (ITU, 2011). However, even this global cooperation has rooted misconceptions, misgivings, resistance and denial.

The urgency to control emergent cyber technologies, to manage access to sensitive and critical information infrastructures may be beyond the reach of the United Nations. NATO, as a military organisation has now taken a more prominent role (although not inclusive of many of the global players such as China, Russia, India and Brazil) in creating the direction and purpose of Cyber Power. However the US and UK (and many EU countries are beginning to) have made it their national priority. There are a plethora of Cyber Strategy Initiatives been produced by authorities, but only the US White House directives (Obama, The Comprehensive National Cybersecurity Initiative, 2010) have had the considerable financial resources to implement the strategies. The UK Government has shown a willingness to develop a comprehensive cyber strategy (Cabinet Office, 2010), it now needs to find the finance to fund its development and in particular in the research of new assurance techniques, trust management and IA Education to promote and sustain a new Assurance Culture.

2.4 Positioning Information Assurance at the Heart of Cyber Operations



Strategic Position

Purpose

It is the confidence that information systems will protect the information they carry and will function as they need to, when they need to under the control of legitimate users.

Information is a critical asset to any organisation or individual, as such it should be safeguarded.

Strategic Position

Environment

The world of Information and its risks is an expansive explosion of the Internet activities and the associated e-business applications.

When combined with the geometric rate of technological changes in IT presents organisations with an environment that significantly increases the degrees of uncertainty.

Strategic Position

Capability

Computer Network Operations using CND to negate CNA and CNE enables operations to employ IA capabilities to respond to unauthorised activities using counterintelligence, law enforcement, policies, monitoring, risk assessment, forensics, accreditation and other security technologies to defend the assets, systems and networks.

Strategic Position

Culture

Information Assurance and security is inherently normative, dealing with complex social and ethical issues such as privacy, access, ownership, liability, reliability and safety.

Norms are an integral part of human life, vary greatly amongst peoples and cultures and are regulated through social structures such as policies and economics.

Figure 26: Strategic Positioning of Information Assurance in the Business Process

The strategic purpose of employing Information Assurance to the Enterprise's Business Process (in particular to the processes of Information Asset Management, IAM) is to enable trusted transactions, storage (and retrieval) and CIS operations; harmonising the issues of interoperability and aligning processes across infrastructural domains and to ensure the protection of its intellectual and knowledge capital. Failure in inappropriate usage, deployment or implementation of employing Information Assurance Architectures (IA^2) can result in serious financial loss, reputational damage and stakeholder's value to the Enterprise, as illustrated in figure 26. Four components of the Thesis Methodology (Purpose, Environment, Capability and Culture) were based on the Johnson and Scholes' ***Exploring Corporate Strategy Model*** (Johnson, Scholes, & Whittington, 2008). The positioning of Information Assurance at the heart of Cyber (Information) Operations is this Thesis's business model and in particular how assured services, information and other assets flow between interoperating partners.

Understanding the needs of the User Community to seamessly transfer knowledge to provide Situation Awareness (SA) and Superior Decision making requires recipicol cognitation and understanding of the Information and Knowledge flows, content, structure and timeliness. Cyberspace provides a 3-Dimensional bridge (Visual, Innovation and Virtual) between the REAL and VIRTUAL Domains of Information flow, acting as the continuum between these two domain and transforming operations from a good to an assured state.

The desired future state of cyber operational security and the aspiration of most security organisations is the maintainance of their systems in a good state, fault & intrusion tolerant and resilient to purposeful attacks, natural events and fault conditions (error, fault, failure). The positioning IA strategy is to transform the system surviability (organisational responsiveness, agility and continuity, robust system architecture and tolerances, data dependability and operational / system safety) and its ability to provide Human-cyber interexchange (tusted, risked managed, secure and with appropriate protection) into an Assured State. The overriding purpose of positioning IA (as illustrated in Figure 27) at the heart of strategic plans for Information (Doctrines, Strategies and Operational policies) is to provide the Enterprise (its social-technical environment) the capability to withstand fault conditions whilst maintaining operational efficiency and value. Information Assurance has to meet the expectations of the DIME communities of interest and the greater global population that is becoming increasing reliant on cyberspace and the Internet of Things. In part this Thesis is attempting to create a culture change through its argued methodology, to adopt and develop its models.

The strategic position of Information Assurance and its Security Mechanisms within the UK Government and in particular the MoD has been recognised by the National Security

Policy (2010). The Government data structures, Information stacks, the knowledge and understandings that are exploited, the needs for, and keeping, qualified cyber operatives and the ability to achieve cyber situational awareness have now been recognised as Strategic Assets. These cyber structures and silos should be trusted and made safe, secure and available and where the failure to protect these assets would significantly impact on individual's lives, society and government functionality within the UK (CESG, 2007).

To qualify the significance of the Economic, Political and Military Values of the strategic value of the Information Assets (that we hold and use) we need to understand the benefits of the decision making process that enables Situational Awareness and the impact it has to our future.

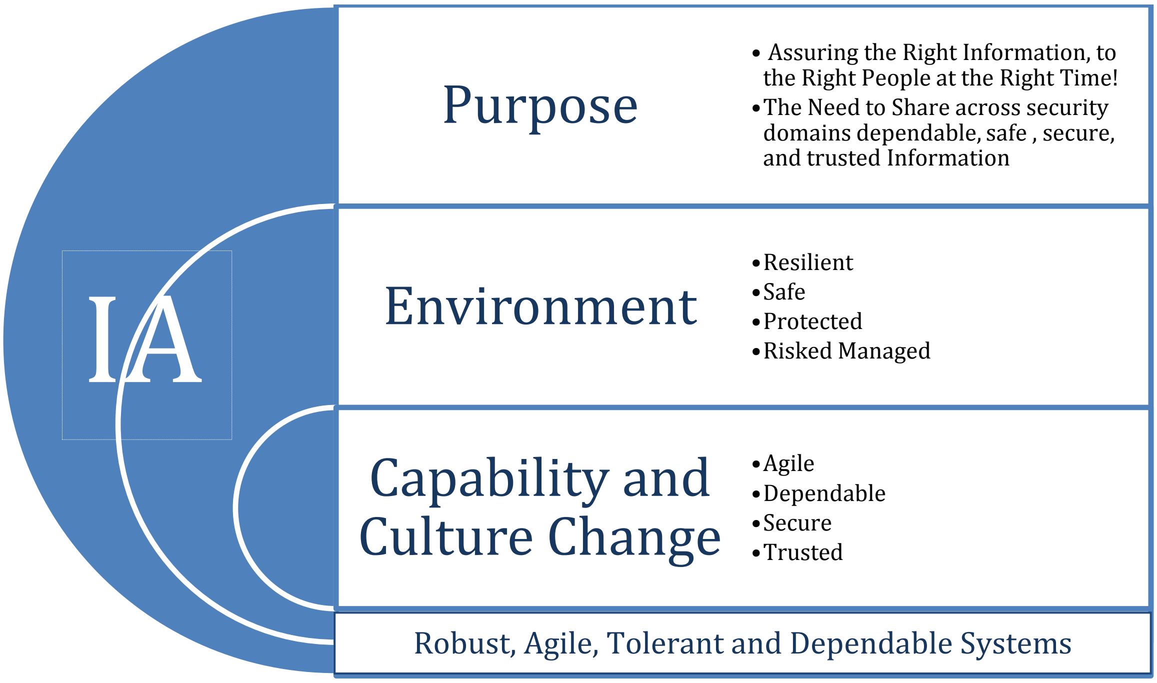

IA
Purpose
• Assuring the Right Information, to the Right People at the Right Time!
• The Need to Share across security domains dependable, safe , secure, and trusted Information
Environment
• Resilient
• Safe
• Protected
• Risked Managed
Capability and Culture Change
• Agile
• Dependable
• Secure
• Trusted
Robust, Agile, Tolerant and Dependable Systems

Figure 27 Strategic Goal of Information Assurance (Richardson C. J., 2008b)

We need to determine the impact of policies, doctrine and working environment, securing the department's strategic capability (offence, defence, resource and competences) and the expectation of politicians and the general public. Toffler (1991) expressed this as part of this Revolution in Military Affairs (RMA); however such a revolution incurs Enterprise risk. Risk Assessment, Analysis, Management and Exploitation should be directed, reassessed and processed throughout the revolving and evolving delivery of strategic, operational and tactical change (the changing Environment, Capability and Culture). Adapting the Johnson and Scholes (2008) Strategic Position Model.

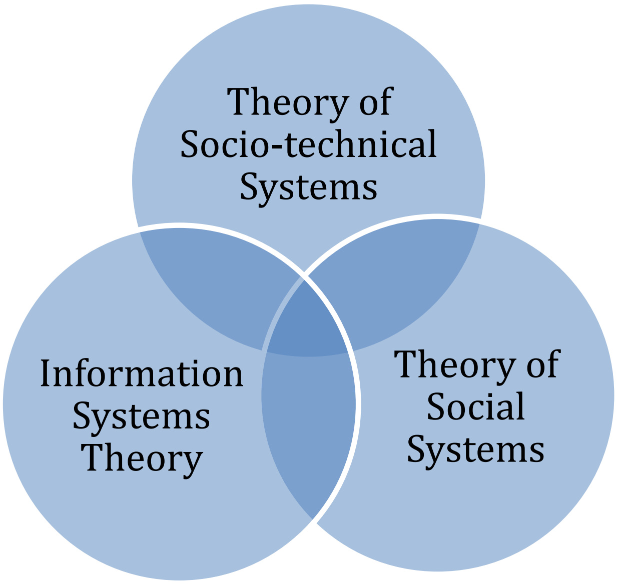


Figure 28: The Social Informatics Venn

The Strategic Positioning of Information Assurance within cyber policy and doctrine can be derived from the many attributes (Technology, Institutions and Culture) of the interdisciplinary study of Social Informatics[29] (Kling, Rosenbaum, & Sawyer, 2005). Applying assurance processes to design of information exchange (policy, economic or social context, education, media and electronic) in society and to the system functions (management, administration, economic, political and operational) of how information is used. The key concept of Social Informatics is that the social scientist view ICTs as a socio-technical network of artefacts, social contexts, and their relationships (Markus & Robey, 1988; Orlikowski & Iacono, 2001).

The Social Informatics Venn (see Figure 28) combines the Information Systems Theory[30] where every system is composed of information, processes and stores information, regardless of its media form (electronic files, quantum of light rays, wireless etc.) to the Theory of Social Systems and Theory of Socio-Technical Systems. This combination, incorporating system theory, information theory, quantum theory and a system theoretic metaphysics has developed the System Matrix Notation which reifies the concept of cyberspace as a tangible coherent space with a deep metaphysical structure and the development of Ogdoadic Concept Map (or Glyph) of the computational paradigm of systems and Cyberspace. The image of an ogdoadic system comprising elements of Information, Interaction, External, Metric Space, Idiom, State Space Internal and Experience as illustrated in Figure 29 has reposition segments in each inward iteration with the four model elements - information, idiom, internal and external - forming a conceptual foundation within which the inner squares arise

[29] Social informatics is the interdisciplinary study of the design, uses and consequences of information technologies that takes into account their interaction with institutional and cultural contexts.

[30] System Theory posits that everything is a system in the sense that the concept *system* can be applied to everything in a meaningful and practical sense. Every *thing* is a system that is composed of sub systems that interact to create that system and so too for each of these sub systems down to some *ground of being.*

(Anandavala, 2005). Professor Toshizumi Ohta (1999) suggested that following from Computational Theory (Carley & Prietula, 1994) that Social Informatics *employs an operational organization as a fundamental methodology.* This is revisited with the development of the Assurance Model in chapter 3.

The strategic alignment of the Ogdoadic Concept of Informatics to the Corporate Strategy Model (Johnson, Scholes, & Whittington, 2008) encompasses Purpose, Environment (external and internal), Capability (and idioms) and Culture. Moreover, an important observation of Professor Ohta, as illustrated in Figure 30 that the auto-genesis paradigm, a phenomenon with respect to human behaviour and social systems, helps to describe the organizing mode in a society (Ohta T. , 1999b; Ohta, Kazunari, & Isamu, 2001). Internet enabled actors can submit and receive multimedia, information and knowledge in ever greater quantities, generating shared situational awareness and cyber awareness. The methodology of operational organization provides visibility, connectivity and the development of the Information Stack.

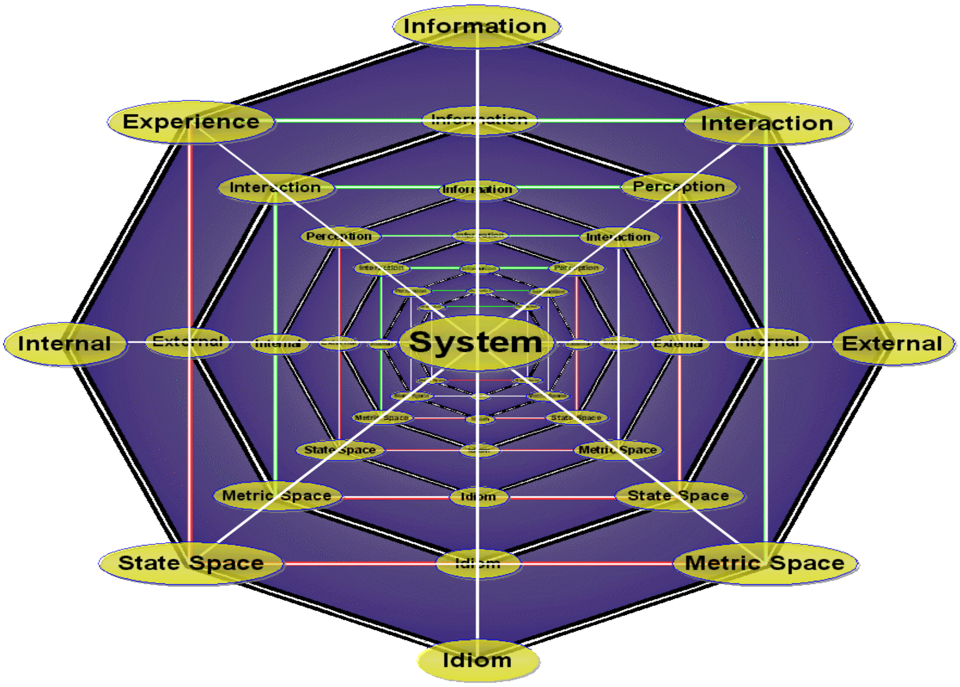


Figure 29: The Ogdoadic Concept Map of the Computational Paradigm

That the IA strategy model will require action (Processes, Resourcing, Practice, Changes and Organising) and that there are Strategic Choices (Enterprise, Foreign, Evaluation, Innovation and Departmental) will determine how expansive, economically, evolutionary and exploitive the assets can be processed securely. However, with the growing reliance of public sector organisations on information comes an increase in the impact of the post-delivery failure of the operational information infrastructure and elements of cyberspace. Information Assurance has to tackle many of the threat issues. The first component of the Thesis Methodology and the Johnson & Scholes Model is the concept of Strategic Purpose which encapsulates the organisations' vision, mission, governance and values. The roles and responsibilities of the corporate managers need to align to new business processes and assurance of the information flows and *this will raise issues of corporate social responsibility and ethics,* (Johnson, Scholes, & Whittington, 2008) *.*

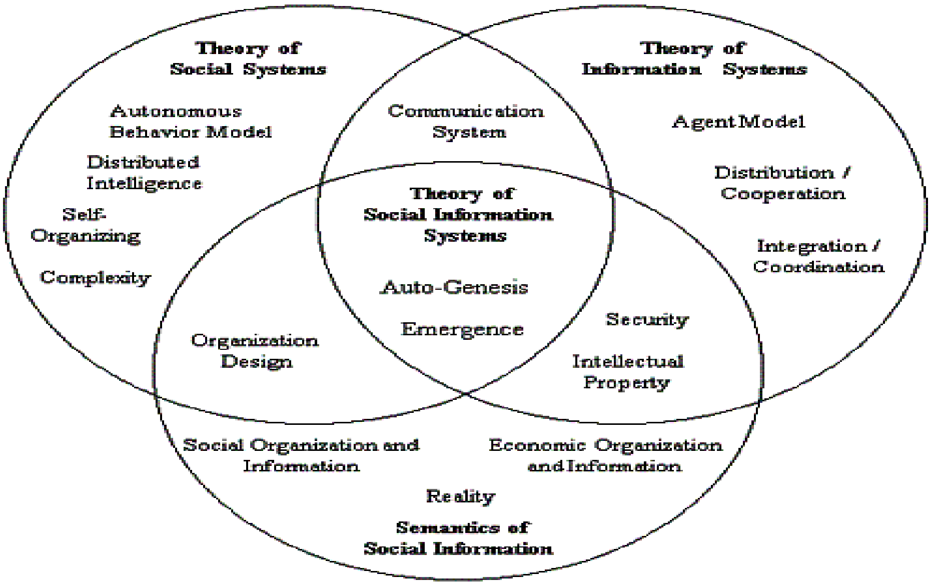


Figure 30: A Framework of Social Information Systems (Ohta & Yamamoto, 1995)

As an asset, information has 4 qualities:

- Information is about something (e.g. a passenger timetable)
- Information is seen as something (e.g. DNA or fingerprints)
- Information is used for something (e.g. algorithms or instructions)
- Information is placed in something (e.g. patterns or videos)

The flow of the military information assets across its 5 complex and inter-aligned domains (Land, Sea, Air, Space and Cyberspace) has to be first class service. Without the timely and effective use of information our commander's decisions may be become jaded, inappropriate or suspect. Consequently the IA purpose is that information has to be clear, accurate, trusted and not compromised, lost, leaked, disseminated, unauthorised, published or corrupted. In positioning IA, the strategic purpose is to: *provide an Information Assurance Capability that will facilitate Cross –Domain Solutions. This capability will need a framework that formulates the assurance implications of interoperability within cyberspace, human factors, protection of networks and secure* *data content, alignment of enterprise architecture, any organisation culture changes, information exploitation, management and service dependability from bridging the air gap between highly classified networks and possible interaction with lower classified networks and the Internet and how it might be done.*

Information Assurance manages the risks to Government, Enterprise and Individual information and its security component (its 3 tenets of Confidentiality, Integrity and Availability- CIA) provides the necessary purpose and confidence that our information systems will protect the data, information and knowledge that they handle and will function as they need to, when they need to, under the control of legitimate users. This confidence is becoming increasingly important and IA is an essential enabler of the Transformational Government vision, as recognised by the UK National IA Strategy (2007). The contextual strategic environment for the positioning of IA within the organisation is under constant change owing to the complex Diplomatic (political), Intelligence, Military and Economic (DIME) usage of Information around the social-technical changes of the Enterprise, its mission and its legal framework. Furthermore has skills and awareness changes in the workforce, these will result in emergent changes to the environment and its system domains. These inter-aligned domains have a complex PESTEL[31] context to a risky world of expansive utilization of the assets, infrastructures and the many pervasive technologies and application. There is ever increasing, explosive usage of Internet PESTEL activities and associated e-business applications. The rate of change, its evolution has major impact on the structure and new direction of the MoD (Strategic Defence and Security Review, 2010)

IA Capability has two main components:

1. System Survivability, and
2. Cross-Domain Solutions

The greater part of the strategic capability of Information Assurance has been discussed within Chapter 3 and the cross-domain solutions for system interoperability. One of the four Engineering Aims was to create a contextual framework for the strategic positioning of Information Assurance that will provide an assured CIS environment (see figure 89) and a capability to provide resilient and dependable services across a secure and protected (critical) information infrastructures. These

[31] PESTEL – Political, Economic, Social, Technological, Environmental (green) and Legal

capability requirements are discussed as elements of a Defence Jigsaw, which when combined provide an integrated model for the strategic positioning of IA for System Survivability and Cross Domain Solutions (System Interoperability). Culture change is necessary, since the publication of the National Information Assurance Strategy (Cabinet Office, 2007) there has been significant strategic drift and a failure to create necessary changes. The National Security Policy Framework (Cabinet Office, 2011) has produced a correction to this drift but the initiative is under resourced (there is insufficient skilled practitioners working in the UK) and underfunded. The process of cultural change is not a primary focus of this thesis; however its paradigm influences every aspect of information assurance, from an historical, organisational, ethical and psychological perspective. The impact of culture needs to assessed in any assured environment and the Johnson and Scholes model provides a useful methodology to examining and analysing the effects of cultural change using a Culture Web. By analysing the factors in each Venn sector as illustrated the analysis can see what is working, what isn't working, and what needs to be changed.

The Cyber Defence Jigsaw

The four methodical components (Purpose, Environment, Capability and Culture) provide a firm foundation to build a conceptual Strategic Information Assurance model and the established corporate cases that used the Johnson & Scholes contextual model has created additional credibility and capability for the IA model's development. However, to make the positioning model more specific, manageable and utilitarian, the conceptual model needs to encapsulate the social-technical issues of an assured CIS environment.

Securing Cyberspace with technology and policies to provide Cross Domain Solutions requires a practical development of the Information Assurance Model and methodologies that will provide assurance both to the IX and IO components of the Information Stack (as discussed in chapter 3). For the MoD, the Information Security element of model also needs to meet the define roles and responsibilities of its Security Officers and the accredited system security policy (JSP 440). The influence of the Assurance components (Structured, Dependable, Secure and Trusted attributes) can be mapped to the four elements of the CIS environment (Communities of Interest, Systems, Networks and Facilities) as illustrated in Figure 31. The four anchoring pivots (Data Security and Access Security Mechanisms, and the roles and System Security Officer and Network Security Officer) of this assured model provide a chain of responsibilities and activities across the 4 domains (System, Network, Facilities and Communities of Interest). Over layering these 4 domains are the 8 components of Information assurance (Architecture, Resilience, Dependability, Safety, Security, Protection, Trust and Risk Management).

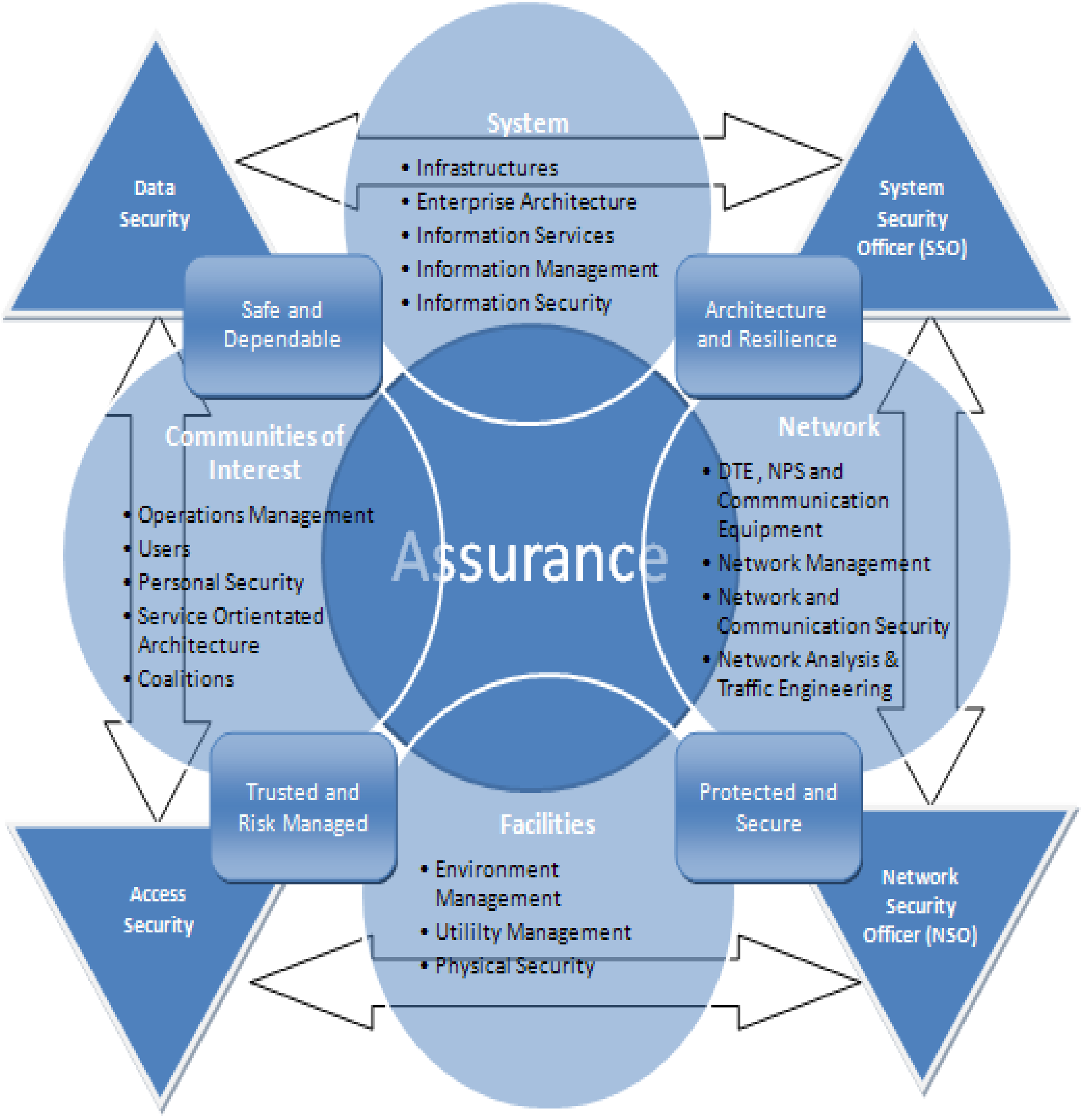


Figure 31: The Alignment of the Information Assurance across the CIS Domain

The alignment of the information assurance can be interpreted from the observation of the four lines of interoperability. For example the interaction of Data across the System Domain is managed by the System Security Officer who is responsible for the system architecture (its compliance and accreditation), its resilience (the system tolerances and continuity) to ensure data dependability and operational safety. This operation manages the flow of data through the information stack (the Information Technologies deployed, the supporting Information Infrastructure, the Services allocated, the conformity and compliance Management procedures and practices and the exploitation of the information for knowledge transfer and shared situational awareness. The logical and risk conditions of the model needs to be tested within a cyber-range using corporate simulations and exercised by some penetration and fault testing. The conceptual component of this model is examined in chapter 3.

The Perceived Risk to the Assured CIS Domain

The Technological revolution that has radically changed the worlds of Communication, information-processing, health and transportation has eroded borders, altered migration and allowed individuals the world over to share information at a speed inconceivable two decades ago. **United Nations, 2004**

Another component of the Cyber Jigsaw is the perceived cyber risk (degrees of expected and real Threats, Vulnerabilities and Impact to information systems and their provided services and data storage) and its effect on Government, Business, Society and the Military (Vatis, 2001; Whitman, 2004; and Jakobsson & Zulfikar, 2008) masks the actual risk (Schneier, 2006, Robert, 2006 and Jaquith, 2007). Cyber threats and the risk to information infrastructures cause Fears, Uncertainties and Doubts (FUD) in Governments and the Online Communities. Until recently (Estonia, 2007 and Georgia, 2008), there have been few explicit public examples of network catastrophes or national infrastructure exposures which can be easily attributed to Cyber War (Puran, 2003 and Baker, Waterman, and Ivanov, 2009). Analysis of cyber threats and cyber security appears to over emphasise the smart (but limited) impact of Cyber War (Paquet and Saxe, 2005) in attacking national (information) infrastructures (Jackson et al, 2007 and Jaquith, 2007), describing most incidents as simple criminal activities that intimidate citizens and e-commerce. Furthermore most nations are more robust and resilient to these threats:

To understand the vulnerability of critical infrastructures to cyber-attack, we would need for each target infrastructure a much more detailed assessment of redundancy, normal rates of failure and response, the degree to which critical functions are accessible from public networks and the level of human control, monitoring and intervention in critical operations. **(Lewis, 2002)**

However, in 2010 Western Governments and the United Nations have escalated the potential damage to society of these Cyber Threats and have started to expose critical Infrastructure damage, cyber war and cyber terrorism scenarios (President Obama, 2010 and Fowlie 2010). The US Defence Department has investigated about 250 *"serious, sophisticated*" cyber intrusions into government networks and have concluded that these threats were so severe that they now designating cyberspace as a fifth domain of warfare. The US Attorney-General, Robert McClelland, said that *"It's very difficult to identify the source of attacks; often they can be routed through other countries or other players*." In April 2010, China Telecom briefly rerouted Internet traffic destined to some highly sensitive US websites, effectively hijacking the Internet. This was reported by the US-China Economic and Security Review Commission who stated that the Chinese Telecom Company sent incorrect routing information destined for the websites of the US Senate, the Office of the Secretary of Defence, NASA and the Commerce Department, but they were not clear whether it was unintentional or had intent. The US Defence Secretary Robert Gates warned that cyber-attacks posed a huge future threat and urged more joined-up efforts between the US military and civilian agencies (BBC, 2010).

The UK's National Security Strategy (Cabinet Office, 2010) has stated that Cyber Attacks to be one of the biggest security threats facing the nation and has categorised it as a Tier 1 threat, paring international terrorism and major accidents. HMG's Technical Authority to Cyber Defence and Information Assurance, The UK's Communications Intelligence Agency GCHQ, indicated the scale of the problem to the National Information Infrastructure (NII) when its Director, Iain Lobben, revealed "*that each month more than 20,000 "malicious" e-mails were sent to government networks, of which 1,000 were deliberately targeted at them.*" Lewis (2002) argues that: *The lines between domestic and foreign, private and public, or police and military are blurring, and the nature and requirements of national security are changing rapidly. The most important implications of these changes for cyber security may well be that national policies must adjust to growing interdependence among economies and emphasize the need for cooperation among nations to defeat cyber threats.* The World Summit on the Information Society (WSIS 2003) *recognized the real and significant threat posed by inadequate confidence and security in the use of ICTs and the proliferation of cybercrime.* This universal recognition of the ubiquity of Information, its pervasiveness in society, the failing to protect the privacy of this asset has led the UN to produce the Global Cyber security Agenda (GCA) as a framework for international cooperation on cyber security[32]. The Vulnerability (and hence the risk) of the National Information

[32] UN General Assembly has outlined elements for creating a global culture of cyber security through several resolutions, including: resolution 64/L.8 (2009)***'Creation of a Global Culture of Cyber security'*** (Second Committee) and Resolution 64/L.39 (2009) ***'Developments in the field***

Infrastructures has increased with the ubiquitous computing environment; the internet of things; cloud computing and mobile data mash ups that are constantly being exposed and threaten with the plethora of daily online activities that have become automated.

The (embedded) microprocessor and Hybrid market is far greater than the PC market and possible Cyber-attacks like chipping (King, *et al*, 2008 and Adee, 2008) in this space are causing great concerns to businesses, critical infrastructure providers and Governments. The UK's Foreign Secretary William Hague said that, unless addressed, this could threaten the UK's "*economic welfare*". The risk is greater where there has been a vast growth and reliance to remote computer networks access, particularly by the mobile phone networks and other wireless systems (WiFi, WiMax, LTE, etc.) and is of particular concern to military authorities who have service NGO VPNs. Furthermore with the malware such as the smart targeted Stuxnet Virus there is an increased worldwide hacking vulnerability to industrial and infrastructure applications as illustrated, especially those used for SCADA (Supervisory Control and Data Acquisition). The global shift from proprietary networks to using the insecure open access TCP/IP Internet based operations has over the past 25 years created extensive avenues of inappropriate access. Information Assurance and network security; law enforcement and cyber defences have to become more effective to ensure that critical and national infrastructures are robust and resilient. Modern threats are more blended attacks as figure 32 illustrates from its first wave hacking of individual PCs to mass attacks on the mobiles and the internet of things. Assuring the Internet will be a long and probably impossible process, but the first steps are being made and if more national resources become available, just maybe we might start closing some doors.

Information Assurance is defined in HMG IA Standard No 2 Risk Management and Accreditation of Information Systems (v 3.1 October 2008) as '*the confidence that information systems will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users'*. The definition's language was derived from a CESG's security perspective (the tenets of security are Confidentiality, Integrity and Availability) rather from a more (a) purposeful and holistic perspective of applying (b) trustworthy capabilities to Information Operations and Information Asset Control, (c) creating a trusted environment to operate and

of information and telecommunications in the context of international security' (First Committee) maintain the critical information infrastructures and the business processes that rely upon these infrastructures and (d) to change the culture of the enterprise to become more efficient, compliant and risk mitigating. Building the necessary architecture to mitigate the risks to the vulnerabilities and potential threats to the Enterprise, its CIS domains and Information Operations will require a number of integrated analytical and evaluation processes.

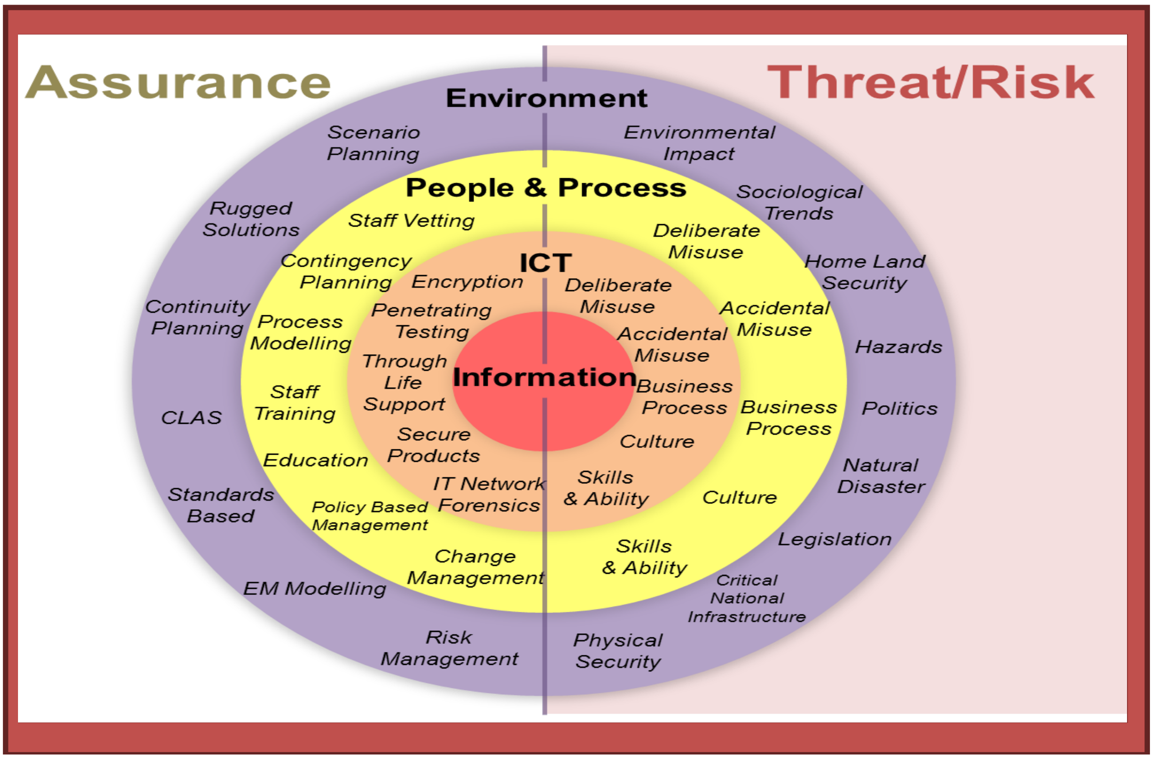


Figure 32: The HCI of Assurance and Potential Threats (Richardson & Sinderberry, 2008)

The above figure 32 illustrates the enabling activities (Environment, People & Process and ICT) that surround the management, control and usage of Enterprise Information and the constant pressure on Assurance practitioners, employees and executives to mitigate the threats and risk to the Enterprise. The figure illustrates the complexity of the task involved in Assuring the Enterprise Information owing the numerous issues highlighted that are often loosely coupled creating further emergent (and often unknown) properties. Understanding what to align within the Assurance process is critical to the success of its implementation. Any failure, omission or delay may result in a vulnerability that can readily assaulted by CNA and CNE. The purpose of the strategic IA model is to give direction, governance and maturity to the Enterprise, its board members and employees. Its mission is to provide a structured; resilient; dependable; safe; secure; protected; risk managed and trusted usage of its CIS domain.

The Strategic IA Model

"Information is a significant component of most organizations' competitive strategy either by the direct collection, management, and interpretation of business information or the retention of information for day-to-day business processing. Some of the more obvious results of IS failures include reputational damage, placing the organization at a competitive disadvantage, and contractual noncompliance. These impacts should not be underestimated." **The IIA Research Foundation**

The military have many strategies, and those centred on Information Superiority and Information Operations (IO) are fluid at best. Information Operations is essential for the successful execution and efficiency of military (joint) operations. The US Military have drafted a new Information Operations Doctrine which emphasises its pillars (the domains that IO owns) and its core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security as illustrated in figure 99. The strategic importance of Information Assurance is that these operations are conducted with trustworthy devices, technologies, networks, infrastructures, systems, services, applications, data storage and retrieval, architectures, policies, procedures and good practice. IA has complex and daunting requirements to fulfil. The UK's military domain security framework (MoD, 2010) has structured Information Assurance to provide trustworthiness to (almost) all components (except CIS Resilience and Document Security) of its CIS Security Framework. Resiliency is the ability to avoid, minimize, withstand, and recover from the effects of adversity, whether natural or manmade, under all circumstances of use and consequently when it is applied to the Cyberspace, it becomes a constituent component of Information Assurance. Critical Information Infrastructures (CII) requires resilient and tolerant architectures which are trustworthy under operational stress and assures high availability, continuous operations, and disaster recovery. Information operations within the Government, Industry and Military sectors are diverse and complex. These CII operations have independently expanded into loosely couple arrangements (often with controls or strategic architecture) and evolved into large systems of systems with many producing (and often unknown) emergent properties; creating new vulnerabilities and attack vectors. Normally these integrating operations have operated satisfactorily in loosely coupled arrangements. However, for these operations to be resilient under stress, more than loosely coupled arrangements are needed. The strategic positioning of Information Assurance will need to define the engineering challenges of resilient, fault and intrusion tolerant socio-technical

Enterprises. Operational recovery time (a service objectives) to adverse effects among the DIME sectors must be coordinated, interoperability of information sharing and platform operations must be assured, distributed supervisory control protocols must be in place, and operation sensing and monitoring must be embedded. These capabilities cannot be expected to evolve in a loosely coupled environment. They must be holistically specified, architected, designed, implemented, and tested if they are to operate with resilience under stress. A management, process, and engineering maturity framework is necessary to advance the assurance of software security, business continuity, system survivability, and system of system resiliency capabilities. From a strategic IA point-of-view, HMG needs to impose a maturity framework for guiding CII operations and interoperability. Such a framework should develop the future evolution of our Critical Information Infrastructures along the lines of common management, process, and engineering dimensions whose collective result would be a harmonious operation and resilience even under stress among these systems. Assuring resilient CIS domains under stress should be organized as a 5 level maturity model (as illustrated in Table 4). The objective is to drive the business case of CII operations and produce an enterprise commitment to achieve the goals of each level (2 to 5) and build upon them as indicated:

Level 1	Ad Hoc- State of Affairs: Inability to advance and exhibiting evidence of apathy, denial, management inaction, and lack of IA engineering know how
Level 2	Enterprise Assurance Commitment Management- Goal: Demonstrate commitment to Information Assurance through strategic management, harmonised interoperability, internal processes, and defence in depth.
Level 3	Enterprise Business Continuity Process Maturity- Goal: Demonstrate business continuity assurance through compliance and configuration management, accreditation, external standards and product engineering.
Level 4	System Survivability Engineering- Goal: Demonstrate the achievement of system survivability through the management of faults and failures, sustainability processes, aligned CDS and IA best practices.
Level 5	System of Systems Resiliency Engineering- Goal: Demonstrate the achievement of cross-domain resiliency through the management of external interactions and dependencies, the control of distributed supervisory processes, and the practice of Next Generation, High Assurance software engineering.

Table 4: IA Resiliency Maturity Model

Information is both an asset and potential liability to its owners. HMG's Information Governance policies have established that (Government) Departmental Accounting Officers (AOs), through their Senior Information Risk Owners (SIROs) and their Information Asset Owners (IAOs) are to become accountable for the adequate protection of their information (collected, processed and stored) within their

Departments. Consequently these AOs will need to introduce holistic Information Assurance policies, procedures and practices that include effective Business Continuity Plans, Information Risk Management (IRM), Security Information and Event Management (SIEM) and a culture change programme of IA awareness, adaptation and compliance. This introduction to IA and its compliance has been encapsulated in the CESG Information Assurance Maturity Model (IAMM) as illustrated in table 5.

IA	Process	Level 1 – Initial	Level 2 – Established	Level 3 – Business Enabling	Level 4 – Quantitatively Managed	Level 5 – Optimised
Embedding IRM Culture Within the Enterprise	**Leadership & Governance**	Board recognition that information is a vital business asset and IA is an integral requirement of corporate governance.	Board members understand and accept their responsibility for IA implementation	Board exercising due diligence to the effective discharge of IA	Board monitors progress towards embedding IA policy across the Dept.	Assured Department's Information and its external stakeholder's key business asset are fully embedded within the Dept's culture and are subject to a regime of continuous improvement.
	Awareness Training, & Education	A programme of annual information risk awareness training is instituted	Dept. personnel undergo annual risk awareness training	A programme of pre-appointment training is instituted for all staff	Accurate details of training received by all staff are collated and reported	
	Information Risk Management	A comprehensive information risk policy is in place.	The Accreditation status of all existing CIS is determined and the information risks are identified within risk registers	All CIS that are critical to the business have been subject to Accreditation	Residual risks are to be tolerated and quantified. The Main Board is fully aware of the total level of risk involved.	Risk exposure of the Department is within Its risk appetite
Implementing Best Practice IA Measures	**Through-Life IA Measures**	Required to take a coordinated and systematic approach to through-life IA measures.	The status of the through-life IA measures employed across the Department is determined and gaps are identified	Systematic, through-life processes are in place to assure all IS which are critical to the Dept.'s business.	Level 3 processes are extended to embrace all of the Department's IS.	Incident and problem management processes adapt to new risks and problems.
	Assured Information Sharing	Required to define and manage how information is shared across the Department's boundaries	Network boundaries are defined and policies for sharing and managing information across these boundaries	A comprehensive protective monitoring regime is implemented to provide situational awareness and enable essential information flows to be maintained.	Level 3 measures are extended so that incident mgt. moves from being reactive to proactive.	Network boundaries and the associated protective monitoring regime is continually improved to reduce the departmental and collective, shared exposure to information risk.
Effectiveness	**Compliance**	Established compliance regime to confirm the effectiveness of IRM against mandated (minimum) standards. Annual Reporting	The Dept. has a comprehensive IRM compliance regime. They have an External IA Review	Critical IA Review and internal audit Recommendations are actioned and progress tracked.	IA incident mgt. processes are fully assured by internal audit. The Main Board is aware of the significant areas of the Department's non-compliance	There are no critical or significant IA audit issues. Independent assessment of the Department's approach to IA shows that it is aligned with the National IA Strategy.

Table 5: Abridged CESG Information Assurance Maturity Model (Cabinet Office, 2010)

These AOs need to assure their arrangements sufficiently reveal any business impact upon the on-going programmes in Transformational Government (Cabinet Office, 2005) and their Department's information risk as directed under the HMG Security Policy Framework (HMG SPF, 2010). CESG had also imposed an Information Management Maturity Model (IMMM) to measure compliance by Department Chief Information Officers (CIOs). However a number of the IMMM objectives have been swept up by the current IAMM and the publication of Good Practices such as the MoD's JSP 747. Although the IAMM (Version 4.0) has a considerable list of Departmental requirements and compliances, many of its practitioners will find evidence for upwards grading with little oversight from its auditors, the National Audit Office. Consequently the current maturity model is probably flawed, as it is a top down approach and juniors always want to paint a positive picture to please their seniors (a very common problem within the military where Captains are established as ITSOs in establishments with many senior officers flaunting or ignoring best practice) and can be considered as nothing more than a check list. Information assurance is everybody's responsibility and therefore a non-hierarchical approach must be used for its compliance.

One of the most significant transformations in the S*tate of Art* of Cyberspace has been the blurring of the lines of demarcation across network boundaries in joint actions, coalition partnership and the Internet of Things. Consequently these IA maturity models need to evolve, but this requires agile movement of the goal post which is often counter-productive (most people resist change, in particular any change to their normal operations) in most organisations. Information Assurance has to establish a new cultural awareness that promotes change. Future internet and System of Systems research will require a much wider remit than just for networks and transportation (ISO Model Layers 1 to 4). It will need to encompass domains previously seen as purely application areas, for example, like information access, processing and human-cyber interfacing (layers 5 to 7). Models work when their user community engage in their usage…getting them to engage is a priority!

Human Factors of Assurance

> *"The internet has the potential to become a ubiquitous and universal channel for socializing and creative expression"* **(European Commission, 2010)**

The Internet is both Diverse and Inclusive, just about anyone with network connectivity can "*surf the net*" but there still is a social divide with those without connectivity (or with those who refuse to connect). This globally homogenous network of networks has expanded and evolved with technology advances, organisational needs and user demands. The semantics of the socio-technical domain has changed with the each iteration of the world-wide-web, (Spivack, 2007). However, greater inclusivity also constitutes a greater risk to the online community and it's Assurance

One of the most important Human Factors in the socio-technical Enterprise is the concept of Trust. Psychologists have had difficulties to precisely define Trust in its social context, but as an Assurance Dimension it has become an increasing important design issue and an operational necessity (Michael, Hestad, & Pedersen, 2002).

Research has shown, "*if trust is not present, if there is no confidence, expectation, belief and faith in an information system, then there will be no willingness to rely on any such system,"* (Chopra & Wallace, 2003).

In developing trust in Cyberspace the human factors involved are both contributionary to the society and also can become anti-social, criminal or offensive. The moral and ethical conduct of individuals online has little policing and little political will to police the internet (Jewkes, 2003). As the internet expands more criminal activity is noted; as it evolves, a new conjunction of criminal opportunities arise and as it becomes more exploited, more online crimes are committed. *We need to examine features of the components of cyberspace to determine the extent to which people will have greater predispositions to crime, new resources available to them to commit crime and many other factors. At the same time, we need to assess the extent to which those who develop the new cyberspace systems have incentives to adopt measures that will make cyberspace less attractive for criminals and crime promoters (those who make crimes more likely, for example, by providing 'inside information', passwords, tools, incentives and encouragement, etc., or merely by being careless with their own security) wherever they are found.* **(Collins & Mansell, 2003)**

As figure 33 illustrates, a key consideration from the IA perspective are the causal relationships between the components of cyber trust and e-crime prevention, and in particular the development of an understanding of the causes of crime in the Cyber Domain (Collins & Mansell, 2003). The Social Values of the Communities of Interest (COIs) place considerable influence and expectations to the equality and diversity of the IA Trust Dimension, entrusting the integrity of the services, security of transactions and the privacy of the information used, stored or transmitted. The figure depicts some of the key components and issue areas in the cyberspace system. Each of these is recursively related to the others, forming a highly complex system that is populated by many different agents, both human and non-human.

The local social relationships have been expanded by the process of Globalisation and international virtual communities that have reshaped DIME strategies and linked individuals to a common cause, event or culture. Technical innovation of Information Technologies and IT Services have open new inclusive communities for collective thinking, sharing and knowledge transfer creating new requirements and paradigms for online social morality and ethics.

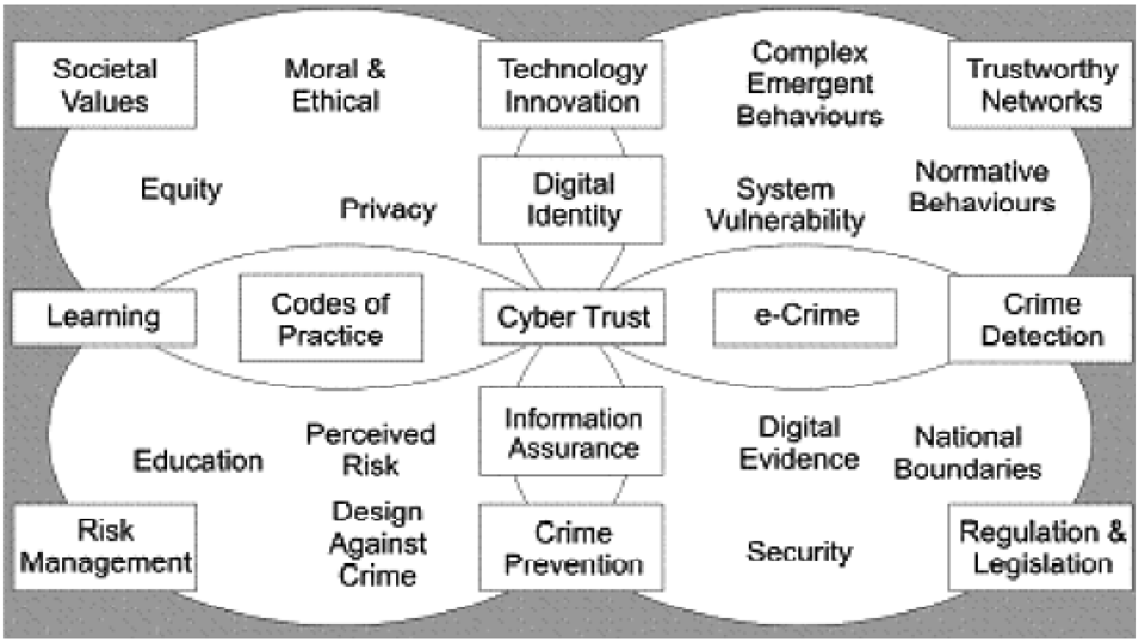


Figure 33: Cyber Trust and Crime Prevention-Web of Components (Collins & Mansell, 2003)

These new standards require better models, interpretation and an inclusive code of good practices that can be championed by all online users. In many aspects we are just beginning to learn what our trusted socio-technical enterprises are capable of and these emergent properties acquire further research and development. To entrust the Information Domain, the communities and enterprises have to understand the risks involved in the virtual environment and the processes it supports. Risk Mitigation and Enterprise Risk Management (ERM) are other important aspects of Information Assurance which requires awareness, training and education. In particular, understanding the problems of residue risk, perceived risk and actual risk is necessary to all users. Too many enterprises are either complaisant to regulatory standards or ignorant to their vulnerabilities as risk assessments have become automated to the compliance of check boxes rather than investigating and understanding the actual risks involved, (Grossack, 2012).

Creating Trustworthy networks, the system designers and equipment manufacturers are implementing the need of enterprises through technologies and infrastructures. However, very little has been done in creating an assured architecture in the engineering of theses system; in particular in the research of IA Architecture in System Engineering and experiments of assured system of systems designs on cyber ranges. More research is required in understanding the system vulnerabilities, the emergence of complex behaviours and a better understanding of system and human normative behaviour whilst online. This research will help provided a more trustworthy environment, innovative assured technologies and secure our digital identities.

To create trust in Cyberspace, Information Assurance has to provide strategies, governance, policies and mechanisms that can detect e-Crimes, cyber-attacks and malicious cyber network exploitation. The IA Models and implementation need to provide the authorities preventive and tolerant capabilities, the ability to gain and analysis digital evidence and create secure operating domains within the current regulatory and legislative environment. Trust in Cyberspace shouldn't be taken for granted; it requires Assurance to make it trustworthy and commitment to make it resilient, dependable, safe and secure.

The Model has a cyclic activity rotating the roles of Assurance Practitioners to the System, Network, Facilities and Communities of Interest domains and the interspersing (Purpose to Systems; Capability to Networks; Environment to Facilities and Culture to Communities); interrelationship of the Human-Cyber Interexchanges (IERs and Essential Elements of Friendly Information – EEFI); interdisciplinary (Engineering, Psychology, Social Science, Law and Business) domains of strategic management. This rotational process recognises the dependencies (and interdependencies) between systems and critical information infrastructures and the importance to achieving (and /or undermining) cross-domain solutions for resilient safe, secure and dependable operations. This is an important strategic component of Information Assurance and there are considerable research avenues (in particular those conducted by Professors Robin Bloomfield and Kevin Jones at the Centre for Software Reliability, City University London) been explored to determine the consequences and complexities of dependability between cyber domains and the cascading effects that occur as systems fail (Al-Kuwaiti, Kyriakopoulos, & Hussein, 2009; Bloomfield, Buzna, Popov, Salako, & Wright, 2010). Having safe (available, useable, maintainable and scalable) operational processes that the user communities can rely upon (trusted, secure and protected) is a further dimension of Assurance that needs to be researched, in particular to system functionality that can gracefully collapse (rather than crash) to error, fault and failure conditions, becoming resilient and tolerant to cyber-attacks and intrusions and having robust critical infrastructures that survive and provide business continuity.

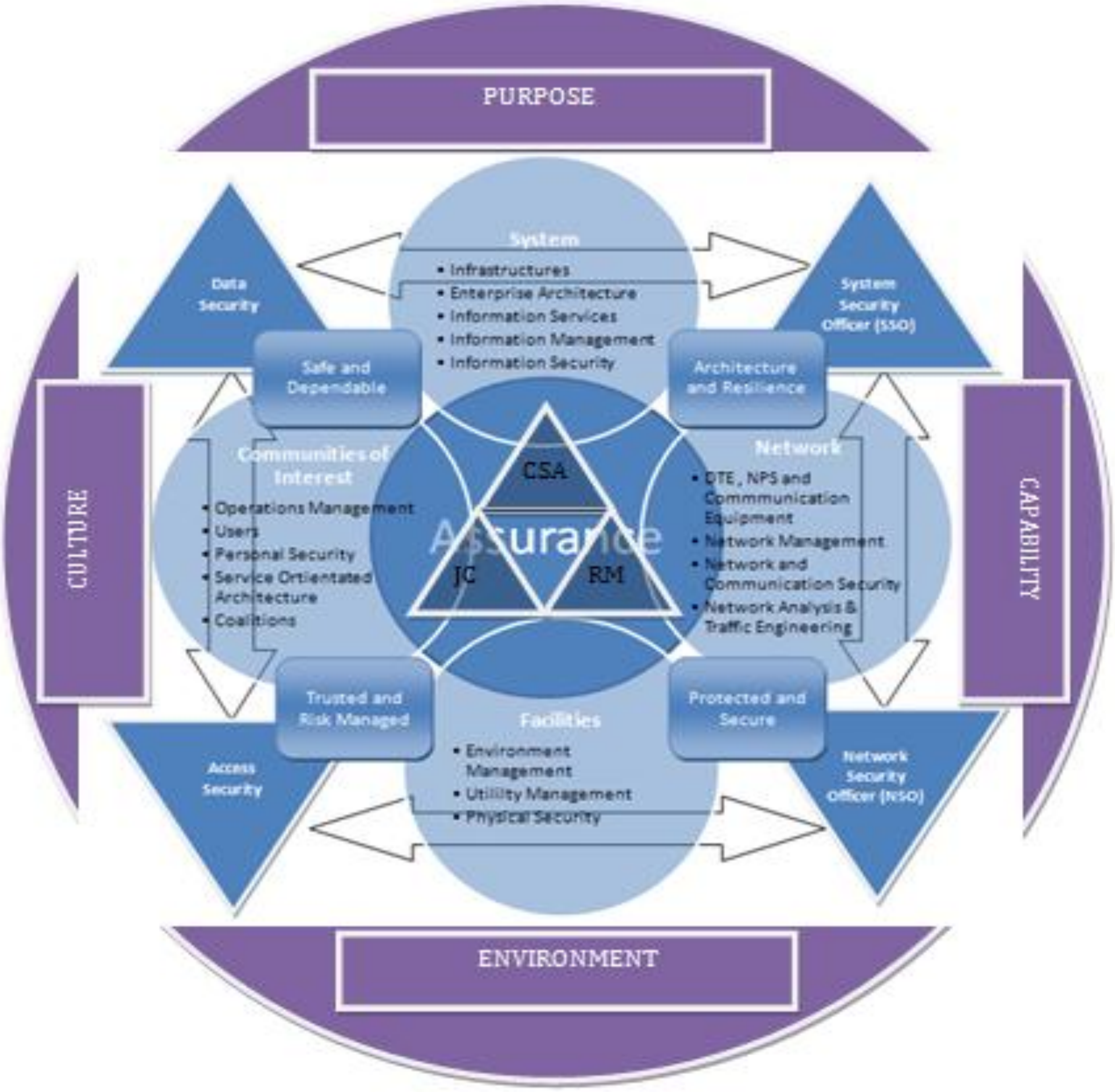


Figure 34: The Composite Strategic Information Assurance Model

The current IA maturity model is highly focus on Information Risk Management (IRM) and largely misses the more important elements of Trust Management and this thesis recommends an improvement to the model as illustrated in Table 10. The IAMM does however recognise the equally important measures required for people awareness, training and education. The Government now needs to quantify and qualify what are acceptable Training and Educational Standards and publish the National Occupational Standard (NOS) for Information Assurance. The jigsaw has many important components to cover the capability gaps we have in our systems. In particular to the alignment of the 8-Dimensions of IA is need to find Cross-Domain Solutions, System Tolerance, Risk Mitigation, Compliance and maintenance of Shared Situational Awareness. This creates additional, but necessary, complexity to a highly integrated, relational concept.

Table 6: The Extended Enterprise Information Assurance Maturity Model

IA	Process	Level 1 – Initial	Level 2 – Established	Level 3 – Business Enabling	Level 4 – Quantitatively Managed	Level 5 – Optimised
Embedding IRM Culture Within the Enterprise	**Leadership & Governance**	Executive recognition that information is a vital business asset and its assurance is required by governance.	Executives understand and accept their responsibility for IA implementation	Executives exercising due diligence to the effective discharge of IA	Executives monitors progress towards embedding IA policy across the Dept.	Assured Enterprise Information and its external stakeholder's key business asset are fully embedded within the Dept's culture and are subject to a regime of continuous improvement.
	Awareness Training, & Education	A programme of annual information risk awareness training is instituted	Enterprise personnel undergo annual risk awareness training	A programme of pre-appointment training is instituted for all staff	Accurate details of training received by all staff are collated and reported	
	Information Risk Management (IRM)	A comprehensive information risk policy is in place.	The Accreditation status of all existing CIS is determined and the information risks are identified within risk registers	All CIS that are critical to the business have been subject to Accreditation	Residual risks are to be tolerated and quantified. Executives are fully aware of the total level of risk involved.	Risk exposure of the Department is within Its risk appetite
Information Exploitation (IX)	**Enterprise Information Management (EIM)**	Enterprises attains some awareness about information management Establish and redefine its current Service Level Agreements.	Enterprise and IT leaders react favourably to the demand for consistent, accurate and faster information across key business units.	Enterprises perceive and qualify information as necessary for improved business performance and optimisation. Monitor Service Level Agreements.	Enterprises perceive information as critical for business. The organization has implemented significant portions of EIM, including a consistent information infrastructure	Enterprises exploit information across the entire information supply chain, with service-level agreements that are continuously reviewed
	Information Services	Technical - Communication protocols exist	Syntactic - Introduction of common IERs.	Semantic – Introduction of ITIL	Pragmatic – Embedded SOA Meta-tagging Documents	Dynamic – Fully realised socio-technical IS systems.
	Interoperability	Isolated (manual)	Connected (peer-to-peer)	Functional (distributed)	Domain (Integrated)	Enterprise (Universal)
	Data Quality	Uncertainty	Awakening	Enlightenment	Wisdom	Certainty
Implementing Best Practice IA Measures	**Through-Life IA Measures**	Required to take a coordinated and systematic approach to through-life IA measures.	The status of the through-life IA measures employed across the Department is determined and gaps are identified	Systematic, through-life processes are in place to assure all IS which are critical to the Dept.'s business.	Level 3 processes are extended to embrace all of the Department's IS.	Incident and problem management processes adapt to new risks and problems.
	Resilience & Sustainability	Required to define and design a resiliency and tolerances into the current architecture	Defined and managed Enterprise IA Commitment	Established and tested Enterprise Business Continuity Process Maturity	System Survivability Demonstrate the achievement of system survivability through the mgt. of faults and failures, sustainability processes, aligned CDS and IA best practices.	System of Systems Resiliency Engineering- Demonstrate the achievement of cross-domain resiliency.
	Assured Information Sharing	Required to define and manage how information is shared across the Department's boundaries	Network boundaries are defined and policies for sharing and managing information across these boundaries	A comprehensive protective monitoring regime is implemented to provide situational awareness and enable essential information flows to be maintained.	Level 3 measures are extended so that incident mgt. moves from being reactive to proactive.	Network boundaries and the associated protective monitoring regime is continually improved to reduce the departmental and collective, shared exposure to information risk.
	Trust Management	**Identification** **Access-Controlled**	**Authentication** **User-Profiled**	**Reputational** **Client-centric**	**Vetted** **Federated**	**Valued** **Collaborative**
Effectiveness	**Compliance**	Established compliance regime to confirm the effectiveness of IRM against mandated standards. Annual Reporting	The Dept. has a comprehensive IRM compliance regime. They have an External IA Review	Critical IA Review and internal audit Recommendations are actioned and progress tracked.	IA incident mgt. processes are fully assured by internal audit. The Main Board is aware of the significant areas of the Enterprise non-compliance	There are no critical or significant IA audit issues. Independent assessment of the Enterprise approach to IA shows that it is aligned with the National IA Strategy.
Trustworthy	**Assurance**	Establishing an IA Strategy and Audit. Implementing an Information Security Management System (ISMS)	Fault Tolerant System of Systems with graceful degradation of services and functionality SIEM implemented	Adherence to the ISO/IEC 27001 standard and the ISF Best Practices Implementing a Culture Change to Information Asset Management.	Automated IA Auditing and Risk Assessment. Cyber Power and Shared Awareness Monitored and Controlled	Aligned and harmonised Cross-Domain interconnectivity and operations. Full Business Continuity and Recovery Planning Agile Shared Situational Awareness

CHAPTER 3:

Modelling the Assurance Component

Information assurance (IA) *is defined as "information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.* **Taxonomy of Information Assurance, 2003**

Information Assurance (IA) *is delivered through the assessment of information in relation to:-*

- *Confidentiality - The property that information is not made available or disclosed to unauthorised individuals, entities, or processes*
- *Integrity - The property of safeguarding the accuracy and completeness of assets. This may include the ability to prove an action or event has taken place, such that it cannot be repudiated later*
- *Availability - The property of being accessible and usable upon demand by an authorised entity.* **Ministry of Defence, 2011**

These two definitions provide a clear indication that the institutional establishment has formulated that Information Assurance is the risk adjusted reasoning behind the usage of Information Security and its Protection mechanisms. In this chapter, that narrow definition is redefined and expanded with arguments that Information Assurance should be about the empowerment of the Social-Technical Enterprise to create a trustworthy environment based on trusted communities of interests. Trust is a very difficult virtue and is often considered the most noble of mankind; we want to trust people, services and enterprises; and most often our trust is reciprocated providing the bond to human society. However, we also fear being let down, used or our trust being abused. Information Assurance is about bringing trust into Cyberspace, across heterogeneous systems, in our exploitation and reliance of shared Information and the ability to trust another person whom we have never met, but who shares our community of interest. "*Economic life is pervaded by culture and depends on moral bonds of social trust. This is the unspoken, unwritten bond between fellow citizens that facilitates transactions, empowers individual creativity, and justifies collective action,"* (Fukuyama, 1995). Trust is the foundation of the Socio-Technical Enterprise and the very basis of this real and virtual global economy. "*The speed at which Trust is established with clients, employees and constituents—is the essential ingredient for any high–performance, successful organization,"* (Covey, Covey , & Merrill, 2008).

Chapter 1 argued for the need and purpose for Enterprise assurance is to provide a resilient, dependable and safe environment that will change and shape the Enterprise culture to become a trusted, sustainable operation capable of delivering its strategic goals and mission. This strategic positioning of IA (Chapter 2.4) provides a framework for the assurance of Knowledge, Information and Data process, storage and transit; thereby providing the architecture of the interoperability of technology to the human-cyber interexchange and the organisation structures which form from its business processes. The IA component of the Information Domain is in fact based on 8-Dimensions: Structure (Organisational and Architecture), Resilience, Dependability, Safety, Security, Protection, Risk Management and Trust.

Assuring the Information Domain has progressed from the idea that it's a function of security (*confidentiality, integrity, availability, access control; authentication; privacy, non-repudiation and communication security* as declared by the ITU-T X.805) to this thesis declaration that it's a function of a Socio-Technical Enterprise where Enterprise defines the scope of industrious, systematic activity that creates a (profitable) business organization which will return value to its stakeholders through their readiness to embark on new ventures (with a high degree of boldness and energy), cross-domain interaction and their contribution to the business processes. Creating a technology intensive enterprise requires purpose; an engaging environment; harmonised and aligned capability across agile human-cyber inter-exchanges and superior decision making in a shared situation and culture. Since enterprises are complex socio-technical systems, the effective use Information Exploitation (IX) and Information Operations (IO) in the enterprise decision making process can be structured and analysed through the adoption of Enterprise Architecture (Ross, Weill, & Robertson, 2006). Nightingale and Rhodes (2007) define Enterprise Architecture (EA) as a set of views (Strategic, Policy Process, Organisational, Knowledge, IT, Product and Service) which by: "*Applying holistic thinking to design, will evaluate and select a preferred structure for a future state enterprise to realize its value proposition and desired behaviours.*"

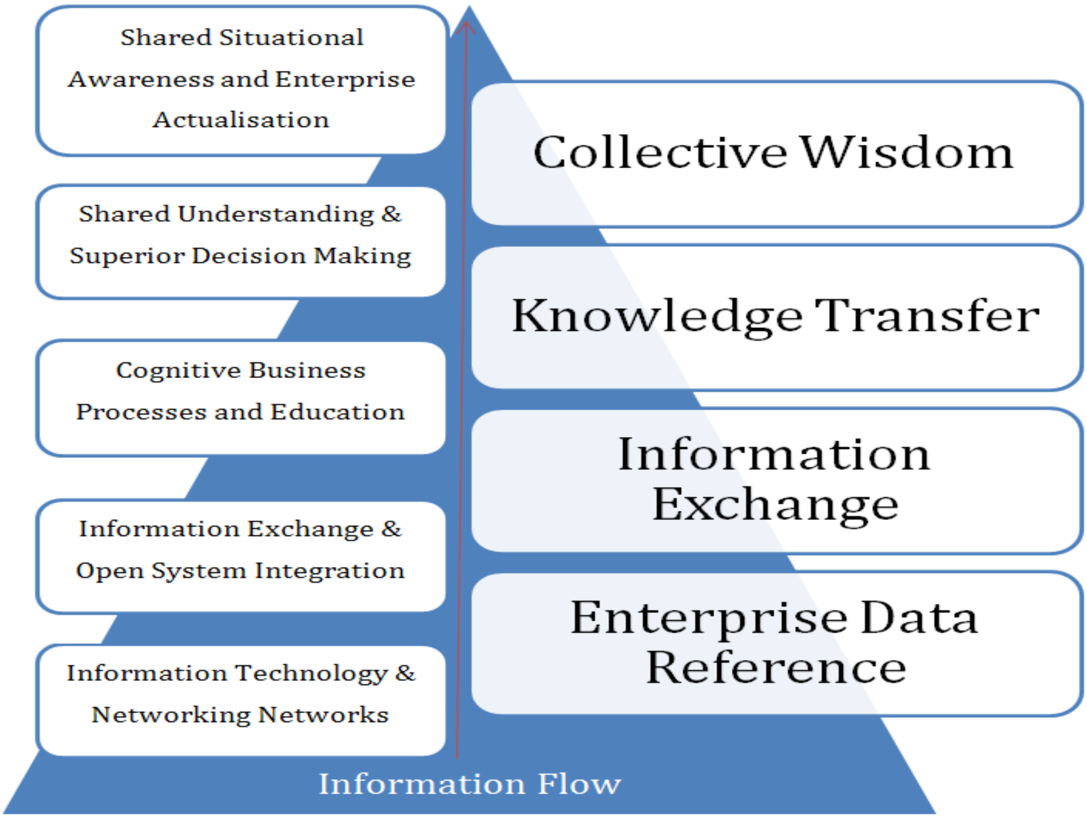

Shared Situational Awareness and Enterprise Actualisation
Shared Understanding & Superior Decision Making
Cognitive Business Processes and Education
Information Exchange & Open System Integration
Information Technology & Networking Networks
Collective Wisdom
Knowledge Transfer
Information Exchange
Enterprise Data Reference
Information Flow

Figure 35: The Information Pyramid Reference Model to Socio-Technical Enterprises

The Data Reference Component represents the transformation of Enterprise Data across service platforms and IT infrastructures; technical services; data sensors; data monitors; data processing; (hardware and software) product outputs and the interfacing of communication and data networks (protocols, standards and data structures). The US Government Data Reference Model (DRM) describes this collaboration process as that "*enables agencies to describe the types of interaction and exchanges that occur between the Federal Government and citizens*" through the categorisation, structure and exchange of Data, (FEA, 2005). The Information Exploitation component of the pyramid reference model is discussed in detail in sub-chapters 3.3 and 3.4 where it examines the transformation of data into Information Flows across the operational cyber processes (Information Operations), Information Archiving and the Human-Cyber Interexchanges (Information Technologies, Infrastructures, Services, Management, Assurance and Exploitation). The Knowledge Transfer component of this pyramid reference model exhibits the Business Processes of the Socio-Technical Enterprise which spontaneously reorganize the Enterprise Open Systems to states of greater heterogeneity and complexity whilst achieving a "steady state" at which it can perform Cognitive Processing, Knowledge Management (KM), Knowledge Transfer and Decision Making across the Human-Cyber divide.

The Collective Wisdom of the Socio-Technical Enterprise, its ability to *learn*, *be selective and, within limits, self-regulating* are the hallmarks of an Open System (Trist, 1981). Although not parts of this thesis remit, Open System Architecture is an important component of an Enterprise as it contributes to Enterprise Actualisation which exists through its interoperability with the products and services of other Enterprises and the evolving social interconnectivity. The creation of Shared Situational Awareness is the goal of Enterprise Coalition and Partnership which is underpinned by a culture of Trust and an understanding of the risk appetite of the Enterprise.

3.1 Assured Knowledge Transfer

Coalition military partners, and in particular the US and UK (and more recently UK-France) have recognised the importance of transnational alliances for the conduct of joint action operations and the need to create Cyber Environments that can Assure Knowledge Transfer and dissemination of Information. This recognition has not been lost with Governments, Businesses, NGOs and Charities (Brown, Khagram, Moore, & Frumkin, 2000; Sogge, 2011; The White House, 2011).

The UK military vision of the "*coalitions of the willing*" (MoD, 2003) is that joint action will be across all levels of the operational spectrum (from policing actions, humanitarian assistance to theatre operations) and will require its Network Enabled Capability (NEC) to provide close interoperability across the multi-lateral force deployment. *"This interoperability will bring its own set of technological, ideological, organisational, procedural and cultural idiosyncrasies to the theatre operations…The rapid, opportunistic exploitation of situational contingencies, the need to self-synchronize and the requirements to synergistically marshal diverse military assets in the context of agile force structures, require the ability to exploit and share information in ways that* *transcend the traditional boundaries of national affiliation and operational environment;"* (Smart & Shadbolt, 2007)

The DIME evolution in Cyberspace has generated many challenges for the Socio-Technical Enterprise at all levels (Government, NGOs, Military, Multi-nationals and SMEs). The US Centre for Strategic and International Studies CSIS paper "*Cybersecurity, Two Years Later*" (CSIS, 2011) commented that after their previous report to the 44th US President (CSIS, 2008) when "*cyber-security was not a major issue for public policy"* that the overriding problem of security was intrinsically complex involving commercial interests, concerns for privacy and the insecurity of systems to worms like Stuxnet. "*We thought then* (2008) *that securing cyberspace had become a critical challenge for national security, which our nation was not prepared to meet. In our view, we are still unprepared;"* (CSIS, 2011). Enterprise Architecture provides a methodology to examine these challenges and the US Federal EA has created a common approach to this analysis as illustrated in figure 36.

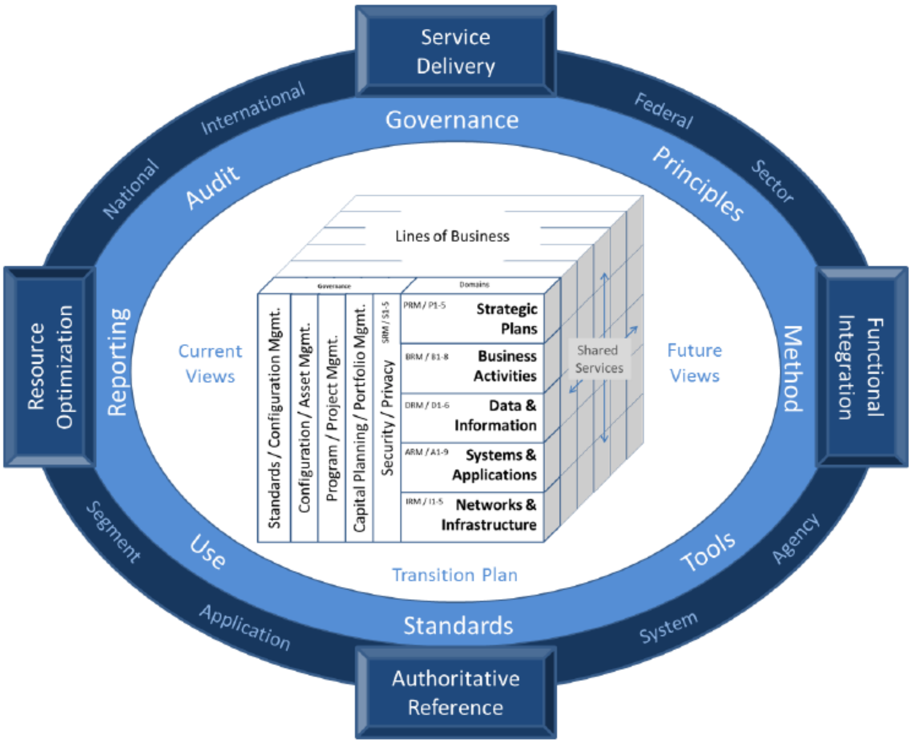


Figure 36: The Common Approach to the US Federal Enterprise Architecture

Social-Technical Enterprise exists through regular commerce in Service and Product Delivery, Functional Integration, Resource Optimisation and Information Interexchange with other Enterprises, Institutions, and persons that has been created in its external social environment (as scoped by the FEA's 8 Levels - International; National; Federal;

Sector; Agency; Segment; System and Application). *The Enterprise requires physical supports for its activities - a workplace, materials, tools, and machines - a stable organization of people able and willing to modify the material throughput or provide the requisite services*; (Trist, 1981). The Cycle-Rubik nature of the FEA Common Approach Framework segments the organisation's line of business as a current view (Governance and Domain) and the shared services as a future view using eight basic elements (Governance; Principles; Method; Tools; Standards; Use; Reporting and Audit).

Enabling Architecture

Driving EA into an organisation requires a cultural change as it require alignment and integration of its shared services across the 5 Domain (6 if you include the cross threading domain of security) from Strategy, through Business Activities, Information Exchange, Systems and Infrastructure.

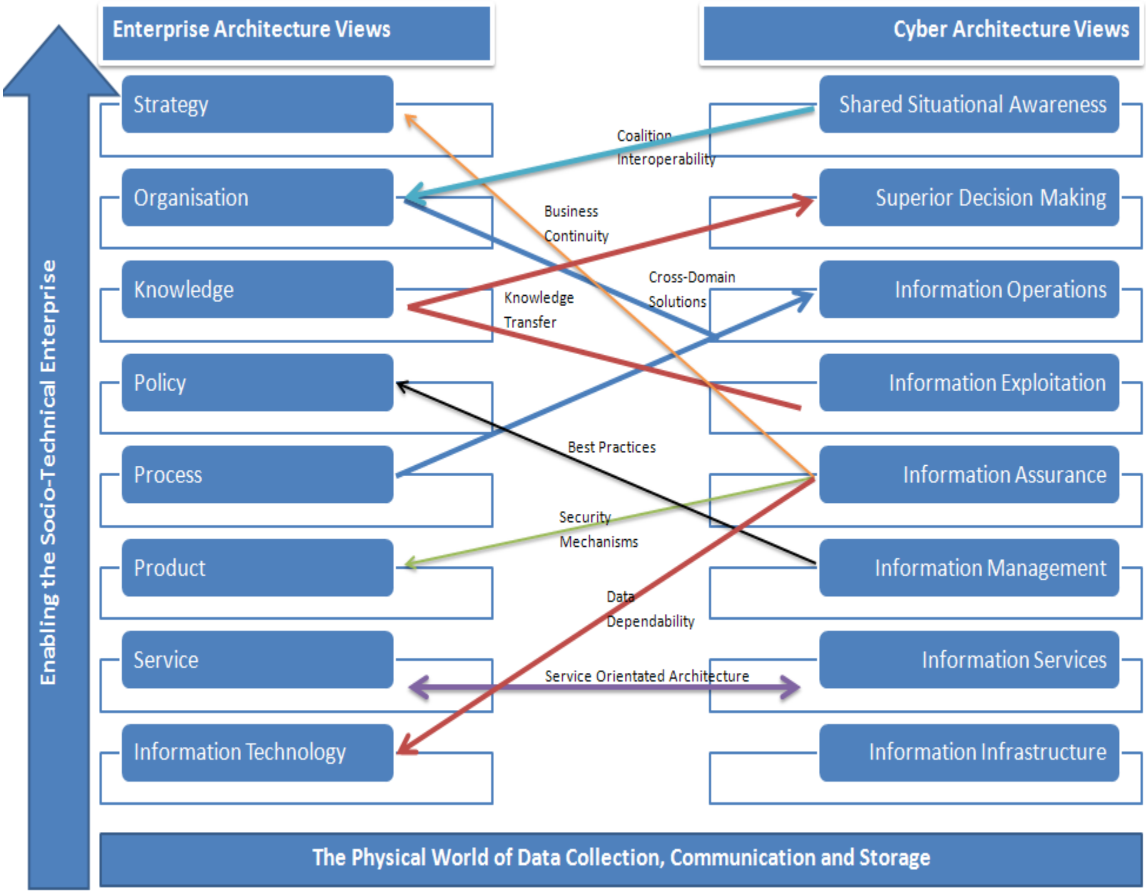


Figure 37: The Enabling Architecture of the Socio-Technical Enterprise (Richardson C. J., 2012)

This alignment requires us to rethink the common approach as the current model fails to visualise the effects of (cross-thread) security and in particular a cyber-architecture view of the information flow and it's Information Assurance across the Socio-Technical

Enterprise. Figure 37 illustrates further cross-threading of the Enterprise Views as an enabling architecture for the Socio-Technical Enterprise (Richardson C. J., 2012).

The model enabling architecture maps the Enterprise view that these interationships are both multi-lateral and multi-layered. Both stacks (The Enterprise and Cyber Views) are founded upon the common "***real world***" of network of networks (e.g. the Internet). This physical world of data collection, process, transit and storage has been regulated by international law and consensus from its online communities of interest where the Internet Corporation for Assigned Names and Numbers (ICANN) manages Internet domain names and IP addresses; The Triangle of Cyber Governance (Mayer-Schonberger, 2002) create Free Markets for Internet Commerce (Winn, 1997) and the memorandum Request for Comments (RFC) administered by the Internet Engineering Task Force (IETF), on behalf of the Internet Society, describes the behaviours, methods, research and innovations applicable to the interworking's of Internet-connected systems (IEFT, 2012).

Whilst Enterprises create, develop and maintain the computer and IT products that build these networks, it's the usage of these IT networks as information infrastructures that has created Cyberspace and this is encapsulated in the stack of the Enterprise Architecture Views. The service that hosted on these cyber platforms are the starting points for most Human-Cyber interconnectivity, whether it is the software routing table of a network switch or the next Application on a Smart Phone these products bridge the divide between the Real and Virtual Worlds. The business processes that drive the creation of the products are operation decisions of the Enterprise management that are reflected in their policies, procedures and practice. These views generate the corporate knowledge and the organisational hierarchy, reporting chains, roles and responsibilities. The strategic direction of the Enterprise is generated from an understanding of its capabilities and the missions it intends to pursue.

Whereas, the Information-Stack (I-Stack), in the Cyber Architecture is concerned with flow of information from the structuring, processing, transmission and storage of data as information across its virtual logical infrastructures and upwards to create an Information resource capable for exploitation, decision making and building of a shared situational awareness.

Organisation's Inherent Inabilities

"Knowledge about something is called declarative knowledge. A shared, explicit understanding of concepts, categories, and descriptors lays the foundation for effective communication and knowledge sharing in organizations. Knowledge of how something occurs or is performed is called procedural knowledge. Shared explicit procedural knowledge lays a foundation for efficiently coordinated action in organizations. Knowledge why something occurs is called causal knowledge. Shared explicit causal knowledge, often in the form of organizational stories, enables organizations to coordinate strategy for achieving goals or outcomes;" **(Zack, 1999).**

In the creation of the Knowledge Economy, the interoperability of socio-technical enterprises has becoming a unifying feature. The *tacit* or *explicit* nature of Knowledge requires it to be managed as both as an object (a thing to be stored and manipulated) and process (of simultaneously knowing and acting; i.e. applying expertise). Within this new economy there is an increasing role for Explicit Knowledge (corporate wisdom, procedure manuals, product literature, or computer software).

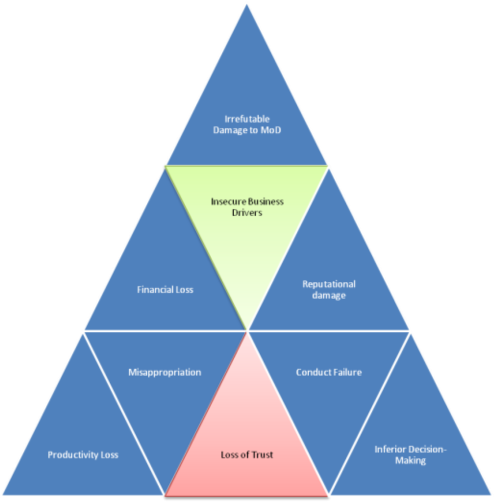


Figure 38: System Security Failings: Insecurity in the Enterprise and its operations

The assurances to the social element of the Enterprise Knowledge Transfer, Memory Archiving, Expertise and Knowledge Management are far more complex than the technical protective solutions of encryption, physical isolation and alternate site storage, business continuity training, redundant system provision and the use of RAID and Cloud technologies. Inter-exchanging Enterprises must efficiently and effectively capture and share their knowhow, expertise and business products whilst protecting their intellectual property rights and knowledge assets. It's their ability to bring their shared knowledge that will bring new opportunities and reduce the threats. Corporate knowledge has intangible components rarely exhibited in technological systems but are readily identified and have become vulnerable to threats and attacks within the Socio-Technical Enterprise. If these threats manifest themselves into attacks and their security fails, These Enterprises could degrade to a sequence of deleterious debilitating and disaffecting socio-technical event which could equally lead to irrefutable damage to the Enterprise. Too few Enterprises have appropriate Knowledge Management policies and capabilities to leverage and protect their Knowledge Capital. The agile socio-technical environment has a complexity of rapid changes to their share awareness with technological discontinuity; emergent properties, insidious exploitation and malicious cyber-attacks as well as time sensitivity of their information flows and the use of obsolete data. Collective and critical decisions are made from the Knowledge, Expertise and Information available. This environment has to be resilient, robust and trusted.

Introducing Information Assurance to the Enterprise

Bringing Trust into the Socio-Technical System to safeguard operations and risk manage the threats is the strategic purpose of Enterprise Information Assurance as illustrated in figure 39.

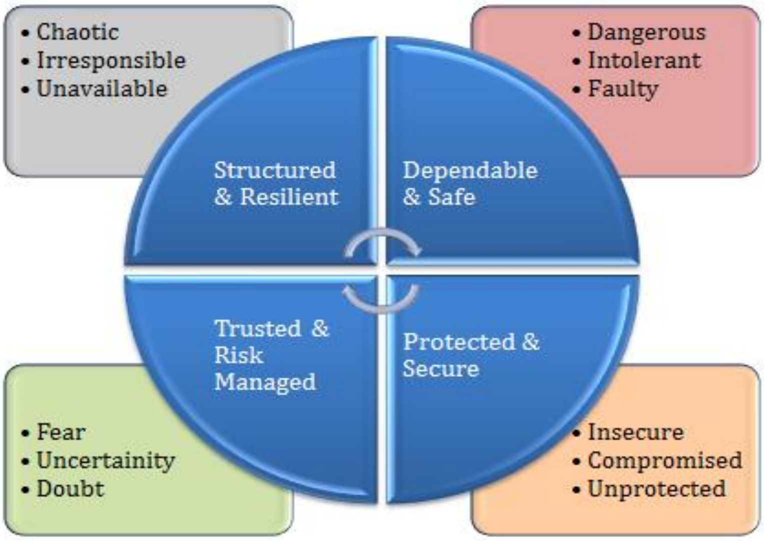


Figure 39: The Assured Space – Structured, Dependable, Secure and Trusted

The key attributes that assured space offers to the Socio-Technical Enterprise are:

1. Information Assurance provides effective and timely exploitation of information through the provision of dependable, resilient operations and mitigates the contagion of fear, uncertainty and doubt within Cyberspace.
2. Information Assurance is fundamental to all aspects of the Enterprises business processes from the successful conduct of its Information operations to the management of its Knowledge and Information assets.

3. Information Assurance ensures stakeholder confidence that Information Systems Risks are managed pragmatically, appropriately, and in a cost-effective manner that maintains the value of the Enterprise.

These attributes can be mapped across the components of cyberspace as illustrated in figure 40. The defensive nature of this map illustrates the key issues of an Assured Enterprise: (1) its physical systems are made safe and protected by a (2) cyclic array of functions (deterrence, restoration, removal, detection and attribution) under the control of (3) the CND Operations; (4)the resilient system architecture and awareness of the human factors involved allows for greater understanding of motivation and intent which allows for (5) better risk and trust management of (6) the Information Flows that provide better decision making, knowledge transfer and creation of a Cyber-based Shared Situational Awareness for the protected communities of interest.

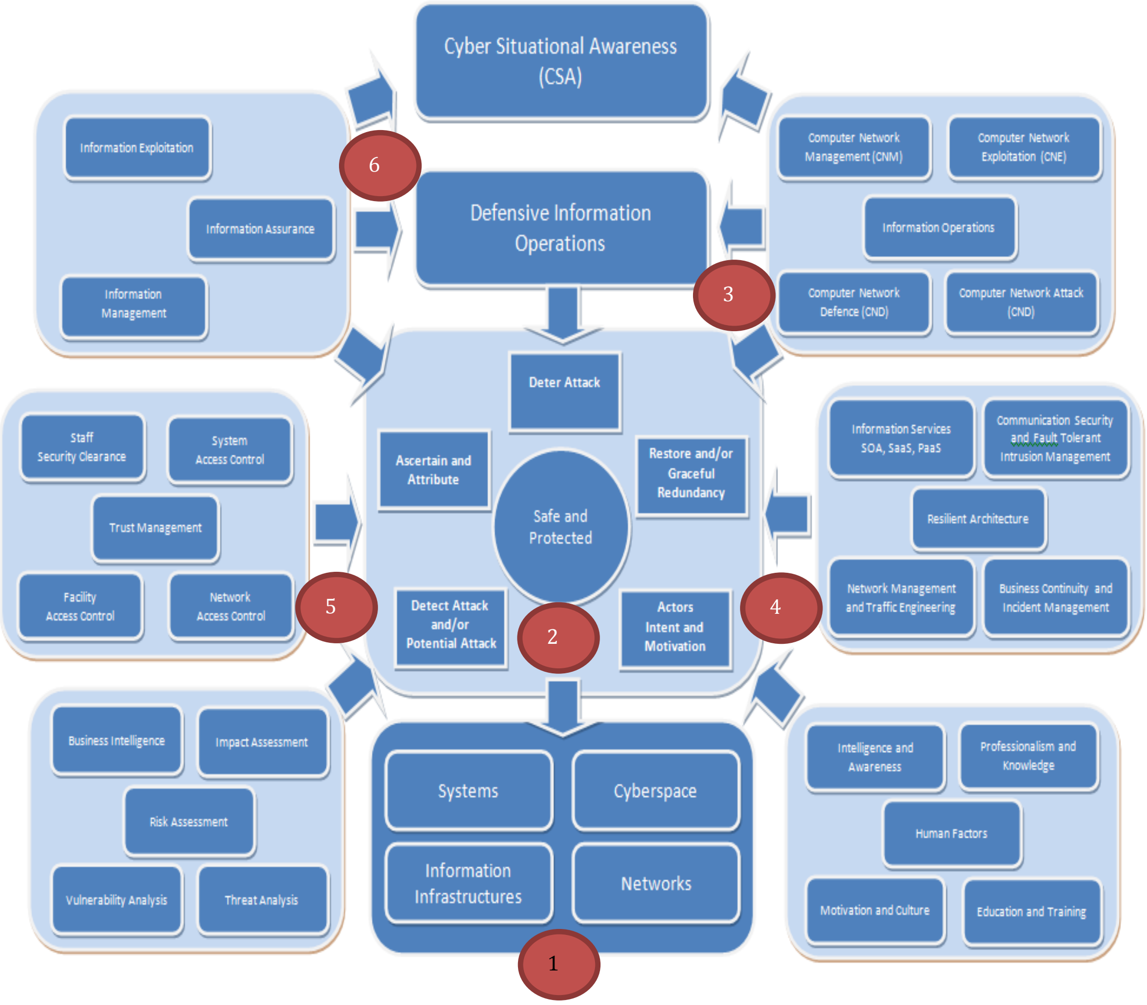

Cyber Situational Awareness (CSA)
Information Exploitation
Information Assurance
Information Management
6
Defensive Information Operations
Computer Network Management (CNM)
Computer Network Exploitation (CNE)
Information Operations
Computer Network Defence (CND)
Computer Network Attack (CND)
3
Deter Attack
Ascertain and Attribute
Restore and/or Graceful Redundancy
Safe and Protected
Detect Attack and/or Potential Attack
Actors Intent and Motivation
2
Staff Security Clearance
System Access Control
Trust Management
Facility Access Control
Network Access Control
5
Information Services SOA, SaaS, PaaS
Communication Security and Fault Tolerant Intrusion Management
Resilient Architecture
Network Management and Traffic Engineering
Business Continuity and Incident Management
4
Business Intelligence
Impact Assessment
Risk Assessment
Vulnerability Analysis
Threat Analysis
Systems
Cyberspace
Information Infrastructures
Networks
1
Intelligence and Awareness
Professionalism and Knowledge
Human Factors
Motivation and Culture
Education and Training

Figure 40: Mapping the Defensive Components of a Socio-Technical Enterprise (Richardson C. J., 2012)

The 3-Layers of Understanding

Cyberspace interfaces the real and virtual world of our human endeavours. It's a real domain of computers, switches, storage area networks, data protocols, communication devices and network of networks whilst the virtual world expands our mind, cognitive powers and imagination. A domain of computer generated art, games, programmes, animated objects and massive computational power. Cyberspace is a creative domain rich in adaptability, opportunities and innovation, but also a complex, vulnerable state of human exploitation, crime and hostility. The project of Cyber Power by the Socio-Technical Enterprises is a dichotomy of Taoism, the white domain of trustworthy endeavours and the black domain of hackers and malice. However, as in the real world of human interaction, the contextual continuum of cyberspace has many shades of grey in its Tao world and this is reflected in figure 120 with its 3 stack components of understanding: Knowledge, Information and Data.

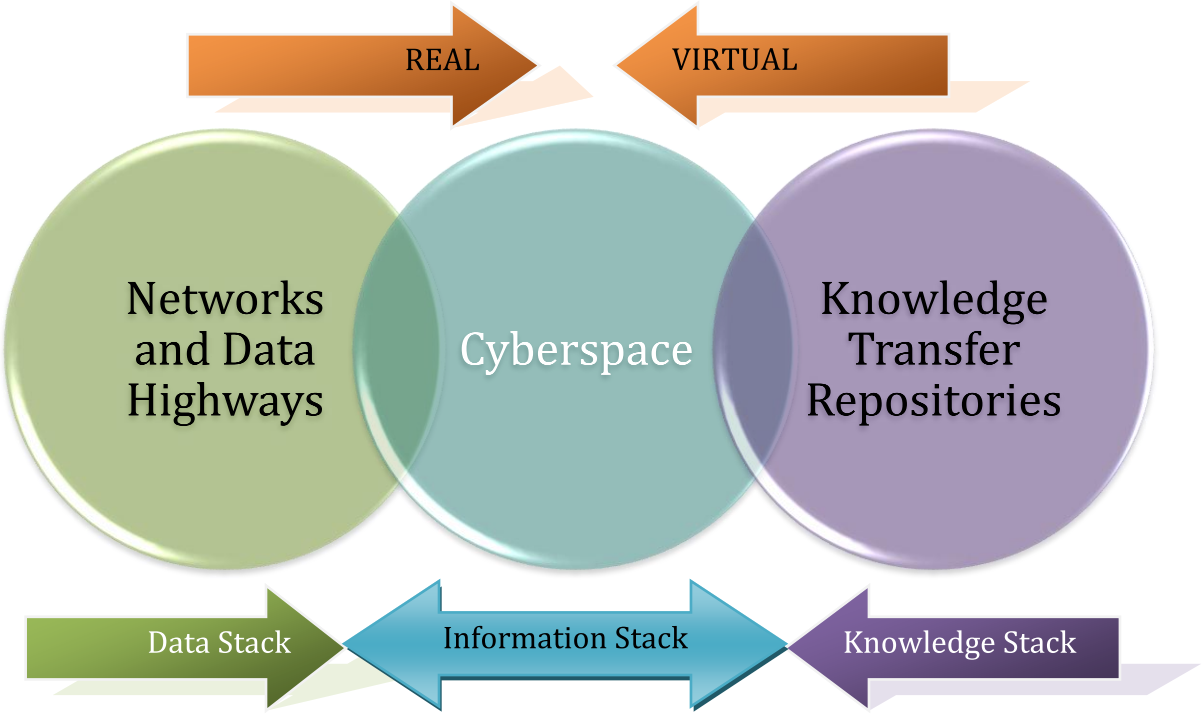


Figure 41: The Contextual Continuum of Real and Virtual Space

The first layer is the Data Stack (D-Stack) that provides for networked devices, entities and sensors to collect, disseminate, process and store digital material. The rate of growth and exchange of data across these networks of networks places many demands on network and traffic engineering: increased bandwidth; dense multiplexing; faster computing (increasing the CPU's million instructions per second rate- MIPS) and greater use of fibre-optic switching networks. The ease with which these demands increases with the escalation of data, data services and data storage overwhelms the physical infrastructures and has created a more agile, but more vulnerable, environment of virtual machines and cloud communities. These virtual domains are dependent to the system architectures they are based upon. These architectures although expedient to the demands of users are also an Enterprise security risk to the social-technical communities that rely upon them, (MacIntosh, 1998; Zittrain, 2008).

The second layer is the Information Stack (I-Stack) that provides a seamless transformation and transmission of data structures (information) across the Information Infrastructures hosted in Cyberspace. This Information Domain has many influencing doctrines (IX, IA, IM, IO and IW), policies and practices that determine the quality, presentation and dissemination of the Information assets. The third layer is the Knowledge Stack (K-Stack) which is a domain that is recipient of the Information presented and the experience of the communities of interest. The human-Cyber Interexchanges are formulated within this domain as we begin to understand the emergent nature of cyberspace and the adaptation of new commodities, entities and services that evolve the socio-technical Enterprises. Information Assurance and Enterprise Architecture provide a lens to this Cyber Domain. It is the nature of building bridges to close down the gaps in our knowledge, system capability, skills, experience and education that enthuses our desire and necessity to understand how the interdependencies of these 3 stacks create the new real and virtual world of the Socio-Technical Enterprise.

Business Drivers

Cyberspace and the world created by the operations and interconnections of Socio-Technical Systems and the Enterprises that sustain them is a rapidly changing environment. Enterprise Architecture and its business drivers benefits the organisation as it provide long-term structure and direction to the superior decision making process, business processes and the Enterprise Shared Situational Awareness as illustrated in table 13. This creates a business imperative for the success of Enterprise Architecture that paradoxically becomes increasing harder to implements as the changes to system capabilities and the environment accelerate. The key to successful implementation of Enterprise Architecture is to make it relevant to real-time operations and to-date most implementations have not fully lived up to expectations.

Table 7: Business Drivers and Benefits of Enterprise Architecture (Jones J. , 2012)

Enterprise Architecture Business Drivers	
	• Leveraging New Technology • Compliance • Increase Profitability • New Markets • Business Value Generation • Rapidly Changing Business Environment • Better Utilization of Resources • Mergers and Acquisitions • Integrating a number of cultures in a disparate organization • Collaborative working with external parties • Getting people within an organization to work together effectively • Achieving compliance with Government regulations in a cost effective manner
Enterprise Architecture Business Benefits	
	• Creates an structured environment for Superior Decision Making • Promote a climate of continuous business evolution, improving everyone's quality of work and deliverables • Enhance business flexibility by providing an adaptable framework, more supple structures and best business practices • Share skills, experience and knowledge to increase asset values • Generates the business technology infrastructures to deliver cost effective results • Bring business resources together to create a boundary-less business

Understanding business systems that builds cyberspace and appreciating them as socio-technical systems in the context of enterprise architectures is in itself a major piece of research and development. Enterprise Architecture aims to provide a coherent approach for analysing the driving (strategic, operational and tactical) business and technological factors that lead to strategic business aims, goals and missions. The essential component to the efficient implementation of EA is properly aligning the people, process and technology aspects of the enterprise to business drivers which firmly lies within the domain of Information Assurance. Studying the architecture of Enterprises can transform behavioural use cases, operational assumptions and constraints and how the business drivers provide the basis for planning and designing an information system and the creation of a shared awareness and superior decision making as illustrated in figure 42. The alignment of Information Services and Technology for Enterprise System Interoperability allows for the availability of trustworthy knowledge, information and data services whilst ensuring traceability and reducing risk of decision promotes a more sustainable, efficient and effective Socio-Technical Enterprise.

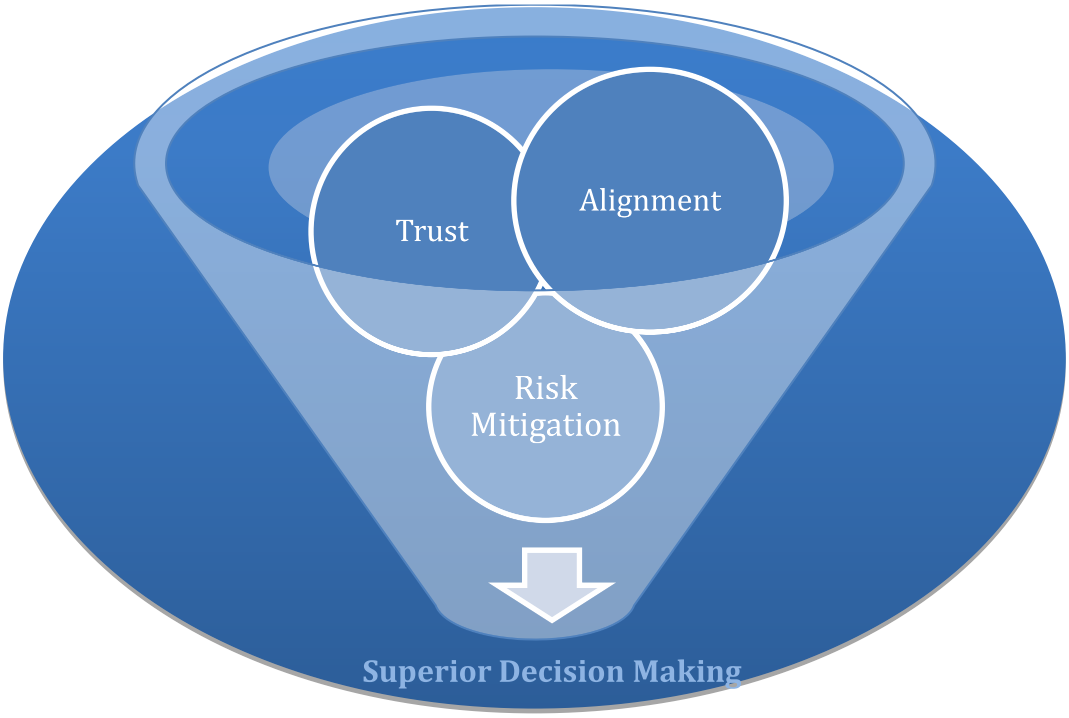


Figure 42: Enterprise Architecture Business Drivers

Information Vision

Modern society is increasingly reliant on the storage, processing and transmission of information. Ensuring the integrity, security and privacy of information is thus paramount, regardless of whether the information is at the level of the citizen or at a national or international level. Moreover, future trends (as outlined in the Information Society Technologies Advisory Group (ISTAG, 2004) *report, for example) in the so-called Ambient Intelligent Space* (ISTAG, 2003) *will only increase the role of information and our reliance on it. This brings with it great opportunities to enhance our quality of life, but at the same time, presents major challenges in terms of the privacy and integrity of personal information.* **(Martinelli & Quisquater, 2005)**

Western Critical Information Infrastructures are becoming more highly dependent upon the global cyber infrastructure. The increased automated and complex interconnections where network routings between Private Enterprises and Government Agencies (Gasper, 2010) has made it less practical to erect barriers between military and civilian operations (Glebocki Jr., 2008) and many current barriers and information fortresses are actually operating against national interests (Hundley & Anderson, 1995; Allor, 2007; Dunlap, 2008). There is a common understanding that achieving greater security in information and communications technology (ICT) would increase its development and diffusion, with concomitant benefits in many fields. While this technology is already spreading rapidly, it will only be possible to translate our physical interactions into electronic interactions if sufficient trust and confidence exist in the systems that process our information. The integrity, security, quality and privacy of information and communication are thus paramount, in everything from personal information transfer to government and critical infrastructures. It is now widely agreed that lack of trust in systems will prevent their widespread adoption. As a consequence, the development and deployment of systems with strong effective security is vital. In addition, modern ICT systems may consist of up to several thousands of computation and communication resources whose number dynamically changes and thus are getting closer to creating Cyber communities; irrespective of the geographical location of the assets. In this new framework, the capability to represent, create, negotiate, monitor and evolve trust relationships in a secure way becomes mandatory.

Trust and security are key enablers of the Information Society. For citizens to use and feel comfortable with e-Government services they must have confidence that their online services are trustworthy and secure. Similarly, for consumers and SMEs to use e-commerce and e-business they need confidence in the security of online transactions and that the data presented is timely, relevant, consistent and accurate. As access to the Internet diversifies, from PCs to digital TVs, mobile phones and wireless devices, people feel increasingly concerned about the protection of their assets and privacy in this networked world. These aspects will become more and more important as we move towards the smart digital environments based on many interacting objects, devices and systems. In the future, personal area networks and embedded computer chips will be everywhere in our cars, our homes and even in our clothes.

Security in such extensive inter-connected environments will require solutions very different to those of today, and its social acceptance will require totally novel approaches to identity and privacy management through user-friendly and trustworthy interfaces, taking into account the privacy needs and data protection regulations in place. Underlying the service and user interface level we must give attention to the information and network security infrastructure. Modern service organisations, such as banking and finance, healthcare, energy, transport and others, rely on ICT for data exchange and control, creating strong mutual dependencies. These critical information infrastructures must be dependable and resilient, protecting against malicious attacks, ensuring tolerance towards and recovery from attacks, and adaptable to the changing security requirements. "*Information Superiority enables decision-makers at all levels in* *all environments to make timely and informed decisions. It therefore contributes to the Defence Information Vision by delivering benefits in agility, effectiveness and efficiency, "* **(MoD, 2011).**

The four, enduring, key benefits derived from the Defence Information Vision (MoD, 2011)are:

1. ***Improved Effectiveness** – Our outputs are better when they are enabled by improved information flows;*
2. ***Agility** – Information can be accessed and manipulated whenever and wherever required, subject to affordability and security constraints;*
3. ***Efficiency** – Operational and their supporting processes are more efficient, both because information flows through them better, and Management Information is available to govern them;*
4. ***Compliance** – We comply with our legal and cross-Government obligations, so that we can focus our resources on supporting operations, while maintaining the Departmental reputation.*

The effects that underline the benefits of MoD's Defence Information Vision are: Strategic Alignment, Accessibility and Trust; Value for Money and Information Exploitations and these fall within the conclave of the Information Assurance Domain and create further benefits to the Department.

Superior Decision Making

"Decision making is the process of sufficiently reducing uncertainty and doubt about alternatives to allow a reasonable choice to be made from among them. This stresses the information-gathering function of decision making. It should be noted here that uncertainty is reduced rather than eliminated. Very few decisions are made with absolute certainty because complete knowledge about all the alternatives is seldom possible. Thus, every decision involves a certain amount of risk. If there is no uncertainty, you do not have a decision; you have an algorithm - a set of steps or a recipe that is followed to bring about a fixed result," **Robert Harris, 2009.**

> *"An accurate description of information requirements is a prerequisite for effective information management,"* **(Choo, 2002).**

Generally, people make poor and/or risky decisions, often with "*gut*" instinct rather than gleamed cognitive knowledge, risk assessment and accurate intelligence. Decision-

Making should be considered a sophisticated aspect of Assurance, provisioned with better information sharing, better understanding, and some taught effective techniques and skills of what decision making involves, people would acquire superior decision making. This understanding would make decision making a *study of identifying and choosing alternatives based on the values and preferences of the decision maker* (Harris R. , 2009; MoD, 2009). Within the structured military hierarchy, the C2 apparatus and the soldier's roles and responsibilities are well defined, exercised and evaluated. Training, reflection and operational tours complement and increase their body of knowledge. Military commander's problem solving and decision making processes are essentially co-ordinated tasks of planning, directing, and controlling where problem solving knowledge is acquired mainly from military actors: instructors, advisors, commanders, staff or from peer group learning in most training scenarios, combat situations and operational planning. These actors provide multiple perspectives (deriving from their expertise, experiences and knowledge) to time and often resourced constrained situations and in high tempo operations their decision making processes in joint actions can be unstructured, incommensurable, generating conflicts of interests and inaccuracies to the joint operational picture with intangible and often ambiguous quantitative or qualitative apparatus providing, using and disseminating disjointed and misleading information and where often the time sensitivity pressure and limited resources combine to cause uncertainties and doubts arising from unexpected internal and external situations.

A military operation is a complex, interaction of men, technology, weapon platforms, communications and the projection of force. The operational activities need reliable, trusted information that can be passed seamlessly across multiple security domain, forces, organisations, networks and individual by respecting complex and possibly conflicting sets of policies, but above all the information needs to accurate, timely and managed. The Information Value Chain as illustrated in Figure 43 supports the NEC Benefit Chain as it illustrates that a seamless flow of information needs which are "*contingent, dynamic and multifaceted*" (Choo, 2002) to get the right information at the right time to make the right decisions (MoD, 2005). The model's primary activities involve the direct handling and management of information resources, these resources are analysed in ways that increase their value: information acquisition, information processing and information distribution and finally through cognitive processes it is acted upon and learnt. Although this model generates and manages the flow of information, it does not provide objectivity or governance to the management and administration of information.

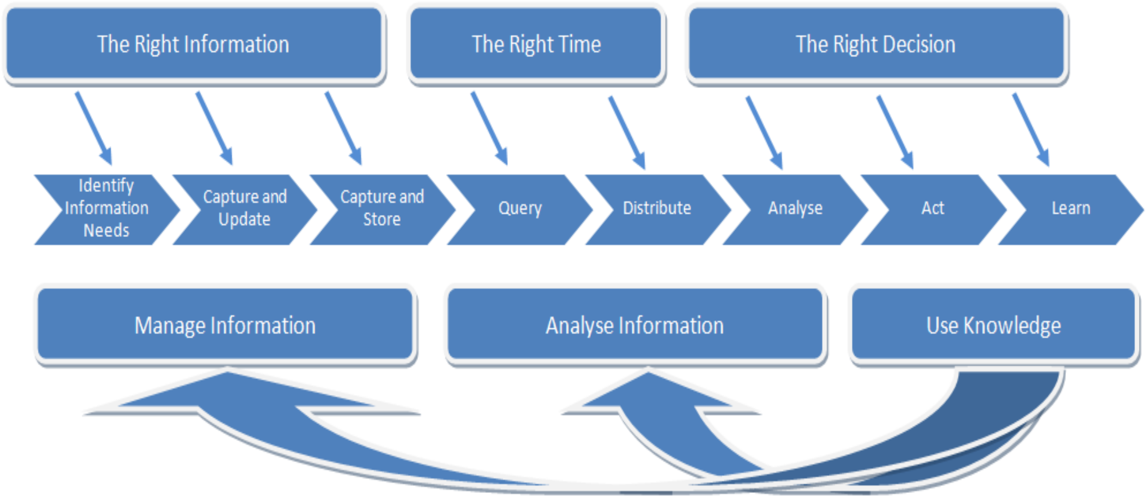


Figure 43: Information Value Chain for government, (Gresham & Andrulis, 2002)

Making a decision implies that there are alternative choices to be considered, and in such a case we want not only to identify as many of these alternatives as possible but to choose the one that has the highest probability of success or effectiveness and best fits with our goals, desires, lifestyle, values, etc. Within the military, and in particular the joint information environment, Dull (2006) stated that the changes in the Joint Doctrine needed to take account that decision making was biased by five key assumptions:

1. *Quality of information of value to decision makers is subject to influence from geography, language, culture, religion, organization, experience, or personality.*
2. *Decisions are made based on information available at that time*
3. *Third, the relevant aspects of the information environment and processes used to make decisions are understandable.*
4. *Fourth, it is possible to affect the information environment of decision makers through psychological, electronic, or physical means.*
5. *Finally, the effectiveness of actions relative to an objective is measurable*

(Dull, 2006)

Information is critical for every aspect of modern life (Brown & Duguid, 2002) and the quality of information largely determines the quality of decisions made, and, ultimately it affects the quality of activity and action outcomes in organizations and in the society in general (Stvilia, Twidale, & Smith, 2006). The Information Assurance of these five assumptions can provide protection (psychological, electronic, or physical), dependability (reliability, safety and continuity) and integrity to the Information flow and provide asset value and this can provided at the strategic level as well as operationally. Information Quality can be summarised by the following eight key attributes:

ACCURATE	**Information must be true, verifiable, and not deceptive. Accurate information is based on empirical data and can be validated by comparing sources or checking for internal consistency.**
CURRENT	The information must be applicable to the present time. Keeping information concurrent requires a process of storage and destruction.
RELEVANT	Relevant information applies to the interests of the individuals who use it for the decisions they are facing. It should reduce a person's uncertainties about work and education while facilitating choice and planning.
SPECIFIC	**For information to be specific, it must contain concrete facts. General observations are often interesting and can provide a background for further analysis, but specific facts are essential to realistic planning and decision making.**
UNDERSTANDABLE	People using information must be able to comprehend it before they can use it. Data must be analyzed and converted into words. The content of the message should avoid ambiguities and be informative to the intended audiences.
COMPREHENSIVE	The information should include all the important categories within its scope of coverage.
UNBIASED	This characteristic is about the motivation or purpose for which the information is being produced and delivered. It is unbiased when the individual or organization delivering the information has no vested interest in the decisions or plans of the people who are receiving the information.
COMPARABLE	The information presented should be of uniform collection, analysis, content, and format so that you can compare and contrast the various occupations, programs of study, and schools.

Table 8: Attributes of Information Quality (Wang R. Y., 2005a)

Asset value can be constructed by the Information Value Chain (Schwolow & Jungfalk, 2010) as illustrated in Error! Reference source not found. which remonstrates the MoD nformation model of action and behaviour (MoD, 2009b) however develops Porter's classic Value Chain Model (Porter M. E., 2001) and taking accounts of Choo's process model of information management (Choo, 2002). Furthermore, this model usage of Senge's five disciplines: Systems Thinking,; Achieving Personal Mastery; Shifting Mental Models; Building Shared Vision, and Team Learning . These provides momentum towards system engineering and organised learning (Senge, Kleiner, Roberts, Ross, & Smith, 1994) and Marchand's Information Technology practice capability framework

(Marchand, Kettinger, & Rollins, 2002a) allowed Schwolow and Jungfalk to formulate their Framework for Strategic Information Management Although the Information Value Chain model doesn't explicitly cover Dull's observations to generating decision making, it effectively manages and drives the information usage *information-gathering function of decision making*. Whereas, the nested model, Figure 44, is inclusive of Harris's Decision-Making definition to Dull's five points, Information Quality and the two Information Value Chains. This Superior Decision Making Information Framework takes the issues of the Quality of Information (impact of the environment, authority, scope of coverage, and objectivity), its availability (accurate and timely), assurance (structured, managed, dependable, protected and trusted), the need to share (measureable and effective) and the cognitive process of knowledge transfers (making information understandable). These five elements influence and provide direct incentives for individuals and organizations to engage in the Information Management processes of Governance, Administration, Services and Infrastructures.

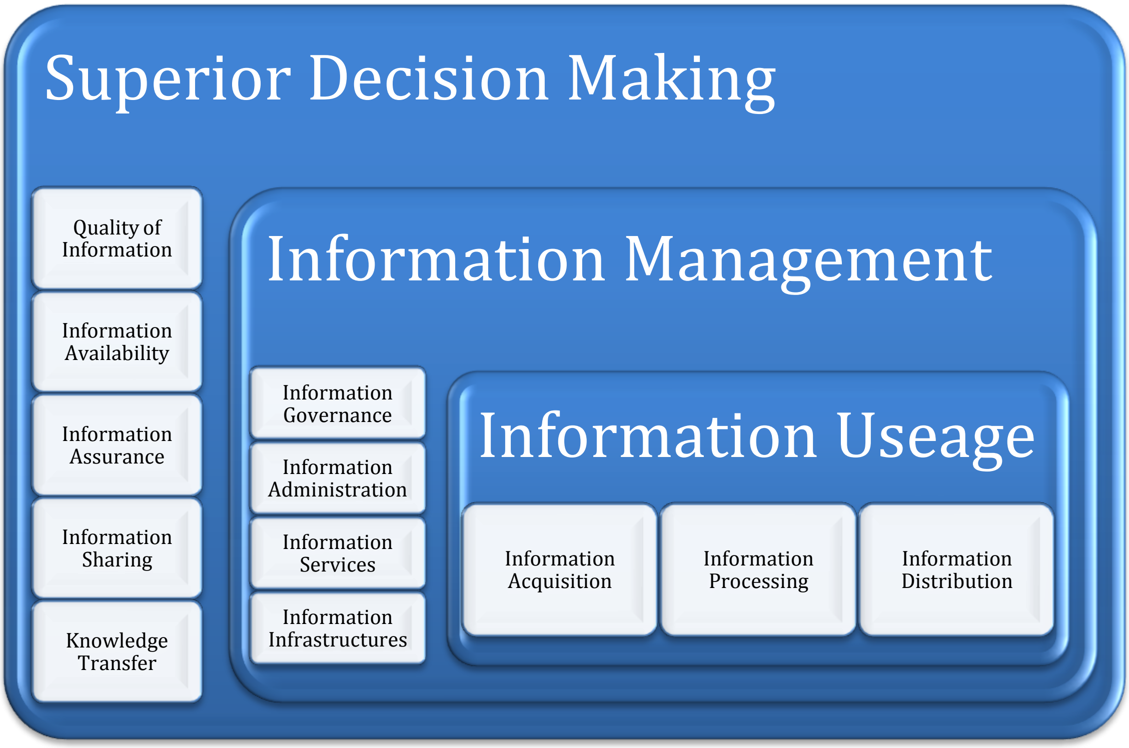


Figure 44: Superior Decision Making Information Framework

Information Governance as expressed by Gartner (2010) is: "*The specification of decision rights and an accountability framework to encourage desirable behaviour in the valuation, creation, storage, use, archival and deletion of information. It includes the processes, roles, standards and metrics that ensure the effective and efficient use of information in enabling an organization to achieve its goals.*"

Numerous Information strategies have commented on its Governance (Cash, et al., 2004; Van Grembergen, 2004; Garson, 2006; Van Grembergen & Dehaes, 2007). The volume and variety of digital information is evolving, exploding and been continually exploited by innovative methods. Structured (appropriately authorised) and transparent services which use information are becoming more instrumented, interconnected and intelligent (Palmisano, 2008).

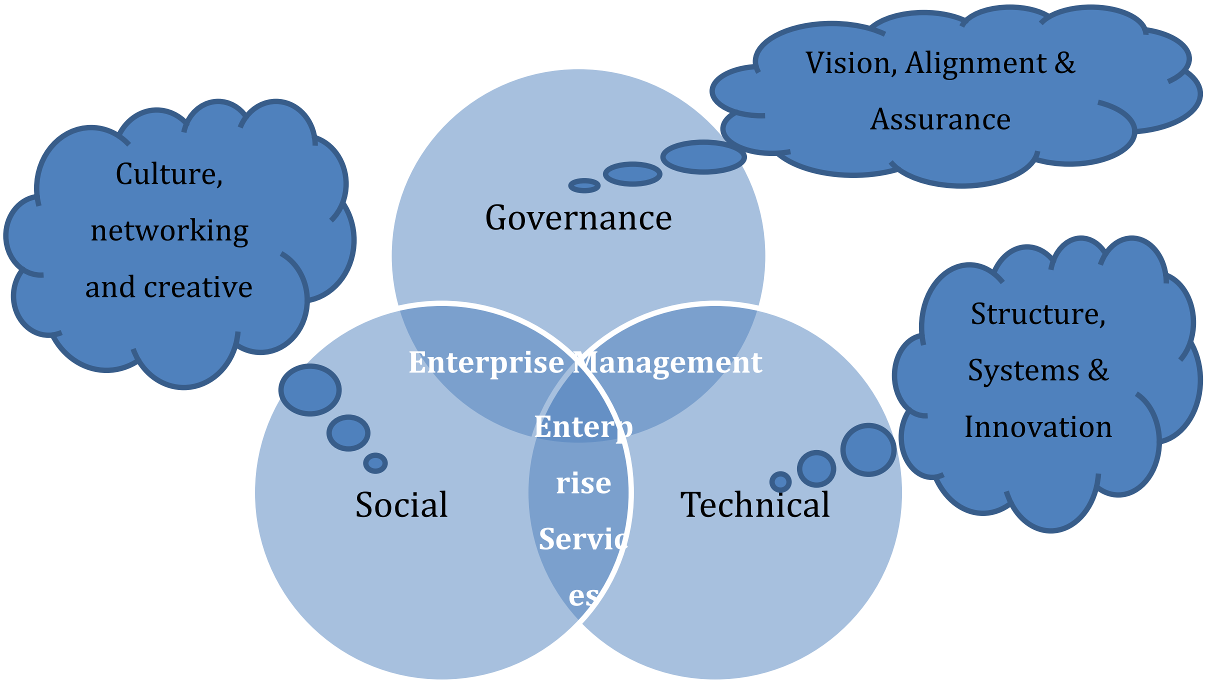

Vision, Alignment & Assurance
Culture, networking and creative
Governance
Enterprise Management
Enterp rise Servic es
Social
Technical
Structure, Systems & Innovation

Figure 45: The Governance of a Socio-Technical Enterprise

Our cyber connected enterprises require their operations to analyse new information faster and make timely decisions for achieving business goals within budget to achieve economic advantages and competitively. Sustainable management of information quality, through the Information Lifecycle and Value Chains is delivered through Information Governance (Salmela, 1997; DeLone & McLean, 2004).

3.2 The I-Stack Model

Cyberspace is a holistic overview of the Real and Virtual Socio-Technical world of online interactions; the World-Wide-Web, Computing networking and capacity and Enterprise Services meeting an increasing demanding community of users. The three underpinning elements of the contextual continuum of cyberspace (figure 120, p 120) were the Knowledge, Information and Data Stacks. This concept of an Information Stack stems from the pyramidal context of transforming data to wisdom and has been represented as the components of Enterprise Information Architecture (EIA). These five components: Knowledge, Information, Enterprise, Technology and Data (as illustrated in figure 128); have been the linchpin for many architectural models, e.g.: Information Architecture for the World-Wide-Web by Louis Rosenfeld and Peter Morville; Decision Driven® Information Architecture by John Fitch and Information Architecture by Richard Saul Wurman at the Information Architecture Institute.

Cyberspace[33] is also a noted component of the 21st Century Information Domain and should have its own part of MoD's Environmental Operating Concepts[34] (EOCs). Current UK Information Security Polices (DIAN 08, 2006; CESG, 2009 and JSP 440, 2010) have declared how the UK military will use Cyber Operations[35] within its current Defence Conceptual Framework (Command, Operate, Inform, Prepare, Project, Protect and Sustain) in light the UK Strategic Security and Defence reviews (2010) this will impose some insurmountable technical obstacles to current doctrine. An adaptive Operational Security (OPSEC), holistic, real and virtual, Information Assured cross-domain cyber solution with an inclusive and extensive risk assessment policy that Bridges the Air Gaps is required.

The mapping out of the Information Domain into clear interdependent, but independent, disciplines is essential for understanding the complex behaviour of the Human-Cyber Interchanges within system domains and system of systems.

[33] JDP 3-70 (2008) "*Battlespace Management*" Ministry of Defence, p 1-3.

[34] The current EOCs are the Future Land Operational Concept (FLOC); the Future Maritime Operating Concept (FMOC). The Future Air and Space Operating Concept (FA&SOC) and the Future Electromagnetic Operating Concept (FEMOC).

[35] DCDC/200080604/JtCon/Operate/Cyber "*A stocktake of MoD's Cyber Capability*" 5 June 2008.

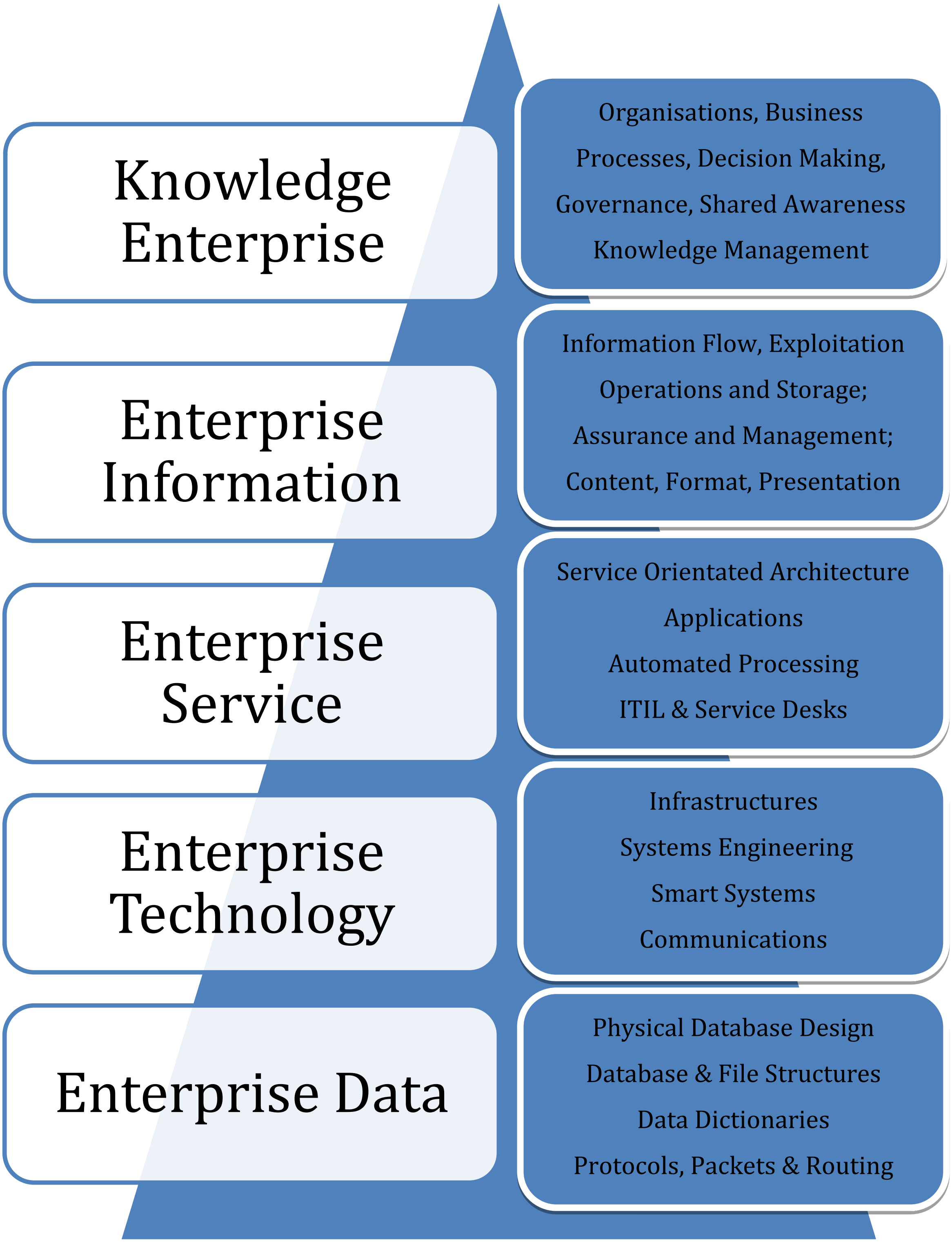

Knowledge Enterprise
Organisations, Business Processes, Decision Making, Governance, Shared Awareness Knowledge Management
Enterprise Information
Information Flow, Exploitation Operations and Storage; Assurance and Management; Content, Format, Presentation
Enterprise Service
Service Orientated Architecture
Applications
Automated Processing
ITIL & Service Desks
Enterprise Technology
Infrastructures
Systems Engineering
Smart Systems
Communications
Enterprise Data
Physical Database Design
Database & File Structures
Data Dictionaries
Protocols, Packets & Routing

Figure 46: Components of Enterprise Information Architecture (EIA)

The Information Stack (I-Stack) is a mapping framework to identify the joint functions of independent components of the Information Domain and their main linkages and dependencies. The purpose of this model is understand the Information Flow across the domain, the interdependent role of Information Operations and Exploitation to enable Enterprise information sharing, transmission and storage in an assured and managed environment as illustrated in Figure 47. The framework encapsulates a number of existing models and places the physical domain of the Internet (and its variants and off-spring) as a component of its Cyberspace.

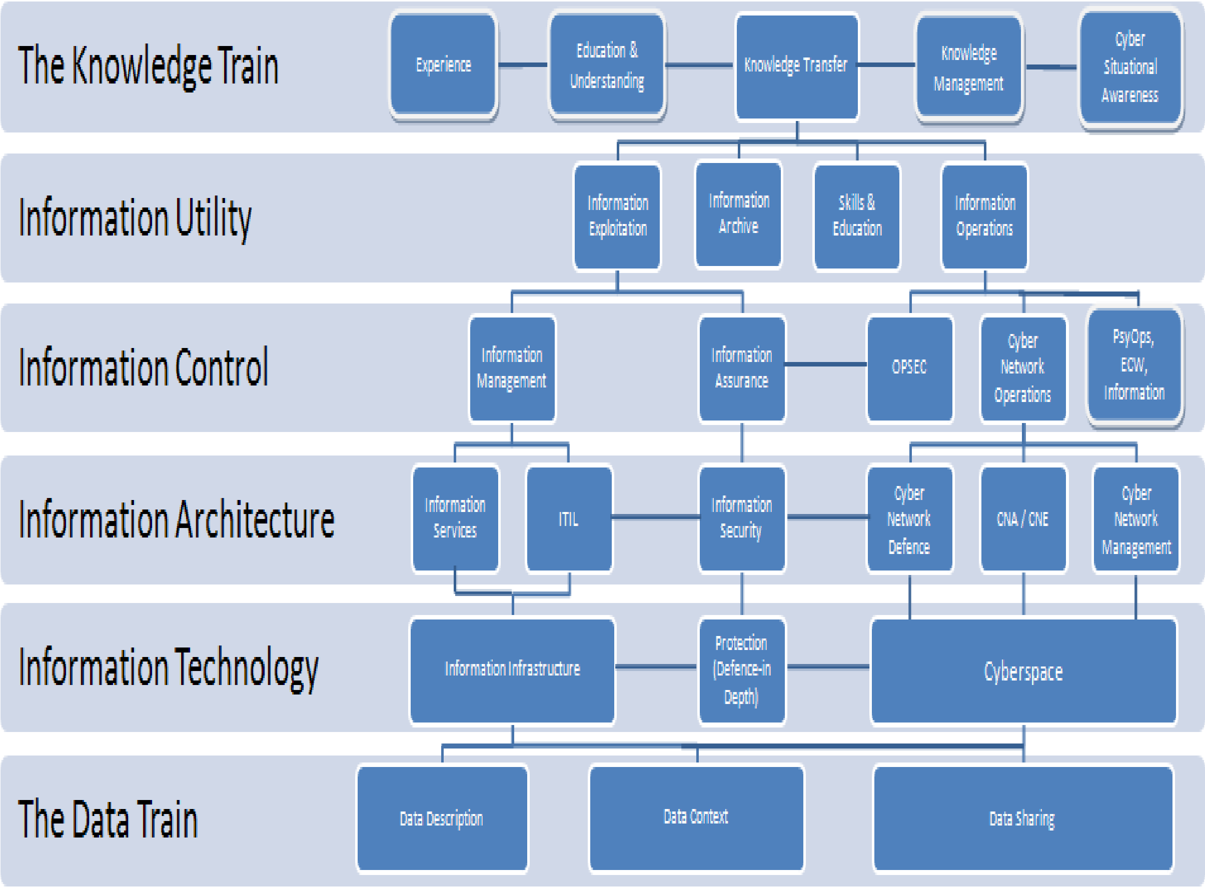


Figure 47: The Information Stack and the Joint Functional Concept

The Socio-Technical Centre of Gravity

MoD's Information Strategy (MoD, 2009; MoD, 2011) declared that we need to be *better informed* to create a *better defence*. The strategy identifies the need to order to protect the information assets and that the Process Owners, Information Assets Owners and individuals need to become aware of the governance and security policies, business drivers and continuity planning, Risks and to be accountable for their roles and responsibilities when handling information. *This needs to be in concert with continued capability development and investment in specialist skills, whilst maintaining close partnerships with OGDs, allies, industry and academia. This will allow the Department to manage its information risk effectively* (MoD, 2011).

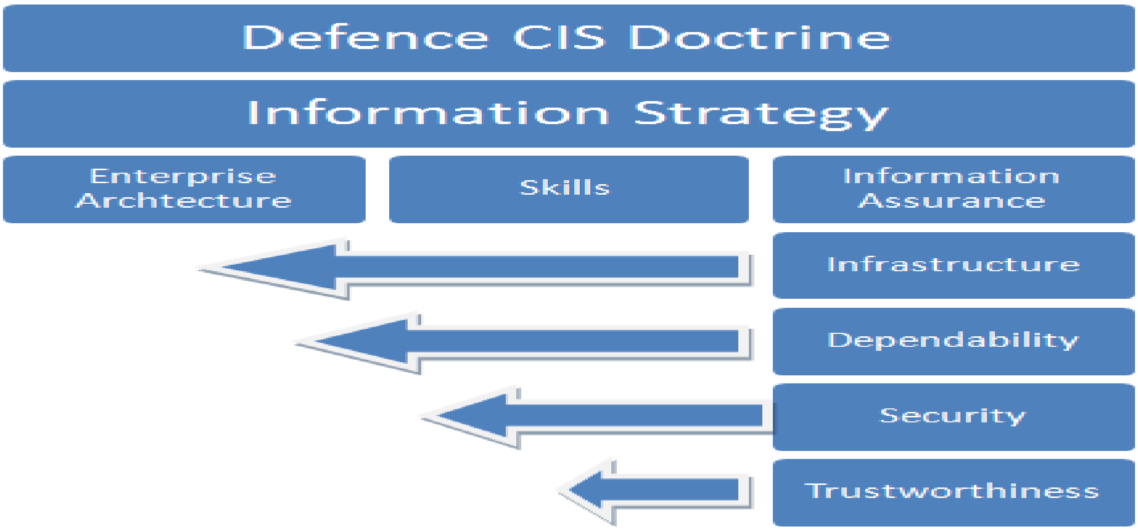


Figure 48: The Influence of Assurance to the MoD S's Information Strategy

The key benefits from adopting this strategy were declared as: Improved Effectiveness; Agility: Efficiency and Compliance. The strategy introduced its 3 MODIS pillars (Enterprise Architecture, Skills and Information Assurance) has recognise the need for strategic positioning of the Information Asset and that its value can be further appreciated through sharing whilst its sensitivity still requires appropriate protection and security. The Ministry of Defence Architecture Framework (MODAF) describes a set of protocols on how MoD will organise information about the business and deliver information to the right person. The second MODIS pillar is concerned with ensuring that the "*right person*" has the necessary skills and behaviours to service, manage, protect and exploit it.

To support better decision-making, information needs to be assessed, analysed, combined with other information and knowledge, and presented in a timely and meaningful way; i.e. information needs to be delivered at the *right time*! The third MODIS pillar is Information Assurance, which ensures that the Information is delivered dependably and securely to the appropriate decision makers, thereby giving it *the right information to the right person, at the time*! In this chapter, the IA Model will develop the themes of how this is achieved and its influence on the two other pillars. The integration of the 3 pillars allows for a more agile, secure and dependable environment, where the systems are resilient, robust, tolerant and protected and information flows are trusted, risked managed and safe through the use of Enterprise Architecture (EA), Information & Data Architectures, Technical Architectures and Information Assurance Architectures (IA^2). Such an assured capability and risk appetite has the potential to Bridge the Air Gaps and allow Cross-Domain Solutions.

The Information Asset as the Centre of Gravity

“T*he centre of gravity is the dominant characteristic of a force, the “hub of all power and movement, upon which everything depends . . . the point against which all our energies should be directed.”* **Carl von Clausewitz, *On War*, 1832**

Without the timely and effective use of information our decisions become jaded, inappropriate or suspect. Whilst assured information is valuable, it’s the context it is used in that values it as a commodity, i.e. information must be relevant. Military Commanders and their strategists develop and execute missions, operations and campaign plans based on a number of factors such as Strategic Purpose, the environment, capability, the threat, Intelligence, Joint Force structure, weapons technology, legal and their own experiences and education (cultural). Education in military doctrine, theories and practice helps the field officers to understand and explain the occurrence of an event or state of nature (MoD, 2010c).

Theory can provide a framework to consider how to approach a problem. It can help one consider issues or questions to solve before making detailed approaches toward developing a theatre strategy or campaign plan. If a theory is sound, then one could use it to solve problems by predicting possible outcomes, identifying potential problems, and finding options to get an opponent to take certain actions or modify his behaviour. Theory can provide a foundation to help military strategists contemplate or evaluate potential courses of actions (Chun, 2010). The use of centre of gravity[36] (Fowler, 2002) has been developed into this Seven Ring Concept Model to illustrate (Figure 135) the possible

[36] US Joint Publication 5–0 defines ***centre of gravity*** as comprising “the characteristics, capabilities, and/or sources of power from which a system derives its freedom of action, physical strength, and the will to fight (take action).

influences of multiple centres of gravity (Economic, Diplomatic, Military, Political, Social and Cyber) affecting the Information Domain. In this model, the complex system property of emergence and the patterns that arise out of the interconnectivity and multiplicity of its node's relatively simple interactions produce integrative levels within the model where the sum of the collective nodes is less than the sum of the whole system. The model thus represents a holistic view of the Information Domain rather than building views from the domains in which it interacts.

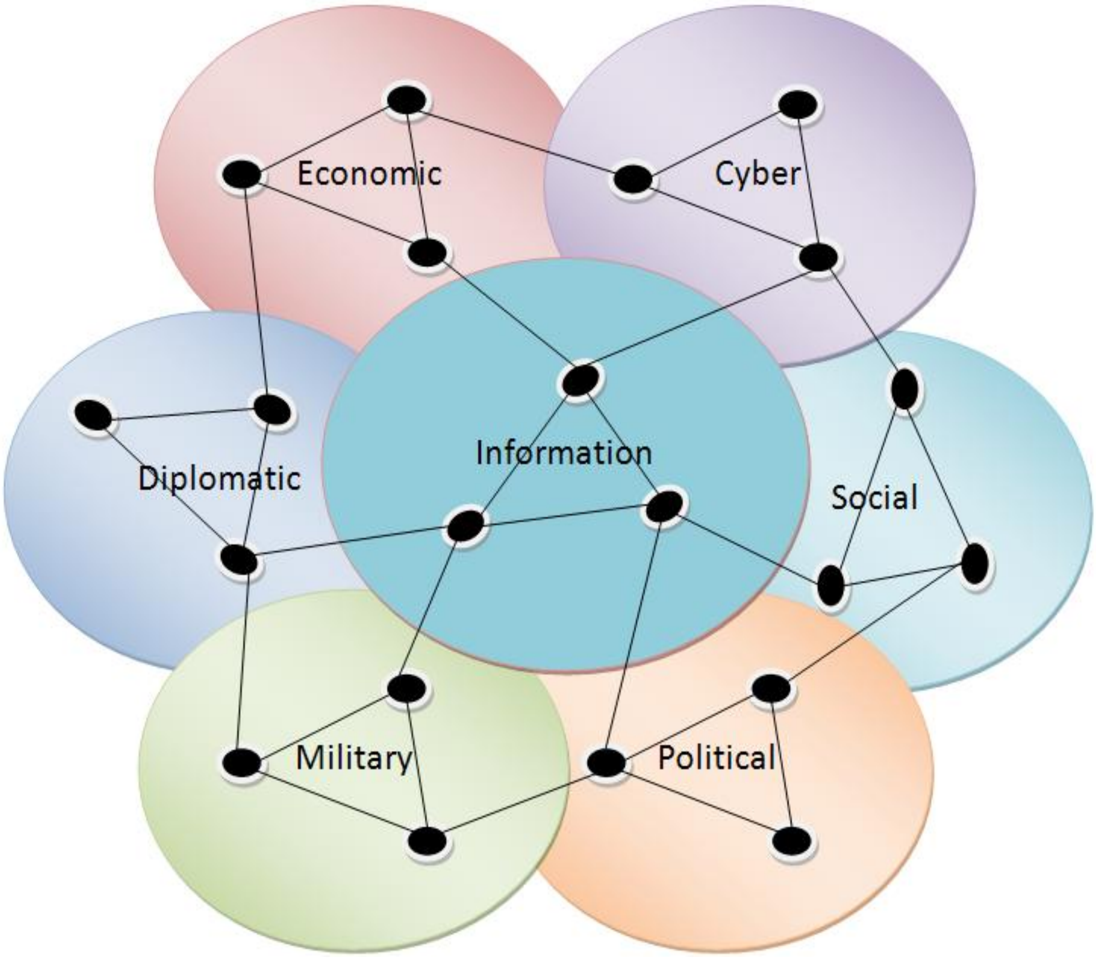


Figure 49: The Strategic Information Asset Seven Ring Concept Model

The heterogeneous nature and any relative importance of the key nodes within each of the seven elements should not have, as properties of that element, strategic or operational effects on those they link to. However, as the model illustrates, the surrounding centres of gravity become subservient to their role when they act interactivity and influences the whole system. It is the emergent consequences of these key nodes (threats and opportunities) and their linkage (that may represent strengths and weakness) that comprise subsystems with an element (thereby creating the individual element's Centre of Gravity) generating new properties when the systematic effect of act collectively with layers of interoperability (inclusive of the Information element) which truly reflect the importance of the Information domain to the global economy.

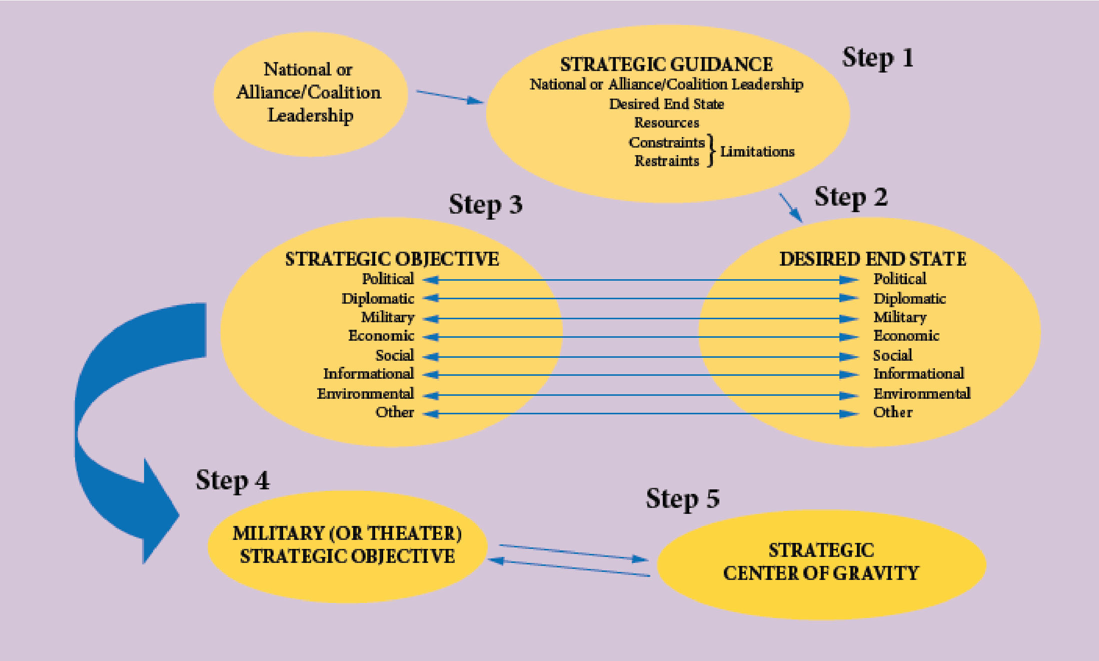


Figure 50: EBO Steps to creating the Centre of Gravity, (Vego, 2006)

EBO needs to link the strategic objective to the desired end state for the steps to creating the centre of gravity cannot be considered in isolation from the military's operational objective as illustrated in Figure 50. It is the objective that determines the situation and subsequently the level and scope of the analysis of enemy and friendly critical strengths and weaknesses. The impetus from EBO is that System of System Architecture has to articulate the positioning of Socio-Technical Enterprise. The strategic objectives of the Enterprise are influenced by the 7-ring concept model and its centres of gravity. This is an important research topic to be explored by the Assurance Community. Emergent properties of complex systems are rarely anticipated and often are unknown. The nodal properties that generate the uncertainties may represent opportunities to the Enterprise but also threats whereas the linkages can be used to determine the strength of assurance against the vulnerabilities the system produces. The understanding of the causal component of Emergence is a major factor in creating a trustworthy environment and will become a bridge linking System Engineering and Information Assurance (SEnIA).

The Policies and Practice Framework

"Information needs to be clear, accurate, trusted and not compromised, lost, leaked, disseminated, unauthorised, published or corrupted." **(Fenz & Ekelhart, 2009).**

The strategic value of this asset is maximised with effective Information Usage; ensuring that it is available as a shared, easily accessible service within an organisation and a sound Information Management Doctrine with good governance, business continuity, administration, dependable infrastructure and services as indicated in the IA Policies and Practice Framework (Figure 51). It is incumbent of any information system used to structure, store, exploit and transfer data has to be capable of tagging and logging the storing, retrieving, moving, copying, modifying and deleting of any information. "*Under the current DoDI 8510.01, IA managers encounter difficult obstacles associated with monitoring IA situational awareness, conducting IA control validation activities, summarizing validation results, and attempting to preserve the IA posture of their systems individually and collectively as part of a larger System of Systems,"* **(Landree, Gonzales, Ohlandt, & Wong, 2010)**

The IA Policies and Practice Framework (Richardson C. J., 2012) provides the practitioner a comprehensive matrix of the important issues of Information Assurance in a Socio-Technical Enterprise. The 12 Domains of the Framework are:-

- Administration Policies
- Auditing
- Risk Management
- Business Continuity
- Personal Security
- Enterprise Security
- Physical and Environment Security
- Communication Security
- Infrastructure Assurance
- Cyber Assurance
- Incident Management
- Standards

The military Cross Domain Solution (CDS) requires an assured system architecture that provides an automotive and/or manual ability to access, transfer and store data between two or more differing security domains (DoD DISA, 2008). The US DoD Cross

Domain Solution is planned to provide net-centric, service-oriented, cross domain information sharing solutions with guaranteed quality of service for authorized users anywhere on the DoD's Global Information Grid (GIG). Within the UK's MoD there is a need resolve the assurance and accreditation concerns of CDS within the ISTAR community.

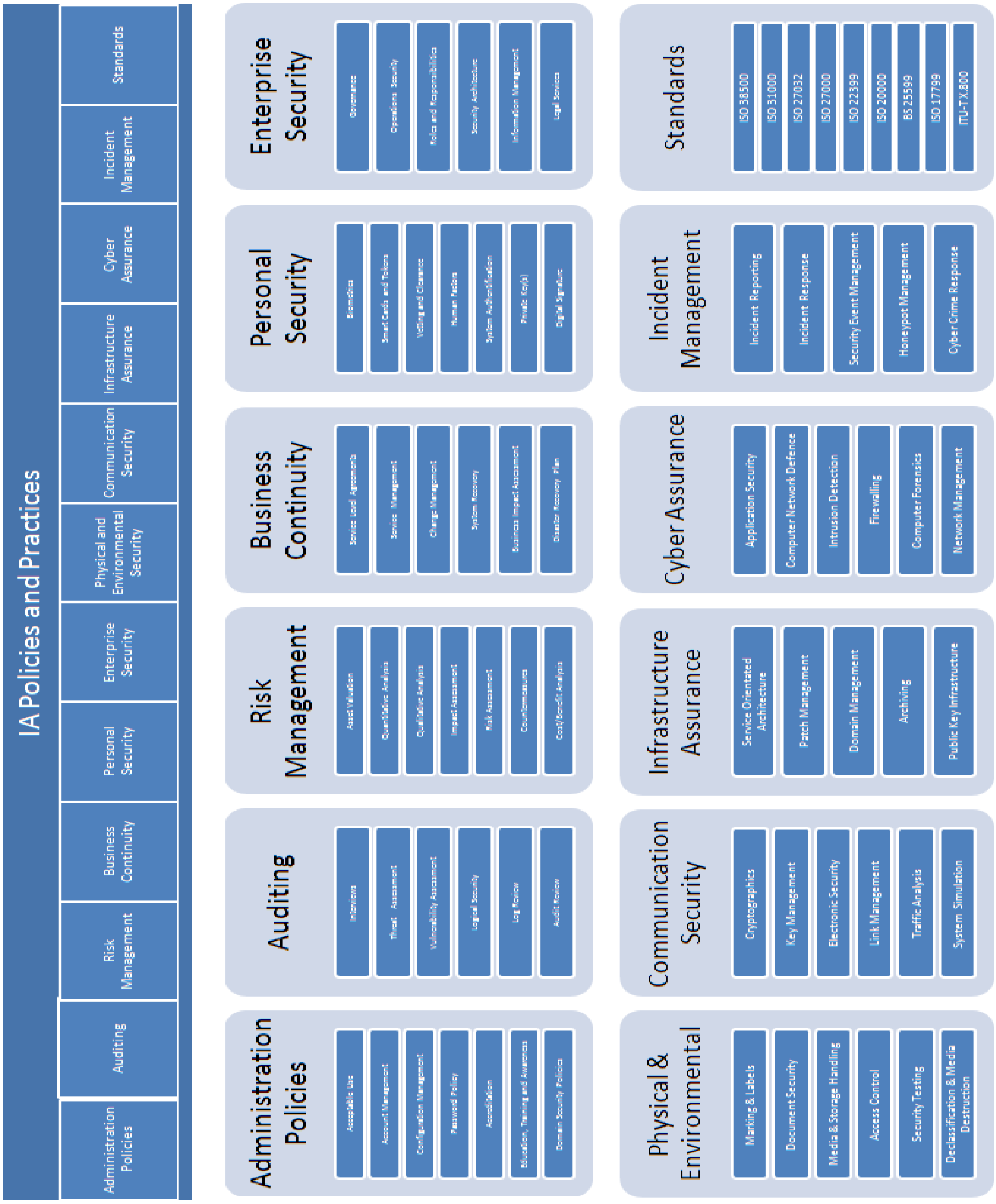
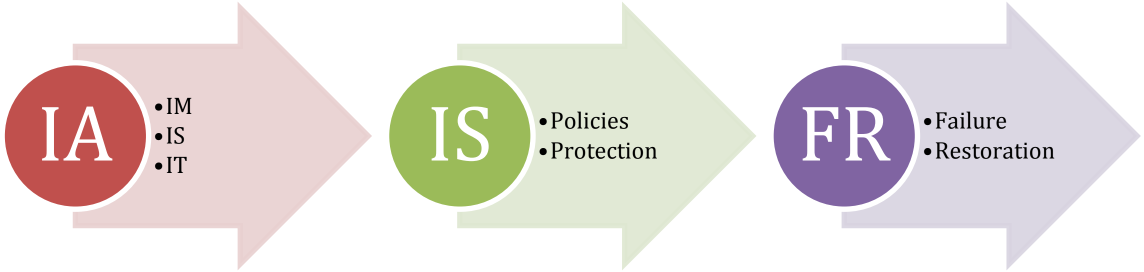


Figure 51: IA Policies and Practices, (Richardson C. J., The Assurance of Socio-Technical Enterprise Operations, 2012)

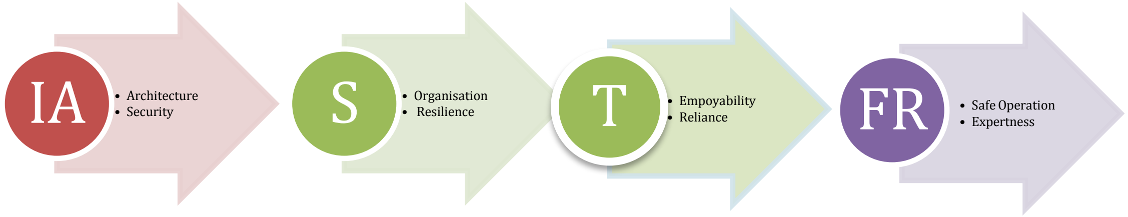
There are a plethora of operational Communication and Information Systems (CIS) which we continue, to want, to integrate both within existing command structures and with our coalition partners. These systems of systems grow out of operational necessity and are becoming more interoperable and integrated platforms that formulate an interdependent, complex Enterprise Architecture (EA) as illustrated in figure 140. Such new EAs will require considerable time and skill to complete full accreditation, and the accreditation process itself will need to converge with all partners. This expansive, evolving environment (SPS Components) will exhibit emergent properties that the stove-piped, single discrete security domain accreditation approach may overlook. Furthermore potential vulnerabilities introduced at the interface between an ever-increasing number of exploitive Information Services and Systems and by increasingly complex network connections may be undiscovered. There will also be consequential expense (cost in time, further analysis, training and verification) implications to assure these aggregated, heterogeneous Information Systems for Accreditation.

The Information Assurance Diamond Model

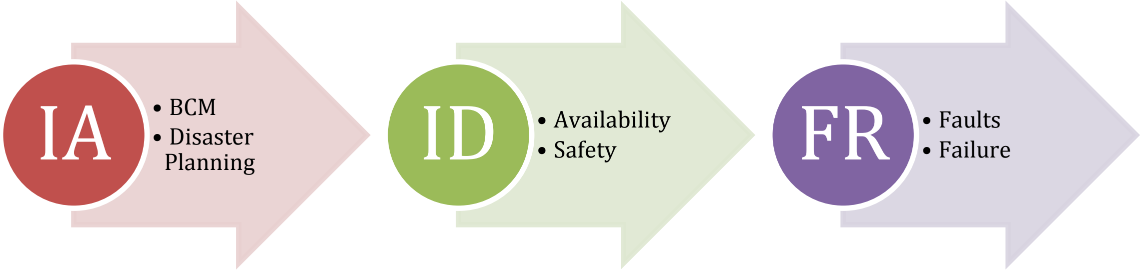
The Information Domain as illustrated in Figure 51 has a number of Enterprises and other formations that exploit the services, systems and archives of the Information Storage and Service Domains. To ensure that the information flow is trustworthy, the model requires a holistic IA Framework. Taking Information Assurance as the focal point of a resilient, robust military network, the central Information Service Domain in figure 140 requires an Information Security policy to protect the Service Domain from any malicious error, fault and failure conditions.



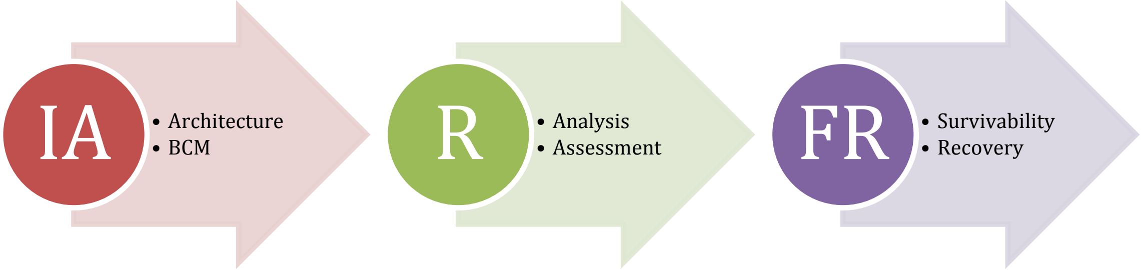
Information Assurance aligns the Information Domain interconnectivity with a structured approach that reflects the trusted roles and responsibilities of the communities of interest, their vetting, clearances and access privileges.



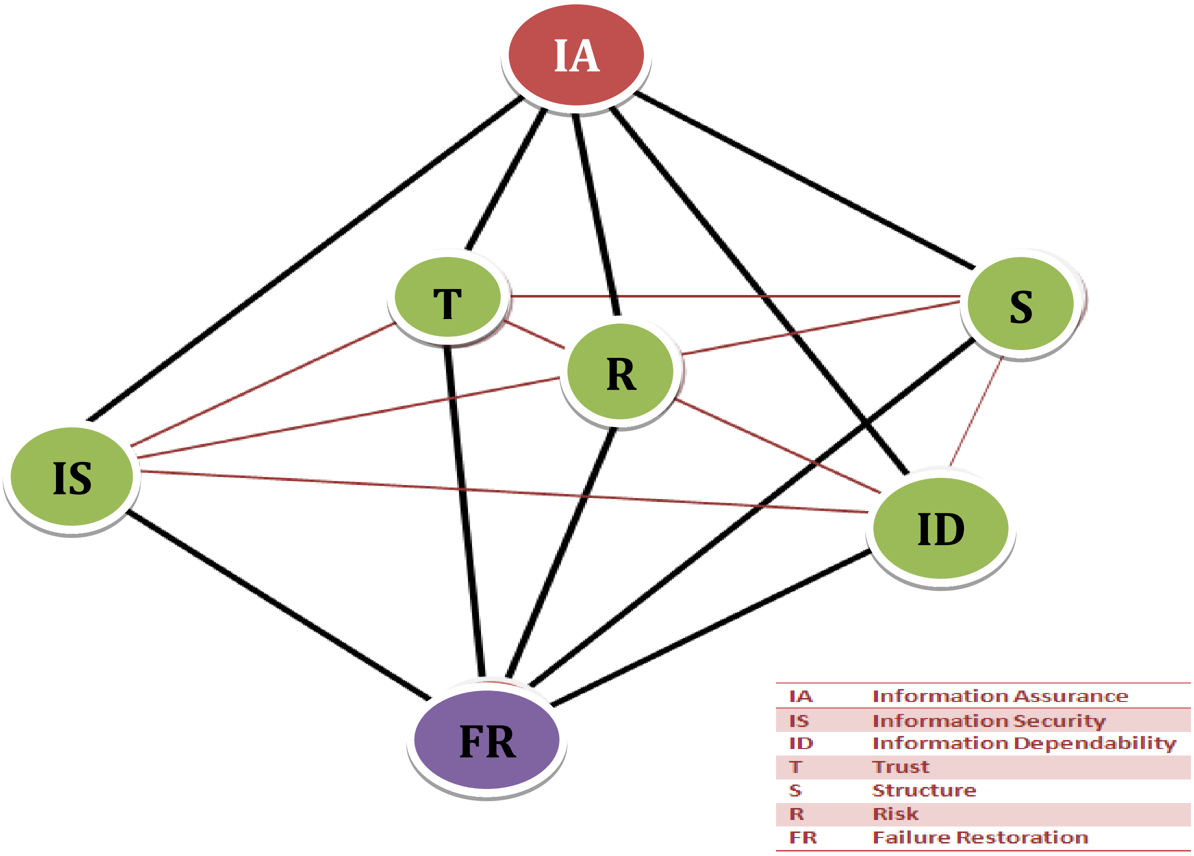
These Enterprise systems need to provide safe and dependable operations to reduce the incidents of system faults and failure.



Risk Management reviews the probalitity of a malicious event and the impact that it might have on the system failing and its ability of recovery.



These conceptual routes of IA providing a robust Socio-Technical Enterprise can be framed as the diamond model as illustrated in Figure 52.



IA	Information Assurance
IS	Information Security
ID	Information Dependability
T	Trust
S	Structure
R	Risk
FR	Failure Restoration

Figure 52: The Information Assurance Diamond Model

The IA Model Quadrant

"Interoperability enabled by Communication and Information Systems37 (IO by CIS) has been defined as...'the ability of systems, units or forces to provide services to and accept services from other systems, units or forces and to use the services so exchanged to enable them to operate effectively together'. ***(MoD ACP167, 2011).***

The basic 4 part model as illustrated in Figure 142 (and developed from Figure 39, p275) doesn't fully illustrate the increasing dependency exhibited with our military communication networks (Brass, Galaskiewicz, & Greve, 2004) and their service architectures (Lund, Eggen, Hadzic, & Hafsoe, 2007) which has significantly heightened concerns regarding their reliability (Soliman & Janz, 2004); security (Phillips, Ting, & Dem, 2002); dependability (Al-Kuwaiti, Kyriakopoulos, & Hussein, 2009); impact to business continuity (Sikich, 2003; VanVactor & Gill, 2010) and operational effectiveness (Cebrowski & Garstka, 1998).

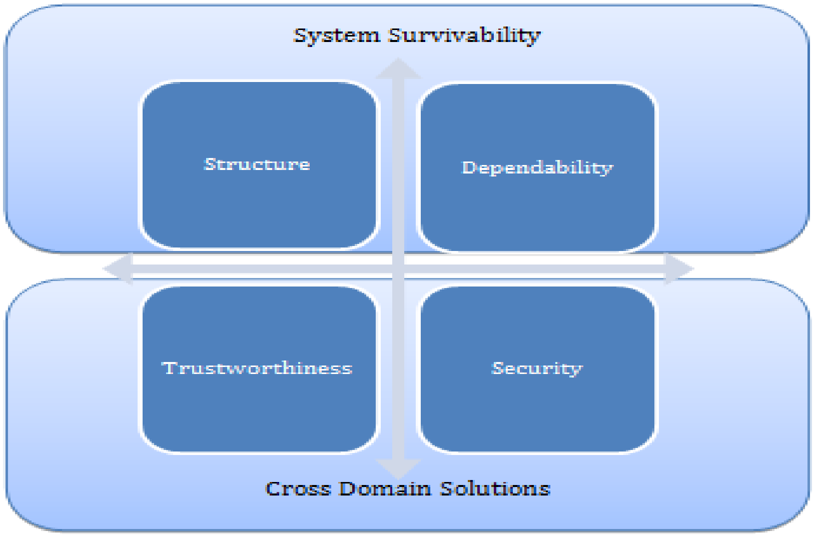


Figure 53: Building the IA Contextual Model Quadrants

[37] IO enabled by CIS management and assurance is mandated by the MoD's Vice Chief of Defence Staff (VCDS). It is mandatory for all UK MOD acquisition projects containing Communication and Information System (CIS) - regardless of financial approval category, lifecycle stage or operational theatre - unless agreed otherwise with the MoD Systems Engineering and Integration Group (SEIG). Available at: http://www.mod.uk/ DefenceInternet/FactSheets/InteroperabilityEnabledByCommunication AndInformationSystemsioByCis.htm (accessed 15th March 2011).

There is a critical dependency on these complex (Lukasik, 2003; Luiijf, Nieuwenhuijs, & Klaver, 2008), highly connected, interacting systems where their interoperability may inherently produce major consequential impact upon critical and cross domain operational infrastructures from minor/simple network intrusion, failure and security violations (Qian, Joshi, Tipper, & Krishnamurthy, 2008). These risks exemplify the cross domain problems, where NEC interoperability and the "*Need to Share*" are now mandated across MoD Networks. Research and development of military systems have often focussed on system functionality with security and dependability being independently pursued. These network fundamentally command and control modern military operations and that their information flows and exploitation are critical to Situational Awareness and Decision Making. The MoD's Information Strategy (MODIS, 2009) linking Enterprise Architecture and Information Assurance have articulated the need to provide robust, dependable, fault-tolerant, secure and trusted networks. Enterprise Architecture and Information Assurance are positioned to converge these capabilities and provide intrusion-tolerant systems. At the 2011 Cyber Warfare Conference, a USCYBERCOM General quoted that with the increased and more sophisticated cyber threat to Government and Military infrastructures and supporting networks that we must "*expect and acknowledge that our networks are already compromised and that we have intrusion*".

> *Our objectives are a secure and resilient United Kingdom, and shaping a stable world. In pursuit of those goals, our highest priorities are tackling terrorism, cyber security, international military crises and national disasters such as floods and pandemics."* Prime Minister David Cameron.

The admission that we cannot have absolute security on firewalled, encrypted, IPS, personnel vetted, air-gapped classified systems is a significant statement from military sources. There are increasing frequent numbers, multiple types of attacks, attack vectors, attack agents and malicious viruses are inflicting constant intrusions to our networks. Measured in the tens of thousands per day, these cyber assaults have become a national concern (Ministry of Defence, 2010).

However, it's not just the dependencies on the performance and functionality of the systems that Enterprise has become reliant upon, but how the systems interact with each other and with the communities of interest. This Human-Cyber interexchange is at the heart of the Socio-Technical Enterprise and Information Assurances provides the many of the trustworthy bridges that exist between these two domains as illustrated in figure 54.

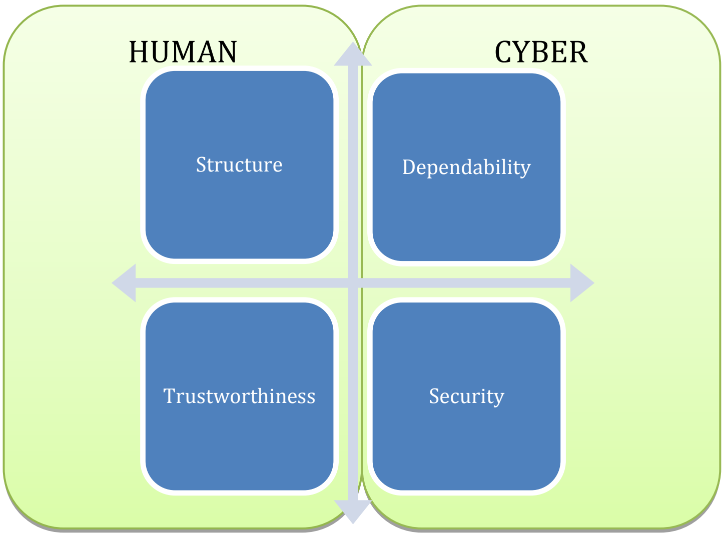
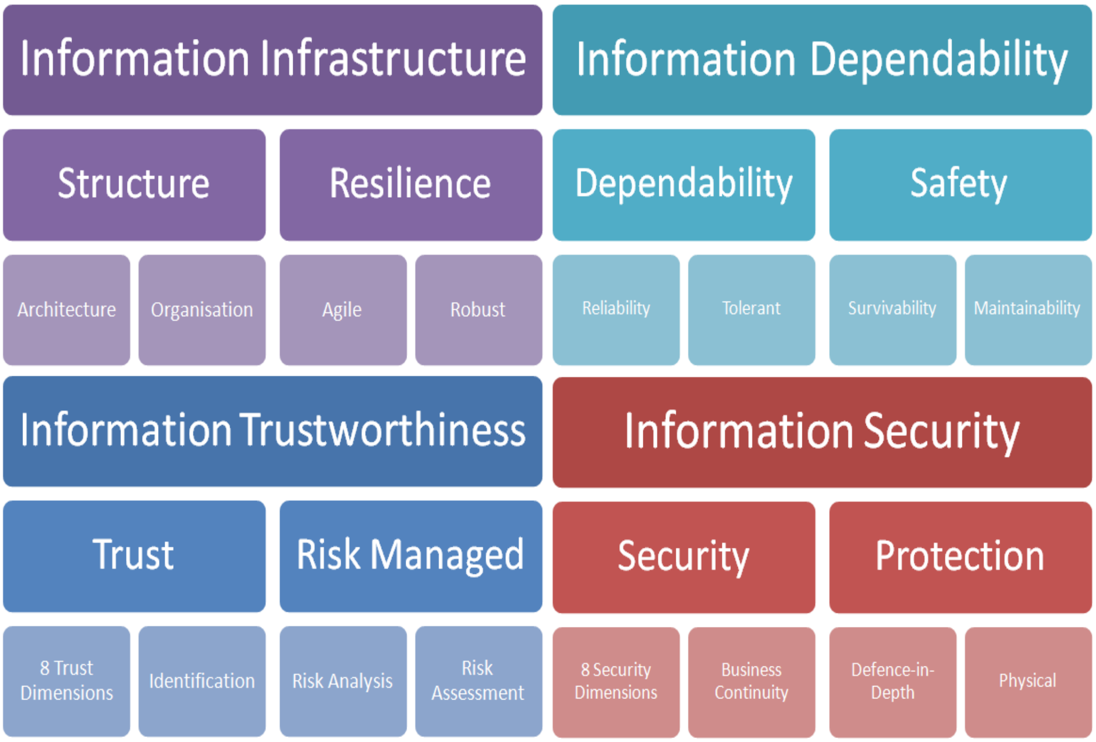


Figure 54: An IA Perspective to the Human-Cyber Interexchange

The IA Model Quadrant, as illustrated in Figure 55, brings back the need to holistically view Information Assurance from four key areas of study:- (1) The System Engineering and Enterprise Architecture of the Information Infrastructure; (2) The investigation and modelling of System Dependencies and Safety; (3) The building of better, more cost effective security and protection devices and (4) controlling change, Human Factors and culture of the environment through Trust and Risk Management.



Information Infrastructure				Information Dependability			
Structure		Resilience		Dependability		Safety	
Architecture	Organisation	Agile	Robust	Reliability	Tolerant	Survivability	Maintainability
Information Trustworthiness				Information Security			
Trust		Risk Managed		Security		Protection	
8 Trust Dimensions	Identification	Risk Analysis	Risk Assessment	8 Security Dimensions	Business Continuity	Defence-in-Depth	Physical

Figure 55: The IA Model Quadrant

The quadrant illustrates the hierarchal construction of the 4 principle disciplines of Information Assurance; however a more holistic view would be depicturing the cyclic nature of those disciplines and their component elements which all interact with each other. The view exhibited in figure 55 demonstrates how architecture can affect the systems information dependency, how safety influences protection, how security is risked managed and how trust affects organisation hierarchies.

The cyclic nature of the model illustrates (as exhibited in Figure 56) the need not to focus not on anyone discipline within the Art and Science of Assurance, but to continue to re-examine, analysis and evaluate its impact, direction and guidelines. IA needs more research and development, more intellectual and industrial debates, more discussion across a greater segment of society and more education in our schools, colleges, universities and workplace. The Socio-Technical Enterprise has to evolve in this new dynamic marketplace, but it has to protect its information assets, its communities of interests, the organisations that work with it and the Enterprises for which its services, products and values that have become to rely upon it. In the Information Age, everybody is becoming connected, and those connections are becoming pervasive and dependent to our society.

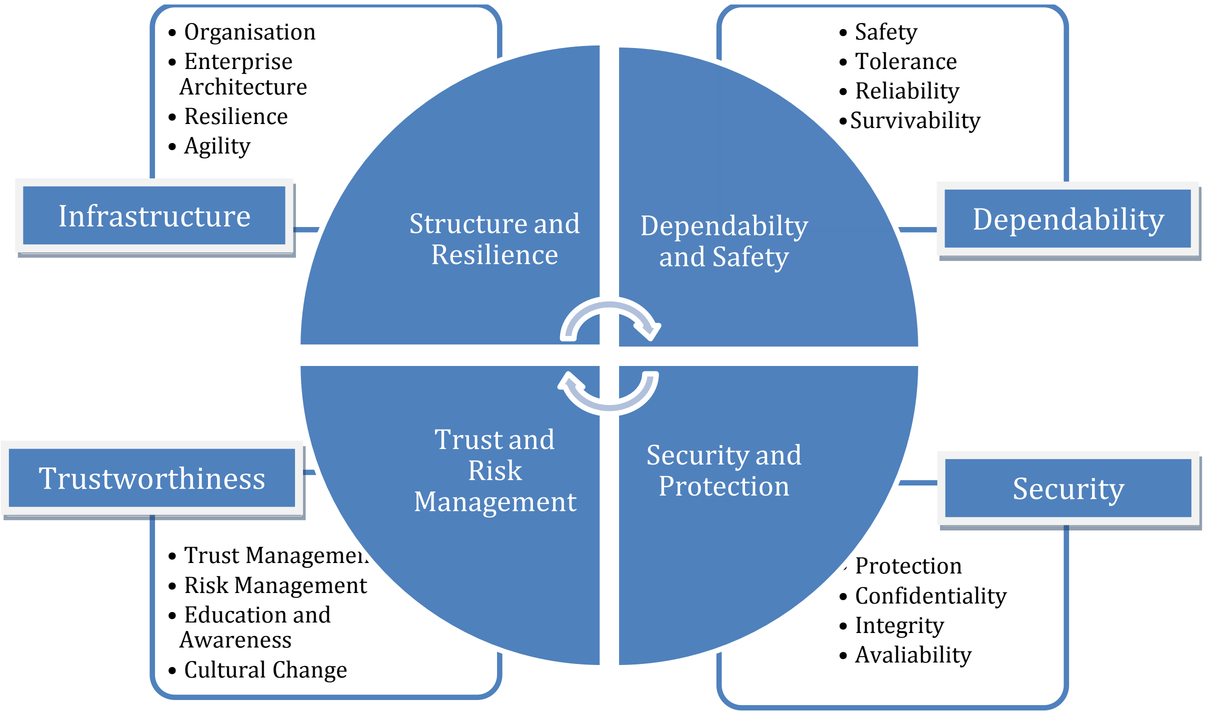


Figure 56: The Cyclic Nature of the IA Model Quadrant

Information Infrastructure: IA Components of Structure & Resilience

In chapter 3, the arguments were focused on the Architecture and Interoperability of the Enterprise. These arguments help create this first quadrant of the IA Model. The Socio-Technical Enterprise will create a changing environment, often led by technological innovation, but will be sustained by its social desire, wants and needs. Information Assurance has to address the business processes and their alignment to other internal and external processes that involves Information Assets, Process, Storage and Transit.

With ubiquitous systems, the complex expansive and evolutionary (Strategic Positioning) environments with ever-changing, agile networks boundaries need Resilience, defined by Jean-Claude Laprie (2008) as the "*persistence of dependability when facing changes*", having tolerance to cope with unanticipated events and boundary changes caused from interoperable interconnection. The classical development of Resilience is of system persistence of service in periods of change that be dependably delivered. These Resilient services can be justifiably called trustworthy in an agile environment.

Table 9: IA Resilience Attributes

	RESILIENCE ATTRIBUTES	
1.	**Tolerance**	Coping with situations exceeding the System's specifications and expectations
2.	**Robustness**	The System retains its ability to deliver services in conditions which are beyond its normal domain of operations
3.	**Adaptability**	Coping with an evolving system and having the ability to evolve whilst executing
4.	**Utility**	The utility and diversity of the system to perform whilst coping with threats
5.	**Accessibility**	Confident access to secure, verifiable and evaluated services

The linkage between the attributes of the systems architecture and the architect of the business processes and Enterprise Structure has many creative and innovative tracks to be researched, developed and pursued. One of the more pressing is the building of tolerances into the socio-technical system. Many technical systems have failed catastrophically when confronted with malicious attacks or major design errors. Information Assurance is a methodology that will question the Enterprise architects to minimise risk and to create policies, procedures, good practice and techniques to ensure robust structures; more tolerant operations; greater utility of services; better access to the community of interests and a more tolerant working environment to intrusion and faults. Socio-Technical Enterprises require an assured purpose, a secure environment, dependable capabilities and a culture of trust.

Information Dependability: IA Components of Dependability & Safety

The second component of the IA quadrant is the disciplines of System and KID dependability and socio-technical system safety. The more complex and integrated our real and virtual worlds become, the more reliant we become on them performing correctly. Enterprises are becoming more dependent on the interdependencies of its systems and those of other Enterprises with its becoming more interoperable with. The sharing environment requires dependable services and information and dependable knowledge management, transfer and understanding which both rely upon dependable data from our data sources.

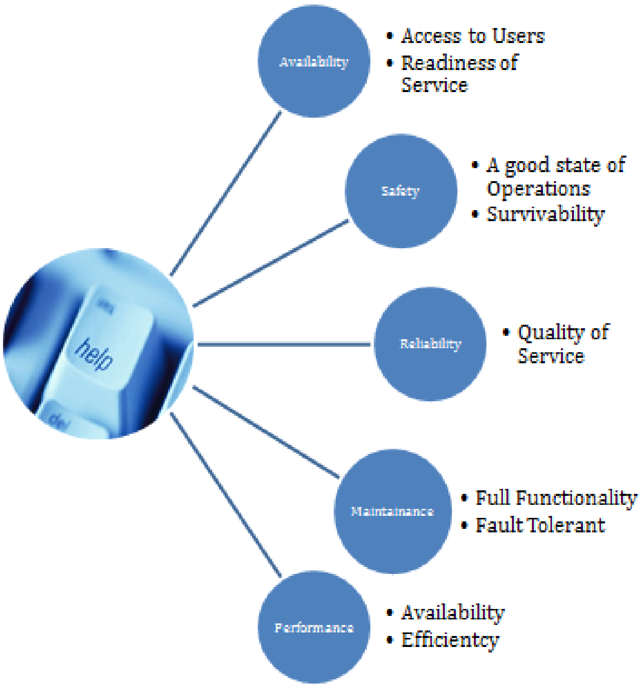


Figure 57: Assured Information Dependability is the fabric of the Socio-Technical Enterprise

System survivability is a cornerstone of Enterprise Assurance. The Socio-technical Enterprise have become custodians of the Critical Information Infrastructures in which our society and culture has adopted and become ever increasing reliant upon. These Enterprises themselves have to become dependable. Figure 146 illustrates that safe and healthy operations, that is routinely checked up (audited), that maintains the good state of its operations within performance tolerances, is agile and flexible to the access needs of its communities; capable of improving its readiness of services (across SOA platforms) and quality (QoS); is good enough to respond to threats and its own vulnerabilities will provide a trustworthy Enterprise capability and ensure system survivability within its own risk appetite. Safe and dependable operations provide firm foundations for a successful Socio-Technical Enterprise and its opportunities to grow in a complex, sometimes hostile, environment. The objective of this Assurance model is to provide a trusted solution to the communities of interest that will allow system confidentiality, integrity, availability, no-repudiation, authentication and access control. The Cross-Domain solution requires a de-confliction of the "*need to share* " aims and objectives and the current "*need to know*" principle where current military systems, implementing the Bell-LaPadula Model (Bell & LaPadula, 1973; Bell, Looking Back at the Bell-La Padula Model, 2005).

Information Security: IA Components of Security & Protection

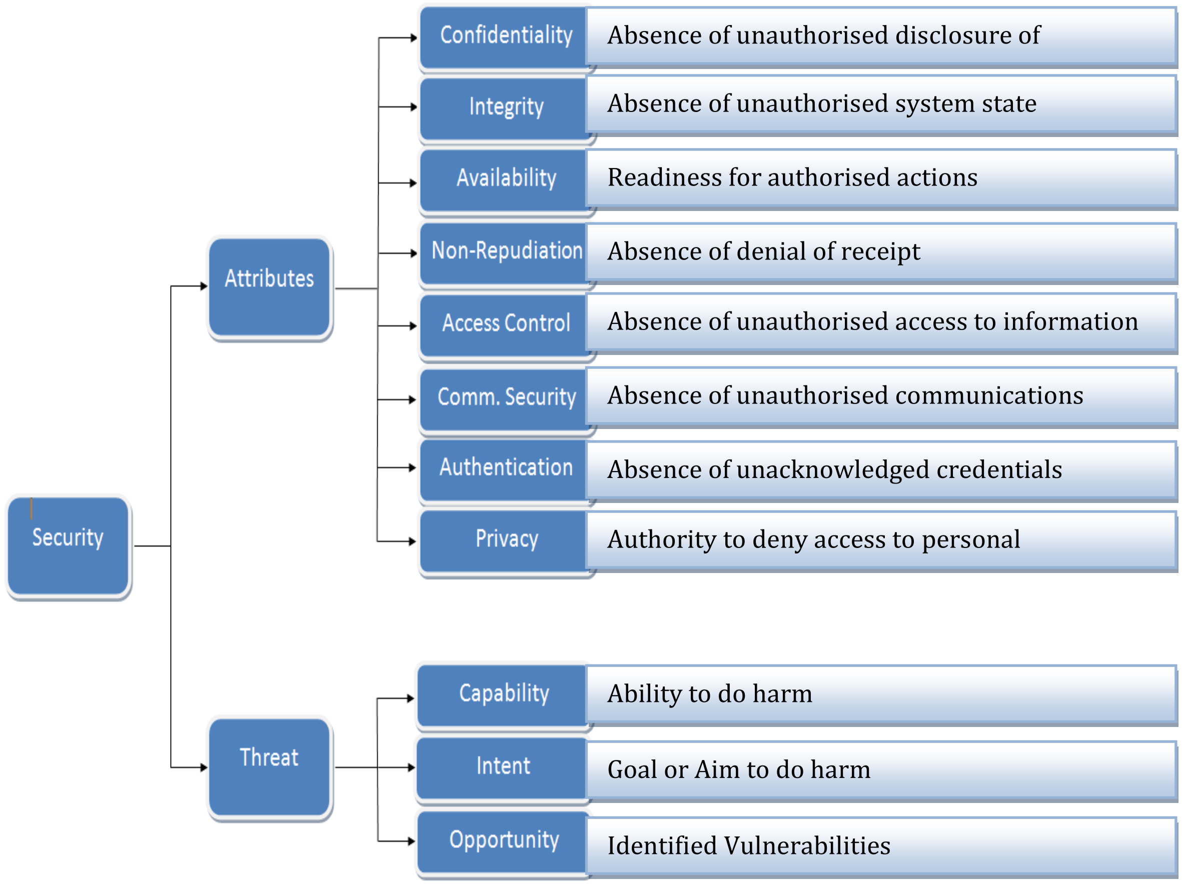

Security
Attributes
Confidentiality
Absence of unauthorised disclosure of
Integrity
Absence of unauthorised system state
Availability
Readiness for authorised actions
Non-Repudiation
Absence of denial of receipt
Access Control
Absence of unauthorised access to information
Comm. Security
Absence of unauthorised communications
Authentication
Absence of unacknowledged credentials
Privacy
Authority to deny access to personal
Threat
Capability
Ability to do harm
Intent
Goal or Aim to do harm
Opportunity
Identified Vulnerabilities

Figure 58: Security Attributes to the IA Model

The Assurance of a System is often cited by its levels of Protection and Security Markings. Information Security is the protection of information and information systems from System Susceptibility and these attributes are listed in figure 58**.** It has been defined as the prevention of unauthorized access, use, disclosure, disruption, tampering, modification, interrupting or destruction in order to provide integrity, confidentiality, and availability (NIST, 2003). A secure system is the absence of unauthorised access to, disclosure of, or handling of, system state (Avizienis, Laprie, Randell, & Landwehr, 2004). Furthermore, the ITU-T X.805 Recommendation (2005) adds 5 more dimensions (Non-Repudiation, Access Control, Communication Security, Authentication and Privacy) as attributes to reduce *System Vulnerability*[38] to the 3 established tenets (Confidentiality, Integrity and Availability) that allow systems to Detect, React and Adapt to deny threat Capability, Intent and Opportunity (Little & Rogova, 2006; Gasper, 2010). To ensure that the security policies, procedures and guidelines are adhered to and accomplished, the Enterprise has to deploy protection mechanisms as illustrated in figure 59.

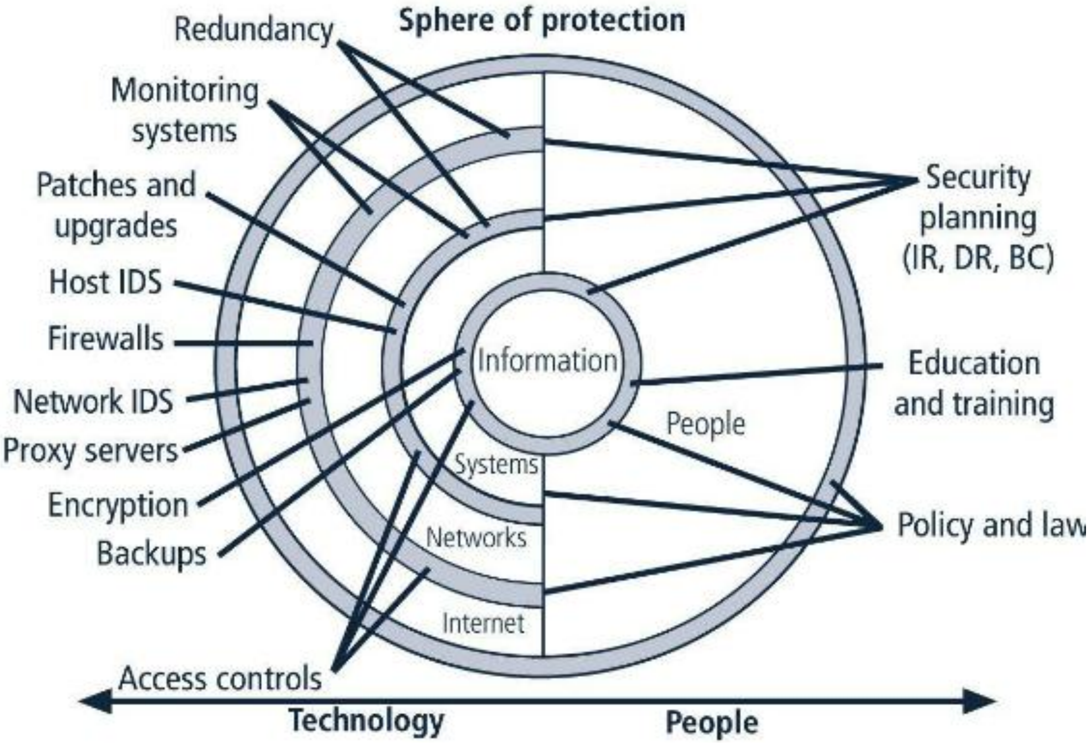


Figure 59: The Sphere of Protection to the Socio-Technical Enterprise (Keller B. M., 2011)

[38] System vulnerability is defined to be the intersection of a system susceptibility or flaw, access to the flaw, and the capability to exploit the flaw.

Information Trustworthiness: IA Components of Trust & Risk Management

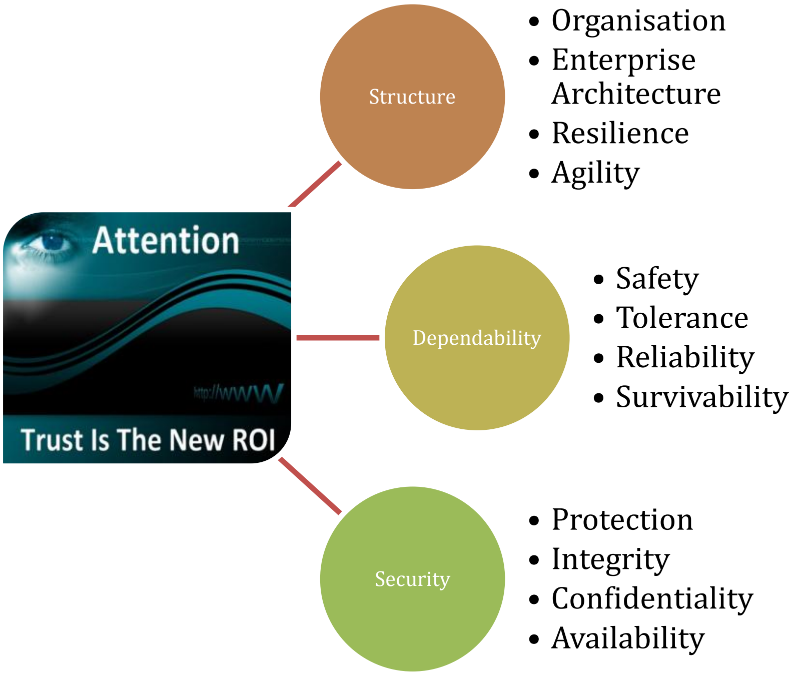
The fourth component of the IA Quadrant is Information Trustworthiness. The heart of the Socio-Technical Enterprise is its ability to manage its risks and maintain trust in both the real and virtual worlds. There are conflicting notions that trust can and cannot exist in Cyberspace (van Swaay, 1992; Committee on Information Systems Trustworthiness, 1999; Minsky, 2003; Sterner, 2011). The emergence of our Information based, networked, society requires people to make superior, trusted, decisions from services, applications and data presented from cyberspace. The building of trust and relationships with online users, clients, customers, suppliers and cyber agents is of major importance to the online economy, social networks and coalition enterprises (Luo, 2002). In our 3 layer model, the Social Domain relies on social networking of the Human-Cyber Interexchange peer-to-peer cyber connectivity. This communicative world is veiled in anonymity, usurpation, covert channelling, coercion and subversion where our Cyber based interactivity and interactions can produce a "*disinhibition effect*" (Suler, 2004) in an uncertain world, where fear and doubt is common place; yet it's our chosen space to social network, conduct e-commerce and publish thoughts, knowledge, media and private details. Can we trust our trust under such circumstances?

The recent EU study looking towards the future of the Internet (European Commission, 2010) identified that culture changes had a face of visibility – that there exists a *balance between ubiquity and security, pervasiveness and privacy, centralization and surveillance. Visibility could be seen in terms of two main "faces" of the internet:*

1. Visible internet applications, obvious to users, requiring input or observability
2. *Invisible internet applications, operating without active user input or observation.*

The report noted that: *Difficulties arise when dealing with the second "face", ie which aspects should be invisible, and how? This concept invokes the multiplicity of the future internet and how it will be manifested. Major sources of multiplicity include: privacy domains – an internet analogue of public and private space; identities; levels of user trust (eg high security retail vs. no-control segments); national or regional internets; and so on.* For the Socio-Technical enterprise, the context of trusts, its maintenance and improvement is cost of doing business in Cyberspace. In fact, trust is the new Return of Investment calculation for its corporate viability and values.

In creating Trust in the Enterprise; how can the Human-Cyber interface can be viewed as a trust relationship? Can we create trust in Cyberspace? These two important questions are still to be resolved in finding Cross-Domain Solutions. An assured solution for the Enterprise architect requires the development of trust, trusted systems and system integrity as well as strategies for achieving dependable, safe and secure services, systems, infrastructures and networks. Is trust a people thing, or can things affect our trust.



- Organisation
- Enterprise Architecture
- Resilience
- Agility

- Safety
- Tolerance
- Reliability
- Survivability

- Protection
- Integrity
- Confidentiality
- Availability

Figure 60: Trust is the new ROI for the Socio-Technical Enterprise

How can we decide when to trust and does trust generate acceptable risk? Can we assure trust? The model allows to the questions to be asked and directs its other 3 quadrants to argue and support solutions. The other component of the quadrant is risk management. which has a direct effect on the security and resilience of a system. The amount of risk in what is acceptable and what is unacceptable derives the Enterprise Risk Appetite. This appetite is maintained if the system performs within agreed tolerances and benefits the Enterprise and its operational capability, however it can be eroded if Risk Management becomes checked boxed, non-compliant, lost in focus or neglected. Intolerances are the nemesis of the Social Technical Enterprise.

3.4 Creating a Reference Model for IA

Information Assurance (IA) *is the assumed responsibility (Corporate Governance) and accreditation of a socio-technical Enterprises across the 5-layers of the Cyber Domain (Geographical, Physical, Logical, Persona and Cyber Persona), inclusive of their Business Processes, Information Operations, Information Exploitation, Management, Services, Technologies and Infrastructures. The socio-technical Enterprise is assured by appropriate levels of maturity and awareness within the 8-Dimensions of Information Assurance (Structure, Resilience, Dependability, Safety, Security, Protection, Trust and Risk Management).* **(Richardson, C.J., 2011)**

Taking the above definition for Information Assurance and building on the modelling of IA Interoperability across the 5-layers of cyberspace and the IA Quadrant Model a Reference Model can be created for Information Assurance as illustrated in figures 61 and 62.

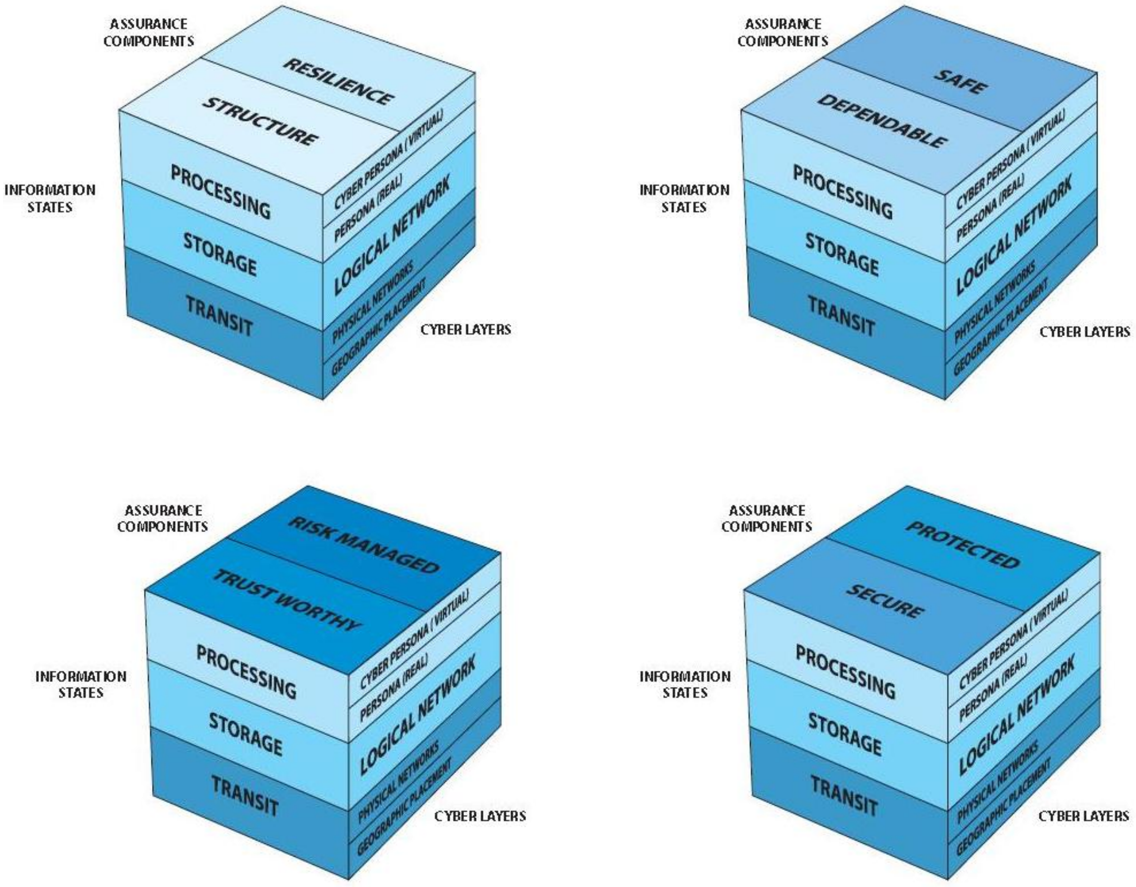


Figure 61: Matching the Quadrant model to the Layers of Cyberspace

Throughout this thesis, the arguments has been presented, analysed, modelled and where possible evaluated to create this IA Reference Model. By taking any of the 3-Dimensions, an IA practitioner can start to analyse a Socio-Technical Enterprise and its Systems from an Information Assurance Perspective.

In Bridging the Gaps, Information Assurance provides a Strategic, Operational and Tactical perspective that allows an Enterprise to function in a robust and resilient manner, with a high degree of dependability, safe and secure operations; protected and risk managed and above all…Trusted.

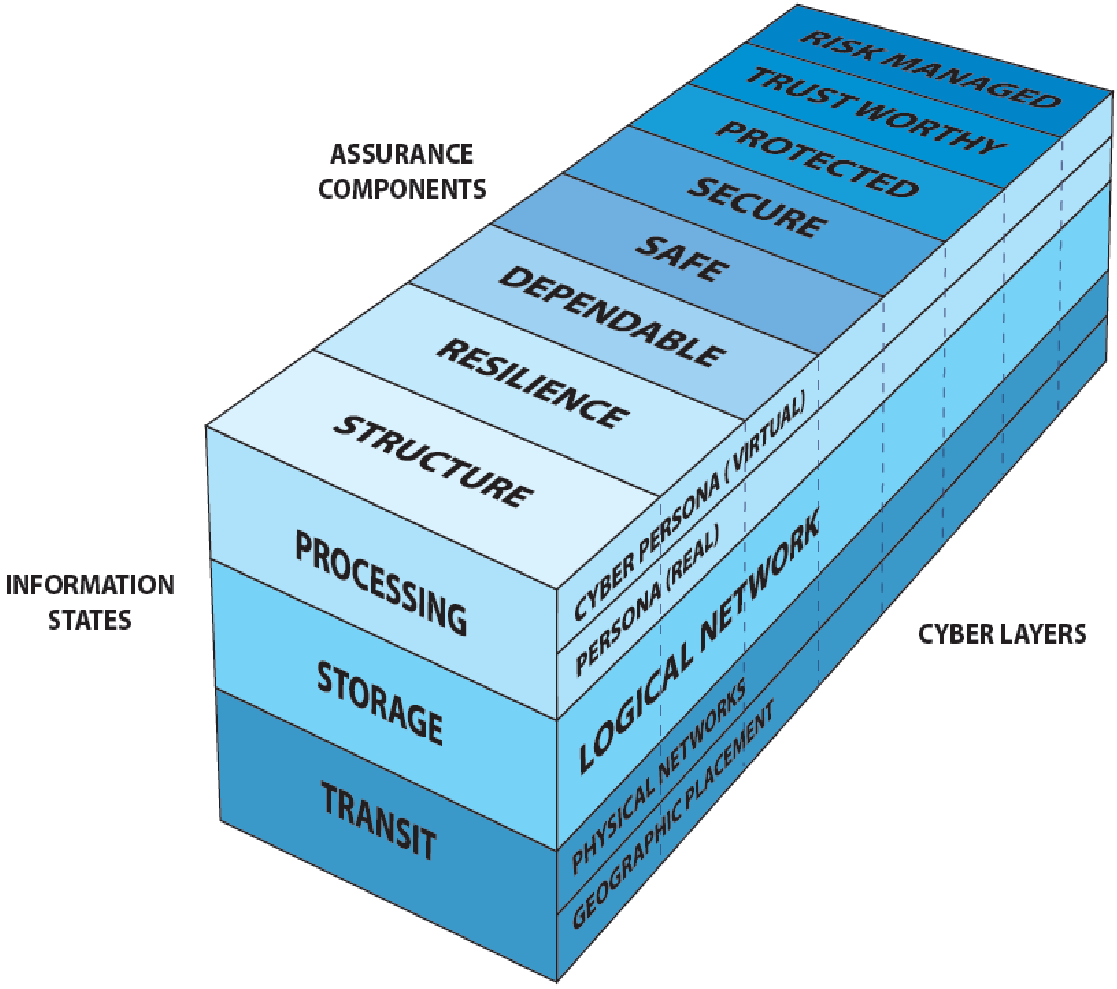


Figure 62: The Information Assurance Cuboid Model

CHAPTER 4:

Bridging Gaps in Education and the Profession

Whether researching new technologies or implementing information risk management initiatives, information security professionals are being held to even more stringent standards than ever before. (Frost & Sullivan, 2008)

Sir Isaac Newton's work once inspired and reassured a world that was ready to be enlightened. His original ideas that "***results were proportional to the forces applied"*** and that "**cause precedes effect"** generated a *determinism* outlook to the world (Baggott, 2004). Determinism has long been used as a classic model to measure the effectiveness of practitioners, including IT executives, managers, and teachers. However, in the light of the digital age has determinism become dated? Do these linear models cease to help today's practitioners to become effective cyber leaders, especially if there were some sudden, unexpected changes?

Determinism measures against a matrix through some linear process to a predictable outcome. It was used to gauge and evaluate our ability to develop skills within the matrix and thereby this *linearity* would enable practitioners to effectively predict and control human systems and human behaviour through some small incremental change (Pentland & Liu, 1999; Burns, 2002). Early UK Network Enabled Capability (MoD, 2009a) skill matrices emulated this deterministic skills process to augment the technological development of Netcentric Warfare with a matrix of defined roles and responsibilities (Alberts, Garstka, & Stein, 1999). The matrix defined the necessary educational and experienced required for each role and how that role fits within the Command and Control (C2) of the Organisation (UK, NATO or some other Coalition). However, this work soon produced a vast database with an ever increasing complexity owing to frequent movement of personnel within MoD. Time in posts was short (normally 2 to 3 years, and sometimes a lot less) and the individuals had few opportunities to engage in skill up-training (for the post they occupied or even prepping for their next post). A more inclusive methodology was needed to provide sufficient capability within an organisation that allows for the agile deployment of its staff and builds the necessary infrastructure for training and education. MoD's Information Strategy (MoD, 2011) recognised that up-skilling was pivotal to its doctrine and exonerated in the UK's Cyber Policy (Cabinet Office, 2011a). Since the publication of the National Information Assurance Strategy (Cabinet Office, 2007) the need to quantify what the professional IA standards were required and the level of education specifically needed have been discussed and with many policies promulgated through many government departments. The Cabinet's Office Central Sponsor for Information Assurance (CSIA) and its General Information Assurance Products and Services Initiative (GIPSI) brought together more representation towards an IA standard from central and local Government, NHS, Criminal Justice Network, Industry, Commerce and Academia. This work was continued later on by CESG, Department of BIS, DfE and the Information Assurance Advisory Council (IAAC). Six years on and the UK still has to create a National Occupational Standard (NOS) for Information Assurance or even produce a comprehensive national framework to supply appropriate training for our cyber security practitioners.

The NOS is essential for Higher Educational Establishments to focus upon the IA issues, skills and education that Government, Industry and the wider online community needs. CESG (the UK's National Technical Authority for Information Assurance) has employed three institutions to develop its deterministic CESG Listed Advisors Scheme (CLAS) for certified Accreditors and IA Advisors: BCS, the Institute of Information Security Practitioners (IISP) and APGM-UK. This exemplifies GCHQ's specific view on the educational standards needed, but fails to recognise those of Industry, the Legal and Accountancy Professions and of the business management of e-commerce. There is a more holistic need for authorities such as CESG, BIS, DfE and IAAC to engage with a wider community and the UKAS Skill Councils (who represent Industry and Academic interests) as their actions, themes and policies will have a ripple effect from any derived national standards to the curricula, to professional development and finally to created the necessary holistic learning environment for IA to flourish both as a science and an art. A National Occupational Standard will provide a necessary bridge and driving forces to the educational gap between what the UK enterprises and their organisations requirements (and retraining) and what training and education can delivery within the current national education framework.

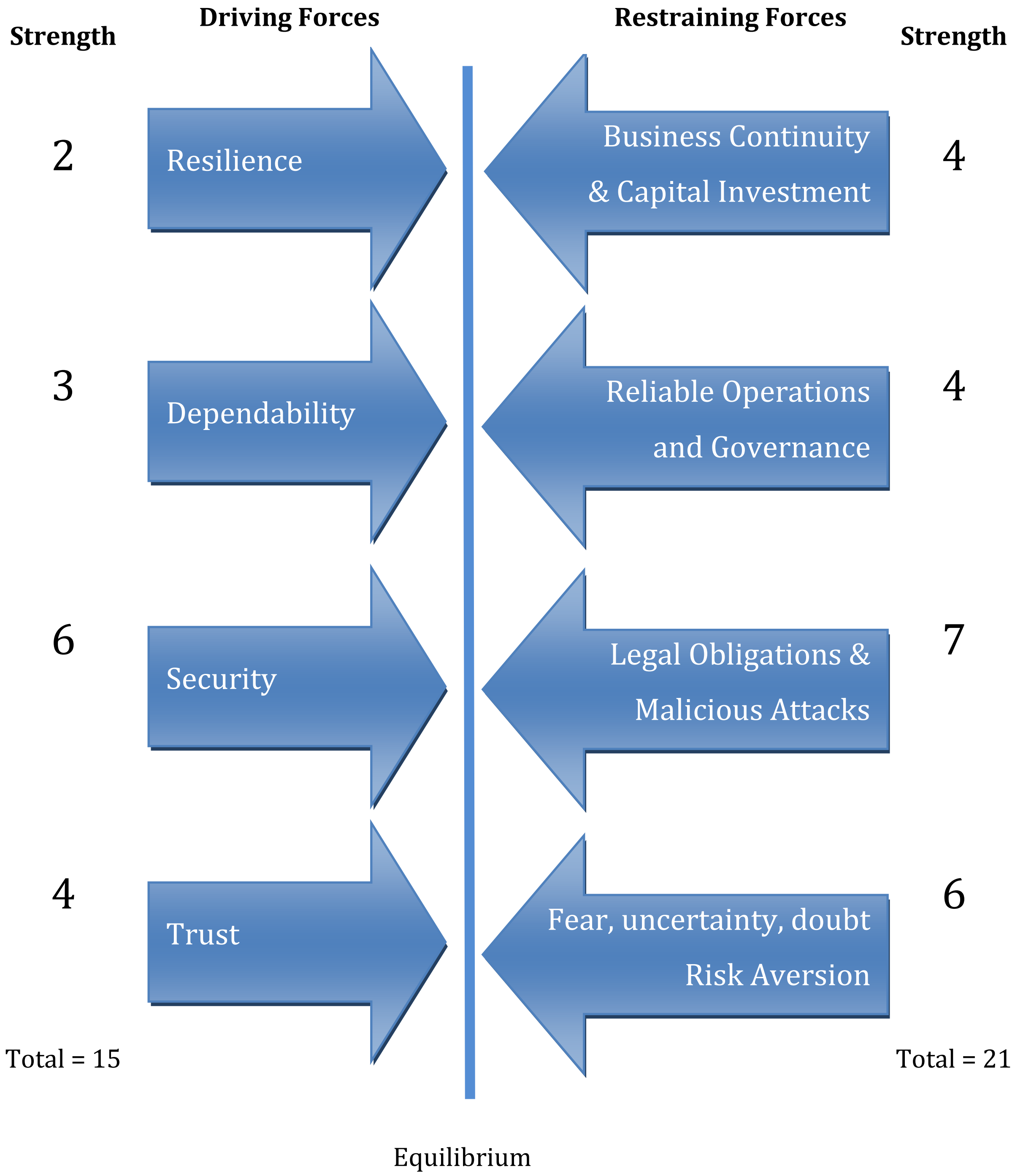

Strength
Driving Forces
Restraining Forces
Strength
2
Resilience
Business Continuity & Capital Investment
4
3
Dependability
Reliable Operations and Governance
4
6
Security
Legal Obligations & Malicious Attacks
7
4
Trust
Fear, uncertainty, doubt Risk Aversion
6
Total = 15
Total = 21
Equilibrium

Figure 63: Force Field Diagram for the Assured Information Operations

Equilibrium is required to be struck between resource allocation and necessity to change. The model (figure 153) illustrates the current imbalances between assurance and corporate reluctance and that the necessity for change would fail if a balance wasn't achieved. The three main applications (Change Management, Productivity Improvement and Decision Making) of Kurt Lewin's (1951) force field model analysis allows IA practitioners to identify and understand the Enterprise's assured state to redress the current shortfalls. The importance of this analysis is its ability to demonstrate where changes are necessary and what forces need to impact. The model has proven to be a powerful decision-making tool as Business Managers can influence the forces to maximise the corporate's risk appetite and potential of changes to succeed. Figure 63 provides strength indicators to designate the scalar levels of influence where: 1 = extremely weak and 7 = extremely strong

Many organisations are only just beginning to recognise Assurance Education; the bulk of their security budgets are paid out on consultancy and technologies; hence the high strength score marks for security and corporate legal obligations such as the Data Protection Act, 1998. Motivation to protect corporate assets has always been strong, but for most acquired information systems the need for security was often an after-thought or became a necessity after some fault condition. This late addition of security mechanisms often led to inappropriate compromises and latent vulnerabilities (Meunier, 2011).

The apparent reluctance businesses to invest time and money in skills training and IA Education, measured as resilience in this model, is in part due to their perceived need to protect corporate assets rather than tackle the more intrinsic problems of changing cultures hence the lower score of 4 in capital investments. Chapter 4 had demonstrated the need for the strategic positioning of Information Assurance and implicitly confirmed the necessity for a good education and training.

With natural disaster like Katarina , terrorists attacks like 9/11 and data losses like TkMax and Sony Play-stations, business continuity has risen in corporate governance, however little has been done to the majority of the critical information infrastructure as the data from the World's Economic Forum (2012) shows that *the latest technologies are increasingly accessible to local industries, but indications relating to confidence in the institutions responsible for developing safeguards, including those that mage the risks of emerging technologies, have not shown proportionate increases.*

4.1 Bridging the Professional Gaps

As first discussed in Chapter 1, there is a capability gap between what we *need to know* and what we know. This lack of knowledge has developed from increasing complex picture of how we operate in cyberspace and the integration and interoperation of technologies, software applications and human ingenuity. The pace of this exploitation of cyber resources has outstretched many of our training and educational programmes leaving many communities of users ignorant of the issues of interoperability and safe operations. Information Assurance in the Community is all about redressing this capability gap and developing good IA practitioners, resourcing their education and continuous specialized training. Corporate Governance mandates adherence to best practice and security policies to assure the safety and protection of their information assets. More than ever there is a need for IA practitioner's specialism to meet current security requirements. *Have our communities of interests become naïve to the complexities of Cyberspace and the Human-Cyber Interfaces?* The frantic and explosive technological pace of the Internet has not produced a corresponding cultural progression towards greater awareness of its emergent properties. Cyber security education remains stubbornly low and user community's exhibit poor behaviour towards security breaches (Cornish, Livingstone, Clemente, & Yorke, 2011).

There are too few practitioners implementing Cross-Domain Solutions and these few are having to cope with restricted budgets, reduced skilled resources and increasing complex network of networks with new properties been routinely discovered or exposed as vulnerabilities. The UK's Cyber policy (Cabinet Office, 2011a) recognises the need to change our attitude to training but it stills underfunds as we consistently fail to provide the necessary resources to train our professionals. Understandably, we all have to work within budgets, but those budgets have to be realistic to the risks involved (Bhagyavati, Agyei-Mensah, Shumba, & Kearse, 2005). When it comes to Cyber Security; Ignorance is bliss: if you don't know something, it can't hurt you - that is to say it causes no discomfort. From childhood we learnt to protect ourselves from harm but we were also willing to explore; as we age, we began to restrain ourselves for the fea**r** of others might do. This becomes more evident with our online experiences which have increasingly obtruded our awareness of its criminality and harm from malware. Cyberspace opens a new world of opportunities and making IA work will protect us in this virtual dimension. A programme of cyber awareness is necessary and Figure 64 illustrates the benefits and consequences of a blissful, exploiting but educated user community.

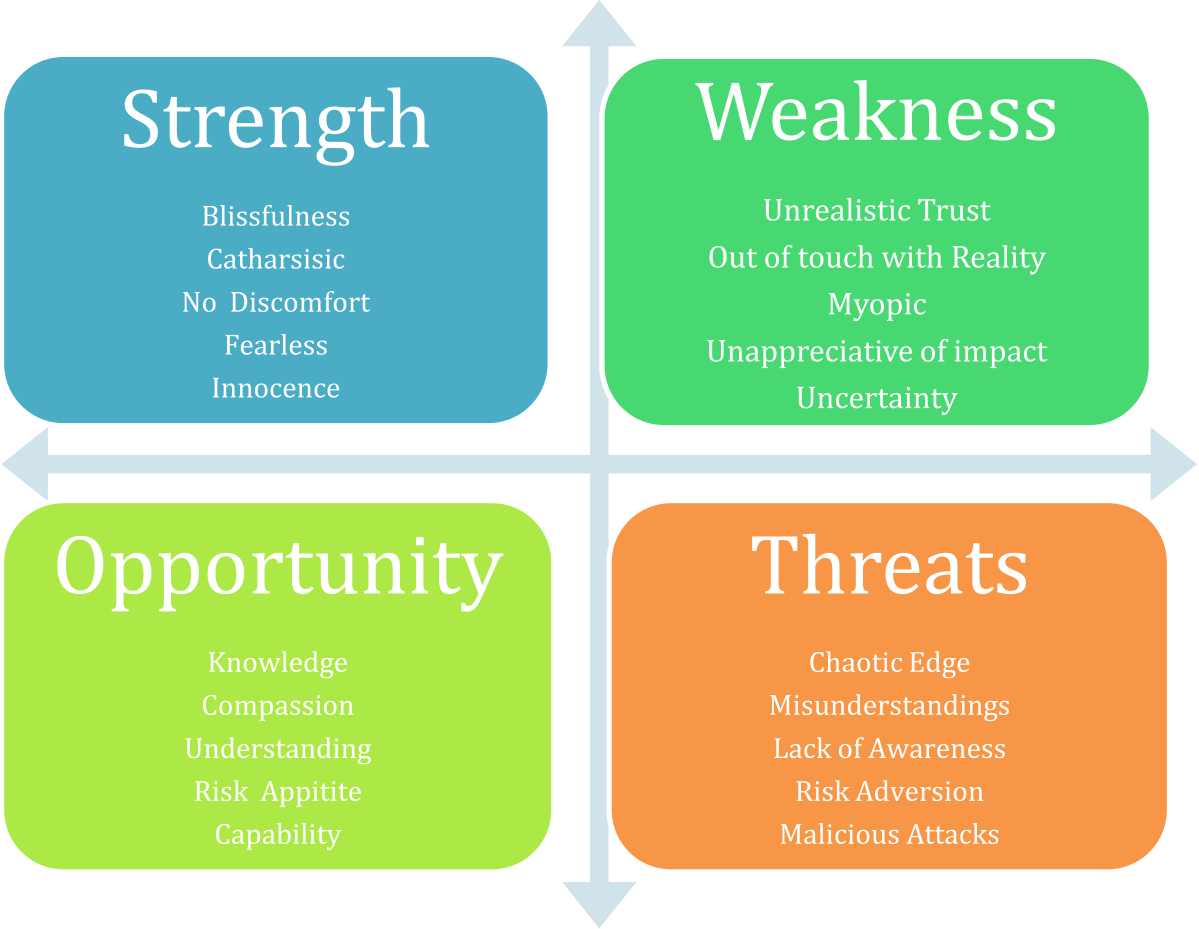


Figure 64: The SWOT of Human Blissfulness in Cyber Communities

The IA Profession needs to provide the knowledge, awareness and understanding to its cyber communities to provide more dependable and safe systems that the users can benefit from, trust, manage and exploit rather than be exploited.

IA in the Defence Community

John Colley, Chairman of ***(ISC)²'s*** European Advisory Board stated that: "*The opportunity for the information security profession is immense. Clearly we must continue to understand the evolving threat landscape coming from increasingly sophisticated criminal factions. We must also stay on top of the technology available to protect against these threats, recognising them as tools, rather than the focus of our jobs. Most importantly, however, we must recognise that our jobs are not only critical to the ongoing running of the business and protection of its assets, but also to its development and strength in the future. We are driving a change in the role of the security professional. Let us make the most of our influence.*"

Fundamentally, security is a compromise to influences, power and agenda and often may be not fit for purpose. Corporate executives have employed and later witness security professionals who did not improve the business situation, but further complicate or cause a degree of disbelieve when they present doomsday scenarios or forecast future major IT failings. These professionals are out to sell services and platforms and exploit the potential threats (malicious attacks to a risk adverse clientele) and weakness (unrealistic trust, fear, uncertainty and doubts) of an uninformed community; as illustrated in figure 111. They expose a proliferation of guidance, policies and security technologies to provide technical solutions to the issues of cyber management, architecture, assurance and exploitation; but they provide very little recognition of the skills, knowledge and education that is needed by the business community to communicate, comprehend and provide necessary cyber assurances for a sharing, informative community of people and cyber actors.

The NEC is an inter-networking cyber dominated world of Information Exploitation (IX) which is both complex and chaotic (Russell & Russell, 1999; Spar, 1999; Wheatley M. J., 2006). Cyberspace has brought about uncertainty in an environment of cyber products, services and layered networks that have slowly lost cohesion as they mash-up (Lee, 2005; Dreyfus, 2008). NEC Command and Control, cyberspace management and leadership not only needs it's personnel more experienced in its many capabilities, but also educated in its architect, processes, procedures and policies (Alberts D. S., 1997). This takes time and the NEC roll-out hadn't prepared adequate time for training and education (Major General Baxter, 2005). This process of development and lack of underpinning know-how has generated many issues, incidents and business process failures within coalition operations in Afghanistan (Kellner, 2008; Rickards, 2010). The following MoD Information Assurance Policy and Standards are the current key documents for Information Assurance and Accreditation.

- The Defence Manual of Security: JSP 440
- Data Protection Act 1998
- HMG Information Security Standards
- Defence Crypto-security Publications
- The Defence Manual of Interoperable Core Network Technologies: JSP 457
- JSP 600 - MoD CIS Policy and Assurance Process
- Defence Co-ordinating Installation Design Authority Manual of Regulations
- JSP 740 – MoD Acceptable User Policy
- JSP 747- Information Management Handbook

The damage caused to the MoD by a lack of awareness of Information Assurance can be serious. Poor configuration of Information Systems, inappropriate behaviour by staff, careless information management, excessive distribution of documents and failing to apply security policies and procedures can expose vulnerabilities, reduce operational edge, expose the MoD to litigation and adversely affect its reputation. At this moment, the MoD has an underfunded and understaffed accreditation process to provide the assurance to an online community of 300,000 users and ineffective Information risk and incident management process, with very few individuals aware of it, understand it or even take heed of their contents when acquainted with it. The new military perspective towards IA (MoD, 2011) is from the premise that it is assures the conduct of Defence business, whether on deployed operations or in the administration of MoD fixed systems. Military IA encompasses all activity needed to assure the critical information on which Defence business relies. From this approach and the model produced in Chapter 3, a new definition of IA can be established: *Information Assurance (IA) is a holistic management process and architecture designed to ensure that the systems and networks employed to manage, store and transit the critical information assets across the human-cyber interfaces and used by an organisation are reliable, resilient, secure and trustworthy; and that tolerant measures and processes are in place to counter malicious activity and inappropriate behaviour, in order to support the business needs of the organisation.*

Up-to-date, readily accessible and, above all, secure information is a critical component of the Defence Community's that now has the drive to implement efficient and cost effective working practices. For the MoD, good IA is ensuring that the integrity of such critical information is maintained, while protecting systems from those that may seek to abuse them. Under the UK Cyber Policy (Cabinet Office, 2011a) this has become a key concern. Above all, the Defence Community requires a survivable voice and data network infrastructure that delivers information in assured manner in the most testing of environments, while allowing it to take advantage of up-to-date technology such as email, the Internet and Virtual Private Networks; e.g. the MoD's Defence Fixed Telecommunications Service (DFTS) has been working since 1997 to ensure that information, ranging from 'unclassified' to 'top secret', can be accessed easily and securely via a fully interoperable infrastructure. However, in life, people don't react to reality; they react to their perceptions of reality and a lot of the MoD's contextual work has not been implemented and its online community is still very ignorant of their roles and responsibilities within cyberspace (Roper, 2005).

Chaos Theory in development of an IA Community

Understanding the need to identify and create the sensitivity, Lorenz's Butterfly Effects, to a dynamically changing, chaotic rich environment formulates and captures issues to initiate, facilitate and support change within the domain influenced by Chaos Theories. The chaos paradigm replaces the ubiquitous paradigm of Newtonian reductionism that postulated a linear, mechanistic view our real world. Zohar, (1990) see quantum physics as the bedrock of chaos that is "*rich with imagery that almost begs application to the experiences of daily life*."

Implicitly, experiencing this phenomenon is being very much involved the concepts of uncertainty through a necessary and directed process of establishing, inventing and modifying government framework and educational structures to generate the new IA profession. Understanding the theories of Zohar (1990), the *Quantum Self* and Zohar (1997) *Corporate Brain* offered an interpretation of Chaos Theory to structure organizations for fundamental transformation. She demonstrates how people must change the thinking behind their thinking. *"rewire the structures of the corporate brain - to operate more fully and achieve genuine fundamental organizational change."*

The Cabinet Office papers on *Transformational Government* (2005) and *The National Information Assurance Strategy* (2007) provides the source for transformational change and which Shelton, (2003) had earlier illustrated could provide an appropriate environment to evolve the paradigm;"*by applying principles found in chaos theory an organization can make 'lemonade out of lemons' and become more responsive to change agents while continuously moving ahead and growing from the inside out without the fear of complete chaos."*

Generating the IA professional qualities, values and continuance in order for it to become established, grow, develop, survive and adapt is a result of this re-invention and creative adaptation to providing a new specialism, the wave/particle dualism establishes a perturbed equilibrium. Dooley (1995) observed that learning organizations such as DCCIS could: "*allows self-organization, rather than attempting to control the bifurcation through planned change. Being "off-balance" lends itself to regrouping and re-evaluating the system's present state in order to make needed adjustments and regain control and equilibrium. By understanding and introducing the element of punctuated equilibrium (chaos) while facilitating networks for growth, an organization can change gears from "cruise" to "turbo" in regard to speed and intensity of* *organizational change. While maintaining an equilibrium state seems to be an intuitively rational method for enabling an organization to gain a sense of consistency and solidarity, existing on the edge of a chaotic state remains the most beneficial environment for systems to flourish develop and grow.*

System management mechanisms deal with order and regularity, security deals with the complexity generated by irregularities. With Information assurance it's the understanding of interlacing architectural complexities and human behaviour produces a complex, dynamic complexity. This complexity has elements of an emerging structure, where the whole is often more than its parts, that there is no disaggregation but there is a lack of knowledge (uncertainty of relevant knowledge) and a degree of blindness and the sensitivity is dependent on the boundary conditions of unpredictable behaviour and bifurcation. Dualism within the Quantum Theory, by a simple transposition can create a security paradigm with a deterministic chaos /assurance dualism. A characteristic of Chaos, as observed by Mitchell (1998) is that complex interactions modelling real (cyber-based) behaviours have demonstrated consistently that the potential outcomes have predictable limits. Thus in a security context, knowing the exact state how the system will end up is a requirement, but this is unrealistic as Heisenberg's Uncertainty principle confirms. The range and the probabilities of possible outcomes has to be constrained, allowing Assurance to take control which is ultimately very realistic. Finding the critical values to provide system assurance is a worthwhile future action and a recommendation to develop beyond this Thesis.

The Right Policy

Netcentric warfare effects-based operations (EBOs) are "*processes for obtaining a desired strategic outcome or effect on the enemy through the synergistic and cumulative application of the full range of military and non-military capabilities at all levels of conflict*" **(Alberts, Garstka, & Stein, 1999)**

EBOs routinely involve complex environments that require information exploitation to enable decision making in multinational, multifunctional collaborative groups and provide shared situational awareness to commanders. These operations pose problems when insecure information resources are required to interoperate with military networks, in particular the Internet has become essential to the military's superior decision benefit chain. Under current UK's information security standards, classified networks have considerable security and risk exposure constraints that reduce system access across strategic, operational and tactical commands. Awareness of how IA affects knowledge and information management and their overall trustworthiness, necessitates further investigation and analysis of the NEC and in particular understanding how IA professionalism plays an important role in shaping the behaviour and the complex nature of the NEC domains. Governments, corporations and the military have undergone *"a transformation in their ability to gather, share and process information. The result is an unprecedented reliance on information infrastructures for their very survival. This dependency creates new opportunities for disruption"* (Anderson 2005). This presents an unprecedented reliance on information infrastructures for their very survival." In one sense, this tautologises the reliance on technology that is new and is by definition "unprecedented" and in another sense, the need for the system's dependency for survival. The claims are false, as "Information" is hardly the highest in the hierarchy of human needs (Maslow, 1943): water, food and shelter, law and order are surely still more important; but the trend toward increasing dependence on IT in our social systems provokes real issues; and whether it is wise to continue the trend of dependency, is a question which all security professionals should be engaged with.

UK's National Information Assurance Strategy (NIAS)

Whether researching new technologies or implementing information risk management initiatives, information security professionals are being held to even more stringent standards than ever before **(Frost & Sullivan, 2008).**

The UK's National Information Assurance Strategy (Cabinet Office, 2007) takes a coherent approach to managing information security and its risk treatment by making it an integral and effective part of normal business process. Information is a valuable asset that must be safeguarded. In the case of information held by public authorities and businesses, especially personal information, people want to be certain that it is held securely, maintained accurately, available when necessary and used appropriately. Information Assurance (IA) is used to assure the management of risk to information and effective IA ensures that the opportunities provided by new technology can be exploited to maximum benefit.

The convergence of interconnected data and systems causes unprecedented increases in the potential and actual security risks to information assets as they passes through an increasingly complex web of systems. Figure 156 illustrates the 2-sides of the HCI coin – FUD and IA. Effective IA education needs to achieve a step change to the security professionalism that overcomes user's fear, uncertainty and doubts. As enterprises, such as the MoD, adopt collaborative business models, based on highly interlinked infrastructures, they are more vulnerable to attack. In the past, the MoD approach was to isolate, but now these highly secure, fortress solutions are no longer fit for purpose; rather the new military enterprise needs to adopt a solid architectural approach to designing secure, joined-up systems that maintain the integrity of the information they hold and what they pass from community of interest to another. In short, visible security needs to be built in from the very outset to allow the interoperability of systems and the architects of such systems have to build high- assurance platforms that will allow these layers of system operability to cross domains, i.e. bridge air gaps.

Core UK Security Principles

1. Ultimate responsibility for HMG security policy lies with the Prime Minister and the Cabinet Office. Departments and Agencies, via their Permanent Secretaries and Chief Executives, must manage their security risks within the parameters set out in this framework, as endorsed by the Official Committee on Security (SO) (see Appendix 2 for MoD's board structure).

2. All HMG employees (including contractors) have a collective responsibility to ensure that government assets (information, property and staff) are protected in a proportionate manner from terrorist attack, and other illegal or malicious activity.

3. Departments and Agencies must be able to share information (including personal data) confidently knowing it is reliable, accessible and protected to agreed standards.

4. Departments and Agencies must employ staff (and contractors) in whom they can have confidence and whose identities are assured.

5. HMG business needs to be resilient in the face of major disruptive events, with plans in place to minimise damage and rapidly recover capabilities (see figure 157 for the threat exposure and mitigation to the UK public sector)

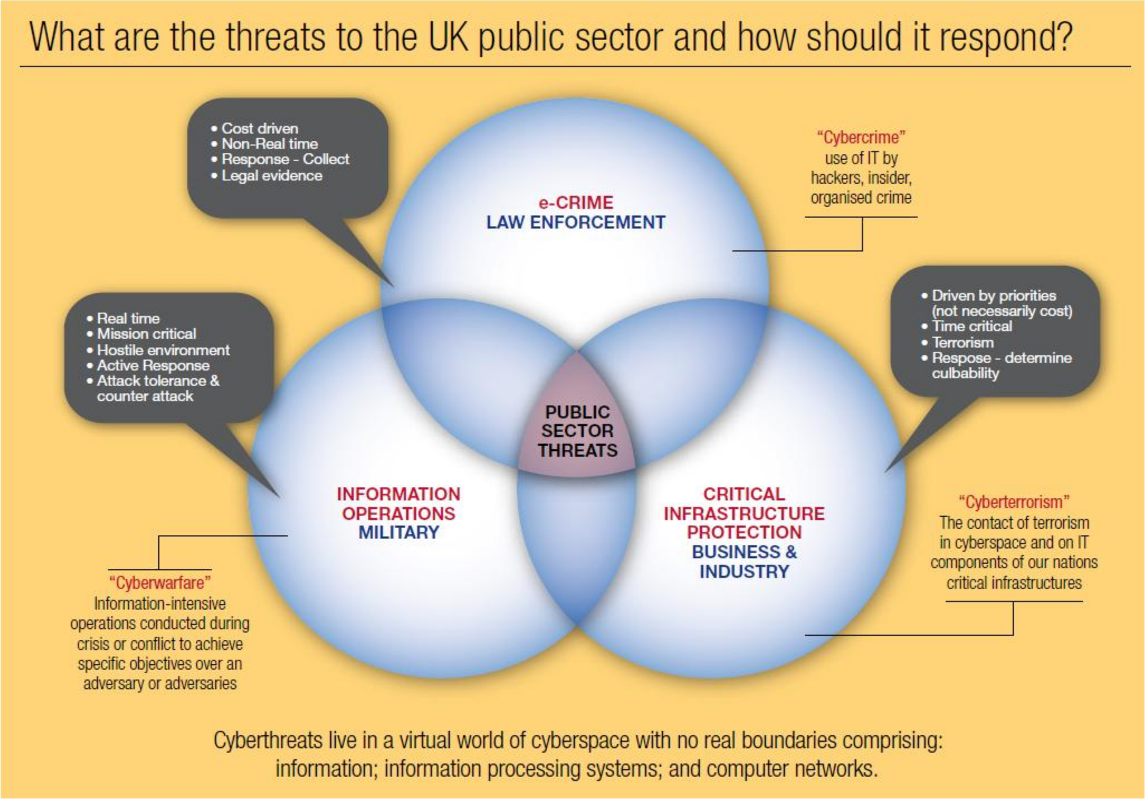

What are the threats to the UK public sector and how should it respond?
• Cost driven
• Non-Real time
• Response - Collect
• Legal evidence
e-CRIME
LAW ENFORCEMENT
"Cybercrime" use of IT by hackers, insider, organised crime
• Real time
• Mission critical
• Hostile environment
• Active Response
• Attack tolerance & counter attack
• Driven by priorities (not necessarily cost)
• Time critical
• Terrorism
• Respose - determine culbability
PUBLIC SECTOR THREATS
INFORMATION OPERATIONS MILITARY
CRITICAL INFRASTRUCTURE PROTECTION BUSINESS & INDUSTRY
"Cyberterrorism" The contact of terrorism in cyberspace and on IT components of our nations critical infrastructures
"Cyberwarfare" Information-intensive operations conducted during crisis or conflict to achieve specific objectives over an adversary or adversaries
Cyberthreats live in a virtual world of cyberspace with no real boundaries comprising: information; information processing systems; and computer networks.

Figure 65: IBM view on UK's information asset threats

Culturally, within MoD, mind-set has to change about how solutions are constructed and this means visibility at strategic defence reviews, operational deployment planning, system design and run time about security attributes, claims, needs and outcomes. The vision for a network enabled MoD also requires a more holistic approach to the National Information Assurance Strategy and to the education of its practitioners. It is no longer sufficient just to secure an organisation's IT assets; the business processes that govern the use of those assets also need to be secure and robust (Cabinet Office, 2011a). This means developing clear processes and policies to govern the way employees, coalition partners and other stakeholders interact with MoD's information, underpinned by a safe and secure infrastructure. Without this combination, the integrity of the Department's business will still be threatened. Only such a multi-faceted approach to Information Assurance that encompasses people, policy, processes and infrastructure will ensure that the risks of joined-up operations can be balanced against the benefits.

The NIAS (2007) strategic outcomes and other IA initiatives such as the HMG IA Maturity Model and Assessment Framework (Cabinet Office, 2010), and modular Code of Connection (Police National Accreditor, 2009) and Risk Managed Accreditation

Document Sets (CESG, 2010) placed on enterprises such as the MoD and the UK's police force (NPIA Information Assurance Capability Team, 2010) can be achieved and evolved by focusing on three IA performance objectives set out in the NIAS. These will have important implications for the way that organisations, particularly within government, do business.

UK National Information Assurance Strategy Objectives (Cabinet Office, 2007)are:

Objective 1: *Clear and effective information risk management by organisations.*

- *Clear board-level ownership and accountability for information risks will be required;*
- *Where information is shared, a single point of risk ownership will be identified.*

That IA should be visible and understood by all Government employees at all levels and across all of its organisations.

Objective 2: *Agreement upon and compliance with approved and appropriate IA standards.*

- *Organisations, particularly those within, or linking to government, will operate within a national framework of IA common standards;*
- *Trust and confidence in the use of information will be maintained through an effective model of compliance with these standards.*

Enterprises are required to take ownership and manage the IA issues, empowering its IA practitioners and ensuring proper consultation it done with stakeholders in the decision benefit chain

Objective 3: *The development and availability of appropriate IA Capabilities.*

- *Government will work more closely with wider sectors in the development of Capabilities' to enable organisations to manage information risks;*
- *These capabilities include: availability of the right products and services; coordinated and appropriate efforts on innovation and research; improved professionalism, and awareness and outreach.*

That there is a common understanding and awareness of the enterprise Risk processes and its mitigation by the communities of interest and this is conveyable across domains, coalition networks and other interoperable systems.

The Broader Social-Contemporary Security

> Information assurance can be an important business enabler, supporting secure, effective and agile information services, but only if a hostic view is taken." Detica white paper, 2008

The traditional (Cyber Layer 1) geographical, defence-based, physical security is no longer the only criterion that defines human well-being and development. Increasingly, security has become a combination of attributes relating to freedom from persecution, want, fear and a broad range of other concerns, such as the security of water, food, energy and environmental security. Aspects of this trend are recognised by the United Nation's '*Responsibility to Protect*' agenda (UN, 2004), which focuses on preventative and developmental lines of activity (including 'pre-emptive' action) rather than purely reactive intervention. However, prevention requires a longer view and proportionately more effort in recognising the indicators of an impending crisis and in tackling the root causes of instability rather than the more obvious symptoms. In turn, early responses may be difficult to determine, but will, in an inter-connected world, always require decisions and intervention across a wide range of activity including economic, diplomatic, military, developmental, humanitarian and now cyber. In military terms, people and their business processes have become the vital ground for Information Operations (IO) which deliberately intervenes and interferes how they go about their business. IO can disrupt, coerce, harass and sabotage across the 5 dimensions of military operations.

Effective holistic education of Information Assurance has to advance understanding through quality education of our leaders, practitioners and the user community the fields of information operations and cyber security including Information management, services, exploitation, security and its assurance, critical infrastructure protection, national security information management, and computer network. The United Nation's '*Responsibility to Protect*' agenda (UN, 2004) has in part contributed to the MoD's Joint Discussion Note JDN 4/05. The JDN illustrates the complex and dynamic strategic environment of the 21st Century and how the department should encompass strategies like the NIAS. Figure 158 illustrates the strategic importance of IA (as discussed in Chapter 4) which aligns the JDN with national policy. The Comprehensive Approach (MoD, 2006) discussion paper signalled that there are significant potential challenges to peace and security to which we need strategies to ensure safety, security and integrity. That these challenges are likely to persist throughout the global environment with the interconnected, globalisation nature of several transnational trends that will affect resources, science and technology, social, military and political dimensions as developed in Chapter 4. The JDN discussion paper describes the world of sovereign states, unequal in development and resources, conflicts and tension seem set to continue among nations and power groupings. The symptoms of crisis will be spawned by a combination of climate change, ideology, greed, ethnic animosity, residual territorial claims, religious fanaticism and competition for resources including agricultural land, mineral wealth, water rights and oceanic resources. The desire for socio-economic improvement and population migration (refugees and Internally Displaced Persons) driven by war, economic and environmental collapse or natural disaster will generate national responses and demands for international assistance and these emergency responses are becoming more dependent on system interoperability and Information availability . Additionally, terrorist actions, communal violence, endemic criminality and ethnic disturbance will continue to complicate international relations, while individuals and commercial interests are likely to have multiple identities, allegiances and cyber proxies. This will compound the protection and security requirements for Critical Information Infrastructures and Emergency Response Services which are often privately run and often controlled by organisations outside the nations they serve.

The Human Dimension in the Social Context of Security

The human security agenda requires a response that is sensitive to the extensive, particular needs of societies, communities and individuals. To this end, all constituent parts of a society (rule of law, education, commercial, humanitarian and health, information, military, economic and diplomacy and governance) should be considered, as well as the history and culture of an individual society as illustrated in figure 66:

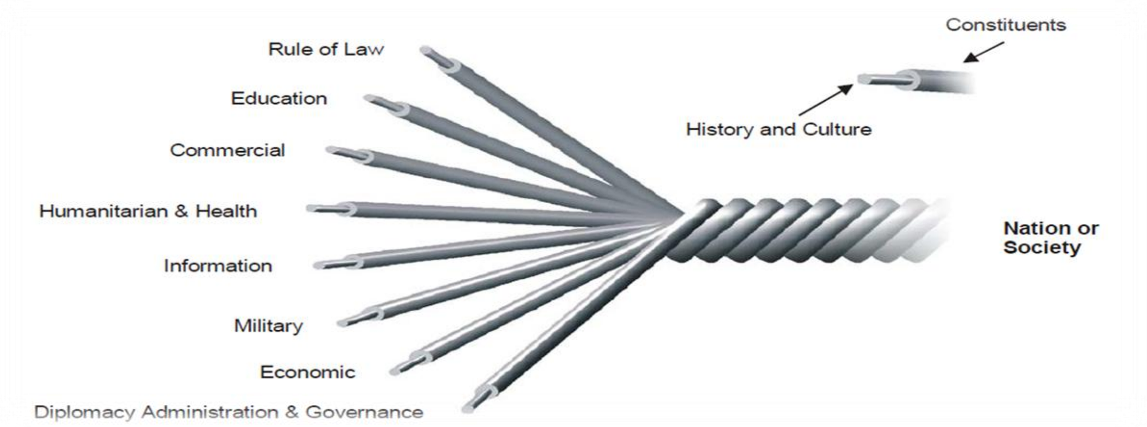
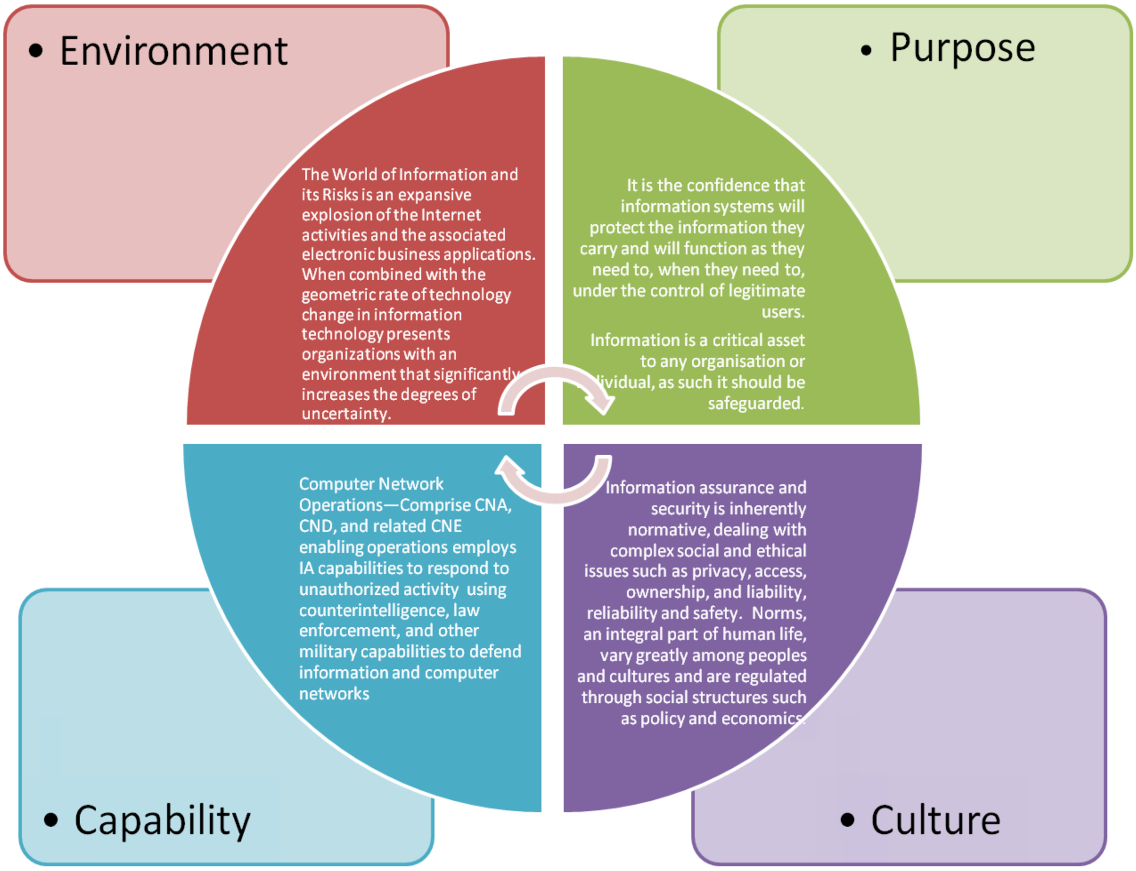


Figure 66: The Constituents of a Society

Only then can a range of appropriate objectives, resources and contributors be established to influence the situation. The spectrum of involvement, doctrinally and familiarly known as the 'Complex of Actors', might comprise other governments, International Organisations, NGOs and private and commercial interests. Additionally, experience has indicated that successful resolution would overwhelmingly rely on the attitude and motivation of the indigenous and/or local population at the heart of the crisis and those in the surrounding region, although care should be taken not to create a dependency culture. Two other groups that should be considered in any responses are opportunists, who seek to benefit from the situation or the perpetuation of a crisis, and spoilers who have an interest in undermining the response.

Implementing NIAS through the Defence System Approach to Training



The World of Information and its Risks is an expansive explosion of the Internet activities and the associated electronic business applications. When combined with the geometric rate of technology change in information technology presents organizations with an environment that significantly increases the degrees of uncertainty.

It is the confidence that information systems will protect the information they carry and will function as they need to, when they need to, under the control of legitimate users.

Information is a critical asset to any organisation or individual, as such it should be safeguarded.

Computer Network Operations—Comprise CNA, CND, and related CNE enabling operations employs IA capabilities to respond to unauthorized activity using counterintelligence, law enforcement, and other military capabilities to defend information and computer networks

Information assurance and security is inherently normative, dealing with complex social and ethical issues such as privacy, access, ownership, and liability, reliability and safety. Norms, an integral part of human life, vary greatly among peoples and cultures and are regulated through social structures such as policy and economics.

Figure 67: The Strategic Positioning of Security

Information is a critical asset for any organisation, and particularly so to the MoD. Its exploitation is fundamental to the achievement of business objectives. The Government's *National Information Assurance Strategy* (NIAS) enables organisations in the UK to fully exploit the benefits of information and communications technology (ICT), while at the same time ensuring that wider UK interests are maintained. The

Central Sponsor for Information Assurance (CSIA) uses the term "Information Assurance" to describe the appropriate management of information risks (that is to ensure the availability, integrity, confidentiality, non-repudiation and authentication of information and information systems) in order that the benefits of ICT are fully realised. The NIAS explains that ownership and responsibility for this strategy for Information Assurance rests with the Official Committee for Security and its chair, the Cabinet Office Permanent Secretary, Intelligence, Security and Resilience.

For effective decision making, information needs to be clear, accurate, trusted and not: compromised, lost, leaked, disseminated, published (without approval) or corrupted. The Rawlinson Report[39] highlighted the need to provide both an educational framework and the IA Profession within MoD. Organisations like the Defence College for Communication and Information Systems (DCCIS) have begun to take a proactive part in delivering the goals of NIAS and responding to Brigadier Rawlinson's observations:-

1. *How NIAS will affect the DCCIS and its training regime and how within the organisation the effect of the IA Professional Framework will have on job specifications and training requirements?*

2. The NIAS calls for a new profession of IA practitioners with a prescribed Government career structure and professional development. This creates an opportunity for the Royal Signals to take an initiative to adopt the NIAS to create an IA trade group in conjunction with its current IS trade group. Existing Operational Performance Statements (OPS) will need modification and enhancement to reflect the IA Framework and to identify how graduates/trainees will meet the necessary prescribed SFIA and NQF standards.

3. How DCCIS can leverage its expertise to establish future accredited IA courses for MoD and other Government Departments for pre-employment training and continuous professional development?

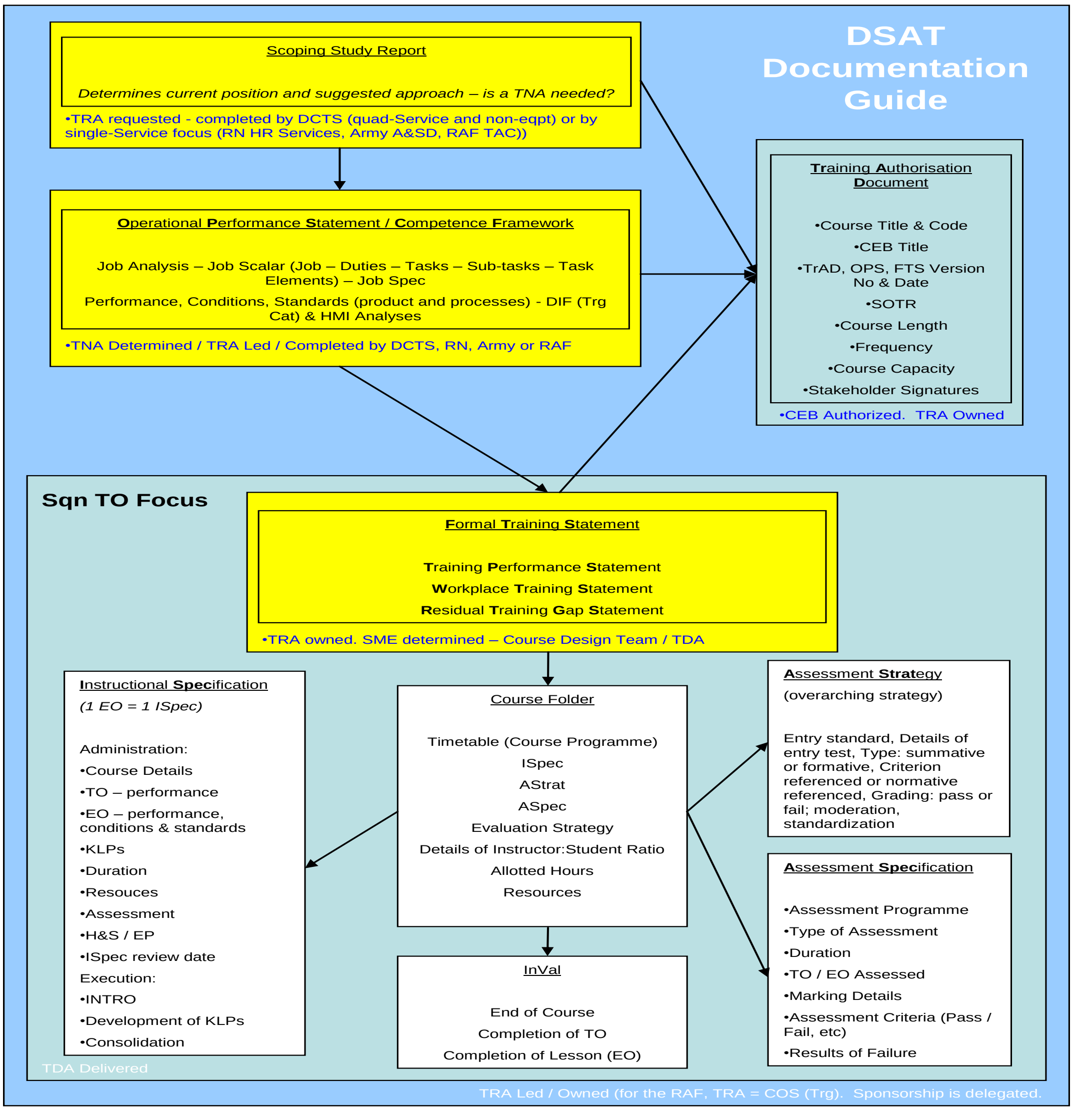
[39] MoD Information Assurance Review 18Nov05

As DCCIS is the MoD's centre of excellence for communications and information systems, then it is incumbent on the college to take a lead in promoting professionalism in IA. Information security and its assurance is an issue with people rather than technology and it is reliant on people, their awareness, ethics and behaviour. This is partially reflected in DCCIS (2011) current training goal to:*"ensure that personnel have an appropriate awareness of information security policies and practice to the extent that their duties require, and to fully understand their responsibilities including their legal obligations".*

A holistic approach to delivering aspects of NIAS through the MoD's own IA Maturity Model will require Training Needs Assessment to identify each post and assign the IA level of competency required to meet the framework and the necessary training requirements for the post holder. NIAS requires that IA practitioners have further specialized training, developing the necessary transferable skills, with focused courses of increasing educational content and the provision of professional development courses. NIAS calls for the development and availability of appropriate IA capabilities and identifies seven specialisms within its professional framework. Many existing roles and posts within the MoD's CIS environment cover in part, or are identifiable as IA functions.

The MoD's Information Strategy (MoD, 2011) framework requires practitioners to obtain educational and transferable skills for these posts. Consequently there is a requirement to assess the current IA post and incumbents against skills, training, educational and Continued Professional Development (CPD) needs of IA Foundation, Practitioner and Subject Matter Experts (SMEs) as illustrated in figure 161. JSP 822 *directs all Defence personnel accountable for, or with influence over, the delivery of Defence capability, the meeting of performance requirements, or the implementation of Defence policy, for which T&E interventions are required. It applies to all decision makers and practitioners employed in the Regular Forces, the Reserves, MOD civilians, and Industry who are engaged in the derivation and assurance of Defence capabilities or performance requirements, and/or the development, delivery, or assurance of associated T&E interventions* (MoD, 2012).

NIAS and the expected National Occupational Standard (NOS) will modify or create through the Defence Systems Approach to Training (DSAT) a new Operational Performance Statement (OPS)/ Competency Framework (MoD, 2012). The DSAT OPS will be required to develop the envisaged Defence IA Practitioner at SO2 / SO3 level, but also targeting supervisors (Yeoman, Foreman & IS supervisors). Specialist's roles such as ITSOs and SACs should also be included. We will also have to derive the OPS to cover the soft issues of Information Assurance. MoD's Network Enabled Capability doctrines of Information Superiority (MoD, 2006; MoD, 2011) have predicated the need for information security and its assurance. Interoperability, Information exploitation and ICT advancements has brought a transformation risks and new trends in information system threats and vulnerabilities. Vulnerabilities introduced by the complexity of the new military information systems and the impact of degraded systems within Information Operations from increasing complex attacks has necessitated the adoption of information assurance. NIAS has identified there is requirement for a change of culture and acceptance of IA to be fundamental to our business goals, which Rawlinson (Rawlinson, 2005) also commented on.



DSAT Documentation Guide

Scoping Study Report

Determines current position and suggested approach – is a TNA needed?

•TRA requested - completed by DCTS (quad-Service and non-eqpt) or by single-Service focus (RN HR Services, Army A&SD, RAF TAC))

Operational Performance Statement / Competence Framework

Job Analysis – Job Scalar (Job – Duties – Tasks – Sub-tasks – Task Elements) – Job Spec

Performance, Conditions, Standards (product and processes) - DIF (Trg Cat) & HMI Analyses

•TNA Determined / TRA Led / Completed by DCTS, RN, Army or RAF

Training Authorisation Document

•Course Title & Code
•CEB Title
•TrAD, OPS, FTS Version No & Date
•SOTR
•Course Length
•Frequency
•Course Capacity
•Stakeholder Signatures

•CEB Authorized. TRA Owned

Sqn TO Focus

Formal Training Statement

Training Performance Statement
Workplace Training Statement
Residual Training Gap Statement

•TRA owned. SME determined – Course Design Team / TDA

Instructional Specification

(1 EO = 1 ISpec)

Administration:
•Course Details
•TO – performance
•EO – performance, conditions & standards
•KLPs
•Duration
•Resouces
•Assessment
•H&S / EP
•ISpec review date
Execution:
•INTRO
•Development of KLPs
•Consolidation

Course Folder

Timetable (Course Programme)
ISpec
AStrat
ASpec
Evaluation Strategy
Details of Instructor:Student Ratio
Allotted Hours
Resources

InVal

End of Course
Completion of TO
Completion of Lesson (EO)

Assessment Strategy

(overarching strategy)

Entry standard, Details of entry test, Type: summative or formative, Criterion referenced or normative referenced, Grading: pass or fail; moderation, standardization

Assessment Specification

•Assessment Programme
•Type of Assessment
•Duration
•TO / EO Assessed
•Marking Details
•Assessment Criteria (Pass / Fail, etc)
•Results of Failure

TDA Delivered

TRA Led / Owned (for the RAF, TRA = COS (Trg). Sponsorship is delegated.

Figure 68: JSP 822: The Defence System Approach to Training (2012)

However, the gaps in our operating processes, business continuity and awareness of the user communities have to be managed, corrected and where necessary a change of culture introduced. Bridging the Gaps in IA Education and Professional Standards is essential for the MoD Information Strategy to gain the benefits it clearly wants from its Operations, Coalition partnerships, Decision Making and achieving Information Superiority. However, DSAT is an expensive process, with considerable overheads in resources, manpower and costs. The MoD has tried over the last 20 years to outsource its Education and Training programmes as a cost saving process. These attempts have concentrated the training (reducing the number of trainees and training establishments) but have failed to attract a private consortium to take over the Defence T&E commitments.

Policy Driven IA Education

Individual security lies with the skills, knowledge and experience that we have in ourselves. An important objective which can be facilitated by DCCIS, to aid the change of culture, is transforming the Defence Information Strategy and the NIAS into a profession development programme that:

a) Provides recognition and career development of transferable skills and knowledge for the profession with timely, supportive, accredited development courses for the MoD and in turn for other Government Departments.
b) Provides an forum for the understanding of the issues and the proliferation of the guidance, policies and security technologies involved in IA

The proposed Information Security Professional Development (ISPD) programme, delivering the Right Skills, to the Right People at the Right Time, supports the NIAS framework and the Institute of Information Security Practitioners structured career path and provides the MoD la clear direction for IA Education and Training to meet the UK's Cyber Security Strategy (Cabinet Office, 2011a). The programme will be geared to provide educational qualification and transferable skills to practitioners as it is intended to help them to stay on top of the available technologies and innovations and thereby sustain our assurance against these threats. Most importantly, the aim of the ISPD is to provide recognition through academic excellence, an understated goal in the NIAS. IA practitioners are not only critical to the on-going running of our core business and protection of its assets, but also to its development and strength in the future. This unique service to provide understanding of the evolving threat landscape coming from increasingly sophisticated attackers should be established within DCCIS.

4.2 Federated Education

Understanding risk at an enterprise level is a fundamental requirement for Information Assurance. While many business drivers are not exclusively related to IA, there are nevertheless many information-based factors, such as information sharing policies, which contribute to overall risk and therefore need to be considered. Holistic IA Education requires methodologies that take a Strategic Position of Security (SPS) of the enterprise to identify key business drivers and risks, which can then be examined from a specific IA perspective. Within the MoD our Information Assurance practitioners need to construct risk-balance cases, which are rigorous appraisals of the risks and their impact, which support the Network Enabled Capability (NEC) decision-making, risk prioritisation and potential trade-offs within the enterprise. Risk owners should be clearly identified and given a better understanding of their risk appetite. The business drivers and prioritised set of MoD's risks should be used to create an IA vision and strategy for the department The holistic approach to effective Information Assurance education will need a more detailed IA curricula derived from business cases and implementation roadmaps for the department going forward.

The Right Skills

"You don't want to open that Pandora's Box, because you never know what Trojan horses will leap out". Rt. Hon Ernest Bevin MP

Pervasive computing, Information Services (IS) and Information Technologies (IT) is as much a part of our lives as Maslow's (1943) pyramid. Information Security, its Assurance and risk management has become technically and holistically challenging to the practitioners and academia. They have become key issues in today's transforming and pervasive information driven world and its complex of actors. Securing our Information assets is critical as it is pushed and pulled around us all 24/7. It is exploited, stored, manipulated, targeted, controlled, stolen and often compromised (US CERT 2008).

"Professionalism" requires a sober and objective approach to risk assessment: but the dilemma for the security industry is that wherever threats are evaluated as remote, the security industry will receive very little attention (funding) from anyone. The IT security sector has been notorious for the way it trumpets any vulnerabilities it finds to one and all, usually well before they have been discovered let alone exploited by anyone else, merely as a means self-publicity and headline-grabbing, in order to attract funding. So the dilemma for the profession is how its “professionalism” will allow it to step out of this maelstrom of self-interest, and convince the public at large that it is objective, and has no particular interest in exaggerating security threats. The record of IT professionals (in general) in the area of proportionate threat assessment is not good (e.g. the Millennium bug that wasn’t). Easy sensationalism is easier than evidence-based threat assessment and scientific objectivity, it would seem. *“We live and work both as individuals and as part of communities* [complex actors], *within organizations and society as a whole. Our understanding and acceptance of the world around us is couched within negotiated meaning of those contexts. Security needs to support users in seeing and negotiating safely on those terms within technologically mediated systems.”* (Adams and Blandford, 2005).

The Computer Security Institute / FBI (2007) reported a *significant upswing* in cybercrime and these criminals are becoming well organised. Motivated individuals and criminal groups see the Internet as a medium to further their causes; disseminate their SPAM and other propaganda; to change, poison, disrupt or destroy existing structures. Information Infrastructures need to become more interoperable and robust; systems more dependable and critical infrastructures have to be trusted. Mitigating complexity to develop and secure NEC systems and their application IA Practitioners have to understand both the enterprise architecture and the adversaries. The knowledge and skills to meet this demand have to be gained and continuously developed and it is incumbent that IA Education has to provide a holistic approach to emergent designs and application complexities (Bishop, 2002; Wasim 2006).

In the virtual world, informed knowledge often has a very short shelf life. Whitman (2004) expounds new vulnerabilities are often found each day and on the same day we can experience a threat. These threats vary from espionage, sabotage, hacking, identity theft, crime to terrorism. The level of sophistication and speed of development of the tools being used to create security breaches and attacks are growing exponentially (Eloff, 2005). This constantly changing, chaotic environment encapsulates why security knowledge needs to be continuously evaluated and disseminated as deployed counter-measures become bypassed and obsolete overnight. Consequently, IA practitioners must be continuously updated with a holistic, concurrent and relevant development programme. Professional Institutions and universities providing IA education have a duty to keep their curriculum innovative and relevant. NIST (2003) has a framework to developing IA education courses. However, Information Assurance is very diverse, combining the disciplines of holism, complexity theories, computer science, information philosophy, CIS engineering, soft systems, forensics, education, psychology, business administration, law, and accounting. The interdisciplinary nature requires cohesive perceptions and perspectives of specialist educators, lecturers and practitioners often requiring different schools to collaborate. Such a multi-disciplinary curricula approach and subsequent integration will require careful planning and implementation. Gibson (2007) posits that the IA profession needs modern business administration skills to the already complex multidiscipline portfolio and figure 162 illustrates the depth of 3 components of this portfolio. Many universities incorporate Information Management, Risk Management and Business Studies modules to their undergraduate and post-graduate courses and they are starting to address the capability gap in our knowledge and expertise of Security, Risk and it Management. Our learning institutions are beginning to produce a growing number of professionals with Information Assurance expertise.

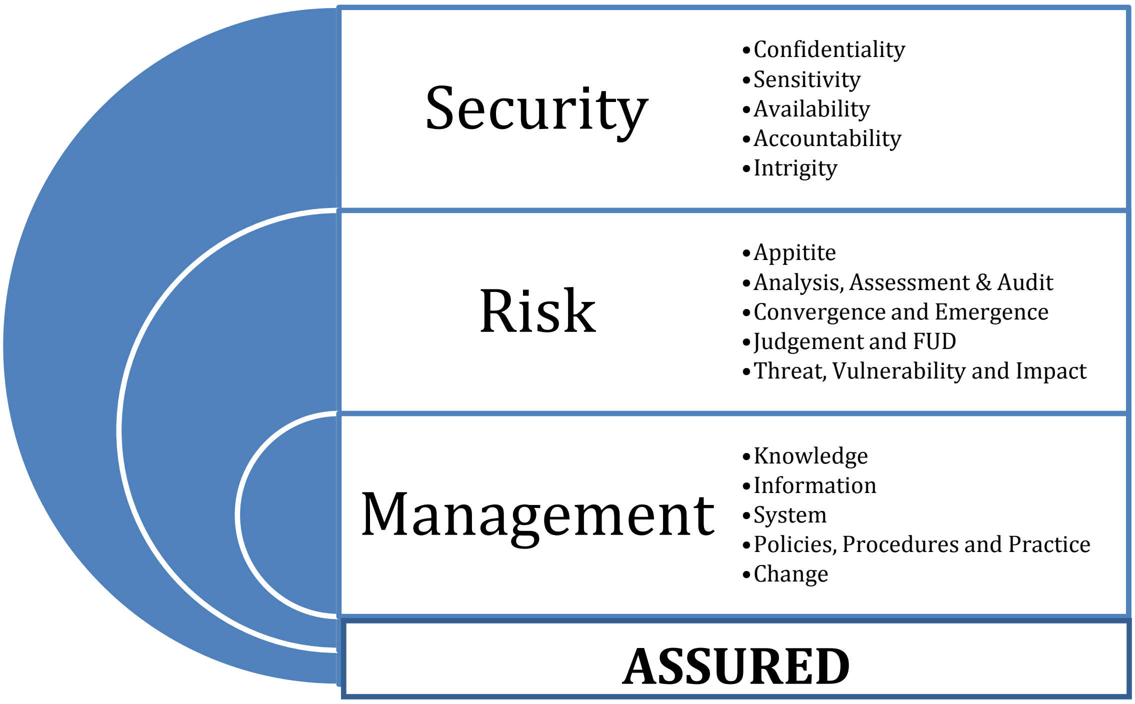


Figure 69: Information Security Management

Security Education

"*Blame human psychology: when it comes to information security, we're simply not built to intuitively rank actual risks. Learn how building threat models can help companies rationalize the biggest security and compliance risks they face,"* Mathew Schwartz 2006.

Figure 70 illustrates the information asset is often seemed wrapped around the technologies and applications that support it, rather than the content of the knowledge it represents. Hence people become distant to the content and rely on the technology as barrier hoping that processes will protect themselves and their systems from vulnerabilities, threats and possible attacks. Often the environment and the organisations that have built it will play an important role to the judgement of these actors in their complex world. We can see that Assurance and its associated Risk Management needs to address all the spheres of influences, to protect the services, organisation, people and the information asset; transposing the vulnerabilities and threats vectors away from the assets to the dimensions of Assurance.

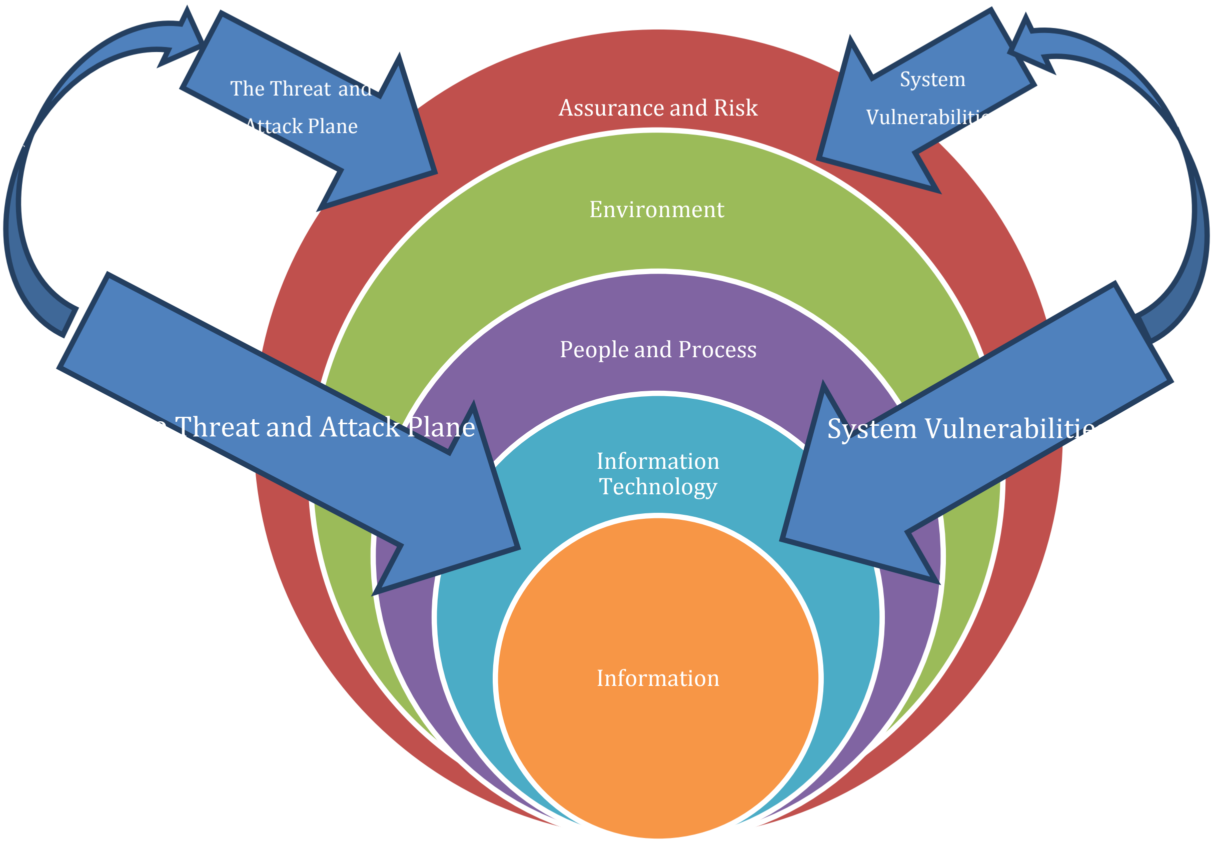


Figure 70: Encapsulating the Assurance of Information

We typically overreact to less risky threats while ignoring bigger, quieter, more long-term hazards. Thus we obsess about laptop encryption, try to automatically monitor for information leaks, while ignoring the threat of insiders or social engineering attacks, and wait for some impending governance, risk, and compliance platform silver bullet to solve all future problems. Lack of information is frequently not the cause of our inability to identify our biggest information security and compliance-related threats. Rather, it's a more fundamental problem. "*We are not adept at making rational security trade-offs, especially in the context of a lot of ancillary information designed to persuade us one way or another*," alleges BT Counterpane Chief Technology Officer Bruce Schneier in a recent essay titled *"The Psychology of Security."* In particular, he identifies five areas "*where perception can diverge from reality*" when it comes to evaluating security trade-offs: risk severity, risk probability, cost magnitude, countermeasure effectiveness, and the actual trade-off itself.

Students and practitioners are faced with many complex, ill-defined challenges with the virtual environment. Information infrastructure and their knowledge silos are been linked, routed and dumped routinely without authority. To be successful practitioners, they will need to be able to solve the ill-defined holistic problems caused by our complex actors and the system of systems architectures. This reflects the nature of the information security environment assessing the risks, threats, and vulnerabilities are only the beginning to assuring and accrediting the systems. This, in-turn poses significant challenges to the educators, who need to prepare the IA professionals to recognize and manage complexity (Janet, 1986).

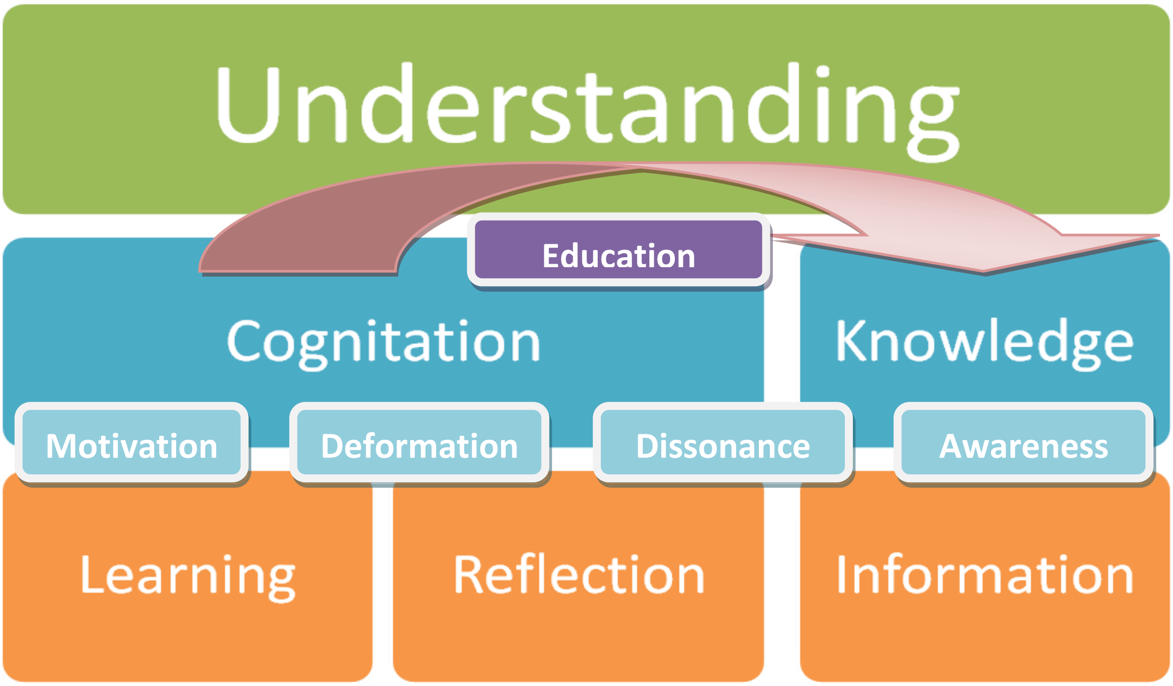


Figure 71: Education facilitating Understanding

Figure 71 illustrates how education facilitates understanding and in particular our curiosity and need to know is a strong motivator as commented by Peter Senge and his *Fifth Discipline* (Senge P. , 1990). However, even though the Defence Strategy calls for better education, it fails to provide suitable and substantial resources to enact a fruitful outcome. Why? - It is not about resources, in particular cash, it is about how we manage our human resources, how we engage in the wider communities of interest and how we educate and make aware those complex actors. Figure 72illustrates the process required to build a Continuum of Understanding as described by Shedroff (1999) and as developed into a learning organisation by Peter Senge.

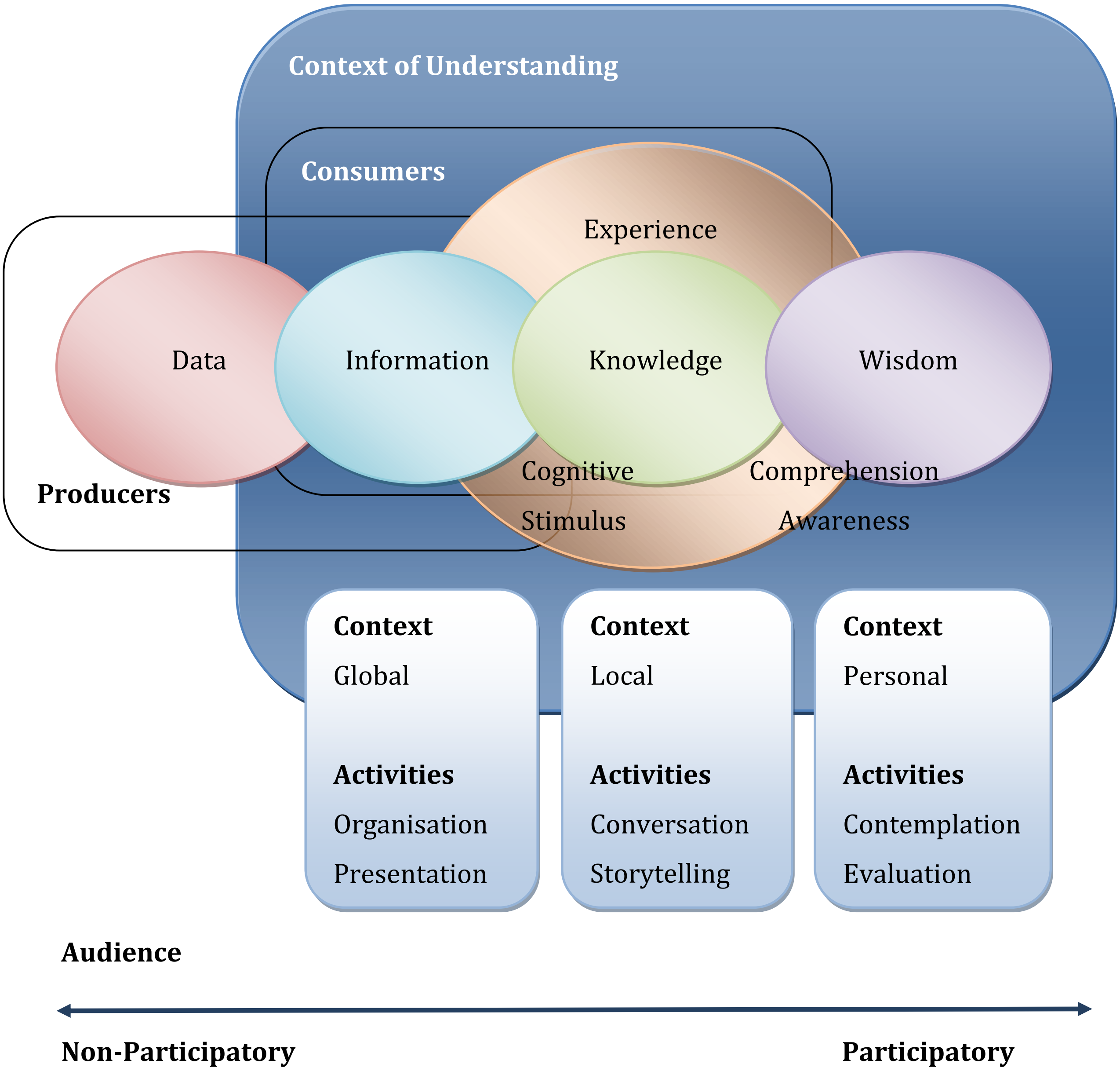


Figure 72: The Continuum of Understanding (Shedroff, 1999)

Higher educational institutions like Bournemouth University have planned and implement BSc courses in Security and considering potential job opportunities (Participatory in Figure 165) in information security want a large number of their undergraduates to enrol. Most students (Consumers in Figure 165) are motivated (Cognitive Stimulus) to acquire practical skills and future security courses will need to cover a wide spectrum (Comprehension Awareness) of security concepts, designs, applications, governance, simulations and practicals including hacking (Brian, 2006). Current University courses are equally popular among the undergraduate and graduate students. At the Defence College there has been a clear distinction in their increasing numbers wanting to undertake security projects. While CIS Management graduate students tend to look for more theoretical projects leading to their theses most undergraduate students are more interested in "hands-on" implementation-oriented projects that are more offensive than defensive (Martin, 2006).

Why would managers, administrators, practitioners and even users want to engage in, develop and relearn Information Assurance? Often we hear "*if the Government educates and trains it personnel, industry will entice away*". In practice this is not apparent. Holistic career minded individuals are not always motivated by salary expectations, many see rewards from achieving objectives and being recognised for doing so. Education is rewarding. We need a shift of mind to develop and foster Senge's *Personal Mastery*, to produce a shared vision from the development of mental models as structured in his book.

The Information Security Professional Development Programme

The soldier's or civilian's Continued Professional Development (CPD) is a process by which individuals take control, taking the responsibility and ownership of their own learning and development, by engaging in an on-going process of reflection and action. This is a process that empowers, excites and can stimulate individual achievements, aspirations and career goals. The Information Security Professional Development Programme (ISPD) is a proposed solution for the professional development of practitioners based on the Government's IA Profession Framework. The aim is to provide a clear career path supported by a certified educational and training programme for Government and NGO security professionals. In particular, there is a greater need to focus on educating existing professional practitioners and accrediting their professional competencies. The ISPD Programme should extend to cover List-X companies and other Government contracted agencies.

More work needs to be done to formalise the ISPD such as scoping a Training Needs Assessment and establishing guidance for the identification of roles and proposed certification of personnel conducting information security functions within the Department, its networked information environment and the security roles across other Government Departments. This extra work will provide the foundation to establishing the National Occupational Standard (NOS) for Information Assurance (currently under discussion between the Skills Council, BIS, CESG and BCS).

The proposed ISPD programme will have three core security disciplines:

- Physical security
- Personnel security
- Information security

However, there are a number of other important NEC security-related topics which, where appropriate, will be included in the curriculum at an appropriate level of complexity. It is envisaged that general security training courses are designed to provide specialized training in areas beyond the core security disciplines. These include Communications Security, Business Continuity, Information Assurance, Operations Security (OPSEC), Information and Risk Management. And Gerald (2006) gives a compelling case for certification and accreditation methods to be incorporated into an information security curriculum.

Table 10: ISPD Levels of Competencies

Level	Competency	NQF Levels
1.	**Basic** training – CBT and distant learning	2
2.	**Practitioner** training and education– Taught and distant learning module courses	3 and 4
3.	**Expert** training and education – Specific taught modules with distant learning material	5,6 and 7

The ISPD would be organised into distinct levels of competencies, illustrated in table 6, will provide the opportunities to gain nationally recognised civilian qualifications through the accreditation of education, training and experience. This is an important component of MoD's personnel strategies since it provides recruiting, development, retention and resettlement benefits. The ISPD training should align the established SFIA / NEC framework against the Qualifications and Curriculum Authority's National Qualification Framework (NQF) and any future Occupational Standard. It would be organised into its distinct levels of competencies as illustrated.

The key element to the ISPD programme is a framework that addresses the following Education and Continuous Professional Development objectives:

1) Develop a skilled profession with a common understanding of the concepts, principles and applications of Information Management; its Security and Assurance for each level to gain information superiority and enhance the confidentiality, integrity and availability of the information infrastructure.

2) Develop a more holistic approach to Information Security and Assurance by aiding the establishment an IA profession.

3) Establish an education, training and awareness baseline, against the SFIA/NEC framework, scoping the technical and management of information security skills amongst personnel performing security, information management, risk management and Information Assurance functions within Government and NGOs.

4) Provide qualified security professionals.

5) Augmenting skills developed through training and experience with the implementation of a professional development programme comprising of residential courses, distributive and computer based training, distance learning, supervised on-the-job training, exercises, examination and certification.

6) Verify, audit and sustain knowledge and skills through standards, qualification testing and certification.

The ISPD should develop and certify some additional material which reflects specific business best practice, legal requirements, technical standards and ethics that are international, contextual and organisation specific (Janine, 2006). While each level in the ISPD programme is open for students meeting certain formal prerequisites, the sequence of CPD modules and degree courses will be designed in such a way as to allow students to progress from NQF levels 3 to 7 without undue overlap or repetition. This would still provide the flexibility for this organisation and other departments to recognise relevant international qualifications but still have the professionals having knowledge of the local content and regulations which are necessary for practising information security.

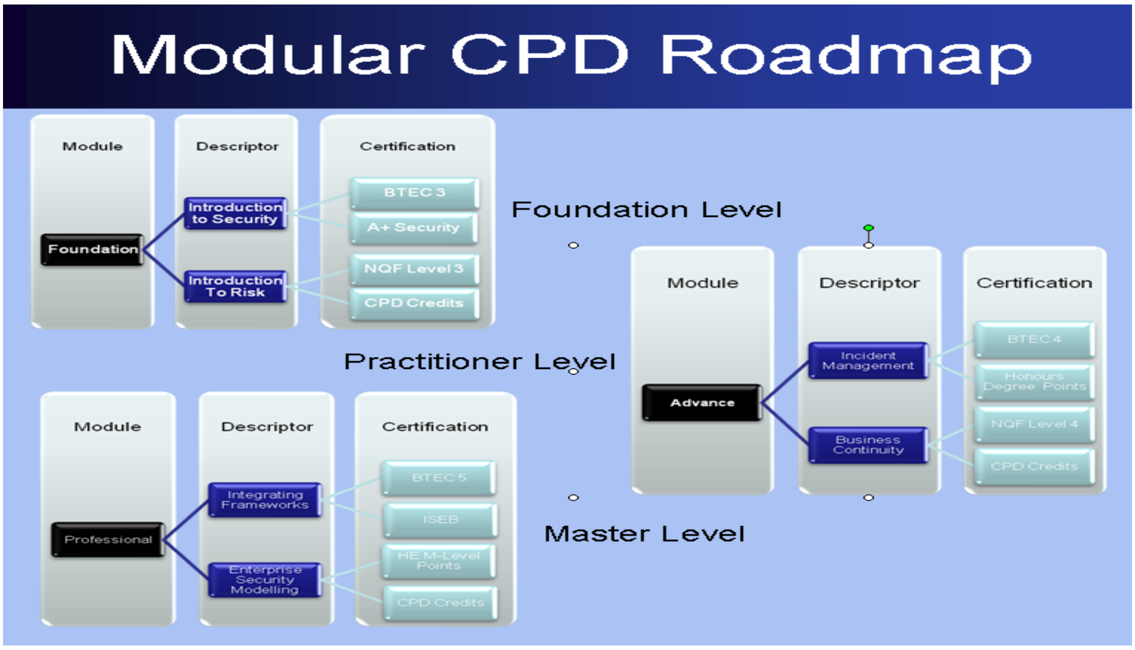


Figure 73: The Proposed Modular CPD Roadmap

The UK's greatest asset is our information, whether its intellectual knowledge, data sources or financial transactions, we need to protect it, and thus we need assurance and this assurance will be provided by accredited professionals, who have a career path with rewards, to secure its confidentiality, integrity and availability to authorised users. The ISPD programme is something long overdue and what the IA community has been asking for. The proposed programme provides the education element to a new structured career path for the security professionals. It will educate them in areas in which they have been entrusted, to protect people, information, facilities, operations, and activities. This initiative will provide the UK trained security professionals with a genuine career path.

The Federated MSc

The opportunity for the information security profession is immense. Clearly we must continue to understand the evolving threat landscape coming from increasingly sophisticated criminal factions. We must also stay on top of the available technology to protect against these threats, recognising them as tools, rather than the focus of our jobs. Most importantly, however, we must recognise that our jobs are not only critical to the running of the business and protection of its assets, but also to its development and strength in the future. We are driving a change in the role of the security professional.

> *"Imagination is more important than knowledge. Knowledge is limited. Imagination encircles the world."* Albert Einstein

Image studying security, its vulnerabilities and failures in a dedicated academy; a depositary of knowledge and incidents; a facility to pursue innovative solution. A place that coordinates IA issues, where threats and attacks can be diagnosed and investigated without compromising commercial sensitivities or the confidentiality of military systems.

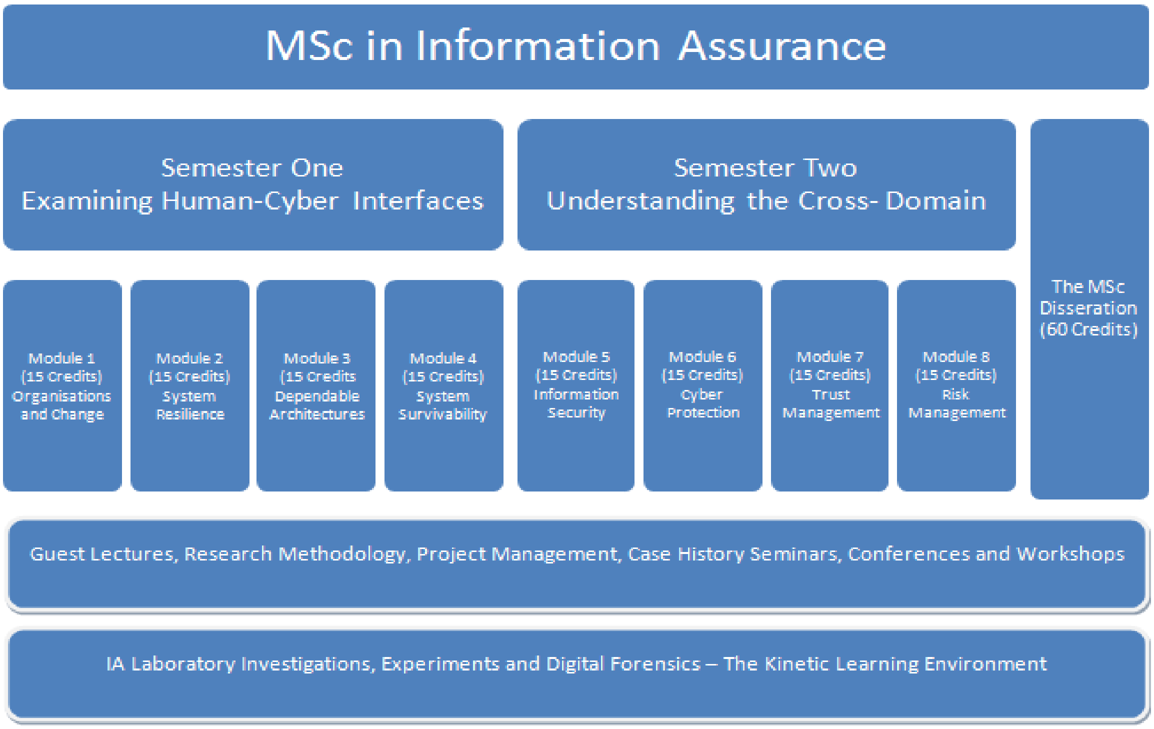
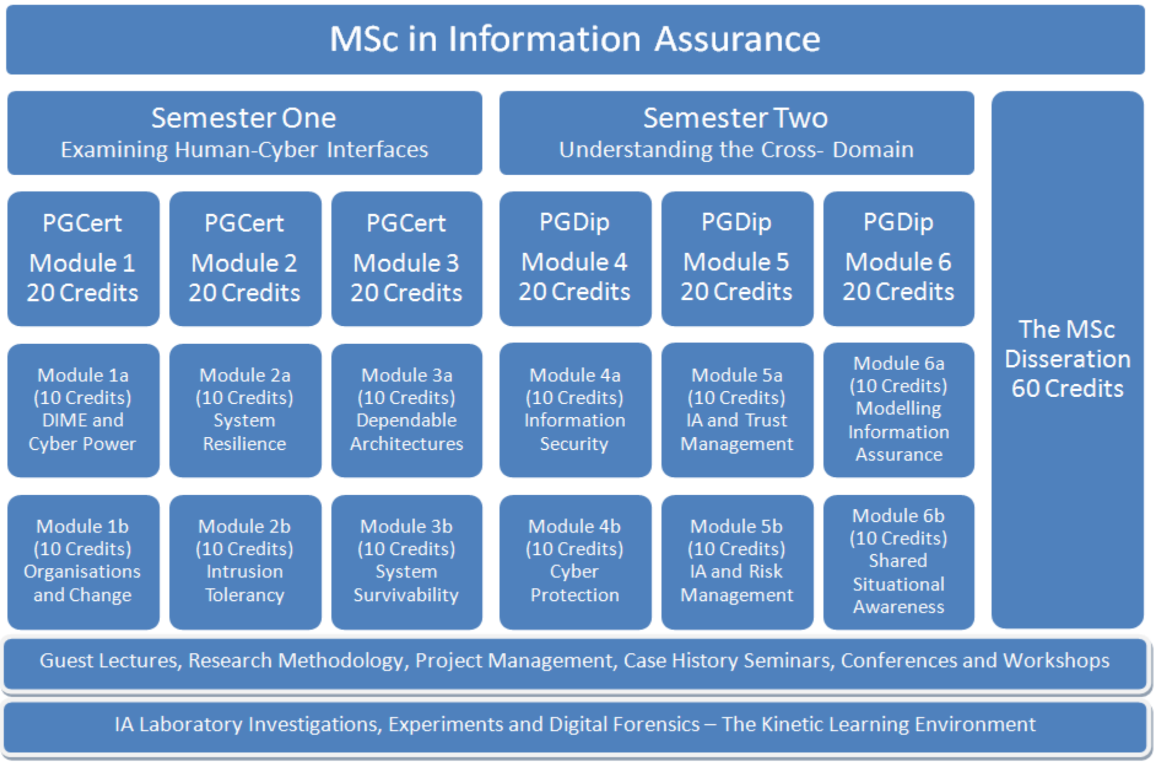

MSc in Information Assurance
Semester One
Examining Human-Cyber Interfaces
Semester Two
Understanding the Cross- Domain
The MSc Disseration (60 Credits)
Module 1 (15 Credits) Organisations and Change
Module 2 (15 Credits) System Resilience
Module 3 (15 Credits Dependable Architectures
Module 4 (15 Credits) System Survivability
Module 5 (15 Credits) Information Security
Module 6 (15 Credits) Cyber Protection
Module 7 (15 Credits) Trust Management
Module 8 (15 Credits) Risk Management
Guest Lectures, Research Methodology, Project Management, Case History Seminars, Conferences and Workshops
IA Laboratory Investigations, Experiments and Digital Forensics – The Kinetic Learning Environment

Figure 74: Proposed Federated Master of Science (MSc) in Information Assurance

Frankly, this is much easier said than done and indeed if the academy operates confidentially, it may have some problems convincing the public that it indeed is a "professional" organisation, rather than just a "closed shop". That there may be difficulties to achieve the aforesaid feedback into development processes if evaluations are classified and hence we will need some way of protecting case details from being inferred from general security advice. Some might argue that the very fact that some organisations do not wish details of security mistakes to become known is symptomatic of inadequate security culture. There is considerable literature about the need for security education and a contrasting perception of little resources to facilitate it. The implementation of an ISPD facilitates the ideal of building a UK IA Academy which can coordinate and accredit CPD courses for Educational and Professional Institutions, Government Agencies and corporations. Focus and efforts should follow, but also, the UK should develop the US programme for National Centre of Academic Excellence in Information Assurance Education established by the U.S. National Security Agency.



MSc in Information Assurance

Semester One Examining Human-Cyber Interfaces			Semester Two Understanding the Cross- Domain			The MSc Disseration 60 Credits
PGCert Module 1 20 Credits	PGCert Module 2 20 Credits	PGCert Module 3 20 Credits	PGDip Module 4 20 Credits	PGDip Module 5 20 Credits	PGDip Module 6 20 Credits	
Module 1a (10 Credits) DIME and Cyber Power	Module 2a (10 Credits) System Resilience	Module 3a (10 Credits) Dependable Architectures	Module 4a (10 Credits) Information Security	Module 5a (10 Credits) IA and Trust Management	Module 6a (10 Credits) Modelling Information Assurance	
Module 1b (10 Credits) Organisations and Change	Module 2b (10 Credits) Intrusion Tolerancy	Module 3b (10 Credits) System Survivability	Module 4b (10 Credits) Cyber Protection	Module 5b (10 Credits) IA and Risk Management	Module 6b (10 Credits) Shared Situational Awareness	

Guest Lectures, Research Methodology, Project Management, Case History Seminars, Conferences and Workshops

IA Laboratory Investigations, Experiments and Digital Forensics – The Kinetic Learning Environment

Figure 75: An Alternative Schedule for a Federated MSc in Information Assurance

Like a number of our universities Bournemouth's BSc scheme of work for their new Information Security and Forensics course has initially focused on various aspects of adding and integrating IA subjects into their existing curricula. The proposed Federated Master of Science (and possibly a Master of Research-MRes) framework are illustrated in Figures 167 and 168 and exhibits the two semester programme examining the Human-Cyber Interfaces and Understanding the IA Cross-Domain with an underpinning selection of core lectures and studies and a laboratory work in the kinetic learning environment of a (SEnIA) cyber –range.

A general outline of the curriculum that is widely recognized and replicated is required and typically a degree course should contain four core modules: "Information Management"; "Security Devices, Mechanisms and Cryptography"; "Information

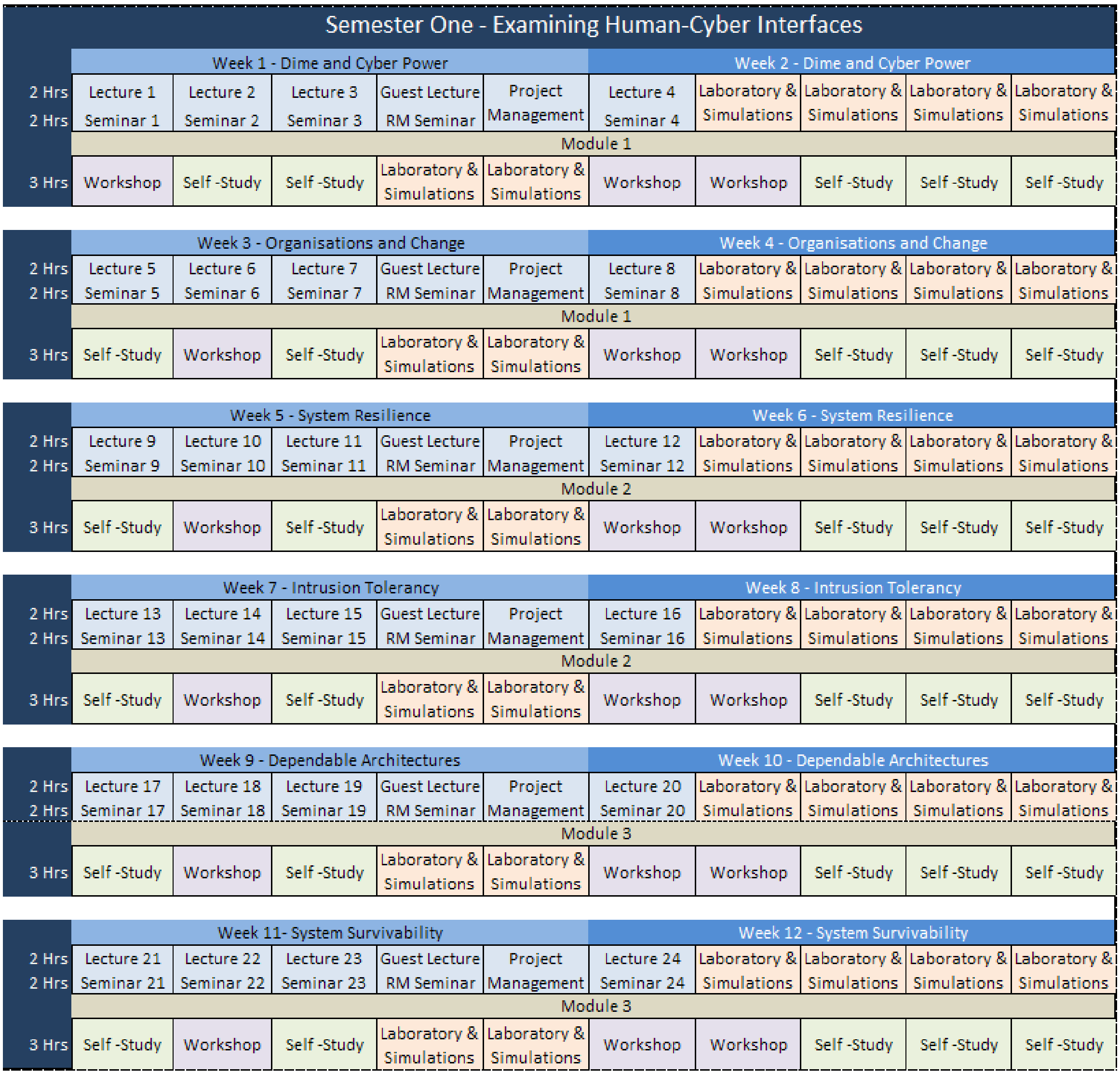
Assurance" and "Computer Security and Network Defence" which should be accompanied by several elective modules and a final project. Bournemouth has recognise that other universities are increasingly offering more dedicated courses that broaden the scope of undergraduate courses to post graduate degrees and diplomas such as The Royal Holloway, University of London, MSc. Degree in Information Security, which first commenced in 1992.

Bridging the capability gap requires more than a few Universities pioneering courses. There should be a national requirement to focus and scope more courses towards professional than academic careers. *Current security courses are typically dictated by faculty research interests, considerable attention has since been devoted to the systematic curricula design process of academic programs particularly at the undergraduate level* (Hjelmås and Wolthusen, 2006). However fascinating, "information forensics" (or the study of vulnerabilities) is really only worthwhile if it leads to general lessons being learned from particular cases; this requires that a vulnerability analysis leads to concrete proposals for changes to the computer systems development process; the aim of these changes should be to eliminate the whole class of vulnerabilities to which the subject vulnerability belongs. Randomised analysis of programmer error is not of much value, but a systematic classificatory analysis stands more chance of improving IT products significantly prior to delivery: a valid goal for any professional IA academy.

So do security professionals have role in dissuading product suppliers from seeing security as their own private business? This dilemma has been a problem for CLEFs operating Common Criteria assessments, since the assessment is generally paid for by the product supplier: if the details of the assessment are not made public, there is always some question about whether the evaluation certificate is just the result of a circular "rubber-stamping" exercise for the sake of getting paid: as Ross Anderson put it, "the real issue is (said to be) 'confidence'; that is, convincing people that systems are secure even when they aren't".

There are challenges and opportunities presented by offering a UK wide IA Education and CPD programme, to be innovated, timely and relevant, to offer a clear progression academically challenging and professionally rewarding education which will enable students pursue further careers in both academia and industry. The IA Academy is an imaginative solution but it can be positioned to facilitate security knowledge management.

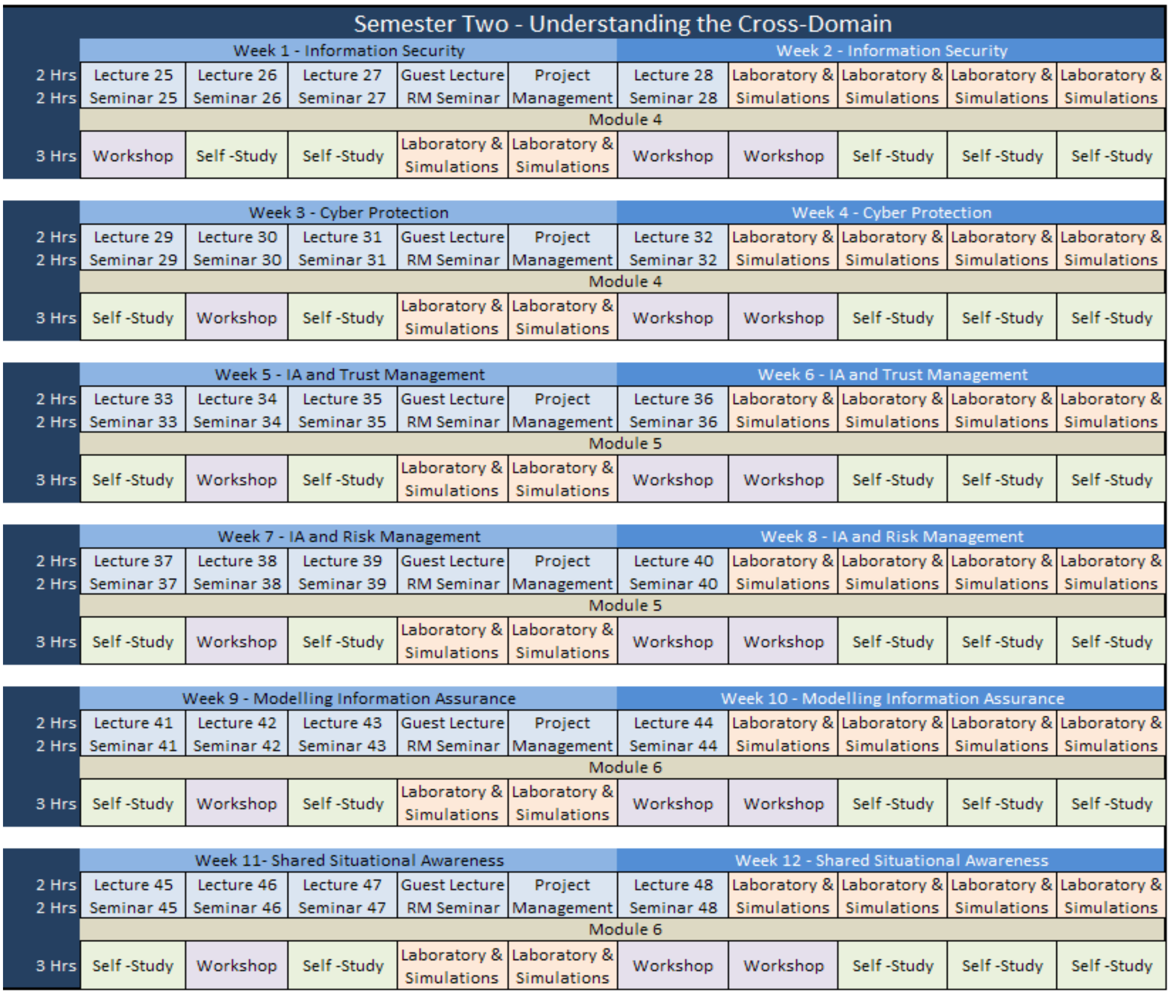
"The control of knowledge is the crux of tomorrow's worldwide struggle for power in every human institution." Alvin Toffler



	Semester One - Examining Human-Cyber Interfaces									
	Week 1 - Dime and Cyber Power					Week 2 - Dime and Cyber Power				
2 Hrs	Lecture 1	Lecture 2	Lecture 3	Guest Lecture	Project Management	Lecture 4	Laboratory & Simulations	Laboratory & Simulations	Laboratory & Simulations	Laboratory & Simulations
2 Hrs	Seminar 1	Seminar 2	Seminar 3	RM Seminar		Seminar 4				
	Module 1									
3 Hrs	Workshop	Self -Study	Self -Study	Laboratory & Simulations	Laboratory & Simulations	Workshop	Workshop	Self -Study	Self -Study	Self -Study
	Week 3 - Organisations and Change					Week 4 - Organisations and Change				
2 Hrs	Lecture 5	Lecture 6	Lecture 7	Guest Lecture	Project Management	Lecture 8	Laboratory & Simulations	Laboratory & Simulations	Laboratory & Simulations	Laboratory & Simulations
2 Hrs	Seminar 5	Seminar 6	Seminar 7	RM Seminar		Seminar 8				
	Module 1									
3 Hrs	Self -Study	Workshop	Self -Study	Laboratory & Simulations	Laboratory & Simulations	Workshop	Workshop	Self -Study	Self -Study	Self -Study
	Week 5 - System Resilience					Week 6 - System Resilience				
2 Hrs	Lecture 9	Lecture 10	Lecture 11	Guest Lecture	Project Management	Lecture 12	Laboratory & Simulations	Laboratory & Simulations	Laboratory & Simulations	Laboratory & Simulations
2 Hrs	Seminar 9	Seminar 10	Seminar 11	RM Seminar		Seminar 12				
	Module 2									
3 Hrs	Self -Study	Workshop	Self -Study	Laboratory & Simulations	Laboratory & Simulations	Workshop	Workshop	Self -Study	Self -Study	Self -Study
	Week 7 - Intrusion Tolerancy					Week 8 - Intrusion Tolerancy				
2 Hrs	Lecture 13	Lecture 14	Lecture 15	Guest Lecture	Project Management	Lecture 16	Laboratory & Simulations	Laboratory & Simulations	Laboratory & Simulations	Laboratory & Simulations
2 Hrs	Seminar 13	Seminar 14	Seminar 15	RM Seminar		Seminar 16				
	Module 2									
3 Hrs	Self -Study	Workshop	Self -Study	Laboratory & Simulations	Laboratory & Simulations	Workshop	Workshop	Self -Study	Self -Study	Self -Study
	Week 9 - Dependable Architectures					Week 10 - Dependable Architectures				
2 Hrs	Lecture 17	Lecture 18	Lecture 19	Guest Lecture	Project Management	Lecture 20	Laboratory & Simulations	Laboratory & Simulations	Laboratory & Simulations	Laboratory & Simulations
2 Hrs	Seminar 17	Seminar 18	Seminar 19	RM Seminar		Seminar 20				
	Module 3									
3 Hrs	Self -Study	Workshop	Self -Study	Laboratory & Simulations	Laboratory & Simulations	Workshop	Workshop	Self -Study	Self -Study	Self -Study
	Week 11- System Survivability					Week 12 - System Survivability				
2 Hrs	Lecture 21	Lecture 22	Lecture 23	Guest Lecture	Project Management	Lecture 24	Laboratory & Simulations	Laboratory & Simulations	Laboratory & Simulations	Laboratory & Simulations
2 Hrs	Seminar 21	Seminar 22	Seminar 23	RM Seminar		Seminar 24				
	Module 3									
3 Hrs	Self -Study	Workshop	Self -Study	Laboratory & Simulations	Laboratory & Simulations	Workshop	Workshop	Self -Study	Self -Study	Self -Study

Figure 76: A detailed sematic of the first proposed IA MSc Semester

Figures 169 and 170 illustrate a detailed sematic timetable for the proposed Federated MSc in Information Assurance. It encourages a high ratio of contact time between students and staff and allocates considerable time for experimentation and system simulation workshops. This paper proposes the development of the IA Professional Framework with a specific security educational programme, the ISPD and developing a network of academia and practitioners through a national centre of excellence. Such a centre will need the resources and cooperation of Government Departments, NGOs, Corporations, training organisations and higher educational institutions.



	Semester Two - Understanding the Cross-Domain									
	Week 1 - Information Security					Week 2 - Information Security				
2 Hrs 2 Hrs	Lecture 25 Seminar 25	Lecture 26 Seminar 26	Lecture 27 Seminar 27	Guest Lecture RM Seminar	Project Management	Lecture 28 Seminar 28	Laboratory & Simulations	Laboratory & Simulations	Laboratory & Simulations	Laboratory & Simulations
	Module 4									
3 Hrs	Workshop	Self -Study	Self -Study	Laboratory & Simulations	Laboratory & Simulations	Workshop	Workshop	Self -Study	Self -Study	Self -Study
	Week 3 - Cyber Protection					Week 4 - Cyber Protection				
2 Hrs 2 Hrs	Lecture 29 Seminar 29	Lecture 30 Seminar 30	Lecture 31 Seminar 31	Guest Lecture RM Seminar	Project Management	Lecture 32 Seminar 32	Laboratory & Simulations	Laboratory & Simulations	Laboratory & Simulations	Laboratory & Simulations
	Module 4									
3 Hrs	Self -Study	Workshop	Self -Study	Laboratory & Simulations	Laboratory & Simulations	Workshop	Workshop	Self -Study	Self -Study	Self -Study
	Week 5 - IA and Trust Management					Week 6 - IA and Trust Management				
2 Hrs 2 Hrs	Lecture 33 Seminar 33	Lecture 34 Seminar 34	Lecture 35 Seminar 35	Guest Lecture RM Seminar	Project Management	Lecture 36 Seminar 36	Laboratory & Simulations	Laboratory & Simulations	Laboratory & Simulations	Laboratory & Simulations
	Module 5									
3 Hrs	Self -Study	Workshop	Self -Study	Laboratory & Simulations	Laboratory & Simulations	Workshop	Workshop	Self -Study	Self -Study	Self -Study
	Week 7 - IA and Risk Management					Week 8 - IA and Risk Management				
2 Hrs 2 Hrs	Lecture 37 Seminar 37	Lecture 38 Seminar 38	Lecture 39 Seminar 39	Guest Lecture RM Seminar	Project Management	Lecture 40 Seminar 40	Laboratory & Simulations	Laboratory & Simulations	Laboratory & Simulations	Laboratory & Simulations
	Module 5									
3 Hrs	Self -Study	Workshop	Self -Study	Laboratory & Simulations	Laboratory & Simulations	Workshop	Workshop	Self -Study	Self -Study	Self -Study
	Week 9 - Modelling Information Assurance					Week 10 - Modelling Information Assurance				
2 Hrs 2 Hrs	Lecture 41 Seminar 41	Lecture 42 Seminar 42	Lecture 43 Seminar 43	Guest Lecture RM Seminar	Project Management	Lecture 44 Seminar 44	Laboratory & Simulations	Laboratory & Simulations	Laboratory & Simulations	Laboratory & Simulations
	Module 6									
3 Hrs	Self -Study	Workshop	Self -Study	Laboratory & Simulations	Laboratory & Simulations	Workshop	Workshop	Self -Study	Self -Study	Self -Study
	Week 11- Shared Situational Awareness					Week 12 - Shared Situational Awareness				
2 Hrs 2 Hrs	Lecture 45 Seminar 45	Lecture 46 Seminar 46	Lecture 47 Seminar 47	Guest Lecture RM Seminar	Project Management	Lecture 48 Seminar 48	Laboratory & Simulations	Laboratory & Simulations	Laboratory & Simulations	Laboratory & Simulations
	Module 6									
3 Hrs	Self -Study	Workshop	Self -Study	Laboratory & Simulations	Laboratory & Simulations	Workshop	Workshop	Self -Study	Self -Study	Self -Study

Figure 77 A detailed sematic of the second proposed IA MSc Semester

In partnership with Bournemouth University, the Defence College is continually developing an innovative security education paradigm. By working closely with other government agencies in developing an information security and assurance curriculum, institutions like Bournemouth University will able to provide a unique and rich learning environment for their students and ensure that government, NGOs and corporate employees gain their Professional Development in relevant practices of Information Assurance. Bridging the capability gap is important and a recognised IA Academy can bring together government agencies and corporations into a resourced research laboratory that will ultimately facilitate the real paradigm. The Academy would be a facility where security problems can be solved with innovation by teams of faculty members, professionals, and students. Qualifying and sustaining IA practitioners is a challenge to be conquered. The Academy will need to progress, develop and implement an Educational and IA CPD programme to train student and existing and newly accredited professionals effectively, economically and with a holistic approach.

4.3 Building an Information Assurance Competency Framework

The IA competency framework set out in this paper is inclusive, and practitioners are encouraged to consider whether any other specialist skills relate to their work, particularly in relation to the Government IT Profession and Knowledge and Information Management Profession.

There are six key strands to the implementation of IA professionalism:

- Professional Competency Framework – described in this document.
- Networking and mentoring.
- Training and opportunities to share common experience.
- Private sector collaboration – the IISP will be key in this area.
- Communication.
- Partnership – working with, and alignment to, Professional Skills for Government, the Government IT Profession, the Knowledge and Information Management Profession and other professions and stakeholder groups, in particular the IISP.

Recognition and understanding of IA

This IA Competency Framework proposes a structure for an IA profession, to which all those with IA responsibilities would belong (although it does not preclude membership of other professions, such as the Government IT Profession, where appropriate). It does not take account of the professional needs of the other specialists with which IA specialists work, such as IT, project management and finance professionals. IA specialists need an appreciation of these other professionals' particular areas and their relationship to both the organisation's business and IA. In the same way, these other professionals need an understanding of the need for IA and the roles of IA professionals. Indeed, all staff need a basic appreciation of IA and their particular responsibility for protecting information within their own sphere of influence. This is comparable to the inclusion of Finance as a core competence within the PSG Framework. This wider understanding of IA is outside the scope of this Competency Framework, but it is vital in ensuring that IA specialists are given proper recognition for their contribution to the organisation's business. In turn, all IA professionals need to ensure that they can communicate effectively with the business, and with others outside IA, in appropriate language.

Although IA is a distinct profession, there are potential areas of overlap with both IT and Knowledge and Information Management, as shown in Figure n below. Members of one profession might therefore also be members of one or both of the others, depending on their role and background. Information Technology (IT) is concerned with the application of technology to enable business objectives. It encompasses a wide variety of specialisms, including design, implementation and operation of information systems. The Skills Framework for the Information Age (SFIA), used as the basis for the Government IT Profession framework, covers a broad church, including such diverse activities as procurement and project management, which are clearly professions in their own right, but with some overlap with the IT profession. Information Assurance holds a similar relationship with IT, in that it is distinct, but with elements of overlap.

The Government IT Profession brings together all IT professionals working across the UK public sector, from new entrants through to the members of the Chief Information Officer (CIO) Council. It is coordinated by the Delivery & Transformation Group within the Cabinet Office, and the CIO Council provides sponsorship and direction from the highest level. Its aim is to create a joined up, government–wide IT profession which provides IT professionals with a career of mutual benefit to the individual and the government. HMG defines Information Assurance as "*the confidence that information systems will protect the information they handle, and will function as they need to, when they need to, under the control of legitimate users*". The IA Profession needed to include roles which provide this confidence by ensuring that the confidentiality, integrity and availability of business information and information systems are appropriate, cost effective and compliant with legislation, regulation and standards. The 2007 UK's National Information Assurance Strategy defines "*the development and availability of appropriate IA Capabilities*", including improved professionalism, amongst its objectives.

The Government's General IA Products and Services Initiative (GIPSI) Profession sub-group subsequently established a competency framework and career structure for the Information Security and Assurance profession. The present need is for a programme to progress and accredit education and professional development of existing practitioners. The framework links the Skills Framework for the Information Age (SFIA), which is currently used by the Government IT Profession, to a career path and expected educational standards. It defines competencies from Entry to Head of

Profession across IA, and expands IA into seven specialisms:

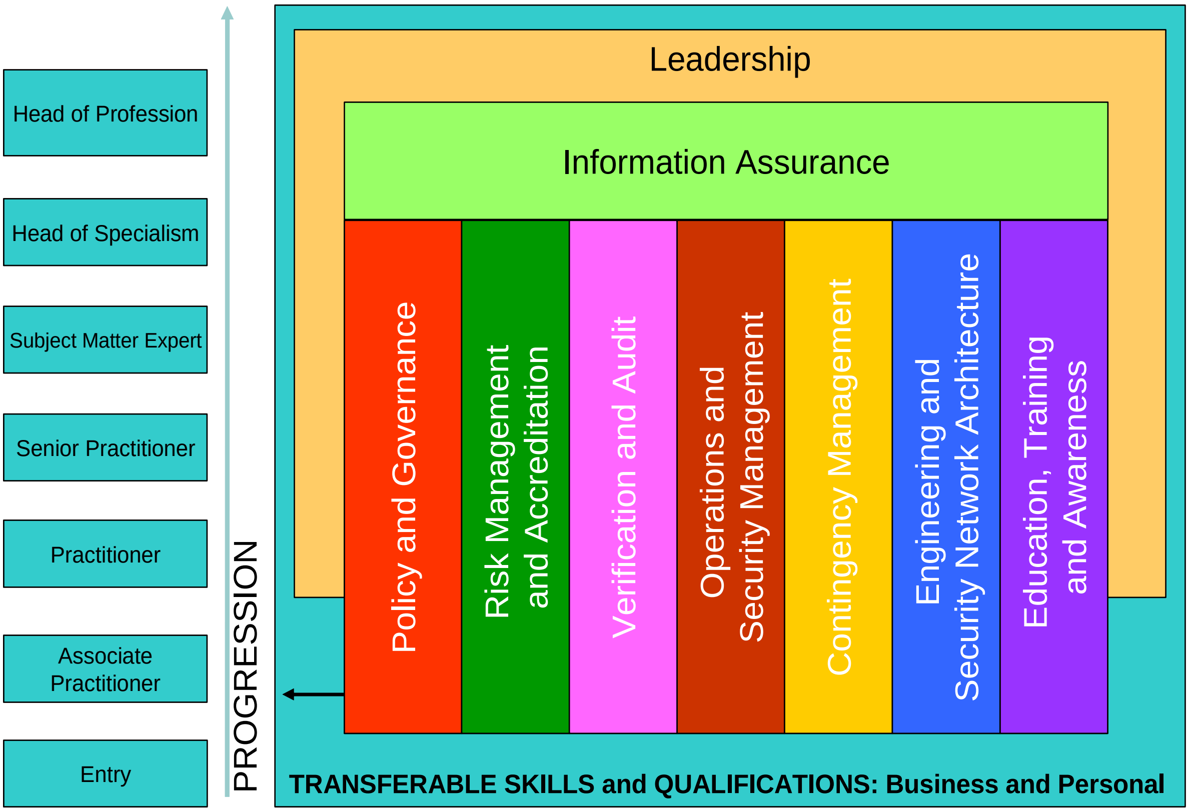


Figure 78: UK Government IA Framework

The Government Framework (also see Annex 5) further identifies the educational and training qualification requirements and the accredited continuous professional development certification through membership of professional bodies such as the Institute of Information Security Practitioners (IISP), BCS and the IET. The qualifications were defined for each level in line with the National Qualification Framework (NQF).

While each level in the ISPD programme is open for students meeting certain formal prerequisites, the sequence of CPD modules and degree courses will be designed in such a way as to allow students to progress from NQF levels 3 to 7 without undue overlap or repetition. This would still provide the flexibility for this organisation and other departments to recognise relevant international qualifications but still have the professionals having knowledge of the local content and regulations which are necessary for practising information security in the UK.

The opportunity for the information security profession is immense. Clearly we must continue to understand the evolving threat landscape coming from increasingly sophisticated criminal factions. We must also stay on top of the available technology to protect against these threats, recognising them as tools, rather than the focus of our jobs. Most importantly, however, we must recognise that our jobs are not only critical to the running of the business and protection of its assets, but also to its development and strength in the future.

Table 11: Competency Levels of an IA Practitioner

Level	Competency	NQF Levels
1.	**Entry** awareness based training	1
2.	**Basic** training – CBT and distant learning	2
3.	**Practitioner** training and education– Taught and distant learning module courses	3 and 4
4.	**Expert** training and education – Specific taught modules with distant learning material	5,6 and 7

We are driving a change in the role of the security professional. The UK's greatest asset is our information, whether its intellectual knowledge, data sources or financial transactions, we need to protect it, and thus we need assurance and this assurance will be provided by accredited professionals, who have a career path with rewards, to secure its confidentiality, integrity and availability to authorised users. The ISPD programme is something long overdue and what the IA community has been asking for. The proposed programme provides the education element to a new structured career path for the security professionals. It will educate them in areas in which they have been entrusted, to protect people, information, facilities, operations, and activities. This initiative will provide the UK trained security professionals with a genuine career path and appropriate accreditation.

Under current UK Information Security standards, classified networks have considerable security and risk exposure constraints that reduce system access across strategic, operational and tactical commands. Awareness of how IA affects knowledge and information management and their overall trustworthiness, necessitates further investigation and analysis of the NEC. IA professionalism plays an important role in understanding the behaviour and the complex nature of the NEC domains.

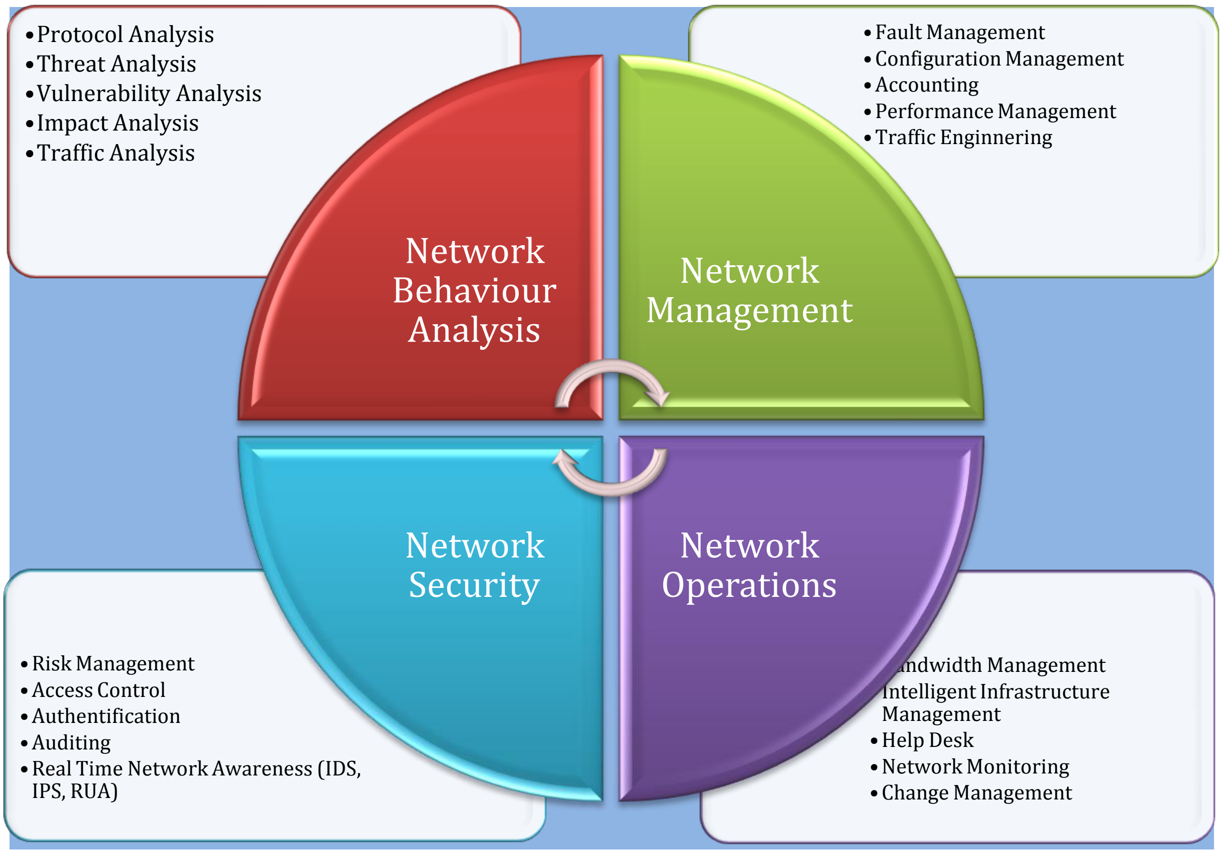


Figure 79: Ignorance of Network Behaviour, Management, Operations and Security

Governments, corporations and the military have undergone "*a transformation in their ability to gather, share and process information. The result is an unprecedented reliance on information infrastructures for their very survival. This dependency creates new opportunities for disruption"* (Anderson 2005). This presents societies with an unprecedented reliance on information infrastructures for their very survival. In one sense, this is tautologous: any reliance on technology that is new is by definition "unprecedented"; in another sense (our dependence for survival), the claim is merely false: "information" is hardly highest in the hierarchy of human needs: water, food and shelter, law and order are surely still more important; but the trend toward increasing dependence on IT in the systems that provide these things is the real issue; and whether it is wise to continue the trend is a question all security professionals are engaged in answering.

CHAPTER 5: Thesis Conclusion – Managing the Holistic Paradigms

"Information Assurance (IA) is the assumed responsibility (Corporate Governance) and accreditation of a socio-technical Enterprises across the 5-layers of the Cyber Domain (Geographical, Physical, Logical, Persona and Cyber Persona), inclusive of their Business Processes, Information Operations, Information Exploitation, Management, Services, Technologies and Infrastructures. The socio-technical Enterprise is assured by appropriate levels of maturity and awareness within the 8-Dimensions of Information Assurance (Structure, Resilience, Dependability, Safety, Security, Protection, Trust and Risk Management)." (Richardson, C.J., 2011)

Cyberspace has transformed our society, the way we do business and it affects our lives in countless ways. We depend on its global connectivity, which delivers information at light speed to most destinations in the world. In the *Internet of Things,* we and system agents order goods, do successful transfer of products to markets, manage financial assets, banking, travel arrangement and social networking to global communities: it affects us, it is beginning to control us and at the same time it offers new hope, freedoms and new opportunities. Cyberspace has become mankind's event horizon.

The goal of the thesis was to research the question does system isolation work. Can we really keep our secret, secret on a *need to know* bases and is this viable in the medium to long term future of Government (Diplomatic); Intelligence; Military and Economic (DIME) communities. The electronic isolation of our information systems is called Air Gapping and it was sensible when our systems were used as administration tools for departments, armed forces and other agencies. Bespoke systems were designed to meet physical electronic attacks, signal interceptions and spectrum analysis, they were often enclosed in TEMPEST shielded facilities and had very few terminals for a very select set of users; such systems are still operated today. However, the information stored in their data files are now needed by many new agents, actors and system users, they need to share intelligence, government communications, mission media and financial transactions with an ever increasing number of suppliers and clients. The original context and contents of these silo-like knowledge repositories may be subject to new analysis, data mining, knowledge transfer and decision making processes. The Socio-Technical Enterprise of the Information Age *needs to share* its Knowledge, Information and Data Assets.

The consequence of this research is to brush-off linearity and drill into complex systems. To look beyond limited lifecycle models, so prevalent in system engineering and enterprise architecture to encompass the problematic human behaviour affecting such systems. This thesis has set out to capture the more torridialG models of interoperability, where each type of system behaviour impinges on the holistic, combined operational pictures of Human-Cyber Interexchanges. The thesis asks the questions and offers some methodology to find the answers from an Information Assurance Perspective. It doesn't have the answers, but it does show how we can get better at making informed and trusted decisions.

What is the research question?

Can Information Assurance provide sufficient Trust and Risk Reduction to allow information processed, stored and communication within highly sensitive (often critical) networks, with their own discrete security domains (including encryption mechanisms), which are often Air-gapped (physically and electronically isolated) to interact safely and securely, particularly across many interoperable networks and including the possibility of interfacing with the Internet.

The Hypothesis questioned can the Socio-Technical Enterprise and transforming Governments, NGOs and the particularly the military afford to risk its most sensitive data to a probably cyber-attack. Stand-alone systems with their own security domains which are physically and electronically isolated; protected from other systems and unauthorized access; are assumed to have a high level of security and are essentially Air-Gapped. Whereas, bridged air gapped systems have made intrusion easier by multiple access points, multiple system integration and uncontrolled access. The Hypothesis further questions whether the operational benefits overcome the potential loss of assets; does the mission goals become realised in a more efficient and superior manner if the communities of interests acted more coherently with a better situational awareness, does the Enterprise have an risk appetite to do better, to share more frequently and encourage greater interoperability with its partners. The wish has been clearly stated, but is the will there? As fear is a very potent barrier.

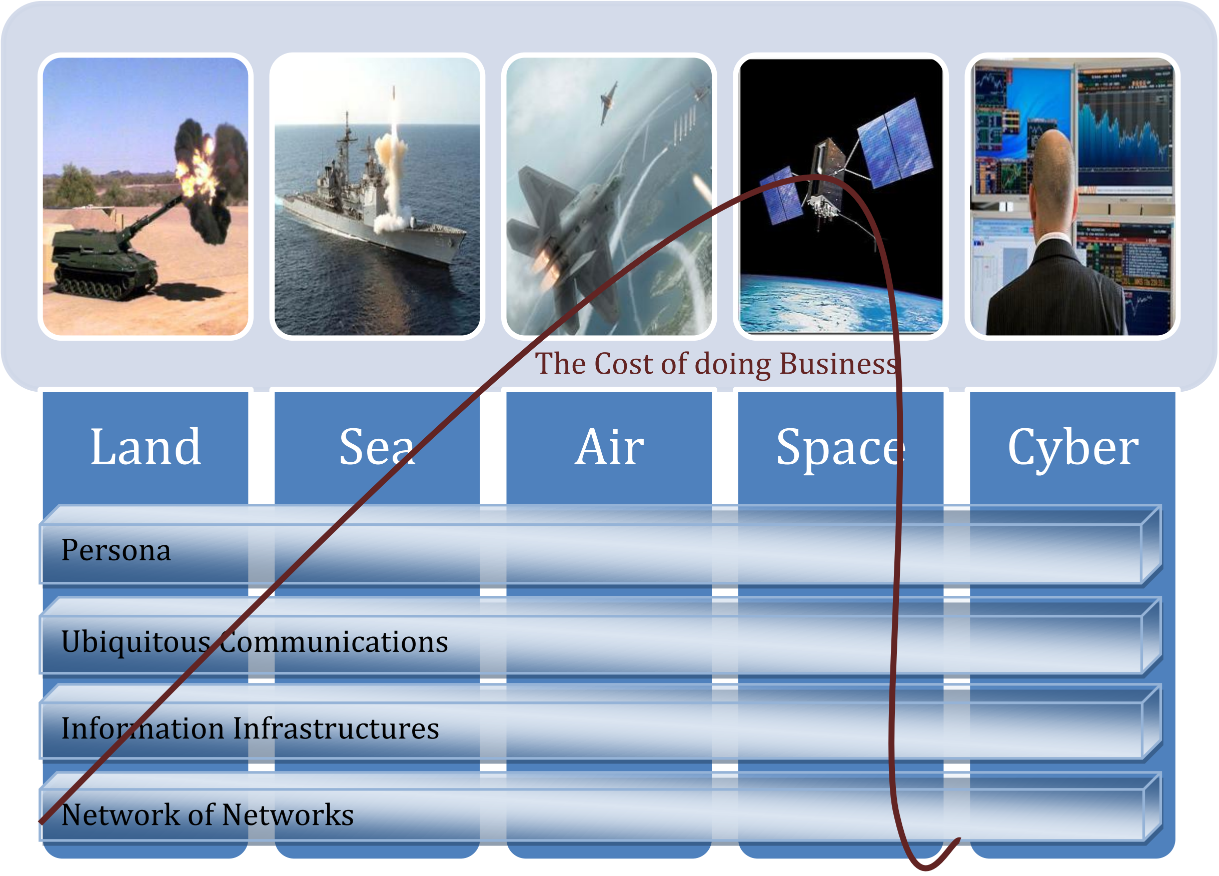

The Cost of doing Business
Land
Sea
Air
Space
Cyber
Persona
Ubiquitous Communications
Information Infrastructures
Network of Networks

Figure 80: The cost of doing business in military cyberspace

To answer the hypothesis a methodology was created to discover the causal effects of Bridging the Air Gap (Figure 24, p16). The methodology road-mapped 6 different paths to argue that Information Assured Socio-Technical Enterprise could, and would, work more efficiently and more effectively even with the risk of loss. However, such a risk had to be managed with more stringent safeguards, a better cross-domain solution and a better understanding of the systems of systems created.

From a military perspective, (figure 80) the cost of doing operations in Cyberspace is considerably cheaper than the other four military domains (Land, Sea, Air and space) and this hasn't gone unnoticed by other State Actors and potential adversaries. The military has to consider, develop, deploy and be willing to use cyber weapons and consequently we have Cyber Warriors who have a serious dilemma in Cyber Network Operations: when to defend and when to attack and is the potential to attack a good defensive policy - deterrence? This dilemma produces a distinction between Information Operations and Information Exploitation as modelled in I-Stack (Figure 47, p133). The Defensive Approach allows IA Policies and Best Practice Framework (figure 51, p139) to identify a comprehensive and coherent metric structure to analysis, manage and evaluate the Enterprise performance against International Standards. The IA metric will provide sufficient Trust and Risk Mitigation to the Enterprise when the system's resilience and dependability components are driven through the Diamond Model (figure 52, p141) to create a more assured Socio-Technical Enterprise.

Meeting the Research Aims

The research aim was to find a balance between protection and availability of Knowledge, Information and Data (the security of the KID components) and the need to exploit the information assets of a Socio-Technical Enterprise. This balance had to trusted, dependable, risk managed and resilient to errors, faults, intrusions and failures. The development of Information Assurance offers such a possibility. The Global and Military information environment demonstrated that bridging the air gap will allow the integration of many organisation (and create many vulnerabilities and attack routes). The safety of the Enterprise System is equally as strong as its security as these Information systems and operations are critical to our society, way of life and most likely our lives. If Information Assurance was to offer any solutions then we had to understand that the critical components of a safe and secure environment is paramount to military success and national security; the context and concepts of Information Assurance had to be thoroughly examined. Building models of the key IA issues provided that examination.

In addressing the primary aims of research into Bridging the Air Gap from an IA perspective this thesis postulated the "need to share" and the active building of inclusive communities of interests through technical to social interoperability has more impact to the overall well-being of a Socio-Technical Enterprise than the risk adverse "need to know" policy and its restrictive, exclusive practice of limiting access. This thesis has met its 5 primary aims and Engineering Objectives (Eos) as summarised in Table 12:-

Table 12: Compliance of the Research Primary Aims

	To provide an Information Assurance Capability that will facilitate Cross – Domain Solutions. This capability will need a framework that formulates the assurance implications of interoperability within cyberspace, human factors, protection of networks and secure data content, alignment of enterprise architecture, any organisation culture changes, information exploitation, management and service dependability from bridging the air gap between highly classified networks and possible interaction with lower classified networks and the Internet and how it might be done. The investigation will also consider when those bridges might be considered an acceptable risk.	EO1: The strategic positioning of IA as the underpinning science of Socio-Technical interoperability, the mapping of the Information Flow (figure 47, p133) ; Security of the Cross-Domain & System Survivability (figure 62, p153) and the effective management and best practice to control the Human-Cyber Interexchange (figure 51, p139) have been explored, modelled and argued within this thesis. Its investigation has produced working models that allow greater understanding, perception and awareness that the application of IA is essential for the trustworthiness of Systems and survivability of Enterprises operating in Cyberspace.
	Establish and develop an information assurance framework and appropriate models to meet operational interoperability requirements; whereby the study shall analysis various contextual and conceptual considerations of aligning and harmonising domain internetworking, thereby offering an assured cross-domain solution to military CIS interoperability.	**EO2:** Chapter 2 (Figure 21, p74): The Composite Model of Interoperability provides an IA Framework that encapsulates Enterprise Architecture; the layering of Interoperability (Figure 5, p19) and systems of systems interoperability.
	Exploring six main topics within the layered environment of Cyberspace (see figures 11, 14 and 25) and thereby framing the Cyber Landscape through modelling IA concepts. Analysing dependable, resilient convergence of technologies and networks and developing a Cyber-Assured Culture through Education; Promoting Transferable Skills & Professionalism will provide a new capability for Information Assurance. IA will demonstrate how to provide solutions to system interoperability; operational	**EO1, EO2 & EO3:** The development of the IA models and their current application to various business (figure 32, p100); Enterprise systems (figure 34, p108) and educational (figure 78, p192) problems is a testimony of importance and application of this research. More has to be done and there are future recommendations. The alignment of the 8-Dimensions of IA is needed to find Cross-Domain Solutions, System Tolerance, Risk Mitigation, Compliance and Maintenance of Shared Situational Awareness. This creates

	benefits; operational security and new community learning outcomes.	additional, but necessary, complexity to highly integrated, relational concepts of the Information Domain and Cyberspace.
	Illustrate the value of this research approach to the network-centric security problems of NEC (and the Global Information Environment as illustrated in **Error! Reference source not found.**) nd highlighting the real human-centric assurance issues to the various layers, domains and environments of an interoperable Cross-Domain Solution and provide a discussion on how the qualitative experience of this research and individual perceptions can be analysed and developed.	**EO1 & EO3:** The Thesis provides sufficient breadth and depth of modelling IA Cross-domain Solutions of Socio-Technical Enterprises (some of which are been actively used by Enterprises) and has recommended to further test the validity and impact of these models in a (SEnIA) Cyber Range.
	To identify, formulate and exhibit this approach and model implementation demonstrating it as a worthwhile Doctoral investigation. The thesis will be a successful project managed research programme with achievable, realistic outcomes within well-defined goals and agreed deliverable products.	**EO4:** The contextual and conceptual modelling of IA as formulated within this thesis has extended the State of Art, knowledge and understanding of the Science of this new Academic Philosophy.

The Human-Cyber Interexchange within a Socio-Technical Enterprise and the coupling across Enterprise Boundaries is a complex and evolving environment with many known and unknown emergent properties that can create new opportunities or jeopardise our societies. The ability to promote and to have: safe and secure, transforming, Information Operations across Cyberspace with protected Critical Information Infrastructures is a tier-1 national priority (Cabinet Office, 2011a). This Thesis has provided the context in which IA may allow Enterprise to meet that priority and the concepts and models of where and how this can be done.

5.1 Business Solutions to the Bridging the Gap

The rise of the Socio-Technical Enterprise, its real and virtual business operations, the ever increasing capacity to process, store and transmit Knowledge, Information & Data (often referred as Big Data); the introduction of Moore's law to computer design creating more powerful petabyte multi-cored machines; the phenomenal growth the Internet of Things (man and virtual agents) and this vast new world and symbiosis of Human-Cyber Interexchange (as illustrated in figure 81) has transformed how Governments, Industry, the military and individuals interact. We are becoming more aware of our environment, more socially connected and much more knowledgeable with vast arrays of Knowledge repositories a few clicks away.

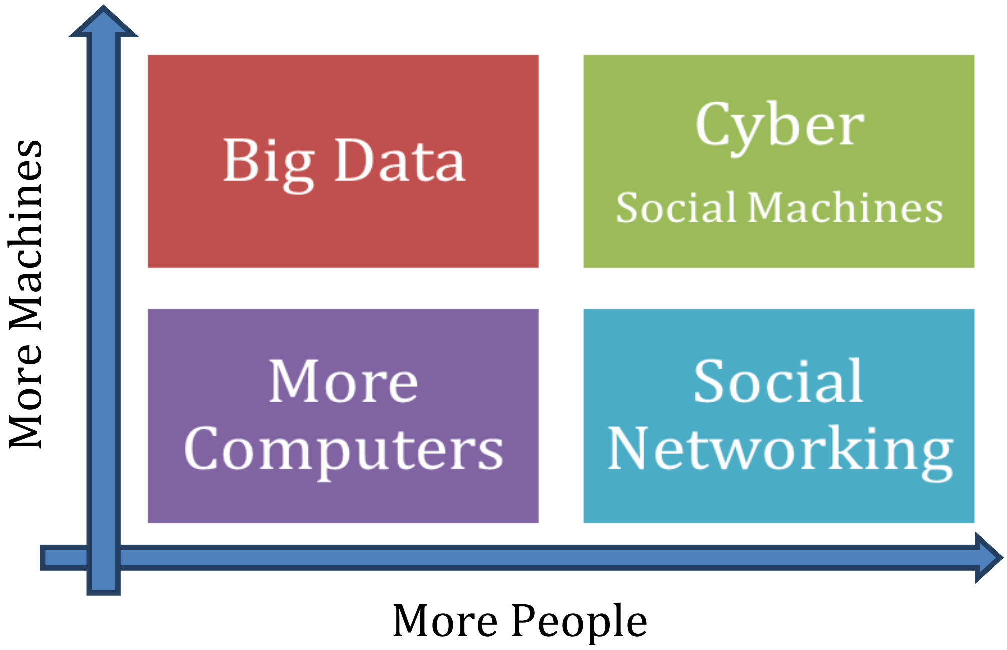


Figure 81: The Socio-Technical System of Man and Machine

The social landscape of the natural (real) word has created the Human-Cyber world and the social-technical enterprises that maintain, expand and evolve. The Social-Technical Enterprise is a Social Machine described by Professor Tim Berners-Lee (Berners-Lee & Fischetti, 1999) as a "*processes in which the people do the creative work and the machine does the administration*" which Theodore Piepenbrock (2004) further described as a dynamic spatial and temporal complex system "*where cause and effect of management's strategies and policies are distant in space and time... Temporal complexity recognizes that policies, decisions, structure and delays are interrelated to influence growth and stability. An enterprise's long-term success therefore is a function of management's ability to control this dynamic complexity.*

This dynamic complexity presents the Enterprise with new, vibrant management challenges, new opportunities to grow on a global scale; interact and access a global audience, to create new communities of interest and to share information to the benefit of all. Newtonian physics betrays this ideal world, for the opposite is true, the challenge is to keep out the unwanted, the criminals, people with malicious motives and actors who want to steal the Enterprise intellectual property. Dynamic complexity also produces fear, uncertainty and doubt (see chapter 3.1, p156), it creates vulnerabilities and weaknesses that can threaten the existence of its business, and the business of others; the spatial nature of the cyber world is that we all are interconnected.

In Cyberspace, the good does outweigh the bad, Social Technical Enterprises are flourishing, social networks are expanding, e-commerce has a phenomenal rate of growth and most of our society's institutions and supporting systems are administered across the Internet. There is cybercrime, but there has always been crime in human society; this is just a different attack pattern that we need to become more aware of these attack profiles and have better socio-technical solutions. Resolving Cyber Attacks and patching our vulnerabilities has become harder, the anonymity of individuals that roam the networks makes policing and attribution much more difficult.

Billions of Dollars have been spent on Cyber Security and the protection mechanisms of network edge devices and anti-virus software and yet, it takes a few $100 and some rudimentary knowhow to penetrate these most sophisticated defences. The protection mechanisms are needed because they do deter, hinder and capture most malicious attacks (CNA) but they are frequently been exposed to social attacks and zero-day vulnerabilities. This natural has kept many Intelligence Agencies arguing for electronic isolation (Air Gapping the Systems) of our more important and sensitive Critical Information Infrastructures, Military Capability and Knowledge Repositories. Nations and Enterprises need to keep their secrets, secret. However even isolated secure data silos have been compromised, penetrated and may still have insider intrusions; absolute security is impossible. Furthermore, these system silos have information that their user communities need to share, amongst themselves and with others. The sharing of information has created new interpretations; new knowledge and understanding; a greater awareness of the problems to be solved and has benefitted the Enterprise with more informed, superior decision making. The shared awareness has greatly improved the mission success, operational performance and efficiency of the Enterprise.

What is required is an Assurance Process that will allow the transfer of KID assets across Enterprise boundaries that will not compromise their operations, but will benefit their social-technical capabilities and strategic goal. This thesis has attempted to find the socio-technical bridges that might be employed to make our sharing of information more trusted, dependable and secure. There are technologies such as encryption, data diodes, intrusion prevention systems and multi-layered authentication and access control that all contribute to the protection of Information Systems and the Information flow across distributed services and databases which are making our cyberspace more secure and protected, but it isn't enough.

As Chapter 3 demonstrated, the layers of interoperability stem from the technical interface to the social systems of organisation and the motivation and psychological human factors. With people, there's always insecurity. The largest single threat to Cybersecurity is the Insider Threat. Information Security needs a new perspective.

Chapters 1 to 4 have argued that this new perspective is Information Assurance and its architecture, framework and models are needed to provide and the resilience, dependability, safety, security, protection, risk managed and trustworthiness of the Socio-Technical Enterprise. Chapter 7 has provided a number of arguments to create IA practitioners and education for the communities of interest. Bridging the Air Gap was never going to be a technical solution. Cross-Domain solutions and system survivability needs informed and knowledgeable IA practitioners to formulate evolve and evaluate the constant variable picture of cyber operations and the flow of information.

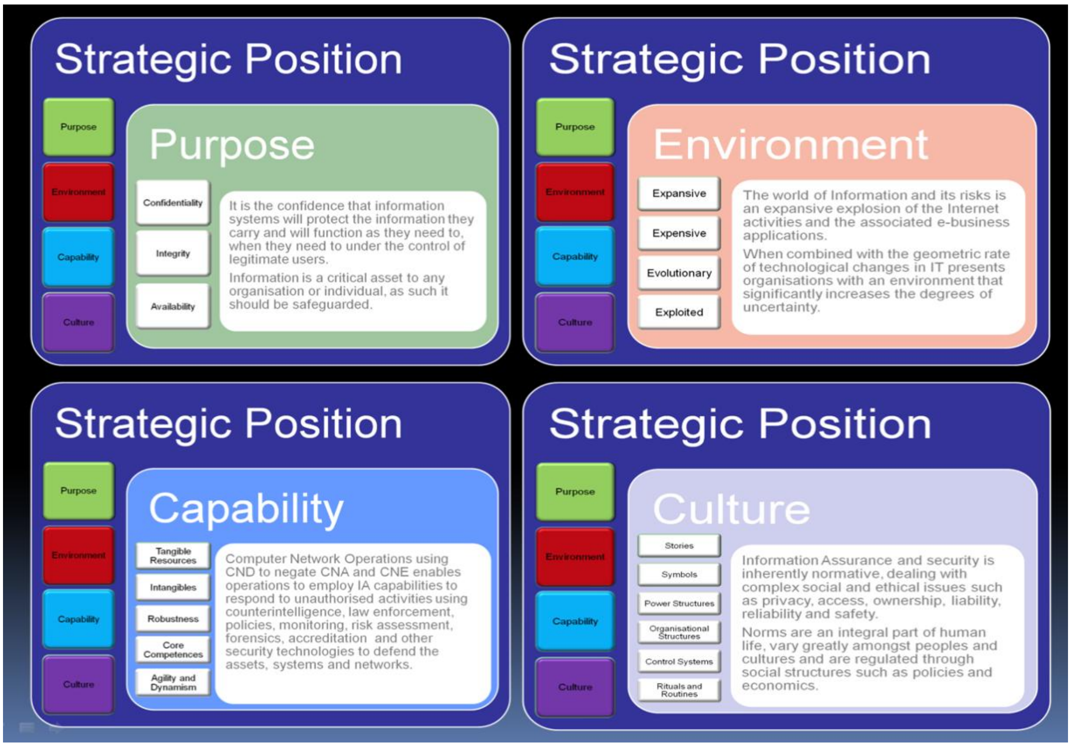
Strategic Reprise

In 2006 a number of on-going conversation were converging on the need to provide a national response and direction for Cyber-security and the protection of our Critical Information Infrastructures and Institutions (Rawlinson, 2005; Cabinet Office, 2005; Dull, 2006). In Afghanistan, NATO was trying to provide a mission secret platform for all communities of interest, including Afghan Government and military agencies. These systems were under constant Advance Persistent Threat (APT) attacks and well published exposures were hurting the reputation and integrity of these communities (Allor, 2007).

In 2007 the UK Government published its National Information Assurance Strategy (Cabinet Office, 2007) which formulated a number of (CSIA) Government Working groups to provide methodologies to implement this strategy and at a Bletchley Park NATO Seminar the concepts of security compromises was raised as a Socio-Technical problem (Richardson C. J., Security: a necessary compromise?, 2007).

In 2008 the US White House published the *Comprehensive National Cyber-security Initiative* (The US National Security Council, 2008) and started to invest money in new military organisation (CYBERCOM), security initiatives and IA education in Government Departments and Universities. This initiative was challenging and demanded improvements to defend national interests and information assets. This theme was promulgated at the NECTISE conference at Leeds University (Richardson C. J., Bridging an IA Capability Gap, 2008) and the drafting of a proposed IA professional framework (Richardson C. J., The IA Professional Framework - Draft White Paper, 2008) to Although these doctrines were based on the development of Information Security attributes and policies, they were only beginning to formulate issues involved with a social-technical environment and in particular in the high-tempo environment of military operations Telic and Herrick. This required a new look at the context and concepts of Information Assurance as initially described at a MSc Guest Lecture, DCCIS, Blandford Forum, (Richardson C. J., Cyber Situational Awareness: The Assurance of Information Operations, 2008b) and the need to federate our networks in theatre. This became a central theme of Chapter 4, the CSIA sponsored GIPSI working Group on Professionalism. This framework was later modified and reintroduced to the competency framework of IA practitioners in Institute of Information Security Professionals (IISP) and then by CESG for IA Practitioners for Government Services. It is now also used for bases for a National Occupational Standard (NOS) currently been formulated by BIS and the Skills Council for IT (e-Skills).

The cyber initiatives have placed Information Assurance as the main policy for the security and protection of Cyberspace and this had become the focus of IA Architecture and Information Management Strategies, (Willett, 2008; MoD, 2009).



Strategic Position

Purpose

It is the confidence that information systems will protect the information they carry and will function as they need to, when they need to under the control of legitimate users.

Information is a critical asset to any organisation or individual, as such it should be safeguarded.

Strategic Position

Environment

The world of Information and its risks is an expansive explosion of the Internet activities and the associated e-business applications.

When combined with the geometric rate of technological changes in IT presents organisations with an environment that significantly increases the degrees of uncertainty.

Strategic Position

Capability

Computer Network Operations using CND to negate CNA and CNE enables operations to employ IA capabilities to respond to unauthorised activities using counterintelligence, law enforcement, policies, monitoring, risk assessment, forensics, accreditation and other security technologies to defend the assets, systems and networks.

Strategic Position

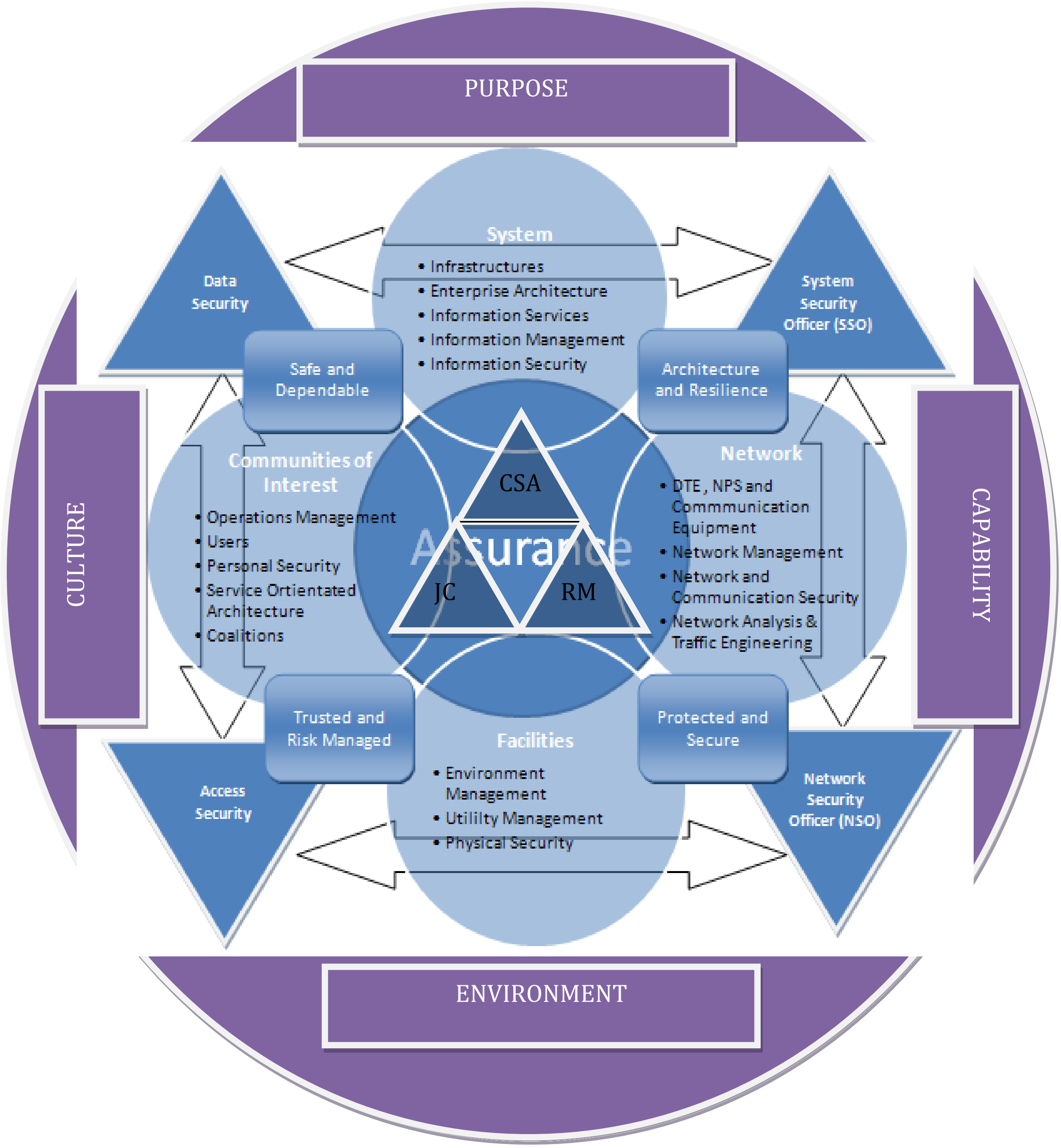
Culture

Information Assurance and security is inherently normative, dealing with complex social and ethical issues such as privacy, access, ownership, liability, reliability and safety.

Norms are an integral part of human life, vary greatly amongst peoples and cultures and are regulated through social structures such as policies and economics.

The strategic Positioning of Information Assurance as argued in chapter 2.4 (Figure 34, P108) has focused IA as a major component of Corporate Governance, Business

Continuity and the trustworthiness of business and decision-making processes (Richardson, C. J., Information Assurance: Holistic and Human Centric, 2011b). This new focus integrated the concepts of strategic business modelling to an IA framework that mapped the follow of Information and the responsibility of the Enterprise to protect its information assets. This formulated a new strategic composite model for IA as illustrated below,



Reprise of the Cross Domain

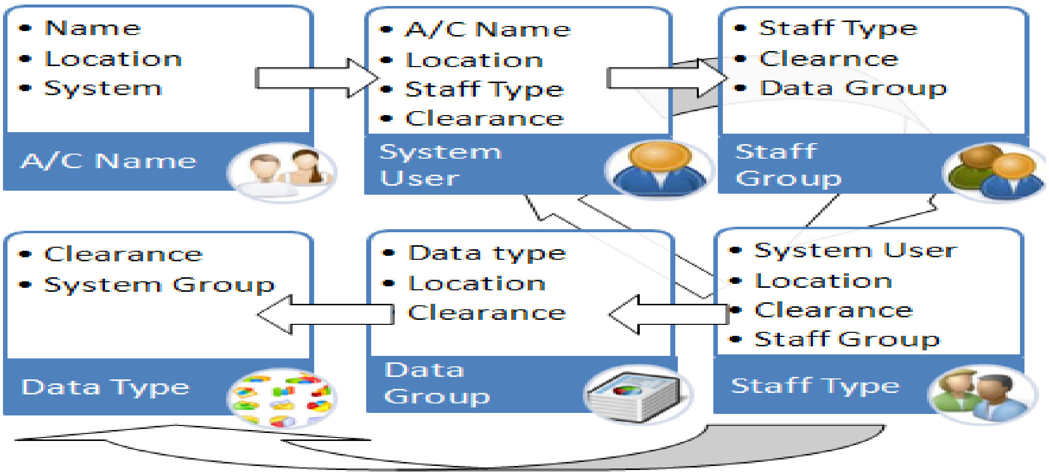


Figure 82: Current MoD System Access Schema

CDS is a main issue of IA (p.8) and has three assurance categories:

1) **Access Solutions**: The development of Geo-positioning, authentication access control system was an important component of developing a Cross-Domain solution. This problem was the instigation of this thesis and a major development programme for MoD IT Access Control. The majority of this work is beyond the classification of this thesis, however it is believed that in the last 5 years, significant progress has been made and a system is currently been evaluated.

2) The need to provide **Cross Domain Transfer Solution** is has been modelled with an IA perspective to Enterprise Interoperability and Layering of Cyberspace. This thesis argues that these two 3-Dimensional models will provide a greater insight to the properties and attributes of CDS and allow for more systematic approach to analysing the potential solutions.

3) **Accredited Solutions**: The Framework proposed in Chapter 6 (Figure 111, p342) provides the assurance for secure and trusted CDS for Information Operations and Exploitation. The next task is to develop the framework as a logical automated software model and experiment its capabilities in a cyber-range.

5.2 Assuring the Human-Cyber Interexchange

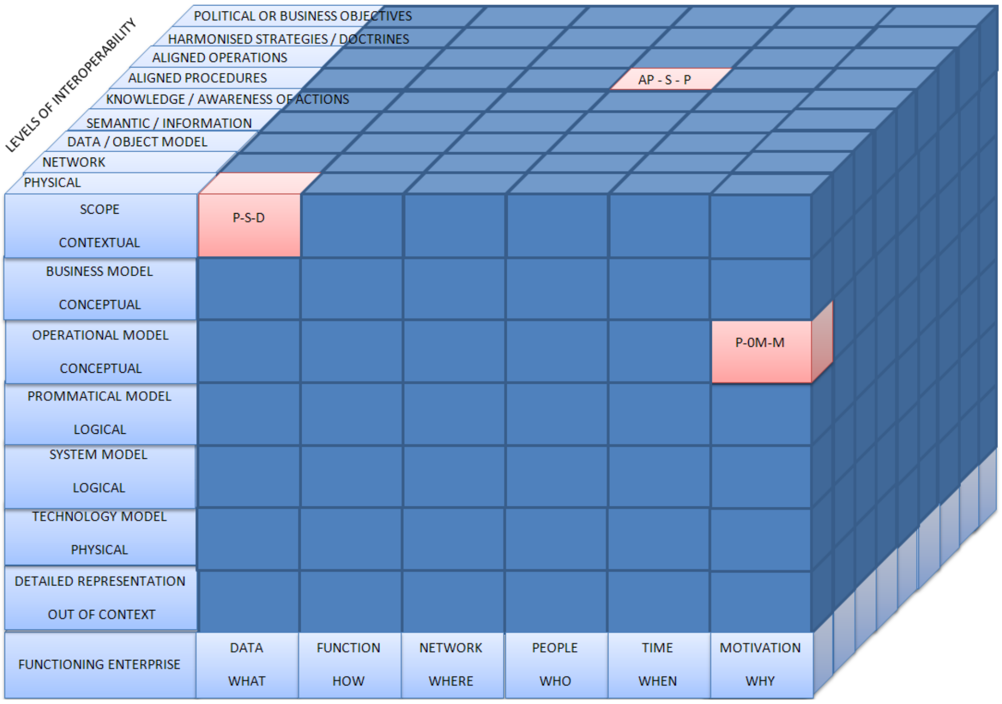
The thesis has presented a number of arguments that has changed the perception of Information Assurance. Some of these arguments still require considerable experimentation and simulation to validate their premise and verify their capability to the communities of interest. However, these models are been analysed and have made impact in the education of the assurance socio-technical systems and engineering of systems. With appropriate and detailed testing, the models will provide the communities an important tool set towards the understanding and control of the Cross-Domain and System Survivability. The EU and HMG are creating a number of research programmes to further investigate Trust in Cyberspace and these models, along with some future recommended research will provide an important perspective.

At the 2011 Cyber Security Conference held in Brussels the challenging consequences of these frameworks and the Human-Cyber Interexchange modelling concepts were introduced (Richardson C. J., Cyberspace: The 5th Domain, 2011). The need to test these models was accepted and the plans for a Cyber Range at DCCIS, Blandford Forum was planned and a financial costed business plan was produced

With the movement of the Engineer Researcher to a new lectureship at Bournemouth University, the Cyber Range concept and proposed simulations and experimentation has been revisited, planned and a multi-million pound revised business plan produced. The new System Engineering and Information Assurance (SEnIA) platform has been incorporated into the University's 2012-2018Strategic Business Plan for the continuation of Socio-Technical System (of systems) research; the development of IA simulations and threat modelling and any possible EU Horizon 2020 research themes.

Reprise of the IA Models

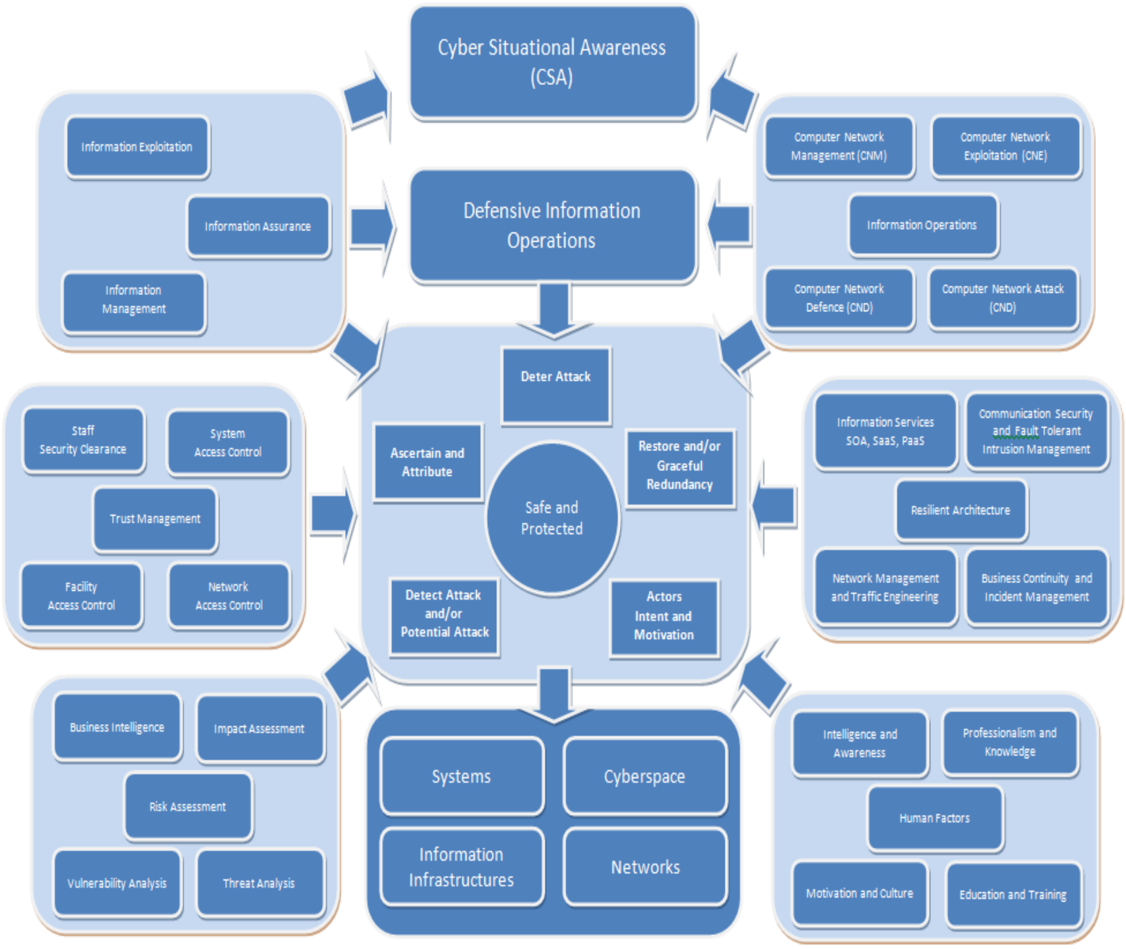
The IA Composite Model of Interoperability (**Figure 21**, p74), as illustrated below, provides a **3-**Dimensional holistic interpretation for the alignment and harmonisation of Enterprise business processes and its architecture with the technical-organisational layers of Interoperability of interconnecting Social-Technical Enterprises.



This composite model creates a new insight to the functionality and issues of CDS and Enterprise interoperability. The 3-D Cuboid utilises the analytical capabilities and functional views of Enterprise Architecture, the identified NCIOC layers of Enterprise Interoperability and Systems of Systems model developed by Carnegie Mellon University.

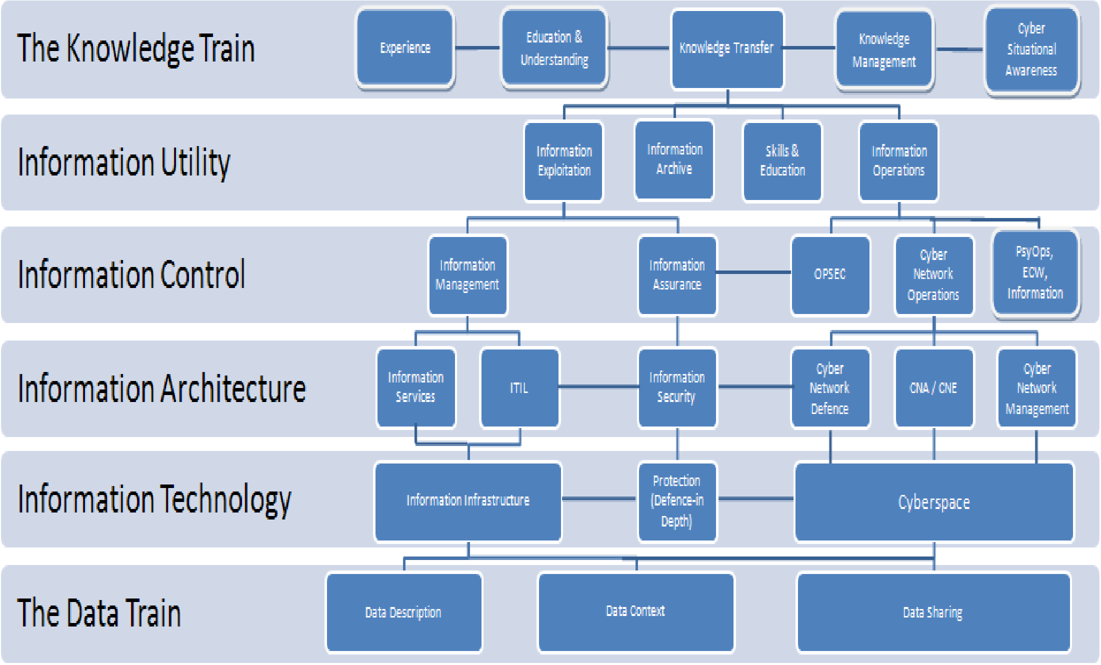
The 378 functional components of this model will provide a holistic, coherent and comprehensive picture of system interoperability of interconnecting Social-Technical Enterprises.

The Assured Cyber Defence Architecture (**Figure 40**, p119), as illustrated below is a jigsaw of components that influence and affect the cyber defence of a Socio-Technical Enterprise. The framework provides a coherent overview of IA Architecture as a methodology to provide Cyber Network Defence and a platform for Shared Situational Awareness and Superior Decision Making.


Cyber Situational Awareness (CSA)
Information Exploitation
Information Assurance
Information Management
Defensive Information Operations
Computer Network Management (CNM)
Computer Network Exploitation (CNE)
Information Operations
Computer Network Defence (CND)
Computer Network Attack (CND)
Staff Security Clearance
System Access Control
Trust Management
Facility Access Control
Network Access Control
Deter Attack
Ascertain and Attribute
Restore and/or Graceful Redundancy
Safe and Protected
Detect Attack and/or Potential Attack
Actors Intent and Motivation
Information Services SOA, SaaS, PaaS
Communication Security and Fault Tolerant Intrusion Management
Resilient Architecture
Network Management and Traffic Engineering
Business Continuity and Incident Management
Business Intelligence
Impact Assessment
Risk Assessment
Vulnerability Analysis
Threat Analysis
Systems
Cyberspace
Information Infrastructures
Networks
Intelligence and Awareness
Professionalism and Knowledge
Human Factors
Motivation and Culture
Education and Training

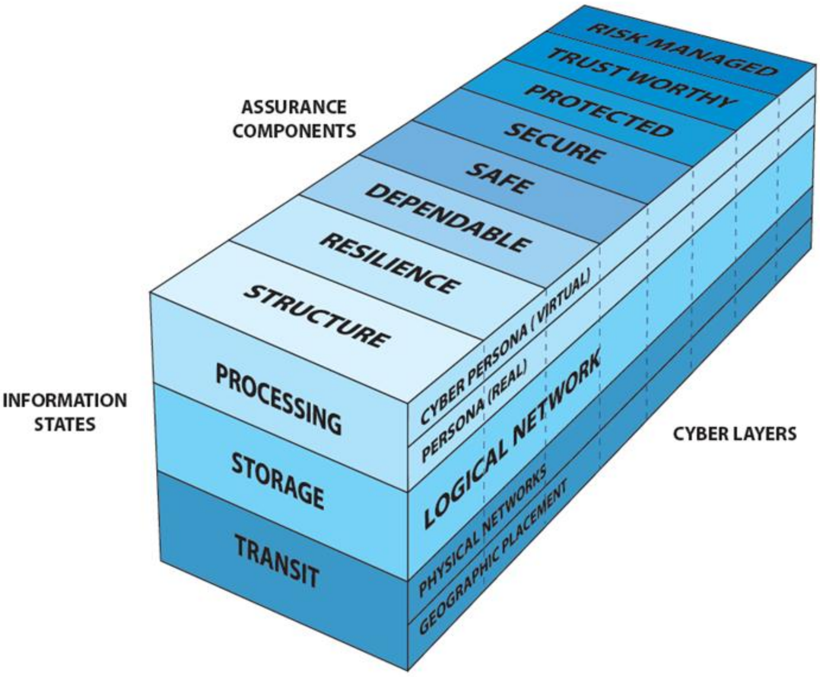
The model identifies 8 domains (with multiple elements) that influence the Cyber Defence and the creation of a trusted Cyber Operation Picture used by the Enterprise Communities of Interest's decision-making processes and shared situational awareness. The ability to control and secure operational and trusted repository information is essential to well-being and efficiency of the Enterprise and the performance of its mission goals.

The Information Functional Concept Model (**Figure 47**, p133) is a six layer model that differentiates the flow of information through a Socio-Technical Enterprise. Formulated on the principle Knowledge comes from Information which comes from Data (KID), the I-Stack Model provides a contextual overview of the Information flows from the physical components of the Data Layer to the virtual components of the Knowledge Layer demonstrating the Human-Computer interactive components of Information Exploitation and Information Operations.



This model provides a new holistic picture of the Information Domain.

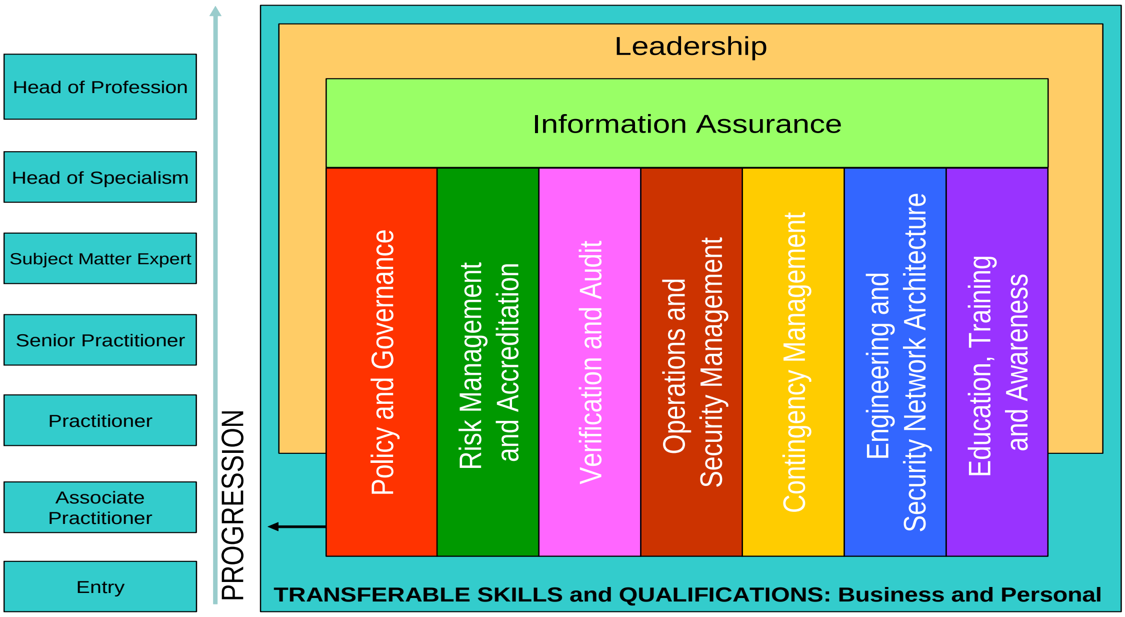
The 4 layers of Information (its technology, Architecture, Control and Utility) provide a framework for many interrelating and interconnecting activities. The model provides a simple relationship of many more established models and best practices such as Information Technology Infrastructure Library (ITIL); The Open Archival Information System (OAIS); The Information Security Forum for Best Practises for Information Security, MoD's Joint Doctrine Publications for Information Operations and Information Management and a host of CESG, RFC, ISO and ITU standards and guidelines, in particular ISO 20000 and ISO 27000.



The Information Assurance Cuboid Model (**Figure 57** p153), is the key model for interpretation of Information Assurance in Cyberspace. The thesis has illustrated the process that structures this 3-

Dimensional Cuboid. The model builds on the argument that there are 8-Dimensions of Information Assurance as presented in the IA Quadrant Model (and themed through the report) which are mapped against the flow of information (Process, Storage and Transit) and the military's perception of the layers of Cyberspace (Geographical, Physical, Logical, Persona and Cyber Persona). The IA Cuboid Model provides a reference to all the attributes of Assurance and allows the practitioner to build policies, procedures and best practices to design, maintain and develop IA in social machines and the Socio-Technical Enterprise.

The IA Skills Framework (**Figure 78**, p192) as illustrated below was derived from the UK's National Information Assurance Strategy (Cabinet Office, 2007) to develop the IA profession (Richardson C. J., The IA Professional Framework - Draft White Paper, 2008). Incorporated in the latest draft of HMG's Information Assurance Competency Framework; the model has also been developed for the UK's National Occupational Standard for Information Assurance:



The framework has been used to create a federated MSc and many of the degree's models are been used for Continuous Professional Development of IT Professionals and other communities interested in Information Assurance Architecture.

5.3 The Future Direction and Studies of IA

History has taught us: never underestimate the amount of money, time, and effort someone will expend to thwart a security system. It's always better to assume the worst. Assume your adversaries are better than they are. Assume science and technology will soon be able to do things they cannot yet. Give yourself a margin for error. Give yourself more security than you need today. When the unexpected happens, you'll be glad you did. **Bruce Schneier, 1997**

The Information Domain has many rooted problems and the potential to provide great opportunities to society, science and business:- the diversity of the markets and Enterprise it supports, the open architecture of the Internet and its protocols (TCP/IP), the pervasive technologies and services that make physical and virtual machines our real world and our motivation to be innovative and creative opportunist or reactionaries, greedy criminal with a thirst for power or money. Cybercrime is, globally, on the increase and has made significant impact of Governments, Multinational and SMEs, Financial Institutions and upon Individuals. It has generated a new Cyber-arms race with potentially ruinous outcomes for the Global Society. The APTs and SMART CNA are exploiting the complexities of interconnected systems, poor security and zero-day vulnerabilities. System Intrusion and passive attacks are common occurrence to DIME Organisation and Governments have finally begun to realise the true magnitude of Cyber Threats. Information Assurance provides a Socio-Technical barrier to malicious Cyber Network Exploitation. It is the rationale for Information Security and Protection Mechanisms; the Risk Management of Business Information Processes; the trustworthiness of Information Assets for superior decision-making; the resilience and tolerance of dependable system of systems and the methodology to understanding and creation of a good state of operations for an information demand, sharing and exploiting global communities of interest. Society needs to understand the need for Assurance; it needs better education and more IA professionals; an awareness of the persistent cyber threats and the knowledge to mitigate the risks of working in cyberspace. Time and Resources are needed to expand the research and development of IA, knowledge transfer to the Enterprises and the education of Individuals. The US Government has made a large financial commitment to bring and implement a national, comprehensive strategy of Information Assurance. The EU has made IA a policy Directive and has made IA a major component of its Horizon 20020 Research Programme. The UK's new Cyber Strategy has started to organise national centres and some research initiatives, but it is not enough.

A number of our large-scale system of systems have been suspended or cut owing to the apparent failure to delivery to cost and functionality. The biggest concern with most of these projects was their lack of awareness to interoperability and its assurance. There is enough evidence and a strong correlation that System and Software Engineering needs High Assurance and that these system architects require better understanding of IA and its impact on the business processes of Socio-Technical Enterprise. IA is about get the right information (accurate and dependable), to the right people (trusted, vetted and in need of the data) at the right time (sensitivity, geographical distributed and accessible). The creation of the System Engineering and Information Assurance (SEnIA) Platform with its 4 Cyber Laboratories; 3 Skunk Workshop Seminar Rooms; the building of 12 PhD IA programmes and the creation of a Federated MSc at Bournemouth University are examples of the commitment that this institution has to the fusion of research, development and education it has towards Information Assurance and the concepts and potential impact this thesis has to its Science and Societal impact.

Reprise Contributions

The following public conference proceeding, symposium and guest lectures have contributed to this thesis:

Richardson, C. J. (2007). Security: a necessary compromise? *NATO Conference, Bletchley Park, 26 June 2007.* Telindus.

Richardson, C. J. (2008a). Bridging an IA Capability Gap. *Realising Network Enabled Capability (RNEC'08), NECTICE, Leeds, UK, 13 October 2008.* NECTISE Loughbourgh University.

Richardson, C. J. (2008b, October 20). Cyber Situational Awareness: The Assurance of Information Operations. *CISM MSc Lecture*. Blandford Forum, Dorset, UK: Defence College of CIS (DCCIS).

Richardson, C. J. (2008c). *The IA Professional Framework - Draft White Paper.* Defence College of Communication and Information Systems (DCCIS), ICT Faculty. Blandford Forum: Cabinet Office.

Richardson, C. J. (2008d). *Managing Information Security and its Assurance.* Blandford Forum: Defence College of Communications & Information Systems (DCCIS).

Richardson, C. J. (2009a). A Holistic Approach to Effective Information Assurance Education. *Military Information Assurance and Security Symposium, MoD Abbey Wood, 16 April 2009.* Cobham Technical Services.

Richardson, C. J. (2009b, November 10). Computer Network Operations: Military Cyber Operations in Theatre. *CISM MSc Lecture*. Blandford Forum, Dorset, UK: Defence College of CIS (DCCIS).

Richardson, C. J. (2011). Cyberspace: The 5th Domain. *Cyber Security 2011, Brussels, Beliguim, 31 May- 1 June 2011.* IQPC.

Richardson, C. J. (2011). Information Assurance: Holistic and Human Centric. *iGRC TD2 Presentation, Birkbeck, University of London Symposium, 15 December 2011.* Bournemouth University

Richardson, C. J. (2012, June 5). The Assurance of Socio-Technical Enterprise Operations. *MSc Information Assurance Module 2*. London, UK.

The themes, concept models and the impact of IA has been taught as degree modules at the Defence College of Communications and Information Systems (DCCIS): MSc Communication and Information Systems Management; BSc (Hons) Telecommunications Systems Management; BSc (Hons) Management of Military Information Systems and the FdSc Communication Systems Management by the Engineering Researcher since October 2005 and recently BSc (Hons) Digital Forensics and Security at Bournemouth University. Furthermore there have been 10 MSc published Dissertations by DCCIS students, supervised by the Engineering Researcher, that have taken military aspects of IA and applied them to operational and system concerns in theatre, within MoD CIS, NATO NEC and with the New Zealand Command and Control Organisations. Bournemouth University is currently assessing both a new MSc and a MRes in Information Assurance and some of the proposed modules are already been taught on its outreach CPD programme with the BBC. There are 3 new PhD Research Programmes in the application of IA in Cybercrime and Policing are been supervised by this Researcher and another 2 have been instigated and await candidature. Some of the models have used by a European Multinational to develop its new business strategy and operations in European Information Security, by UK institutions to develop a Professional Competency Framework for IA practitioners and by the UK Skills Council (e-Skills) to create a National Occupational Standard in Information Assurance. These initiatives have been promulgated through the Cabinet Office, the Information Assurance Advisory Council (IAAC), The Ministry of Defence and a number of conferences. Some Knowledge Transfer Partnerships (KTPs) are currently been developed between Bournemouth University and some local SMEs to encourage a greater dissemination and adoption of this research IA methodology and models.

5.4 IA Bridges

The counter argument to 20th Century Deterrence is knowing how to use Information Assurance in the 21st Century. **Richardson, C. J., 2012**

Information Assurance is the rationale behind Safe and Secure flow of Information assets across the Information Domain of a Social Technical Enterprise. It is not a component of Information Operations, but a component of Information Exploitation. This is a fundamental concept for the Socio-Technical Enterprise when Information operations may have outright offensive (other than penetration testing) component which is ethical (and morally) unacceptable to the IA philosophy. IA is not an operational deterrence, but a trust building process for the Enterprise business process. However IA practices do, and should continue influence Operational Security (OpSec) policies. In building bridges, as illustrated below (figure 17, p65) the thesis has demonstrated that there are a number of methods (see table 13) to provide Information Assurance to the Enterprise.

Table 13: IA Methods to Build Bridges

Bridges to Build	IA Methods
1. The Need to Share	Providing Information Assurance to the Technical to Organisational Layers of Interoperability
2. The Need to Know	Providing Security and Protection Mechanisms (Access control, Encryption, IPS, etc) to maintain System Confidentiality and Integrity
3. Landscape	Human-Cyber Interexchange Federated Networks of Networks Cross-Domain Solutions (CDS) Systems of Systems IA Architecture (SoS IA^2) Socio-Technical Enterprises
4. Domain	Developing a Cross-Domain Solution for System Interoperability and Resilience in Cyberspace.
5. Initiatives	The BU SEnIA platform Initiative The EU FP7 – Theme 10 Security EU Horizon 2020 The SDA Security & Defence Cyber-Security Initiative EPSRC Centre of Excellence in Cyber Security Research

6. Trusting	The IA Cuboid and Diamond models have incorporated the 9-Dimensions of trust into a metric that aligns them to the dynamic components of assurance, the 3 layers of information flow and the 5 layers of Cyberspace. This produces over 30,000 trust entity relationships. (The Cyber Security-Trust relationship alone has 9pp x14bfp x9T-Ds x3(P-S-R) x5(CLs)= 17,010 E-Rs)
7. Learning	A Federated & modular kinetic learning is an important first step in IA education. The practitioners need to understand the working concepts of IA policies in system behaviour and architecture.
8. Good Practice	The IA framework structures many standards, guidelines, working models, legal compliance and established good practices (ISF).

Future Work

The research (Figure 4, p16) had 4 main themes (Strategic Positioning of Information Assurance; developing a Cross-Domain Solution for Interoperability and Resilience within Cyberspace; development of 8-dimensional IA Cuboid and the development of IA Education and its Profession); each component has generated considerable external interest and this has been reflected in table 21.

Table 14: Possible Future Work to this Thesis

	Possible Future Work
1.	Building a relational data model for all (30K+) components of the IA Cuboid and data mine the model for possible linkages, exclusions and external influences
2.	Building a relational data model for the 378 component composite cuboids of the Interoperability Model
3.	Map the IA Policies and Practice Framework to the above two databases and produce a comprehensive IA Reference Model
4.	Simulate threat modelling to OODA operations and impose IA constraints, compliance and policies

5.	Develop a universal Access Control Model for Cross-Domain Operations.
6.	Develop a Meta-tagging PKI for inter-domain Grey Networking with PRIME IP encryption
7.	Create Large-Scale Systems of Systems (physical networks, simulated networks and system-in-the-loop) and test IA policies to current emulated CII systems.
8.	Create a Federated MSc with at least 5 UK Universities
9.	Continue to aid the development of the UK National Occupation Standard
10.	Continue to develop a Professional Competency Standard for IA Practitioners
11.	Influence and help build the EU Policy on Information Assurance
12.	Build and develop the BU SEnIA platform
13.	Build Socio-Technical Enterprise Emulations to test future SoS Architectures

Summary

Bridging the Air Gap has generated a number of key research themes which has been further developed from the original concepts described within this thesis.

Information Assurance is a vibrant and evolving science with numerous UK and European initiatives; particular in Trusted ICT, Assured System Architecture and Cross-Domain Interoperability Solutions. This Thesis has created a number of models to address the current evolving; expanding and exploitative issues involved in IA and the future work will ensure that the research concepts will become impact models for the benefit and safety of Socio-Technical Enterprise and other DIME organisations.

The Research already generate further Government, Industry and Academic Research and Development and is hoped that it continues to add value to the IA community and to the expanding world of Cyberspace.

References

(n.d.).

Committee on Information Systems Trustworthiness. (1999). *Trust in cyberspace.* (F. B. Schneider, Ed.) Washington, D.C., USA: National Academies Press.

EA. (2000). *EA Guidelines for the Accreditation of bodies operating certification/ registration of Information Security Management Systems.* Brussels, Belgium: European co-operation for Acceditation (EA).

Abadi, M. (2000). Security Protocols and their Properties. In *Foundations of Secure Computation, NATO Science Series* (pp. 39-60). Chicago: ISO Press.

Abernethy, K., Treu, K., Piegari, G., & Reichgelt, H. (2005). A learning object repository in support of introductory IT courses. *Proceedings of the 6th conference on Information technology education* (pp. 223-227). Newark, NJ: ACM.

Abraham, F. D. (2005). *Cyborgs, Cyberspace, Cybersexuality and the Evolution of Everyday Creativity.* Retrieved May 2, 2011, from Blueberry Brain Institute (USA): http://www.blueberry-brain.org/chaosophy/Cybersexuality-v4.htm

Abramson, M., Breul, J., & Kamensky, J. (2007). Six Trends Transforming Government:How the interrelated effects of demographics, technology, and new modes of public service delivery are changing the way government is being managed. *The Public Manager*.

Adams, A., & Blandford, A. (2005, July). Bridging the gap between organizational and user perspectives of security in the clinical domain. *International Journal of Human-Computer Studies, 63*(1-2), 175-202.

Adams, C., & Lloyd, S. (2006). *Understanding PKI: Concepts, Standards, and Deployment Considerations, Second Edition* (2nd ed.). Boston, MA: Addison-Wesley Professional, Pearson Education, Inc.

Adelman, S., Moss, L., & Abai, M. (2005). *Data Strategy.* Indianapolis, Indiana: Addison-Wesley Professional.

Akdeniz, Y., Walker, C., & Wall, D. (2000). *The Internet, Law and Society.* Pearson Education, Inc.

Alberts, C., & Dorofee, A. (2002). *Managing Information Security Risks: The OCTAVE (SM) Approach* (1st ed.). Pittsburgh, PA: Addison-Wesley Professional, SEI Series CERT Book, Pearson Education, Inc.

Alberts, D. S. (1997). Agility, Focus, and Convergence: The Future of Command and Control. *The International C2 Journal, 1*(1).

Alberts, D. S. (2002). *Code of Best Practice for Experimentation.* Washington D.C.: CCRP Publication Series.

Alberts, D. S., & Hayes, R. E. (2006). *Understanding Command and Control.* Department of Defence, Office of the Assistant Secretary of Defense (OASD),Command & Control Research Program (CCRP). Washington D.C.: CCRP Press.

Alberts, D. S., & Nissen, M. (2009). Toward Harmonizing Command and Control with Organization and Management Theory. (D. S. Alberts, Ed.) *The International C2 Journal, 3*(2), 1-59.

Alberts, D. S., & Papp, D. S. (2001). *Volume III: The Information Age Anthology: The Information Age Military.* Washington D.C.: DoD C4ISR Cooperative Research Program (CCRP).

Alberts, D. S., Garstka, J. J., & Stein, F. P. (1999). *Network Centric Warfare: Developing and Leverating Information Superiority. 2nd Edition.* Washington D.C.: Department of Defense Command and Control Research Program (CCRP).

Alberts, D. S., Garstka, J. J., Hayes, R. E., & Signori, D. A. (2001). *Understanding Information Age Warfare.* Department of Defense, C3I/Command and Control Research Programme. Washington D.C.: CCRP.

Alberts, D. S., Huber, R. K., & Moffat, J. (2010). *NATO NEC C2 maturity model.* Washington D.C.: DoD Command and Control Research Programme Press.

Alexander, P., Kimmel, G., & Burke, D. (2007). *Security as a System Property: Modeling trust and security in Rosetta.* Lawrence, KS: The University of Kansas, ITTC.

Al-Hamdani, W. A. (2006a). Knowledge flow with information assurance track. *Wasim, A. A.-H. (Proceedings of the 3rd annual conference on Information Security Curriculum Development (InfosecCD). Kennesaw, Georgia, 22-23 September 2006* (pp. 52-57). ACM.

Al-Hamdani, W. A. (2006b). Assessment of need and method of delivery for informationsecurity awareness program. *Proceedings of the 3rd Annual Conference on Information Security Curriculum Development, InfoSecCD 2006, Kennesaw,Georgia, USA, 22-23 September, 2006* (pp. 102-108). ACM.

Al-Kuwaiti, M., Kyriakopoulos, N., & Hussein, S. (2009, Quarter 2). A comparative analysis of network dependability, fault-tolerance, reliability, security, and survivability. *Communications Surveys & Tutorials, 11*(2), 106 - 124.

Allemang, D. (2010). Semantic Web and the Linked Data Enterprise. In D. Wood (Ed.), *Linking Enterprise Data* (p. 23). Springer.

Allen, J. (2005). *Governing for Enterprise SEcurity.* The Software Engineering Institute. Pittsburgh, PA: Carnegie Mellon University.

Allor, P. (2007, August 2007). Understanding and Defending Against Foreign Cyber-Threats. *Journal of Homeland Security, 1*.

Alperovitch, D. (2011). Towards Establishment of Cyberspace Deterrence Strategy. In C. Czosseck, E. Tyugu, & T. Wingfield (Ed.), *3rd International Conference on Cyber Conflict* (pp. 87-94). Tallinn, Estonia: CCD COE Publications.

Anandavala. (2005, October 28). *Information System Theory (IST).* Retrieved May 10, 2011, from Anandavala : http://www.anandavala.info/index.html

Anderson, J., & Rainie, L. (2010, July). *The future of social relations.* PEW Internet and American Life Project. Washington, DC: Pew Research Center.

Anderson, J., & Rainie, L. (2010). *The Future of the Internet.* Washington, D.C.: Pew Research Center .

Anderson, K. (2005). *Hacktivism and Politically. Motivated Computer Crime.* Encurve, LLC.

Anderson, R. (2008). *Security Engineering: A Guide to Building Dependable Distributed Systems* (2nd ed.). Cambridge: Wiley.

Andress, A. (2004). *Surviving Security: How to Integrate People, Process and Technology* (2nd ed.). Auerbach Publications, Taylor & Francis Group.

Ardagna, C. A., Camenisch, J., Kohlweiss, M., Leenes, R., Neven, G., Priem, B., et al. (2010, January). Exploiting cryptography for privacy-enhanced access control: A result of the PRIME Project. *Journal of Computer Security, 18*(1), 123--160.

Armistead, E. L. (2004). *Information Operations: Warfare and the Hard Reality of Soft Power (Issues in Twenty-First Century Warfare)* (1st ed.). Potomac Books, Inc.

Armistead, E. L. (2007). *"Information Warfare: Separating Hype from Reality" Issues in Twenty-First century Warfare* (1st ed.). Potomac Books, Inc.

Armistead, E. L. (2010). *Information Operations Matters: Best Practices.* Potomac Books, Inc.

Armistead, E. L., Kuusisto, R., & Kuusisto, T. (2005). Common Operational Picture, Situation Awareness and Information Operations. *Proceedings 4th European Conference on Information Warfare and Security, University of Glamorgan, UK, 11-12 July 2005* (pp. 175-186). Academic Conferences Limited, Reading, UK.

Army Regulations 25-2. (2009). *Information Assurance.* Department of Defense, Secretary of the Army, Department of the Army. Washington D.C.: Army Study Guide, DoD.

Army Research Laboratory. (2009). *Advanced Decision Architectures for Warfighters: Foundations and Technologies .* (P. McDermott, & L. Allender, Eds.) Adelphi, MD, USA: Army Research Laboratory Advance Decision Architectures Collaborative Technology Alliance.

Arquilla, J., & Borer, D. A. (2007). *Information Strategy and Warfare: A Guide to Theory and Practice (Contemporary Security Studies)* (1st ed.). (J. Arquilla, D. A. Borer, J. Gow, & R. Kerr, Eds.) Routledge.

Arquilla, J., & Ronfeldt, D. (1997). *In Athena's Camp: Preparing for Conflict in the Information Age.* Washington D.C.: RAND National Defense Research Institute.

Arquilla, J., & Ronfeldt, D. (2000). From Cyberspace to the Noosphere:Emergence of the Global Mind. *New Perspectives Quarterly, 17*(1), 18-25.

Arquilla, J., & Ronfeldt, D. (2001). *Networks and Netwars: The Future of Terror, Crime, and Militancy* (1st ed.). Santa Monica, CA: US National Defence Research Institute, RAND Corporation.

Arquillia, J. (2008). *Worst Enemy: The Reluctant Transformation of the American Military.* Chicago, IL: Ivan R. Dee, Publisher.

Ashenden, D. (2005). Governance Principles for Sharing Information in the Network Enabled Capability (NEC) Environment. *4th European Conference on Information Warfare and Security, University of Glamorgan, UK, 11-12 July 2005* (pp. 1-8). Academic Conferences Limited, Reading, UK.

Attina, F. (2008). Multilateral Security Trends. An Analysis of 124 UN, NATO, OSCE, and EUâ€™s Peacekeeping Operations. *ISA's 49th Annual Covention, Bridging Multiple Divides.* San Francisco, CA: ISA.

Avizienis, A., Laprie, J., Randell, B., & Landwhehr, C. (2004, Jan-March). Basic Concepts and Taxonomy of Dependable and Secure Computing. *IEEE Transactions on Dependable and Secure Computing, 1*(1), 11-33.

Avizienis, A., Laprie, J.-C., Randell, B., & Landwehr, C. (2004, JANUARY-MARCH). Basic Concepts and Taxonomy of Dependable and Secure Computing. *IEEE Transactions on Dependable and Secure Computing, 1*(1).

Axelrod, R. M. (1997). *The complexity of cooperation: agent-based models of competition and collabration.* Princeton, NJ: Princeton University Press.

Baber, C., Stanton, N., Houghton, R., & Cassia, M. (2008). Hierarchical Command, Communities of Practice, Networks of Exploration: using simple models to explore NEC Command Structures. *Realising Network Enabled Capability (RNEC'08), NECTICE, Leeds, UK, 13-14 October 2008.* NECTISE.

Baggott, J. (2004). *Beyond Measure: Modern Physics, Philosophy and the Meaning of Quantum Theory.* Oxford: Oxford University Press.

Bagnell, R. J. (2006). Cyber Situational Awareness: The Integration and Role of Visualization in Information Assurance Operations. *Proceedings 11th ICCRTS: Coalition Command and Control in the Network Era, Cambridge, UK, 26-28 September, 2006.* DOD CCRP.

Bailey, M. (2010). "From the Core to the Edge - Information on Demand. *The 4th Annual Unified Cross Domain Management Office (UCDMO) Conference* (p. 1). Boston, MA: Unified Cross Domain Management Office (UCDMO).

Baker, S., Waterman, S., & Ivanov, G. (2009). *In the Crossfire: A global report on the threats facing key industries.* McAfee, Inc.

Barbatsis, G., & Fegan, M. (1999, September). The Performance of Cyberspace: An Exploration Into Computer-Mediated Reality. (M. McLaughlin, & S. Rafaeli, Eds.) *Journal of Computer-Mediated Communications (JCMC), 5*(1).

Barman, S. (2002). *Writing Information Security Policies.* New Riders Publishing.

Bartkiewicz, D., & Hannes, M. (2011). Emerging Cyber Risks: Better Visibility for the Cloud Forecast. (V. Vasquez, Ed.) *Cloudbook: The Cloud Computing & SaaS Information Resource, 2*(1).

Baskerville, R. (1993). Information systems security design methods: implications for information systems development." 25(4): 375-414. *ACM Computing Surveys, 25*(4), 374-414.

Bass, B. (1990, Winter). From transactional to transformational leadership: learning to share the vision. *Organizational Dynamics, 18*(3), 19-31.

Batschelet, A. W. (2007). *Effects-based operations: A New Operational Model?* Carlisle, PA: USAWC Strategy Research Project.

Baumeister, R. F., & Leary, M. R. (1995, May). The need to belong: desire for interpersonal attachments as a fundamental human motivation. *Psychol Bull, 117*(3), pp. 497-529.

Baumeister, R. F., & Leary, M. R. (1995). The need to belong: Desire for interpersonal attachments as a fundamental human motivation. *Psychological Bulletin, 117*, pp. 497- 529.

Bauwens, M. (2005, March 1). *P2P and Human Evolution: Peer to peer as the premise of a new mode of civilization.* Retrieved October 12, 2010, from Foundation for P2P Alternative: http://www.networkcultures.org/weblog/archives/P2P_essay.pdf

Bayles, W. J. (2001, Spring). The Ethics of Computer Network Attack. *Parameters*, 44-58.

Beard, J. (2009). Law and War in the Virtual Era. *American Journal of International Law*, 409-445.

Bell, D. E. (2005). Looking Back at the Bell-La Padula Model. *Proceedings of the 21st Annual Computer Security Applications Conference. Tucson, Arizona, USA*, (pp. 337–351). Reston VA.

Bell, D. E. (2006, November 27). *Looking Back: Addendum.* Retrieved October 11, 2010, from Selfless-Security.offthisweek.com: http://selfless-security.offthisweek.com/presentations/Bell_LBA.pdf

Bell, D. E., & LaPadula, L. J. (1973). *Secure Computer Systems: Mathematical Foundations.* MITRE Corporation.

Bellamy, M., & Gallagher, G. (2011). *Data Centre Strategy G-Cloud & Government Application Store Programme.* The Cabinet Office. London: HMSO.

Benedict, K. (2011, August 24). *Enterprise Mobility, Netcentric Operations and Military Mobility*. Retrieved September 11, 2011, from Mobile Enterprise Strategies: http://mobileenterprisestrategies.blogspot.co.uk/2011/08/enterprise-mobility-netcentric.html

Berenger, R. D. (2006). Introduction: War in cyberspace. (S. C. Herring, Ed.) *Journal of Computer-Mediated Communication, 12*(1), article 9.

Berg, C. (2006). *High-Assurance design: Architecting Secure and Reliable Enterprise Applications.* Addison-Wesley, Pearson Education, Inc.

Berger, A., Brown, C., Kousky, C., & Zeckhauser, R. (2009). The Five Neglects:Risks Gone Amiss. In H. Kunreuther, & M. Useem (Eds.), *Mitigating and Recovering from Natural and Unnatural Disasters.* Philadelphia, PA: Wharton School Publishing.

Berners-Lee, T., & Fischetti, M. (1999). *Weaving the Web: The Original and Ultimate Destiny of the World Wide Web* (1st ed.). London: HarperBusiness.

Bethea, J. R. (2003). *Joint C4I Interoperability – A look at the procees for Army Transformation.* Carlisle Barracks, PA: U.S. Army War College.

Bettini, C., Brdiczka, O., Henricksen, K., Indulska, J., Nicklas, D., Ranganathan, A., et al. (2010, April). A survey of context modelling and reasoning techniques. *Pervasive Mob. Comput., 6*(2), 161--180.

Beznosov, K., & Kruchten, P. (2004). Towards agile security assurance. *Proceedings of the 2004 workshop on New Security Paradigms* (pp. 47-54). Nova Scotia, Canada: Association for Computing Machinery (ACM).

Bhagyavati, Agyei-Mensah, S. O., Shumba, R., & Kearse, I. B. (2005). Teaching hands-on computer and information systems security despite limited resources. *Proceedings of the 36th SIGCSE Technical Symposium on Computer Science Education, SIGCSE 2005, St. Louis, Missouri, USA, 23-27 February, 2005. 37*, pp. 325-326. ACM.

Bieniek, M. (2011). NATO's new Strategic Concept and the Military Transformation of the Alliance. *2011 Ottawa Conference on Defence and Security.* Ottawa, Canada: NATO Deputy Supreme Allied Commander Transformation (DSACT).

Bimrah, K. K., Mouratidis, H., & Preston, D. (2008). iTrust: A Trust-aware Ontologyfor Information Systems Development. *Advances in Computing and Technology, The School of Computing and Technology 3rd Annual Conference, 2008* (pp. 40-51). London: ICGES.

BIS. (2009). *Digital Britain, Building Britain's Future.* London: Department for Business, Innovation and Skills.

Bishop, M. (2002). *Computer Security: Art and Science.* Addison Wesley Professional, Pearson Education, Inc.

Bishop, M. (2005). *Introduction to Computer Security.* Addison Wesley, Pearson Education, Inc.

Bishop, M., Engle, S., Peiser, S., Whalen, S., & Gates, C. (2008). We have met the enemy and he is us. *Proceedings New Security Paradigms Workshop (NSPW) appear, Lake Tahoe, CA, 22-25 September 2008* (pp. 1-12). Association for Computing Machinery (ACM).

Bloomfield, R., Buzna, L., Popov, P., Salako, K., & Wright, D. (2010). Stochastic modelling of the effects of interdependencies between critical infrastructure. In E. Rome, & R. Bloomfield (Ed.), *Proceedings of the 4th international conference on Critical information infrastructures security* (pp. 201-212). Bonn, Germany: Springer-Verlag.

Blyth, A. J. (2001). Information Assurance in the Age of Information Warfare. In Vanguard (Ed.), *15th Annual Vanguard Enterprise Security Conference, Reno, NV, USA. 3-8 June 2001.*

Blyth, A. J. (2010). *Cyber Defence – The Technical Challenge.* Cyber & Influence S & T Centre. Defence Science and Technology Laboratory.

Blyth, A. J., & Beynon-Davies, P. (2000). IS Failure, Trust and Electronic Commerce. *Proceedings 5th Annual Conference of the UK Academy for Information Systems (UKAIS), Cardiff, UK, 26-28 April 2000.* McGraw Hill.

Blyth, A. J., & Kovacich, G. (2001). *Information Assurance: Surviving in the Information Environment.* Springer.

Bobbitt, M. (2000, July). (Un)Bridging the Gap. *InfoSecurity*, pp. 35-37.

Borg, S. (2005, Nov.-Dec). Economically Complex Cyberattacks. *IEEE Security and Privacy, 3*(6), 64-67.

Borg, S. (2005, November). Economically Complex Cyberattacks. (O. S. Saydjari, Ed.) *IEEE Security & Privacy, 3*(6), 64-67.

Borland, R. (2008). *Information Assurance: The coordinated approach to improving Enterprise Data Quality.* Swindon, UK: Nationwide Building Society.

Bourgine, P., Johnson, J., Leskovec, J., & Lambiotte, R. (2008). *Internet Emergent Properties:Cascade of Information in Networks.* Working Group - WG6, Imperial College, London.

Boyce, J. G., & Jennings, D. W. (2002). *Information assurance: managing organizational IT security risks.* Woburn, MA: Butterworth-Hienemann.

Boyd, C. D. (2007, May-June). Army IO is PSYOP: Influencing more with less. *Military Review, 87*(3), pp. 67–75.

Boyd, C. G. (1999). *New World Coming: American Security in the 21st Century.* Washington, DC: The United States Commission on National Security - 21st Century.

Bracken, P. (2007). Financial Warfare. *Orbis - FPRI, 51*(4), 685-696.

Bradley, R. V., Pridmore, J. L., & Byrd, T. A. (2006). Information systems success in the context of different corporate cultural types: an empirical investigation. *Journal of Management Information Systems, 23*(2), 267-294.

Brass, D. J., Galaskiewicz, J., & Greve, H. R. (2004). Taking stock of networks and organizations: A multilevel perspective. *The Academy of Management Journal, 47*(6), 795 - 817.

Braun, N., & Hooper, V. (2009). Cybersecurity Knowledge and Safeguard Implementation: An Exploratory Study. In G. Dhillon (Ed.), *Proceedings of the 8th Annual Security Conference Discourses in Security Assurance & Privacy, Las Vegas, NV, USA. 15-16 April, 2009.* Virginia Commonwealth University.

Brian, A. P. (2006). Teaching students to hack: ethical implications in teaching students to hack at the university level. . *Proceedings of the 3rd Annual Conference on Information Security Curriculum Development (InfoSecCD). Kennesaw, Georgia, USA, 22-23 September 2006* (pp. 197 - 200). ACM.

Broad, R. (2009, November 2). Viewing information as a strategic asset. *Guardian Professional*. London, UK: The Guardian.

Brown, J. S., & Duguid, P. (2002). *The social life of information.* Havard Business School Press.

Brown, L. D., Khagram, S., Moore, M. H., & Frumkin, P. (2000). *Globalization, NGOs and Multi-Sectoral Relations.* The Kennedy School of Government. Cambridge, MA: Harvard University.

Bryman, A. (2007). *Effective Leadership in Higher Education-Summary of Findings.* University of Leicester, School of Management. London: Leadership Foundation for Higher Education.

Buckman, T. (2005). *NATO Network Enabled Capability Feasibility Study Executive.* Brussels: NATO Consultation Command and Control Agency, Communications and Information Systems Division.

Buda, G., Choi, D., Graveman, R. F., & Kubic, C. (2001). Security standards for the global information grid. *Military Communications Conference, 2001. MILCOM 2001. Communications for Network-Centric Operations: Creating the Information Force. 1*, pp. 617 - 621. Linthicum, MD : IEEE.

Burgoon, J. K., George, J. F., Adkins, M., Kruse, J., Biros, D., & Nunamaker, J. F. (2007). Detecting Deception in the Military Infosphere. In C. Wang, S. King, R. Watchter, R. Herklotz, & C. Arney, *Information Security Research: New Methods for Protecting Against Cyber Theats* (pp. 606-627). Indianapolis, Indiana: Wiley Publishing, Inc.

Burns, J. S. (2002, September). Chaos theory and leadership studies: exploring uncharted seas. *Journal of Leadership & Organisational Studies, 9*(2), 42-56.

Burris, R. (2010). *Future Operating Concept- Joint Computer Network Operations.* Maxwell AFB, AL: USAF Air War College.

Busuttil, T. B., & Warren, M. J. (2005). An Approach for Critical Information Infrastructure Protection. *4th European Conference on Information Warfare and Security, University of Glamorgan, UK, 11-12 July 2005* (pp. 53-62). Academic Conferences Limited, Reading, UK.

Bynum, T. W. (2004). Ethics and the Information Revolution. In R. A. Spinello, & H. T. Tavani (Eds.), *Readings in cyberethics* (pp. 13-29). Sudbury, MA: Jones & Bartlett Learning.

Cabanas, K. A., & Huizenga, T. (2005). *Organizing SOCOM for Cross Functional and Geographic Area Operations in the Global War on Terrorism.* Naval War College, Department of the Joint Military Operations. Newport, R.I.: Department of Defense.

Cabinet Office. (2005). *Transformational Government – Enabled by Technology.* London: HMSO.

Cabinet Office. (2007). *A National Information Assurance Strategy.* London: HMSO.

Cabinet Office. (2009). *Public Sector Network Outline Business Case, Version 2.8.* London: HMSO.

Cabinet Office. (2009a). *Cyber Security Strategy 2009.* London: HMSO.

Cabinet Office. (2009b). *National Security Strategy 2009.* London: HMSO.

Cabinet Office. (2010). *A Strong Britain in an Age of Uncertainty: The National Security Strategy.* London: HMSO.

Cabinet Office. (2010). *Data Centre Migration, G-Cloud and Applications Store Programme, Phase 2: Technical Architecture Workstrand Report, Version 1.5.* London: HMSO.

Cabinet Office. (2010). *Greening Government ICT.* London: HMSO.

Cabinet Office. (2010). *HMG IA Maturity Model and Assessment Framework, Version 4.* London: HMSO.

Cabinet Office. (2010). *Operational Efficiency Programme Benchmarking Report for April 2009 to May 2010 .* London: HMSO.

Cabinet Office. (2010). *Strategy for the High Level Design, Version 2.5.* Cabinet Office, Commercial Strategy Team. London: HMSO.

Cabinet Office. (2010b). *HMG Security Policy Framework.* London: HMSO.

Cabinet Office. (2011). *HMG Security Policy Framework: Making Government Work Better.* Cabinet Office. London: HMSO.

Cabinet Office. (2011). *PSN Service Assurance.* London: HMSO.

Cabinet Office. (2011a). *THe UK Cyber Security Strategy: Protecting and promoting the UK in a digital world .* London: The National Archives.

Calder, A. (2005). *The Case for ISO 27001.* Ely, UK: IT Governance Publishing.

Calder, A., & Watkins, S. (2006). *IT Governance: A Manager's Guide to Data Security and BS 7799/ ISO 17799* (3rd ed.). Kogan Page.

Calder, A., & Watkins, S. (2007). *Information Security Risk Management for ISO27001/ ISO 17799.* Ely, UK: IT Governance Publishing.

Campen, A. D. (1992). *The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War.* AFCEA International Press.

Campen, A. D., & Dearth, D. H. (2000). *Cyberwar 2.0: Myths, Mysteries & Reality.* AFCEA International Press.

Campen, A. D., & Dearth, D. H. (2000). *Cyberwar 3.0; Human Factors in information Operations and Future Conflict.* AFCEA International Press.

Campen, A. D., Dearth, D. H., & Goodden, R. T. (1996). *Cyberwar: Security, Strategy, and Conflict in the Information Age.* AFCEA International Press.

Candolin, C. (2005). Securing the Infrastructure in Information Operations. *4th European Conference on Information Warfare and Security,University of Glamorgan, UK, 11-12 July 2005* (pp. 63-72). Academic Conferences Limited, Reading, UK.

Carafano, J. (2005). *The Future of Anti-Terrorism Technologies.* Institute for International Studies. The Heritage Foundation.

Caralli, R. (2004). *Managing for Enterprise Security.* Software Engineering Institute. Pittsburgh, PA: Carnegie Mellon University.

Caralli, R. (2006). *Sustaining Operational Resiliency: A Process Improvement Approach to Security Management.* Software Engineering Institute, Networked Systems Survivability Program. Pittsburgh, PA: Carnegie Mellon University.

Carley, K. M., & Prietula, M. J. (Eds.). (1994). *Computational Organization Theory.* Lawrence Erlbaum Associates, Publishers.

Carmouche, J. (2006). *IPsec Virtual Private Network Fundamentals.* CISCO systems, CISCO Press.

Carr, J. (2005). *Inside Cyber Warfare: Mapping the Cyber Underworld* (1st ed.). (M. Loukides, Ed.) Sebastopol, California, USA: O'Reilly Media.

Cartlidge, A., Hanna, A., Rudd, C., Macfarlane, I., Windebank, J., & Rance, S. (2007). *An Introductory Overview of ITIL® V3.* London: itSMF Ltd.

Carvey, H. (2005). *Windows Forensics and Incident Recovery.* Addison-Wesley, Person Education, Inc.

Cash, D. W., Adger, W. N., Berkes, F., Garden, P., Lebel, L., Olsson, P., et al. (2004). Scale and cross-scale dynamics: governance and information in a multi-level world. *Millennium Ecosystem Assessment Bridging Scales and Epistemologies Conference, Alexandria Egypt,17-20 March, 2004.*

Casola, V., Coppolino, L., & Rak, M. (2006). An Architectural Model for Trusted Domains in Web Services. (A. Abraham, & M. Sambandham, Eds.) *Journal of Information Assurance and Security, 1*(2), 107-118.

Castells, M. (2009). *Communication Power.* Oxford: Oxford University Press.

Castonguay, F. (2011). The Cyber Environment:A Canadian Forces Perspective. *C4ISR Symposium: Optimized Total Ownership Cost – "Affordable & Sustainable Information Dominance",San Diego, CA, 1-3 May 2012.* AFCEA.

Caswell, B., Beale, J., Foster, J., & Faircloth, J. (2003). *Snort 2.0: Intrusion Detection.* Rockland, MA: Syngress.

Cebrowski, A. K., & Garstka, J. J. (1998, January). *Network-Centric Warfare: Its Origin and Future*. Retrieved March 15, 2011, from www.kinection.com: http://www.kinection.com/ncoic/ncw_origin_future.pdf

Cebrowski, A., & Gartska, J. (1998). Network-Centric Warfare: Its Origin and Future. *US Naval Institute Proceedings, January 1998.* Annapolis, MD 21402: US Naval Institute.

Cerf, V. (2007). Emerging Cyber Security Threats and Countermeasures. *Georgia Tech Information Security Center.* GTISC.

CERT Coordination Center . (2003b). *Responding to Intrusions.* Pittsburgh, PA: Carnegie Mellon University.

CERT Coordination Center. (2003a). *Identify Data That Characterize Systems and Aid in Detecting Signs of Suspicious Behaviour.* Pittsburgh, PA: Carnegie Mellon University.

CERT Coordination Center. (2008). *The "Big Picture" of Insider IT Sabotage Across U.S. Critical Infrastructures.* Pittsburgh, PA: Carnegie Mellon University.

CESG. (2001). *HMG Infosec Standard Number 3: Connecting Business Domains.* GCHQ, CESG - The National Technical Authority for Information Assurance. Cheltenham: HMSO (Restricted).

CESG. (2002). *HMG Public Key Infrastructure - Overview.* GCHQ, CESG - The National Technical Authority for Information Assurance. Cheltenham: CESG Information Assurance (IA) Bookstore, 8.1 Ed., (Restricted).

CESG. (2003). *A UK Government Strategy for Information Assurance.* GCHQ, CESG - The National Technical Authority for Information Assurance. Cheltenham: CESG Information Assurance (IA) Bookstore, 8.1 Ed., (Restricted).

CESG. (2004). *Governance Framework for the GSi, Version 1.0.* GCHQ, CESG - The National Technical Authority for Information Assurance. Cheltenham: CESG Information Assurance (IA) Bookstore, 8.1 Ed., (Restricted).

CESG. (2005). *HMG Infosec Standard Number 2: Risk management and accreditation of information systems.* GCHQ, CESG - The National Technical Authority for Information Assurance. Cheltenham: HMSO (Restricted).

CESG. (2006a). *CESG Infosec Memoranda 2:The Risk of Electronic Attack Against HMG Computers and Communications: General Factors.* GCHQ, CESG

- The National Technical Authority for Information Assurance. Cheltenham: CESG Information Assurance (IA) Bookstore, 8.1 Ed., (Restricted).

CESG. (2006b). *CESG Infosec Memoranda 12 - Dealing with Malicious Software.* GCHQ, CESG - The National Technical Authority for Information Assurance. Cheltenham: CESG Information Assurance (IA) Bookstore, 8.1 Ed., (Restricted).

CESG. (2006c). *CESG Infosec Memoranda 28 - Performance and Assurance Standards for Biometric Systems Contributing to Multi-Element Identification and Authentication.* GCHQ, CESG - The National Technical Authority for Information Assurance. Cheltenham: CESG Information Assurance (IA) Bookstore, 8.1 Ed., (Restricted).

CESG. (2006d). *CESG Infosec Memoranda 37 - Intrusion Detection on Managed IT Systems.* GCHQ, CESG - The National Technical Authority for Information Assurance. Cheltenham: CESG Information Assurance (IA) Bookstore, 8.1 Ed., (Restricted).

CESG. (2006e). *CESG Infosec Manual M - Protecting Government Connections to the Internet - Guidance on Internet Connectivity Architectures.* GCHQ, CESG - The National Technical Authority for Information Assurance. Cheltenham: CESG Information Assurance (IA) Bookstore, 8.1 Ed., (Restricted).

CESG. (2006f). *CESG Infosec Manual N - Vulnerabilities of the TCP/IP Protocol Suite.* GCHQ, CESG - The National Technical Authority for Information Assurance. Cheltenham: CESG Information Assurance (IA) Bookstore, 8.1 Ed., (Restricted).

CESG. (2006g). *CESG Infosec Manual P - Protecting Government Connections to the Internet - Firewall Installation, Configuration and Maintenance.* GCHQ, CESG - The National Technical Authority for Information Assurance. Cheltenham: CESG Information Assurance (IA) Bookstore, 8.1 Ed., (Restricted).

CESG. (2006h). *CESG Infosec Manual T - Transport Layer Protocol - Implementation Recommendations for HMG Protectively Marked Material.* GCHQ, CESG - The National Technical Authority for Information Assurance. Cheltenham: CESG Information Assurance (IA) Bookstore, 8.1 Ed., (Restricted).

CESG. (2006j). *CESG Infosec Manual V - Use of IPSec in Government Systems - Implementation Standards.* GCHQ, CESG - The National Technical Authority for Information Assurance. Cheltenham: CESG Information Assurance (IA) Bookstore, 8.1 Ed., (Restricted).

CESG. (2006k). *CESG Infosec Manual W - Secure Information Sharing - Security Guidance for One-way Diode Technologies.* GCHQ, CESG - The National Technical Authority for Information Assurance. Cheltenham: CESG Information Assurance (IA) Bookstore, 8.1 Ed., (Restricted).

CESG. (2006l). *CESG Infosec Manual Z - Use of Tokens for Identification and Authentication in Government Systems .* GCHQ, CESG - The National Technical Authority for Information Assurance. Cheltenham: CESG Information Assurance (IA) Bookstore, 8.1 Ed., (Restricted).

CESG. (2007). *HMG Infosec Standard No 4: Communications Security & Cryptography.* GCHQ, CESG - The National Technical Authority for Information Assurance. Cheltenham: HMSO (Restricted).

CESG. (2009). *HMG IA Standard No.1 (v3.5): Business Impact Level Tables.* London: Cabinet Office / CESG.

CESG. (2010). *HMG Information Assurance Standard No 2: Risk Management and Accreditation of Information Systems, Issue 3.2.* CESG. London: HMSO.

Chang, S. E., & Lin, C.-S. (2007). Exploring organizational culture for information security management. *Industrial Management & Data System, 107*(3), 438 - 458.

Checkland, P. (1981). *Systems Thinking, Systems Practice.* London: Wiley.

Chen, D., Doumeingts, G., & Vernadat, F. (2008, September). Architectures for enterprise integration and interoperability: Past, present and future. *Computers in Industry, 59*(7), 647–659.

Chen, H., & Xu, J. (2006). Intelligence and Security Informatics. *Annual Review of Information Science and Technology, 40*(1), 229-289.

Chen, T. (2009). A Comprehensive Review of Wireless Security. *Security, AssurancProceedings of the 8th Annual Security Conference Discourses in Security Assurance & Privacy Las Vegas, NV, USA 15-16 April, 2009*, *34*, pp. 1-14.

Chesebrough, D. (2006, February 7). Networks and Netcentricity. *The Net-Centric Dialog* .

Choo, C. W. (2002). *Information Management for the Intelligent Organization* (3rd ed.). Medford, NJ: American Society for Information Science and Technology.

Chopra, K., & Wallace, W. (2003). Trust in Electronic Environments. *Proceedings of the 36th Hawaii Conference on System Sciences (HICSS'03), Hawaii, 6-9 January, 2003 . 9*, p. 331.1. Hilton Waikoloa Village: IEEE Computer Society.

Chun, C. K. (2010). John Warden's Five Ring Model and the Indirect Approach to War and Strategy. In J. B. Bartholomees Jr. (Ed.), *U.S. Army War College Guide to National Security Issues, Vol I: Theory of War and* (pp. 311-322). Carlisle, PA: Strategic Studies Institute (SSI) publications.

CISCO. (2012). *Understanding Operational Security*. Retrieved June 10, 2012, from CISCO Security: http://www.cisco.com/web/about/security/intelligence/opsecurity.html

CJCSI. (2011). *CJCSI6510.01F: Information Assurance (IA) and support to Computer Network Defense (CND).* DoD. Washington, DC: Chairman of the Joint Chiefs of Staff.

Claessen, E. (2007, May-June). Discouraging hearts and minds: Democracies and insurgencies. *Military Review, 87*(3), pp. 97–103.

Clarke, R. A., & Knake, R. K. (2010). *Cyber War: The Next Threat to National Security and What to Do About It.* New York, NY, US: ECCO Press, Harper Collins.

Clevenger, G. (2006). Incorporating certification and accreditation coursework into network security curriculum. *Proceedings of the 3rd annual conference on Information security curriculum development. Kennesaw, Georgia, 22-23 September, 2006* (pp. 41-43). ACM.

Clowney, P. (2009, May). Clausewitz and Network Centric Warfare: A Beautiful Marriage. (N. Sage, Ed.) *High Frontier: The Journal for Space & Missile Professionals, 5*(3), 38-41.

Coen, M., & Cullen, D. (2007). *A Framework for Information Systems Management and Governance.* Glasgow: University of Strathclyde.

Cole, B. E. (2009). *Guiding Principles for Stablisation and Reconstruction.* Washington, DC: US Institute of Peace.

Cole, D. R. (2005, January 3). Learning Through the Virtual. (A. Kroker, & M. Kroker, Eds.) *CTheory*, a151.

Collins, B., & Mansell, R. (2003). *Cyber Trust and Crime Prevention:A Synthesis of the State-of-the-Art Science Reviews.* Office of Science and Technology, Department for Business, Innovation and Skills. London: HMSO.

Colwill, C. (2010). *Human factors in information security: The insider threat e Who can you trust these days?* Britsh Telecom, BT Security. London: Elsevier.

Committee of Public Accounts. (2011). *The use of information to manage the defence logistics supply chain .* House of Commons Committee of Public Accounts. London: The Stationery Office Limited.

Committee on National Security Systems. (2010). *National Information Assurance (IA) Glossary.* Washington, D.C.: Committee on National Security Systems.

Connell, J., Lynch, C., & Waring, P. (2000). *Comparing Research Methods: Three Ways of Undertaking Qualitative.* Newcastle: University of Newcastle.

Cook, J. M. (1986). Increasing students security awareness: article II. What C.S. graduates don`t learn about security concepts and ethical standards. In J. C. Little, & L. N. Cassel (Ed.), *Proceedings of the 17st SIGCSE Technical Symposium on Computer Science Education, 1986, Cincinnati, Ohio, USA, February 6-7, 1986* (pp. 89-96). ACM.

Cook, P. (2006, September 13). *Making knowledge management work by learning to share knowledge, skills and experience*. Retrieved May 10, 2010, from I Heard it through the Grapevine: http://www.cul.co.uk/creative/grapevine.htm

Cornish, P., Livingstone, D., Clemente, D., & Yorke, C. (2011). *Cyber Security and the UK's Critical National Infrastructure.* The Royal Institute of International Affairs. London: Chatham House.

Corrin, A. (2011, January 20). DOD tackles information security in the cloud. (B. Rosenberg, Ed.) *Defence Systems*.

Corum, J. S. (2009). Future Battlespace and the US Response. *Baltic Security & Defence Review, 11*(2), 21-39.

Council of the EU. (2010, April). *Council of the European Union*. Retrieved Jul 4, 2011, from Consilium: http://www.consilium.europa.eu/policies/information-assurance?lang=en

Court, G. (2007). Validating the NEC Benefits Chain. *Proceedings of the 12th ICCRTS "Adapting C2 to the 21st Century" Newport, RI, 19-21 June, 2007.* CCRP.

Cover, T. M., & Thomas, J. A. (2006). *"Elements of Information Theory* (2nd ed.). John Wiley & Sons.

Cover, T. M., & Thomas, J. A. (2006a). *Elements of Information Theory* (2nd ed.). Wiley.

Covey, S. M., Covey , S. R., & Merrill, R. R. (2008). *The Speed of Trust: The One Thing That Changes Everything.* New York: Free Press Paperbacks.

Coyle, D. (1999). *The weightless world: strategies for managing the digital economy.* Cambridge, MA: The MIT Press.

Cranston, P., & Davies, T. (2009, January). Global Social Networking. *Future Connect*.

Crocker, M. (2007). Cross-Domain Information Sharing in a Tactical Environment. *CrossTalk - The Journal of Defence Software Engineering*, 26-29.

Cronin, B. (2005). Intelligence, terrorism, and national security. *Annual Review of Information Science and Technology, 39*(1), 395-432.

Crosston, M. D. (2011, Spring). World Gone Cyber MAD: How "Mutually Assured Debilitation" is the Best Hope for Cyber Deterrence. *Strategic Studies Quarterly, 5*(1), 100-116.

CSI. (2007). *CSI Computer Crime and Security Survey.* New York, NY: Computer Security Institute.

CSI. (2011). *CSI Computer Crime and Security Survey.* New York, NY: Computer Security Institute.

CSIS. (2008). *Securing Cyberspace for the 44th Presidency.* Center for Strategic and International Studies. Washington, DC: CSIS.

CSIS. (2011). *Cybersecurity Two Years Later.* Center for Strategic and International Studies. Washington, DC: CSIS.

Cummins, F. A. (2009). *Building the Agile Enterprise: with SOA, BPM and MBM.* Morgan Kaufmann Publishers and the Object Management Group.

Cyber Smart. (2009, March). *Guide to online safety*. Retrieved November 10, 2011, from Commonwealth of Australia: http://www.cybersmart.gov.au/Parents/Resources%20to%20use%20with%20your%20child/Resources%20for%20use%20with%20teenagers.aspx

Dalal, P. (2006). *Cybercrime and cyberterrorism: Preventive defense for cyberspace violations.* Zaporizhzhya, Ukraine: Computer Crime Research Center.

Darley, W. (2007). The missing component of U.S. strategic communications. *Joint Force Quarterly*, pp. 109–113.

Davì, M. (2010). *Cyber security: European strategies and prospects for global cooperation.* European Security and Defence Forum. London: Chatham House.

David, M. W., & Sakurai, K. (2003). Combating Cyber Terrorism: Countering Cyber Terrorist Advantages of Surprise and Anonymity. *Proceedings of the 17th International Conference on Advanced Information Networking and Applications* (pp. 716-). IEEE Computer Society.

Davis, P. (2001). *Effects-Based Operations: A Grand Challenge for the Analytical Community.* Project AIR FORCE, US National Defence Research Institute, RAND.

Dawes, S. S., Cresswell, A. M., & Pardo, T. A. (2009). From ''Need to Know'' to ''Need to Share'': Tangled Problems, Information Boundaries, and the Building of Public Sector Knowledge Networks. *Public Administration Review, 69*(3), 392-402.

Day, W.-W. (2004). *Trust in Cyberspace.* National Chung-Cheng University, Department of Communications. Minhsiung Township, Taiwan: National Chung-Cheng University.

DCDC. (2010). *The Future Character of Conflict.* London: Development Concepts and Doctrine Centre, Ministry of Defence.

De Capite, D. (2005). *Self-defending Networks: The Next Generation of Network Security.* CISCO Press.

Dearth, D. (2002). Shaping the Information Space. *Journal of Information Warfare, 1*(3).

DeLone, W. H., & McLean, E. R. (2004, Fall). Measuring e-Commerce Success: Applying the DeLone & McLean Information Systems Success Model. *International Journal of Electronic Commerce, 9*(1), 31 - 47.

Denize, S., & Young, L. (2007). Concerning trust and information. *Industrial Marketing Management, 36*, .968-982.

Denning, D. (1998). *Information Warfare and Security.* Addison-Wesley Professional; ACM Press.

Denning, D. E. (1976, May). A lattice model of secure information flow. (R. L. Ashenhurst, Ed.) *Communications of the ACM, 19*(5), pp. 236 - 243.

Desman, M. (2002). *Building an Information Security Awareness Program.* Auerbach Publications, Taylor & Francis Group, Informa plc.

DeWitt, J., & Cicalese, C. D. (2006). Contextual integration: a framework for presenting social, legal, and ethical content across the computer security and information assurance curriculum. *Proceedings of the 3rd annual conference on Information Security Curriculum Development (InfoSecCD), Kennesaw, Georgia, 22-23 September, 2006* (pp. 30-40). ACM.

DoD. (2000). *Joint Vision 2020.* Washington D.C.: Department of Defense.

DoD. (2001). *Network Centric Warfare.* Department of Defense (DoD), Networks and Information Integration (NII). Washington D.C.: US Department of Defense.

DoD. (2003). *Information Operations Roadmap.* Washington D.C.: Department of Defense.

DoD. (2005). *Net-Centric Environment Joint Functional Concept.* Washington D.C.: Department of Defence.

DoD. (2006). *Stability Operations: Military Support to Security, Transition, and Reconstruction Joint Operating Concept 2004.* Fort Belvoir, VA: Department Technical Information Center.

DoD. (2006a). *JP 3-13-3: Operations Security.* Chairman of the Joint Chiefs of Staff. Washington D.C.: Department of Defence.

DoD. (2010). *JP1 - Doctrine for the Armed Forces of the United States.* Washington, D.C.: DoD.

DoD. (2010). *UAS Control Segment (UCS) Architecture*. Retrieved April 21, 2011, from UCSArchitecture.org: http://www.ucsarchitecture.org/page/technical_information#architecture

DoD. (2011). *DoD Strategy for Operating in Cyberspace.* Washington, D.C.: Department of Defense.

DoD CIO. (2006). *Information Assurance Component of the GIG Integrated Architecture.* Chief Information Office. Washington D.C.: Department of Defense.

DoD CIO. (2007). *Global Information Grid Architectural Vision: Vision for a Net-Centric, Service-Oriented DoD Enterprise.* Department of Defense, Chief Information Office. Washington D.C.: Department of Defense.

DoD JP 3-13. (2006). Information Operations. *Joint Publication 3-13*.

DoD JP 3-24. (2009). Counterinsurgency Operations. *joint Publications 3-24*.

Donahue, G. (2007). *Network Warrior.* O'Reilly.

Donlon, J. J. (2002). *A Computer Model for determining Operational Centers of Gravity.* Fort Leavenworth, KA: US Army Command and General Staff College.

Dooley, K., & Johnson, L. (1995). TQM, Chaos, and Complexity. *Human Systems Management, 14*(4), 1-16.

Dorion, E., & Boury-Brisset, A.-C. (2005). *Information Engineering in Support of Multilateral Joint Operational Interoperability.* Defence Research and Development Center. Valcartier, Canada: DTIC.

Drahos, P., & Braithwaite, J. (2002). *Information Feudalism: Who Owns the Knowledge Economy?* Earthscan Publications.

Dreyfus, H. L. (2008). *On the internet.* New York, NY: Routledge.

Drucker, P. (1998, August 24). The Next Information Revolution. *Forbes*, 46-58.

DSTL. (1997). *Historical Analysis in Support of C3 systems for the JRDF: Based on historical analysis of 79 amphibious operations.* DSTL Farnborough. Farnborough: Defence Science and Technology Laboratory.

DSTL. (2004a). *High Level ICS/ISTAR Study 2003/04.* Defence Science and Technology Laboratory.

DSTL. (2004b). *A Network-centric operations case study, US/UK coalition combat operations during Operation Iraqi Freedom.* Defence Science and Technology Laboratory.

DSTL. (2005a). *Future Headquarters Requirement Study: Knowledge of Own Forces and Operational Tempo.* Defence Science and Technology Laboratory.

DSTL. (2005b). *Success Factors in CT/COIN Campaigns Working paper I: State and Security Forces' Success Factors.* Defence Science and Technology Laboratory.

DSTL. (2010). *Dual-Use Technology – "Working together Differently" Opportunities in Cyber & Influence.* Cyber & Influence S&T Centre. Defence Science and Technology Laboratory.

DSTL. (2011). *Complex, Dynamic Networks in Cyber & Influence.* Defence Science and Technology Laboratory .

Dull, D. (2006). *Implementing Network-Centric Operations in Joint Task Forces: Changes in Joint Doctrine.* Fort Leavenworth, KS: U.S. Army Command and General Staff College.

Dunlap, J. C. (2008). Towards a Cyberspace Legal Regime in the Twenty-First Century: Considerations for American Cyber-Warriors. *Air University 2008 Cyberspace Symposium*, (pp. 712-723). Maxwell AFB, AL.

Dunn, R., & Moore, S. (Eds.). (2011, February). I want us to be proud of job we do. *Desider*(33).

Dunn, T. N. (2011, October 18). *We'll strike first in cyber warfare*. Retrieved October 19, 2011, from thesun.co.uk: http://www.thesun.co.uk/sol/homepage/news/politics/3878324/Well-strike-first-in-cyber-warfare.html

Dunnigan, J. (2002). *The Next War Zone: Confronting the Global Threat of Cyberterrorism.* New York: Citadel Press Books, Kensington Publishing Corporation.

Edwards, C. (2007). *National Security for the Twenty-first Centry.* London: Demos.

Efthymiopoulos, M. P. (2005). Is NATO in Need of a Renewed Security Concept? *4th European Conference on Information Warfare and Security, University of Glamorgan, UK, 11-12 July 2005* (pp. 83-90). Academic Conferences Limited, Reading, UK.

Ekelhart, A., Fenz, S., Neubauer, T., & Weippl, E. (2007). Formal threat descriptions for enhancing governmental risk assessment. In T. Janowski, & T. A. Pardo (Ed.), *Proceedings of the 1st International Conference on Theory and Practice of Electronic Governance (ICEGOV, Macao, China, December 10-13, 2007. 232*, pp. 40-43. ACM International Conference Proceeding Series.

Ekman, P. (1999). Basic Emotions. In T. Dalgleish, & M. Power (Eds.), *Handbook of Cognition and Emotion* (pp. 45-60). Sussex, UK: John Wiley & Sons Ltd.

Eloff, J., & Eloff, M. (2005, November). Information security architecture. *Computer Fraud and Security*(11), 10-16.

Endsley, M. (1995). Toward a Theory of Situation Awareness in Dynamic Systems. *Human Factors , 37*(1), 32–64.

Endsley, M. (1998). Design and Evaluation for Situation Awareness Enhancement. *Proceedings of the Human Factors Society 32nd Annual Meeting, Santa Monica, CA, 5-9 October, 1998* , (pp. 97-101).

Endsley, M. (2000). Theoretical Underpinning of Situational Awareness- a Critical Review. *Situation Analysis and Awareness*.

Endsley, M. (2001). Designing for Situation Awareness in Complex Systems. *Proceedings of the Second international workshop on symbiosis of humans, artifacts, and environment, Kyoto Japan, 2001*, (pp. 1-13).

Engleman, E., & Strohm, C. (2012, January 31). *Cybersecurity Disaster Seen In U.S. Survey Citing Spending Gaps.* Retrieved Feb 4, 2012, from Bloomberg.com/news: http://www.bloomberg.com/news/2012-01-31/cybersecurity-disaster-seen-in-u-s-survey-citing-spending-gaps.html

Eovito, B. A. (2005). *The Impact of Synchronous Text Based Chat on Military Command and Control.* Fort Belvoir, VA: Defense Technical Information Center.

Estrin, D., Culler, D., Pister, K., & Sukhatme, G. (2002, Jan-Mar). Connecting the Physical World with Pervasive Networks. *IEEE Pervasive Computing, 1*(1), 59-69.

EU. (2002). *Creating a Safer Information Society by Improving the Security of Information Infrastructure and Combating Computer-related Crime.* Commission of the European Communities.

EU. (2005). *Creating a safer information society by improving the security of information infrastructures and combating computer-related crime [COM(2000) 890 final.* Commission of the European Communities.

EU. (2008). *Council of Europe - ETS No. 185 - Convention on Cybercrime.* Commission of the European Communities.

Europa. (2012, March 28). An EU Cybercrime Centre to fight online criminals and protect e-consumers. Brussels, Belgium.

European Commission. (2010). *Towards a future Internet: Interrelation between Technological, Social and Economic Trend.* DG Information Society and Media. Bussels: European Commission DG INFSO.

European Commission. (2012). *Special Eurobarometer 390 - Cyber Security.* Brussels: European Commission, Directorate-General Home Affairs.

Everett, C. (2009, June). Cloud computing – A question of trust. *Computer Fraud & security, 2009*(6), 5-7.

Exon, S. N. (2003). Personal Jurisdiction: Lost in Cyberspace? *Computer Law Review & Technology Journal, 21*(8).

Fan, T., Sun, Y., & Zhao, Y. (2009). An Eco-Defending Architecture for Network Security Based on Immuninty and Mobile Agents. *Proceedings of the Fifth International Conference on Information Assurance and Security, IAS 2009, Xi'An, China, 18-20 August, 2009* (pp. 451-454). IEEE Computer Society.

Farn, K.-J., Lin, S.-K., & Fung, A. R.-W. (2004, October). A study on information security management system evaluation--assets, threat and vulnerability. *Computer Standards & Interfaces, 26*(6), 501-513.

Farroha, B., Whitfield, M., & Farroha, D. (2009). Enabling net-centricity through cross domain information sharing. *3rd Annual IEEE Systems Conference* (pp. 116 - 121). Vancouver, BC: IEEE.

FEA. (2005). *Data Reference Model.* The White House. Washington D.C.: Federal Enterprise Architecture.

Feltovich, P. J., Bradshaw, J. M., & Bunch, L. (2009). *Policy and social barriers to new military information technologies.* Institute for Human and Machine Cognition. Pensacola, FL: Army Research Laboratory Advanced Decision Architectures Collaborative Technology Alliance.

Fenz, S., & Ekelhart, A. (2009). Formalizing Information Security Knowledge. *ACM Symposium on Information, Computer&Communication Security (ASIACCS 2009), Sydney, Australia; 10-12 March, 2009* (pp. 183 - 194). ACM.

Fink, D. (2003). The Law of Unintended Consequences: The 'Real' Cost of Top-Down Reform. *JOURNAL OF EDUCATIONAL CHANGE, 4*(2), 105-128.

Fisher, U. (2001, November). Information Age State Security: New Threats to Old Boundaries. *Journal of Homeland Security*.

Fitzgerald, J. (2008, February 6). Portfolio positioning to capitalise on new trends. *Money Management.*

Fletcher, B., & Hare, D. (2005). *Multi-National Information Sharing: Cross Domain Collaborative Information Environment (CDCIE) Solution.* United States Joint Forces Command Joint Futures Lab. Department of Defense CCRP.

Forsythe, S. L. (2007). An Multi-Level Model of Command and Control (C2). *Proceedings of the 12th ICCRTS "Adapting C2 to the 21st Century" Newport, RI, 19-21 June, 2007.* ommand and Control Research Program.

Fourie, G. (2002). The Evolution of the Information Security Mindset: A hypothesis of stages of Individual and Enterprise Security Maturation. *Security Modeling*, The SANS™ Institute.

Fowler, C. W. (2002). *Center of Gravity - Still relevant after all these years.* Carlisle Barracks, PA: U.S. Army War College.

Fowlie, G. (2010). *Cybersecurity.* New York: International Telecommunications Union Office, United Nations.

Fragkos, G., & Blyth, A. (2005a). Architecture for Near Real-Time Threat Assessment using IDS Data. *Proceedings 4th European Conference on Information Warfare and Security, University of Glamorgan.*

Fragkos, G., & Blyth, A. (2005b). *Security Threat Assessment across large network infrastructures, Safeguarding National Infrastructures: Integrated Approaches to Failure in Complex Networks.* University of Glasgow.

Frank, T. M., & Eisen, J. J. (1982, Winter). Balancing National Security and Free Speech. *Journal of International Law and Politics, 14*(2), 339-420.

Franklin, J. E. (2006). FORCEnet Science and Technology Needs with Potential Solutions. *OASD-NII International Command and Control Research and Technology Symposium, 26-28 September, 2006.* Arlington, VA: Raytheon.

Frigns, T. (2004). *Keeping Secrets, Quantity, Quality and Consequences.* University of Amsterdam, Psychology Research Institute. Amsterdam: University of Amsterdam.

Frost & Sullivan. (2008). *The 2008 (ISC)2 Global Information Security Workforce Study.* Frost & Sullivan.

Frost & Sullivan. (2009). *Growing Sophistication of Cyber Crime Driving.* London: Frost & Sullivan.

Fukuyama, F. (1995). *Trust: The Social Virtues and the Creation of Prosperity* (1st ed.). New York, NY: Free Press Paperbacks; Siomon & Schuster, Inc.

Furnell, S. M., & Papadaki, M. (2008, May). Testing our defences or defending our tests: the obstacles to performing security assessment. *Computer Fraud & Security*(5), 8-12.

Furnell, S. M., Papadaki, M., & Thomson, K. L. (2009a, December). Scare tactics – A viable weapon in the security war? *Computer Fraud & Security*(12), 6-10.

Furnell, S., & Thomson, K.-L. (2009, February). From culture to disobedience: Recognising the varying user acceptance of IT security. (S. Mansfield-Devine, Ed.) *Computer Fraud & Security, 2009*(2), 5-10.

Gable, G. (1994). Integrating Case Study and Survey Research Methods: An Example in Information Systems. (R. Baskerville, & R. Paul, Eds.) *European Journal of Information Systems, 3*(2), 112-126.

Galliers, R. (Ed.). (1992). *"Information systems research: Issues, methods, and practical guidelines.* Oxford: Blackwell Scientific Publications.

Galliers, R. D., & Land, F. F. (1987). Choosing Appropriate Information Systems Research Methodologies. *Communications of the ACM, 30*(11), 900-902.

Galliers, R. D., Markus, M. L., & Newell, S. (Eds.). (2006). *Exploring Information Systems Research Approaches: Readings and Reflections.* London: Routledge.

GAO. (2005). *Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities.* Washington D.C.: United States Government Accountability Office (GAO).

Garson, G. D. (2006). *Public information technology and e-governance: managing the virtual state.* London: Jones & Bartlett Publishers, Inc.

Gasper, P. D. (2010). *Cyber Threat to Critical Infrastructure 2010-2015: Increased Control System Exposure.* Idaho National Laboratory.

Geers, K. (2008, August 27). Cyberspace and the changing nature of warfare. *SC Magazine*. (I. Armstrong, Ed.) New York, NY: Haymarket Media, Inc. Retrieved February 22, 2009, from http://www.scmagazine.com/cyberspace-and-the-changing-nature-of-warfare/article/115929/

Ghosh, S. (2004, March / April). The Nature of Cyber-attacks in the Future: A Position Paper. *Information Systems Security*.

Gibb, R. W. (2000). *A Theoretical Model to Attack the Enemy's Decision-Making Process.* Naval War College, Joint Military Operations. Newport, RI: DoD.

Gibson, S. D. (2007). Corporate Security Education: Towards Meeting the Challenge. *Security Journal, 20*(2), 142.

Gjelten, T. (2010, July 19). Cyberwarrior Shortage Threatens U.S. Security. *NPR News.* Washington, DC: NPR.

Glebocki Jr., J. (2008). *DoD Computer Network Operations: Time to Hit the Send Button.* U.S. Army War College. Carlisle, PA: DoD.

Gleick, J. (2011). *The Information: A History, a Theory, a Flood.* New York: Pantheon.

Gooden, L. R. (2009, May). Protecting Our Most-Powerful Weapon System: Information. (N. Sage, Ed.) *High Frontier: The Journal for Space & Missile Professionals, 5*(3), 42-43.

Goodman, S. E. (1996, December). War, information technologies, and international asymmetries. *Commun. ACM, 39*(12), 11-15.

Gordon, J. (2007). Cyber Weaponization: Analysis of Internet Arms Development. In J. Stamey (Ed.), *Computer Security Conference, Myrtle Beach, SC.* Digital University Press.

Goucher, W. (2009, March). The reality of trust. (S. Mansfield-Devine, Ed.) *Computer Fraud & Security, 2009*(3), 14-15.

Graham, S. (2011, February 23). When Life Itself is War: On the Urbanization of Military and Security

Doctrine. *International Journal of Urban and Regional Research*.

Gresham, M. T., & Andrulis, J. (2002). *Information value chain.* Somers, NY: IBM Institute for Business Value.

Grimes, R. (2005). *"Honeypots for Windows: Configure and Manage Window's Honeypots," the Expert's Voice.* Apress: Springer.

Grossack, V. (2012). Too Good to Be True. In D. Schraub, & R. F. Wolf, *Risk Metrics for Decision Making and ORSA.* (pp. 11-14). Schaumberg, IL: Society of Actuaries.

Guido, B. (2007). E-government global readiness report 2008 from e-government to knowledge management. In T. Janowski, & T. A. Pardo (Ed.), *Proceedings of the 1st international conference on Theory and practice of electronic governance. Macao, China, 10-13 December, 2007. 232*, p. 3. ACM.

Habig, C. (2011, February 5). *Cyberspace Presents Complex Global Challenges.* Retrieved March 15, 2011, from Munich Security Conference: http://www.securityconference.de/Program.425+M578c0183589.0.html?&L=1

Haidt, J., & Joseph, C. (2007). The moral mind: How 5 sets of innate moral intuitions guide the development of many culture-specific virtues, and perhaps even modules. (P. Carruthers, S. Laurence, & S. Stich, Eds.) *The Innate Mind, 3*, 367-391.

Haimes, Y. Y. (2011). On the Complex Quantification of Risk: Systems-Based Perspective on Terrorism. *Risk Analysis*.

Halle, A. M. (2009). *Cyberpower as a Coercive Instrument.* The Air University, School of Advanced Air and Space Studies. Maxwell AFB, AL: Air University Press.

Halleen, G., & Kellogg, G. (2005). *Security Monitoring with Cisco Security MARS.* Cisco Press.

Hanseth, O. (2002). *From systems and tools to networks and infrastructures - from design to cultivation. Towards a theory of ICT solutions and its design methodology implications.* Retrieved January 8, 2011, from Department of Informatics, University of Oslo: http://heim.ifi.uio.no/~oleha/Publications/ib_ISR_3rd_resubm2.html

Harrington, J. (2005). *Network Security: A practical approach.* Elsevier.

Harris, R. (2009, December 2). *Introduction to Decision Making*. Retrieved February 11, 2011, from Virtual Salt: http://www.virtualsalt.com/crebook5.htm

Harris, S. (2008, May 31). *China's Cyber-Militia.* Retrieved Nov 20th, 2009, from http://www.triprosec.net/pdf/china_cyber_militia.pdf.

Hayat, M. (2005). *Domain Based Security Threat-Analysis.* Southampton: University of Southampton.

Hayat, Z., Reeve, J., & Boutle, C. (2005). *Domain Based Security: Improving Practices.* Southampton: BAe SYSTEMS Integrated System Technologies.

Healey, M. (2012, February 3). *2012 State of Clould Computing.* Retrieved February 6, 2012, from InformationWeek: http://reports.informationweek.com/abstract/5/8658/cloud-computing/research-2012-state-of-cloud-computing.html

Heiser, J., & Nicolett, M. (2008). *Assessing the Security Risks of Cloud Computing.* Gartner Research. Gartner.

Hejnova, P. (2010). Beyond Dark and Bright: Towards a more Holistic understanding of Inter-Group networks. *Public Administration, 88*(3), 741-763.

Held, D., & McGrew, A. (2010). Globalisation: The Global Transformations Website. In J. Krieger (Ed.), *Oxford Companion to Politics.* Oxford: Oxford University Press.

Heller, P. S. (2009). Globalisation and the Welfare State. *Global Economic Symposium 2009.* Plön Castle, Schleswig-Holstein, Germany: Global Economic Symposium (GES).

Heller, P. S. (2009a). Globalisation and the Welfare State. In D. J. Snower (Ed.), *Global Economic Symposium (GES), Plön Castle, Schleswig-Holstein, Germany, 10-11 September 2009.* GES.

Helvik, B. (2004). Perspectives on the dependability of networks and services. *Telektronikk (100th Anniversary Issue: Perspectives in Telecommunications), 3*, 27-44.

Henry, M. G. (2004). Trustworthy 100-year digital objects: Evidence after every witness is dead. *ACM Trans. Inf. Syst., 22*(3), 406-436.

Heylighen, F. (1994, October 17). *Cyberspace*. Retrieved July 20, 2012, from The Principia Cybernetica Web: http://pcp.lanl.gov/cybspace.html

Hjelmås, E., & Wolthusen, S. D. (2006). Full-spectrum information security education: integrating B.Sc., M.Sc., and Ph.D. programs. *Proceedings of the 3rd annual conference on Information security curriculum development. Kennesaw, Georgia,22-23 September, 2006* (pp. 5-12). ACM.

Hjelmås, E., & Wolthusen, S. D. (2006a). Full-spectrum information security education: integrating B.Sc., M.Sc., and Ph.D. programs. *Proceedings of the 3rd annual conference on Information security curriculum development. Kennesaw, Georgia* (pp. 5-12). ACM.

HM Treasury. (2004). *The Orange Book: management of risk – principles and concepts," .* London: Her Majesty's Stationary Office. .

HMG Canada. (2008). *Multi-Agency Situational Awareness System Architecture Model.* Montreal, Canada: HMSO.

Hobbins, W. T. (2005, Spring). Airmen on the Battlefield: Warfighting Integration in Support of Special Operations Forces. *Air & Space Power Journal, XIX*(1), 67-79.

Holden, M. (2011, February 17). *Cyber crime costs UK $43.5 billion a year: study*. Retrieved February 17, 2011, from Reuters: http://www.reuters.com/article/2011/02/17/us-britain-security-cyber-idUSTRE71G35320110217?feedType=RSS&sp=true

Hollander, E. P., & Offerman, L. R. (1990). Power and leadership in organizations: relationships in transition. *American Psychologist, 45*(2), 179-189.

Honavar, V., Miller, L., & Wong, J. (1998). Distributed Knowledge Networks. *IEEE Information Technology Conference, Syracuse, NY , USA , 1-3 September 1998* (pp. 87 - 90). IEEE.

Hongladarom, S., & Entz, A. (2003). Turning Digital Divide into Digital Dividend: Anticipating

Thailand's Demographic Dividend. *Demographic Dividend, College of Population Studies, Bangkok Thailand, 6 November, 2003.* Chulalongkorn University.

Hoopes, J., Bawcom, A., Kenealy, P., Noonan, W. J., Schiller, C. A., Shore, F., et al. (2009). *Virtualization for Security: Including sandboxing, Disaster Recovery, High Availability, Forensic Analysis and Honeypotting.* (J. Hoopes, Ed.) Burlington, MA: Syngress publishing, Inc.

Hopkins, N. (2011, May 30). UK developing cyber-weapons programme to counter cyber war threat. *The Guardian*. (A. Rusbridger, Ed.) London, UK.

Howard, M., & Lipner, S. (2005). *The Security Development Lifecycle: A Process for Developing Demonstrably More Secure Software.* Seatle: Microsoft Press, Microsoft Corporation.

Hsiao, R.-L. (2003). Technology fears: distrust and cultural persistence in electronic marketplace adoption, 12 (2003), pp.. *Journal of Strategic Information Systems, 12*, 169–199.

Hughes, K. J. (2002). *Domain Based Security: enabling security at the level of applications and business processes.* Farnborough: QinetiQ Ltd.

Hughes, K. J. (2002). *Domain Based Security: enabling security at the level of applications and business processes.* Malvern, UK: QinetiQ.

Hughes, K. J., & Robinson, C. L. (2001). *Managing Infosec Risk in Complex Projects.* Malvern, UK.: QinetiQ.

Huitt, W. (2007). Maslow's hierarchy of needs. *Educational Psychology Interactive*, 1-5.

Hundley, H., & Anderson, R. (1995, Winter 1995-1996). Emerging challenge: security and safety in cyberspace. *Technology and Society Magazine, 14*(4), pp. 19 - 28 .

Hurley, M. (2001, April 4). *Network Air Gaps - Drawbridge to the back Office.* Retrieved September 22, 2009, from SANS Institute: http://www.sans.org/infosecFAQ/firewall/gaps.htm

Hutchinson, W. (2005). Information Security: a Misnomer. In C. Valli, & A. Woodward (Ed.), *Proceedings of the 3rd Australian Information Security Management Conference, Perth, Western Australia, 30th September 2005* (pp. 33-37). School of Computer and Information Science, Edith Cowan University, Western Australia.

Hutchinson, W. (2005). The 'Will' and Information Operations. *4th European Conference on Information Warfare and Security, University of Glamorgan, UK, 11-12 July 2005* (pp. 151-156). Academic Conferences Limited, Reading, UK.

IATF. (2002). *Defense in Depth.* Washington D.C.: Information Assurance Technical Forum.

IEFT. (2012). *Request for Comments (RFC).* Retrieved July 30, 2012, from The Internet Engineering Task Force (IETF): http://www.ietf.org/rfc.html

Ilachinski, A. (1997). *Towards a Science of Experimental Complexity: An Artifical Life Approach to Modelling Warfare.* Alexandria, VA: Center for Naval Analysis.

ISO. (1999). *Industrial automation systems - Concepts and rules for enterprise models.* ISO Technical Committee 184, Industrial automation systems and integration. Geneva: The International Organization for Standardization.

ISTAG. (2003). *Ambient Intelligence: from vision to reality.* Luxembourg: Office for Official Publications of the European Communities.

ISTAG. (2004). *Grand Challenges in the Evolution of the Information Society.* Information Society Technologies. Luxembourg: Office for Official Publications of the European Communities.

ISTAG. (2006). *Shaping Europe's Future through ICT.* Information Society Technologies . Luxembourg: Office for Official Publications of the European Communities.

ISTAG. (2009). *Recommendations on Future and Emerging Technologies.* Information Society Technologies. Luxembourg: Office for Official Publications of the European Communities.

ITU. (2006). Final Acts of the Plenipotentiary Conference. *Plenipotentiary Conference.* Antalya: International Telecommunication Union.

ITU. (2007). *Chapter 5: Challenges to building a safe and secure Information Society. World Information Society Report: Beyond WSIS.* Retrieved June 1, 2010, from International Telecommunication Union: http://www.itu.int/osg/spu/publications/worldinformationsociety/2007/WISR07_full-free.pdf

ITU. (2007). *Meeting Report: Regional Workshop on Frameworks for Cyber Security and CIIP.* International Telecommunications Union, ITU-D. Buenos Aires, Argentina: International Telecommunications Union.

ITU. (2008, September 2). Global Cybersecurity Agenda. *ITU Corporate Strategy Division*. Geneva, Switzerland: International Telecommunication Union (ITU). Retrieved June 10, 2011, from http://www.itu.int/osg/csd/cybersecurity/gca/

ITU. (2009a). *ITU Toolkit for Cybercrime Legislation.* Geneva: International Telecommunications Union.

ITU. (2009b). *Understanding Cybercrime: A Guide for Developing Countries.* Geneva: International Telecommunications Union.

ITU. (2009c). *National Cybersecurity/CIIP Self-Assessment Tool.* Geneva: International Telecommunications Union.

ITU. (2010). *Measuring the Information Society 2010.* Geneva: International Telecommunications Union.

ITU. (2011). *ITU-D ICT Applications and Cybersecurity (CYB): National Strategies.* Geneva: International Telecommunications Union.

ITU-T Rec. X.509. (2005). *X.509 : Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.* Geneva: ITU-T Publications.

ITU-T X.805. (2005). *ITU-T X.805 Security Architecture for Systems Providing End-to-End Communications.* Geneva: ITU.

Jabbour, K. S. (2009, May). The Science and Technology of Cyber Operations. (N. Sage, Ed.) *High Frontier: The Journal for Space & Missle Professionals, 5*(3), 11-15.

Jabbour, K. S. (2010, August). The Time Has Come for the Bachelor of Science in Cyber Engineering. (N. Sage, Ed.) *High Frontier: The Journal for Space & Missile Professionals, 6*(4), 20-23.

Jackson, B. A., Chalk, P., Cragin, R. K., Newsome, B., Parachini, J. V., Rosenau, W., et al. (2007). *Breaching the Fortress Wall. Understanding Terrorist Efforts to Overcome Defensive Technologies.* National Defense Research Institute, Defense Technical Information Center. Santa Monica, CA: RAND Coporation.

Jackson, K. (2010). DOD Moves Forward with Cloud Computing. (V. Vasquez, Ed.) *Cloudbook:The Cloud Computing & SaaS Information Resource, 1*(2).

Jain, G. (2005). Cyber Terrorism: A Clear and Present Danger to Civilized Society? *Information Systems Education Journal, 3*(44).

Jakobsson, M., & Myers, S. (2007). *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft.* John Wiley and Sons.

Jakobsson, M., & Zulfikar, R. (2008). *Crimewave: Understanding New Attacks and Defences.* Symantec Press, Pearson Education, Inc.

Jamka, J. (2009). Capabilities Gap Analysis Status Update. *3rd Annual UCDMO Conference 2009.* Adelphi, MD: Cross Domain Management Office (UCDMO).

Janssen, M. (2007). Adaptability and accountability of information architectures in interorganizational networks. *Proceedings of the 1st international conference on Theory and practice of electronic governance* (pp. 57--64). Macao, China: ACM.

Jaquith, A. (2007). *Security Metrics: Replacing Fear, Uncertainty and Doubt.* Addison-Wesley, Pearson Education, Inc.

Jensen, M. J., Danziger, J. N., & Venkatesh, A. (2004). *Civil Society and Cyber Society: Culture Governance and Democratic Politics.* Center for Research on Information Technology and Organizations. Irvine, CA: University of California.

Jewkes, Y. (2003). Chapter 2 - Policing the Net: crime, regulations and surveillance in cyberspace. In Y. Jewkes, *Dot.Cons: Crime, Divance and Identity on the Internet* (pp. 15-35). Cullumpton, Devon, UK: Willian Publishing.

Jiang, Y., Gan, Y., Zhou, J., & Cai, Z. (2009). A Model of Intrusion Prevention Base on Immune. *Proceedings of the Fifth International Conference on Information Assurance and Security, IAS 2009, Xi'An, China, 18-20 August, 2009* (pp. 441-444). IEEE Computer Society.

Jobbagy, Z. (2003). *Literary Survey on Effects Based Operations.* The Hague, NL: TNO Physics and Electronics Laboratory.

Jog, N. (2001). The Dimensions of the Cyber Universe. In J. Kelemen, & P. Sosík (Ed.), *6th Proceedings European Conference, ECAL 2001 Prague, Czech Republic, September 10–14, 2001. 2159*, pp. 681-684. Springer.

Johnson, C. W. (2006). *What are Emergent Properties and How Do They Affect the Engineering of Complex Systems.* University of Glasgow, Department of Computing Science. Glasgow: University of Glasgow.

Johnson, G., Scholes, K., & Whittington, R. (2008). *Exploring Corporate Strategy* (8th ed.). Harlow: Prentice Hall, Financial Times, Person Education Limited.

Johnson, J. D. (2010, November 3). *Never Worry About Security*. Retrieved January 4, 2011, from Symantec Connect: http://www.symantec.com/connect/articles/never-worry-about-security

Jones, A. (2002). Protecting the Critical National Infrastructure – Development of a Method for the Measurement of Threat Agents in an Information Environment," 7(2), . *Information Security Technical Report, 7*(2).

Jones, A. (2003). A Methodology for the Assessment of the Capability of Threat Agents in an Information Environment. *Journal of Information Warfare, 2*(2).

Jones, A., & Ashenden, D. (2005). *Risk Management for Computer Security: Protecting your Network and Information Assets.* London: Elsevier Butterworth-Heinemann, Elsevier Inc.

Jones, A., & Kovacich, G. L. (2002b). What InfoSec Professionals Should Know About Information Warfare Tactics by Terrorists. *Computers & Security, 21*(2), 113-119.

Jones, A., & Kovacich, J. (2002a). What InfoSec Professionals Should Know About Information Warfare Tactics By Terrorists – Part 1. *Computers & Security, 21*(1), 35-41.

Jones, A., Kovacich, G. L., & Luzwick, P. G. (2002a). Everything You Wanted to Know about Information Warfare but Were Afraid to Ask, Part 1. *Information Systems Security, 11*(4), 9-20.

Jones, A., Kovacich, G. L., & Luzwick, P. G. (2002b). Global Information Warfare: How Businesses, Governments, and Others Achieve Objectives and Attain Competitive Advantages. *Information Systems Security, 11*(5), 15-23.

Jones, J. (2012). *Business Drivers and Benefits of Enterprise Architecture*. Retrieved February 10, 2012, from Architecting the Enterprise: http://www.architecting-the-enterprise.com/enterprise_architecture/business_drivers_and_benefits_of_enterprise_architecture.php

Jones, Q., & Rafaeli, S. (2000). What Do Virtual "Tells" Tell? Placing Cybersociety Research into a Hierarchy of Social Explanation. *Proceedings of the 33rd Hawaii International Conference on System Sciences. 1*, pp. 1011--. IEEE Computer Society.

Jonsson, E. (1998). An Integrated Framework for Security and Dependability. *Proceedings of 1998 ACM workshop on New Security Paradigms* (pp. 22-29). Charlottesville: Association for Computing Machinery.

Jormakka, J., & Mölsä, J. V. (2005). Modelling Information Warfare as a Game. *Journal of Information Warfare, 4*(2).

Jøsang, A., Keser, C., & Dimitrakos, T. (2005). Can We Manage Trust? *Trust Management: Lecture Notes in Computer Science, 3477*, 13-29.

Joseph, S., Daniel, J. R., Surdu, J. R., & Carver, C. A. (2001). The IWAR range: a laboratory for undergraduate information assurance education. *Proceedings of the sixth annual CCSC northeastern conference on The journal of* *computing in small colleges. Middlebury, Vermont* (pp. 223 - 232). Consortium for Computing Sciences in Colleges , USA.

Julisch, K. (2008). Security compliance: the next frontier in security research. *Proceedings of the 2008 workshop on New Security Paradigms* (pp. 71-74). Lake Tahoe, CA: Association for Computing Machinery (ACM).

Kaempf, G. L., Klein, G. A., Thordsen, M. L., & Wolf, S. (1996, June). Decision Making in Complex Naval Command-and-Control Environments. *Human Factors, 38*(2), 220-231.

Källqvist, L. (2008). *Introduction to NCOIC.* Saab, Corporate Strategy and Business Development. Washington, DC: NCOIC.

Kaplan, B., & Duchon, D. (1988). Combining Qualitative and Quantitative Methods in Information Systems Research: A Case Study. *Ninth Annual International Conference on Information Systems, Minneapolis, MN, November 30-December 3, 1988* (pp. 45-68). ACM.

Kaplan, B., & Maxwell, J. A. (1994). Qualitative Research Methods for Evaluating Computer Information Systems. In J. G. Anderson, C. E. Aydin, & S. J. Jay (Eds.), *Evaluating Health Care Information Systems: Methods and Applications* (pp. 45-68). Thousand Oaks, CA: Sage.

Kaplan, B., Truex, D. P., Wastell, D., Wood-Harper, A. T., & DeGross, J. I. (Eds.). (2004). *Information Systems Research: Relevant Theory and Informed Practice.* Norwell, MA: Kluwer Academic Publishers.

Karatzogianni, A. (2004). The Politics of 'Cyberconflict'. *Politics, 24*(1), 46-55.

Karlsson, R., & Hägg, M. (2005). *Counter-terrorism Information Operations.* Retrieved June 21, 2010, from Institute of Communication Studies: http://ics.leeds.ac.uk/papers/pmt/exhibits/3123/HaeggKarlsson_Counterterrorism_IO%5B1%5D.pdf

Katz, E., & Lazarsfeld, P. (2006). *Personal influence: The part played by people in the flow of mass communications.* Transaction Pub.

Keller, B. M. (2011). *Protection Mechanisms in Security Management.* Retrieved July 3, 2012, from Docstoc: Documents and Resources for Small Businesses & Professionals: http://www.docstoc.com/docs/111899542/Protection-Mechanisms-in-Security-Management

Keller, R., Carrigan, N., Atkinson, S. R., Clarkson, P. J., & Johnson, P. (2008). Collaboration and Information Sharing in NEC Networks. *NECTISE.* Leeds: Loughborough University.

Keller, R., Carrigan, N., Atkinson, S. R., Clarkson, P. J., & Johnson, P. (2008). Collaboration and Information Sharing in NEC Networks". *Realising Network Enabled Capability (RNEC'08), Leeds, UK, 13-14 October, 2008.* NECTISE Loughborough University.

Kelley, O. (2008). *Cyberspace Domain: a war fighting substantiated operational environment imperative.* Carlisle Barracks, PA: U.S. Army War College.

Kellner, D. (2008). Networked Centric War born out of RMA. In A. Huhtinen, & J. Rantapelkonen, *Messy Wars* (p. 205). Finn Lectura.

Kelly, J., & Kilcullen, D. (2006). Chaos versus Predictability: A Critique of Effects-Based Operations. *Special Edition: Effects-Based Strategy, Security Challenges, 2*(1), 63-73.

Kelly, O. L. (2008). *Cyberspace Domain: A Warfighting substantiated Operational Environment Imperative.* U.S. Army War College. Carlisle Barracks, PA: U.S. Army War College.

Kennedy, K., & Soligan, J. (2010). *Joint, Alliance and Coalition C2 Integration and Interoperability.* Washington D.C.: U.S. Joint Forces Command.

Keohane, R., & Nye, J. (1999). Power and Interdependence in the Information Age. In J. Nye, & E. Karmarck (Eds.), *Technology.Gov.* USA: Hollis.

KGS. (2011). *Data Maturity Model.* Retrieved June 18, 2011, from KForce Government Solutions: http://www.kforcegov.com/services/DataConfidence/DataMaturityModel.aspx

Khalilzad, Z. M., & White, J. P. (1999). *Strategic Appraisal: The Changing Role of Information Warfare.* Washington D.C>: RAND.

Khalilzad, Z., & J.P., W. (1999a). *The Changing Role of Information in Warfare," Project AIR FORCE.* US National Defence Research Institute. San Clara, CA: RAND.

Khan, U. M., & Hussain, M. (2009). Quantification of Cyber Security. In G. Dhillon (Ed.), *Security, Assurance and Privacy: Organizational Challenges: Proceedings of the 8th Annual Security Conference Discourses in Security Assurance & Privacy Las Vegas, NV, USA 15-16 April 2009. 27*, pp. 1-11. Security Conferences.

Khan, U., & Hussain, M. (2009). Quantification of Cyber Security. *Security, Assurance and Privacy: Organizational Challenges Proceedings of the 8th Annual Security Conference Discourses in Security Assurance & Privacy Las Vegas, NV, 15-16 April 2009.* Security Conferences.

Khatri, N., & Ng, H. A. (2000). The role of intuition in strategic decision making. *Human Relations, 53*(1), 57-86.

Kierkegaard, S. M. (2005). Cracking Down On Cybercrime, Global Response: The Cybercrime Convention. (R. Harris, Ed.) *Communications of the IIMA, 5*(1), 59-66.

Killmeyer, J. (2006). *Information Security Architecture: An Integrated Approach to Security in the Organisation* (2nd ed.). London: Auerbach Publications, Taylor and Francis Group.

King, S. B. (2010). *Military Social Influence in the Global Information Environment: A Civilian Primer.* St Francis University, Psychology Department. Lorretto, PA: The Society for the Psychological Study of Social Issues.

King, S., Tucek, J., Cozzie, A., Grier, C. J., & Zhou, Y. (2008). Designing and implementing malicious hardware. *Proceeds of LEET '08 which was co-located with Usability, Psychology, and Security 2008.* San Francisco, CA: USENIX.

Klein, G., Drury, J., Pfaff, M., & More, L. (2010). The Evolution of C2 - COAction: Enabling Collaborative Option Awareness. *15th ICCRTS.* DOD CCRP.

Kling, R., Rosenbaum, H., & Sawyer, S. (2005). *Understanding and Communicating Social Informatics: A Framework for Studying and Teaching the Human Contexts of Information* *and Communications Technologies.* Medford, NJ: Information Today, Inc.

Klopfer, E., Osterweil, S., Groff, J., & Haas, J. (2009). *The Instructional Power of Digital Games, Social Networking Systems.* Massachusetts Institute of Technology. Cambridge, MA.: Creative Commons.

Knapp, K. (2009). *Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions.* New York: Hershey.

Knight, D. W. (2001). The Fourth Wish: Operational Information Management and Situational Awarenees. *Canadian Military Journal*, 33-40.

Koffman, E. a. (2007). New paradigms for introductory computing courses. In G. Lewandowski (Ed.), *Proceedings Proceedings of the 38th SIGCSE technical symposium on Computer science education,Covington, Kentucky, USA, 7-10 March, 2007. 39 (1)*, pp. 67-68. ACM.

Kolb, D. G. (2008, January). Exploring the Metaphor of Connectivity: Attributes, Dimensions and Duality. *Organization Studies , 29*(1), 127-144.

Kollock, P., & Smith, M. (1996). Managing the Virtual Commons: Cooperation and Conflict in Computer Communities. (S. Herring, Ed.) *Computer-Mediated Communication: Linguistic, Social, and Cross-Cultural Perspectives*, 109-128.

Kossiakoff, A., Sweet, W. N., Seymour, S. J., & Biemer, S. M. (2011). *System Engineering: Principles and Practice* (2nd ed., Vol. Wiley Series in Systems Engineering and Management). (A. P. Sage, Ed.) Hoboken, NJ: John Wiley & Sons, Inc.

Kovacich, G. (2003). *The Information Systems Security Officer's Guide.* London: Butterworth-Heinemann, Elsevier.

Kramer, F. D., Starr, S. H., Wentz, L., & Zimet, E. (2007). Frameworks and Insights Characterizing Trends in Cyberspace and Cyberpower. *12th International Command and Control Research and Technology Symposium - Adapting C2 to the 21st Century.* Newport, RI: The CCRP Press.

Kramer, F. W., Starr, S., & Zimit, E. (2007a). *Frameworks and Insights Characterizing Trends in Cyberspace and Cyberpower ,".* The Center for Technology and National Security Policy. Washington D.C.: National Defense University.

Krämer, N. C. (2008). Theory of mind as a theoretical prerequisite to model communication with virtual humans. *Proceedings of the Embodied communication in humans and machines, 2nd ZiF research group international conference on Modeling communication with robots and virtual humans* (pp. 222--240). Bielefeld, Germany: Springer-Verlag.

Krekel, B. (2009). *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation.* The US-China Economic and Security Review Commission . McLean, VA: Northrop Grumman Corporation .

Kubic, C. (2009). *An Assured GIG Enterprise: Overview of the IA Component of the GIG.* National Security Agency, Information Assurance Architecture and Systems Security Engineering Group. San Diego, CA: Unified Cross Domain Management Office (UCDMO).

Kücklich, J. R. (2009, October). Virtual Worlds and Their Discontents: Precarious Sovereignty, Governmentality, and the Ideology of Play. *Games and Culture, 4*(4), 340-352.

Kuehl, D. T. (2009). *Cyberspace to Cyberpower: Defining the Problem* (1st ed.). (F. D. Kramer, S. H. Starr, & L. K. Wentz, Eds.) Washington D.C.: National Defence University and Potomac books.

Kueter, J. (2010, August). Cybersecurity: Challenging Questions with Incomplete Answers. (N. Sage, Ed.) *High Frontier: The Journal for Space & Military Professionals, 6*(4), 28-30.

Landoll, D. (2006). *The Security Risk Assessment Handbook: A complete Guide for Performing Security Risk Assessments.* London: Auerbach Publications, Taylor & Francis Group, Informa plc.

Landree, E., Gonzales, D., Ohlandt, C., & Wong, C. (2010). *Implications of Aggregated DoD Information Systems forInformation Assurance Certification and Accreditation.* Santa Monica: RAND National Defence Research Institute.

Lane, J., Heus, P., & Mulcahy, T. (2008, April). Data Access in a Cyber World: Making Use of Cyberinfrastructure. *Trans. Data Privacy, 1*(1), 2-16.

Lapke, M., & Dhillon, G. (2005). *Power Relationships in Information Systems: Security Policy Formulation and Implementation.* Richmond, VA: Virginia Commonwealth University.

Laprie, J.-C. (2008). *From Dependability to Resilience.* Université de Toulouse, LAAS-CNRS, Toulouse.

Laudon, K. C., & Laudon, J. P. (2007). *Management Information Systems* (10th ed.). Prentice Hall.

Lavoie, B. F. (2004). *The Reference Model for an Open Archival Information System (OAIS).* Office of Research. Dublin, OH: OCLC Online Computer Library Center, Inc.

Lawrence, T. E. (1920, October). The Evolution of a Revolt. *Army Quarterly and Defence Journal*.

Leavitt, N. (2009, January). Is Cloud Computing Really Ready for Prime Time. *Computer Magazine*, pp. 15-20.

Lee, M. H. (2005). *An Empirical Study for Cohesion of Virtual Internet Community.* Tainan City, Taiwan (R.O.C.) : National Cheng Kung University (NCKU).

Lehtinen, R., Russell, D., & Gangemi, G. (2006). *Computer Security Basics* (2nd ed.). New York: O'Reilly.

Lekkas, D. (2003). Establishing and managing trust within the public key infrastructure. *Computer Communications, 26*, 1815-1825.

Lesser, I., Hoffman, B., Arquilla, J., Ronfeldt, D., Zanini, M., & Jenkins, B. (1999). *Countering the New Terrorism: Implications for Strategy.* San Clara, CA: The RAND Corporation.

Lessig, L. (2004). The Law of Cyberspace. In ,. R. Spinello, & H. T. Tavani (Eds.), *Readings in cyberethics* (pp. 134-144). Sudbury, MA: Jones and Bartlett.

Leune, K., Papazoglou, M., & van den Heuvel, W.-J. (2004). Specification and querying of security constraints in the EFSOC framework. *Proceedings of the 2nd international conference on Service oriented computing. New York, NY, USA* (pp. 125--133). ACM.

Levine, J. (2010, July). *Information Realism: Quantum bit in the Cyberspace.* Retrieved October 10, 2010, from www.digicult.it:

http://www.digicult.it/digimag/article.asp?id=1852

Levine, J. (2010a). *Informational Realism: Quantum bit in the Cyberspace.* Retrieved October 10, 2010, from Digicult: http://www.digicult.it/digimag/article.asp?id=1852

Leweling, T., & Walters, R. (2005). The Evolution of US Military Conceptions of Information Warfare and Information Operations, 1979-2004: An Initial Report. *4th European Conference on Information Warfare and Security, University of Glamorgan, UK, 11-12 July 2005* (pp. 195-204). Academic Conferences Limited, Reading, UK.

Lewicki, R. J., & Wiethof, C. (2006a). Trust, Trust Development, and Trust Repair. In M. Deutsch, P. T. Coleman, & E. C. Marcus (Eds.), *he Handbook of Conflict Resolution: Theory and Practice* (2nd ed., pp. 92-119). San Francisco, CA: Jossey Bass.

Lewis, J. (2002). *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats.* Washington D.C.: Center for Strategic and International Studies.

Lewis, T. G. (2006). *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation.* Wiley - Interscience.

Liang, Q., & Xiangsui, W. (2002). *Unrestricted Warfare: China's Master Plan to Destroy America.* Pan American Publishing Company.

Libicki, M. (2007a). *Conquest in Cyberspace: National Security and Information Warfare.* Cambridge: The RAND Corporation, University Press.

Libicki, M. C. (2007). *Conquest in Cyperspace: National Security and Information Warfare.* New York: Cambridge University Press.

Libicki, M., & Lt Gen Elder, R. (2010, August). Mission Assurance in the Face of Cyber Attacks. (N. Sage, Ed.) *High Frontier: The Journal for Space & Missile Professionals, 6*(5), 24-27.

Liebeskind, J. P. (1997). Keeping Organizational Secrets: Protective Institutional Mechanisms and their Costs. (J. Chytry, Ed.) *Industrial and Corporate Change, 6*(3), 623-663.

Liles, S., & Liles, S. (2009, November 11). *Cyber warfare: The intelligence community*. Retrieved March 15, 2011, from Selil: http://selil.com/?p=1573

Lin, H. (2009, July-Aug.). Lifting the Veil on Cyber Offense. *Security & Privacy, 7*(4), 15 - 21 .

Little, E. G., & Rogova, G. L. (2006). An Ontological Analysis of Threat and Vulnerability. *FUSION 2006.* Buffalo, NY: Center for Cognitive Science.

Lochart, A. (2004). *Network security Hacks: 100 Industrial-Strength Tips and Tools.* New York: O'Reilly.

Logan, D. (2010, January 11). What is Information Governance? And Why is it So Hard? Gartner.

Logeman, K. M. (2005). *Effects-Based Operations: Success Across the Spectrum of Conflict.* Naval War College, Joint Military Operations. Newport, RI: DoD.

Lowder, J. (2008, September 4). *The Difference between Quantitative and Qualitative Risk Analysis*. Retrieved May 20, 2010, from Evident-Based Solutions for Information Security GRC: http://www.jefflowder.com/the-difference-between-quantitative-and-qualitative-risk-analysis-and-why-it-matters-part-1/

Lt Gen Croom, C. (2010, August). The Cyber Kill Chain: a Foundation for a New Cyber Security Strategy. (N. Sage, Ed.) *High Frontier: The Journal for Space & Missile Professionals, 6*(4).

Luiijf, H., Nieuwenhuijs, A. H., & Klaver, M. (2008). Critical infrastructure dependencies 1-0-1. *Infrastructure Systems and Services: Building Networks for a Brighter Future (INFRA)* (pp. 1-3). Amsterdam: IEEE.

Lukas, A. (2000). *Tax Bytes: A Primer On the Taxation of Electronic Commerce.* Washington, DC: Cato Institute's Center for Trade Policy Studies.

Lukasik, S. J. (2003). Vulnerabilities and Failures of Complex Systems. *International Journal of Engineering, 19*(1), 206-212.

Lund, K., Eggen, A., Hadzic, D., & Hafsoe, T. (2007, October). Using web services to realize service oriented architecture in military communication networks. *Communications Magazine, 45*(10), 47-53 .

Luo, Y. (2002, October). Building Trust in Cross-Cultural Collaborations: Toward a Contingency Perspective. (D. C. Feldman, Ed.) *Journal of Management, 28*(5), 669-694.

Lupovici, A. (2011, December). Cyber Warfare and Deterrence:Trends and Challenges in Research. *Military and Strategic Affairs, 3*(3), 49-62.

Lynn, W. J. (2010, September-October). Defending a New Domain: The Pentagon's Cyberstrategy. *Foreign Affairs*, 97–108.

MacIntosh, J. P. (1998). Connectivity: The Space,Tempo and Exploitation of Risk in the Information Age. In A. D. Campen, & D. H. Dearth, *Cyberwar 2.0: Myths, Mysteries and Reality* (p. 398). Fairfax, VA: AFCEA Press.

MacIntosh, J. P., Reid, J., & Tyler, L. R. (2011). *Cyber Doctrine: Towards a coherent evolutionary framework for learning resilience.* London: Institute for Security and Resilience Studies.

Macklin, T., & Jenket, P. (2004). Achieving Cross-Domain Collaboration in Heterogeneous Environments. *Coalition C4ISR Architectures and Information Exchange Capabilities. 12*, pp. 1-18. The Hague, The Netherlands: RTO IST Symposium.

Macnamara, J. (2010). *The 21st century media (r)evolution: emergent communication practices.* New York: Peter Lang Publishing, Inc.

Maconachy, M. V., Schou, C. D., Ragsdale, D., & Welch, D. (2001). A Model for Information Assurance: An Integrated Approach. *Proceedings of the 2001 IEEE, Workshop on Information Assurance and Security, US Military Academy, West Point, NY, 5-6 June 2001.* IEEE.

Madsen, W. (1999, November). Trust in Cyberspace. (S. Mansfield-Devine, Ed.) *Network Security, 1999*(11), 18-19.

Maj Gen Webber, R., & Ware, M. E. (2010, August). Cyberspace Mission Assurance: A New Paradigm for Operations in Cyberspace. (N. Sage, Ed.) *High Frontier: The Journal for Space & Missile Professionals, 6*(4), 3-7.

Major General Baxter, R. (2005, Spring). Ned Ludd Encounters Network-Enabled. *RUSI Defence Systems*, 34-36.

Major Springman, J. A. (1998). *The Relationship Among Tasks, Centers of Gravity, and Decisive Point.* US Army Command and General Staff College, School Of Advanced Military Studies. Fort Leavenworth, KS: Defense Technical Information Center.

Majoris, R. (2010). *Cyber Warfare as an Operational Fire.* Newport, RI : Naval War College, Joint Military Operations Department.

Marceau, C. (2002). An evolutionary approach to cyber security. In C. Marceau, & S. Foley (Ed.), *NSPW '02: Proceedings of the 2002 workshop on New Security Paradigms, Virginia Beach, Virginia, 23-26 September 2002* (pp. 108 - 109). ACM.

Marchand, D. A., Kettinger, W. J., & Rollins, J. D. (2002a). *Information Orientation The Link to Business.* New York, NY: Oxford University Press.

Marks, P. (2009, Mar 14). Cyber-attack, a clear and present danger. *New Scientist, 201*(2699), 18-19.

Markus, M. L., & Robey, D. (1988). Information Technology and Organizational Change: Conceptions of Causality in Theory and Research., 34(5), . *Management Science, 34*(5), 583-598.

Martinelli, F., & Quisquater, J.-J. (2005, October). Security and Trust Management. (P. Kunz, Ed.) *ERCIM News, 63*, pp. 8-9.

Maslow, A. (1943). A Theory of Human Motivation. *Psychological Review, 50*(4), 370-396.

Mattis, J. N. (2008, October). USJFCOM commander's guidance for effects-based operations. *Joint Force Quarterly (JFQ)*.

May, C. J., Hammerstein, J., Mattson, J., & Rush, K. (2006). *Defense in Depth: Foundations for Secure and Resilient IT Enterprises.* The Software Engineering Institute. Carnegie Mellon University.

Mayer-Schonberger, V. (2002, Winter). The Shape of Governance: Analyzing the World of Internet Regulation. *Virginia Journal of International Law, 43*(1), 605.

Mazanec, B. M. (2009, Spring). The Art of (Cyber) War. (I. Berman, Ed.) *The Journal of International Security Affairs, 16*.

McConnell, J. (2010, July 14). An American Cyber Expect on Cyberwar. (N. Gardels, Interviewer) Booz, Allen and Hamilton.

McConnell, J. M. (2008). *Vision 2015: A Globally Networked and Integrated Intelligence Enterprise.* Washington D.C.: Director of National Intelligence.

McCumber, J. (1991). Information Systems Security: A Comprehensive Model. *Proceedings 14th National Computer Security Conference.* Baltimore, MD: National Institute of Standards and Technology.

McDermott, J., Kim, A., & Froscher, J. (2003). Merging paradigms of survivability and security: stochastic faults and designed faults. *Proceedings of the 2003 workshop on New Security Paradigms* (pp. 19-25). Ascona, Switzerland: Association for Computing Machinery (ACM).

McGinnis, D. R., & Comstock, K. (2005). *The Implications of Information Assurance and Security Crisis on Computing Model Curricula.* Grand Junction, CO: Mesa State College.

McHugh, J., & Gates, C. (2003). Locality: a new paradigm for thinking about normal behavior and outsider threat. *Proceedings of the 2003 workshop on New Security Paradigms* (pp. 3-10). Ascona, Switzerland: Association for Computing Machinery (ACM).

McIntyre, M., & Flemming, S. (2001). Netcentric Warfare for Dynamic Coalitions:Implications for Secure Interoperability. *RTO IST Symposium on "Information Management Challenges in Achieving, n Quebec, Canada, 28-30 May 2001. 21*, pp. 1-12. NATO Research and Technology Organisation.

McKnight, W. L. (2002). What is Information Assurance. *Crosstalk: The Journal of Defense Software Engineering*.

McNab, C. (2004). *Network Security Assessment.* New York: O'Reilly.

McNeal, A. C. (2004). Information Assurance: Structure From the Fog. *Air & Space Power Journal*.

Meiter, J. S. (2006). Network Enabled Capability: A Theory Desperately in Need of Doctrine. *Defence Studies, 6*(2), 189 - 214.

Metz, S. (2000). *Armed Conflict in the 21st Century: The Information Reveloution and Post-Modern Warfare.* Carlisle, Pennsylvania: Strategic Studies Institute, United States Army War College .

Metz, T. F., Garrett, M. W., & Hutton, J. (2006, May - June). Massing Effects in the Information Domain: A Case Study in Aggressive Information Operations. *Military Review*, 2-12.

Meunier, P. (2011). Classes of Vulnerabilities and Attacks. In J. G. Voeller, *Wiley Handbook of Science and Technology for Homeland Security.* Wiley.

Michael, D. C. (2006). Information security: examining and managing the insider threat. *Michael, D. C. (2006). "Information Proceedings of the 3rd annual conference on Information security curriculum development* (pp. 156-158). Kennesaw, Georgia: ACM.

Michael, J. B., Hestad, D., & Pedersen, C. (2002, Winter). Incorporating the Human Element of Trust into Information Systems. (R. J. Lamb, Ed.) *IAnewsletter, 5*(1), 4-8.

Microlink. (2011, May 10). *SIGACT Tracking and Operations Response Management (STORM) Cloud.* Retrieved May 10, 2011, from Microlink Solution Briefing: http://www.microlinkllc.com/Documents/STORM%20Cloud%20Solution%20Briefing.pdf

Mikaelian, T. (2009). *An Integrated Real options Framework for model-based identification and valuation of options under uncertainty.* Dept. of Aeronautics and Astronautics. Cambridge, MA: Massachusetts Institute of Technology.

Mikko, T. S. (2001). A paradigmatic analysis of conventional approaches for developing and managing secure IS. *Mikko, T. S. (2001). "A paradigmatic analysis of conventional approaches for developing and managing secure IS." Proceedings of the 16th international conference on Information security: Trusted information: the new decade challenge* (pp. 437-452). Paris, France : ACM.

Mikroyannidis, A., & Theodoulidis, B. (2006). Heraclitus II: A Framework for Ontology Management and Evolution. *Proceeding of the 2006 IEEE /*

WIC / ACM International Conference on Web Intelligence, Hong Kong, China, 18-22 December, 2006 (pp. 514-521). IEEE Computer Society.

Miller, C. R. (1979). A Humanistic Rationale for Technical Writing. *College English, 40*(6), 610-617.

Ministry of Defence. (2010). *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review.* London: Ministry of Defence.

Mink, M., & Freiling, F. C. (2006). Is attack better than defense?: teaching information security the right way. *Proceedings of the 3rd annual conference on Information security curriculum development* (pp. 44-48). Kennesaw, Georgia: ACM.

Minsky, N. H. (2003). Regularity-Based Trust in Cyberspace. *Trust Management Lecture Notes in Computer Science*, 1071-1072.

Minsky, N. H. (2003). *Regularity-Based Trust in Cyberspace.* Rutgers University, Department of Computer Science, New Brunswick, NJ.

Mitchell, G. W. (1998). *The new math for leaders, useful ideas from chaos theory.* Carlisle, PA: USAWC Strategy Research Project, U.S. Army War College.

Mittrick, M., Richardson, J., & Kaste, R. (2008). *A Policy Driven Information Exchange Network.* U.S. Army Research Laboratory . Baltimore, MD: DoD.

MoD. (2002). *JWP 3-80: Information Operations.* London: The Ministry of Defence.

MoD. (2003). *Delivering Security in a Changing World.* Ministry of Defence. London: The Stationary Office (TSO).

MoD. (2005). *Joint Service Publication 777: The NEC Handbook.* London: HMSO.

MoD. (2006). *JDN 4/05: The Comprehensive Approach.* JDCC. London: The Ministry of Defence.

MoD. (2006). *Joint Doctrine Note (JDN) 4/06: Information Management.* London: HMSO.

MoD. (2006). *JSP 777: Network Enabled Capability Handbook.* Command and Battlespace Management (Land) - CIP. London: The Ministry of Defence.

MOD. (2007). *Asset Management Strategy.* London: Ministry of Defence.

MoD. (2007). *Joint Doctrine Publication 3-80.1: OPSEC, Deception and PSYOPS.* London: The Minisitry of Defence.

MoD. (2009). *JSP 747: Information Management.* Information Coherence Authority for Defence (ICAD). The Ministry of Defence.

MoD. (2009). *MoD's Information Strategy.* London: Ministry of Defence.

MoD. (2009). *NEC- Understanding Network Enabled Capability.* London: Ministry of Defence.

MoD. (2009a). *Understanding Network Enabled Capability.* London: The Ministry of Defence.

MoD. (2009b). *Ministry of Defence Information Strategy (MODIS).* The Chief Information Office. London: Ministry of Defence.

MoD. (2010). *JSP 440: The Defence Manual of Security, Version 3.8.* DDefSy. London: The Ministry of Defence (Restricted).

MoD. (2010). *JSP 541: Alerts, Warnings and Response, Version 3.0.* Defence Security and Assurance Services (DSAS) . London: The Ministry of Defence, (Restricted).

MoD. (2010). *Strategic Defence and Security Review (SDSR).* London: Ministry of Defence.

MoD. (2010). *The Defence Green Paper, Adaptability and Partnership: Issues for a Strategic Defence Review.* London: Ministry of Defence.

MoD. (2010c). *Army Doctrine Publications- Operatations.* London: British Army's Electronic Battle Box, DCDC.

MoD. (2011). *MOD Information Strategy 2011: Better Informed, Better Defence.* London: Ministry of Defence.

MoD. (2012). *JSP 822: The Governance and Management of Defence Training & Education.* The Royal Air Force, Training Education Skills and Resettlement Division . London: HMSO.

Moffat, J. (2003). *Complexity Theory and Network Centric Warfare* (Vol. Information Age Transformation Series). Washington D.C.: CCRP Publications.

Mora, E. (2012, June 13). Panetta Warns of Cyber Pearl Harbor. *CNSNews.com*. (T. P. Jeffrey, Ed.) Alexandria, VA. Retrieved June 14, 2012, from http://cnsnews.com/news/article/panetta-warns-cyber-pearl-harbor-capability-paralyze-country-there-now

Morabito, A. J., & Gatchel, T. L. (2001). *NATO command and Control: Bridging the Gap.* Newport, Rhode Island: US Naval war College.

Morris, E., Levine, L., Meyers, C., Place, P., & Plakosh, D. (2004). *System of Systems Interoperability (SOSI):Final Report.* Software Engineering Institute. Pittsburgh, PA: Carnegie Mellon University.

Morris, E., Levine, L., Meyers, C., Place, P., & Plakosh, D. (2004). *System of Systems Interoperability (SOSI): Final Report.* The Software Engineering Institute. Pittsburgh, PA : Carnegie Mellon University.

Murphy, D. (2010, May-June). Attack or defend? Levering information and balancing risk in cyberspace. *Military Review*, pp. 88–96.

Nain, D., Donaghy, N., & Goodman, S. (2007). The International Landscape of Cyber Security. (D. W. Straub, S. Goodman, & R. L. Bask, Eds.) *Advances in Management Information Systems, 11*, 196 - 227.

Nain, D., Donaghy, N., & Goodman, S. (2008). The International Landscape of Cyber Security. In D. Straub, S. Goodman, & R. Baskerville, *nformation Security: Policy, Processes, and Practices.* New York: M.E. Sharpe.

NATO. (2002). *Vulnerability of the Interconnected Society.* Oslo, Norway: North Atlantic Treaty Organisation.

NATO. (2003). *NATO C3 Technical Architecture Reference Model for Interoperability.* NATO Communications and Information (NCI) Agency, NC3A. Brussels: North Atlantic Treaty Organisation (NATO).

NATO. (2006). *NEC Vision and Concept.* The North Atlantic Treaty Organisation, The Military Committee. Brussels: The North Atlantic Treaty Organisation.

NATO. (2007). *Cyber-Terrorism - a serious threat to peace and security in the 21st Century.* Brussels: North Atlantic Treaty Organisation.

NATO. (2007). *Management Approach to NATO Network Enabled Capability.* Brussels, Belgium: North Atlantic Treaty Organisation.

NATO. (2007a). *Introduction to Network Enabled Capability Security Research Strategy.* Rome, NY: US Air Force Research Laboratory, Information Directorate.

NATO. (2007b). *RTO-TR-IST-045 - NEC Security Research Strategy.* Neuilly-sur-Seine, France: NATO Research and Technology Organisation.

NATO. (2008). *Defending against Cyber Attacks.* North Atlantic Treaty Organisation.

NATO. (2010). *The New Strategic Concept.* Lisbon: North Atlantic Treaty Organisation.

NCIOC. (2008). *NCOIC Interoperability Framework.* Washington, D.C.: Network Centric Operations Industry Consortium - NCOIC.

NECSI. (2004). *Characteristics of Systems of Systems.* Cambridge, MA : New England Complex Systems Institute.

Neugent, B. (2009). Reciprocity. *3rd Annual UCDMO Conference.* Los Angeles: Unified Cross Domain Management Office (UCDMO).

Newman, R. C. (2006). Cybercrime, identity theft, and fraud: practicing safe internet - network security threats and vulnerabilities. *Proceedings of the 3rd annual conference on Information security curriculum development. Kennesaw, Georgia, 22-23 September, 2006* (pp. 68-78). ACM.

Newman, R. C. (2006). Cybercrime, identity theft, and fraud: practicing safe internet - network security threats and vulnerabilities. *Proceedings of the 3rd Annual Conference on InformationSecurity Curriculum Development, InfoSecCD 2006, Kennesaw,Georgia, USA, 22-23 September, 2006* (pp. 68-78). ACM.

Nichiporuk, B. (1999). U.S. Military Opportunities: Information-Warfare Concepts of Operation. In Z. Khalilzad, & J. White (Eds.), *Strategic Appraisal: The Changing Role of Information in Warfare* (pp. 179-215). Santa Monica, CA: RAND.

Nightingale, D. J., & Rhodes, D. H. (2004). Enterprsie Systems Architecting: Emerging Art and Science. *MIT Engineering Systems Symposium* (pp. 1-13). Cambridge, MA: Massachusetts Institute of Technology.

Nikander, P. (2001). Users and Trust in Cyberspace. *Security Protocol Lecture Notes in Computer Science, 2133/2001*, 36-42.

NISCC. (2004a). *NISCC Policy and Good Practice: Good Practice Guide to Telecommunications Resilience.* National Infrastructure Security Co-Ordination Centre. London: NISCC.

NISCC. (2004b). *NISCC Assurance Report for "The CNI Organisation".* National Infrastructure Security Co-ordination Centre. London: NISCC.

NIST. (1994). *Federal Information Processing Standards Publication 186: Digital Signature Standard (DSS).* Computer Systems Laboratory, U.S. Department of Commerce. Gaithersburg, MD : National Institute of Standards and Technology.

NIST. (2001). *NIST Special Publication 800-32: Introduction to Public Key Technology and the Federal PKI Infrastructure.* Information Technology Laboratory, Computer Security Division. Gaithersburg, MD: National Institute of Standards and Technology.

NIST. (2003). *SP800-59 Information Security: Guideline for Identifying an Information System as a National Security System.* Gaithersburg, MD: National Institute of Standards and Technology.

NIST. (2003a). *NIST Special Publication 800-50: Building an Information Technology Security Awareness and Training Program.* National Institute of Standards and Technology, Computer Security Division . Gaithersburg, MD: Computer Security Resource Center, Information Technology Laboratory, NIST.

NIST. (2003b). *NIST Special Publication 800-59: Guideline for Identifying an Information System as a National Security System.* National Institute of Standards and Technology, Computer Security Division . Gaithersburg, MD: Computer Security Resource Center, Information Technology Laboratory, NIST.

NIST. (2005). *NIST Special Publication 800-52: Computer Sercurity.* Information Technology Laboratory, Computer Security Division. Gaithersburg, MD: National Institute of Standards and Technology.

NIST. (2006a). *NIST Special Publication 800-89: Guide to Intrusion Detection and Prevention Systems (IDPS).* National Institute of Standards and Technology, Computer Security Division . Gaithersburg, MD: Computer Security Resource Center, Information Technology Laboratory, NIST.

NIST. (2006b). *NIST Special Publication 800-100: Information Security Handbook: A Guide for Managers.* National Institute of Standards and Technology, Computer Security Division . Gaithersburg, MD: Computer Security Resource Center, Information Technology Laboratory, NIST.

NIST. (2007). *NIST Special Publication 800-94: Recommendation for Obtaining Assurances for Digital Signature Applications.* National Institute of Standards and Technology, Computer Security Division . Gaithersburg, MD: Computer Security Resource Center, Information Technology Laboratory, NIST .

NIST. (2008). *NIST Special Publication 800-64: Security Considerations in the System Development Life Cycle.* National Institute of Standards and Technology, Computer Security Division . Gaithersburg, MD: Computer Security Resource Center, Information Technology Laboratory, NIST .

NIST. (2009a). *NIST Special Publication 800-16: Information Security Training Requirements: A Role- and Performance-Based Model.* National Institute of Standards and Technology, Computer Security Division. Gaithersburg, MD: Computer Security Resource Center, Information Technology Laboratory, NIST.

NIST. (2009b). *NIST Special Publication 800-53: Recommended Security Controls for Federal Information Systems and Organizations.* National Institute of Standards and Technology , Computer Security Division. Gaithersburg, MD: Computer Security Resource Center, Information Technology Laboratory, NIST.

NIST. (2009c). *NIST Special Publication 800-117: DRAFT Guide to Adopting and Using the Security Content Automation Protocol (SCAP).* National Institute of Standards and Technology , Computer Security Division. Gaithersburg, MD: Computer Security Resource Center, Information Technology Laboratory, NIST.

NIST. (2009d). *NIST Special Publication 800-127: DRAFT Guide to Security for Worldwide Interoperability for Microwave Access (WiMAX) Technologies.* National Institute of Standards and Technology , Computer Security Division. Gaithersburg, MD: Computer Security Resource Center, Information Technology Laboratory, NIST.

NIST. (2010a). *NIST Special Publication 800-119: DRAFT Guidelines for the Secure Deployment of IPv6.* National Institute of Standards and Technology, Computer Security Division. Gaithersburg, MD: Computer Security Resource Center, Information Technology Laboratory, NIST.

NIST. (2010b). *NIST Special Publication 800-125: DRAFT Guide to Security for Full Virtualization Technologies.* National Institute of Standards and Technology , Computer Security Division. Gaithersburg, MD: Computer Security Resource Center, Information Technology Laboratory, NIST.

NIST. (2010c). *NIST Special Publication 800-128: DRAFT Guide for Security Configuration Management of Information Systems.* National Institute of Standards and Technology , Computer Security Division. Gaithersburg, MD: Computer Security Resource Center, Information Technology Laboratory, NIST.

Norman, A., & Lucas, P. (2000). *Information Architecture and the Emergent Properties of Cyberspace.* MAYA Design Group, Inc.

Norman, A., & Lucas, P. (2005). Information Architecture and the Emergent Properties of Cyberspace. *InterJournal Complex Systems*.

Norquist, B. (2004). Governmental Effects upon the Cyber Security Decision Making Cycle. *Security Modelling, 18*.

Norton. (2011). *Internet Security Threat Report (ISTR), Volume 16.* Mountain View, CA: Symantec.

NPIA Information Assurance Capability Team. (2010). *Police Service IA Strategy 2010 - 2013.* Association of Chief Police Constables of Scotland (ACPOS), National Policing Improvement Agency. London: NPIA National Police Library.

Nucci, A., & Papagiannaki, K. (2009). *Design, Measurement and Management of Large-scale IP Networks: Bridging the gap between theory and practice.* Cambridge: University Press, Cambridge.

Nunes, M. (1995, June). Jean Baudrillard in cyberspace: Internet, virtuality, and postmodernity. *Style, 29*(2), 1-13.

O'Rourke, C., Fishman, N., & Selkow, W. (2003). *Enterprise Architecture: Using the Zachman Framework.* London: Thomson Course Technology.

Obama, P. (2009a). *Assuring a Trusted and Resilient Information and Communications Infrastructure.* Washington D.C.: The US President, White House.

Obama, P. (2009b). *U.S. Cyber Security Plan.* The US President, White House: Washington D.C.

Obama, P. (2010). *The Comprehensive National Cybersecurity Initiative.* Washington, D.C.: The White House.

Obama, P. (2010). *U.S. Cyber Security Progress.* Washington D.C.: The US President, White House.

Obama, P. (2011). *International Strategy for Cyberspace.* Washington, DC: The Office of the President of the United States, White House.

OECD . (1992). *The recommendations of the Council concerning Guidelines for the Security of Information Systems; GD(92)10.* Paris, France: The Organisation for Economic Co-operation and Development.

OECD. (1986). *Computer-related Crime: Analysis of Legal Policy.* Paris, France: The Organisation for Economic Co-operation and Development.

OECD. (2002). *Guidelines for the Security of Information Systems and Networks.* Paris, France: The Organisation for Economic Co-operation and Development.

OECD. (2005). *The definition and Selection of Key Competencies.* Paris: Organisation for Economic Co-operation and Development.

OECD. (2006). *The Development of Policies for the Protection of Critical Information Infrastructures (CII): DSTI/ICCP/REG(2006)15/FINAL.* Paris, France: The Organisation for Economic Co-operation and Development.

OECD. (2007). *Malicious Software (Malware): A Security Threat to the Internet Economy.* Paris, France: The Organisation for Economic Co-operation and Development.

OECD. (2008a). *The Future of the Internet Economy: A Statistical Profile.* Paris, France: The Organisation for Economic Co-operation and Development.

OECD. (2008b). *Recommendation of the Council on the Protection of Critical Information.* Paris, France: The Organisation for Economic Co-operation and Development.

OGC. (2007). *Management of Risk: Guidance for Practitioners.* London: Office of Government Commerce, The Stationary Office.

OGC. (2008). *Best Management Practice: ITIL V3 and ISO/IEC 20000.* London: Office of Government Commerce.

Ohta, T. (1999). he Japanese Way of Management: A Reminiscence of Professor Takehiko Matsuda. *Invited Paper at the Meeting of the International Federation of Operations Research Societies (IFORS'99), Beijing, China, 1999.* Operations Research Society of China .

Ohta, T. (1999a). The Japanese Way of Management: A Reminiscence of Professor Takehiko Matsuda. *Invited Paper at the Meeting of the International Federation of Operations Research Societies (IFORS'99), Beijing, China, 1999.* Operations Research Society of China.

Ohta, T. (1999b). A Cyber Commons: An Exploration of Social Information Systems in a Digital Society. *Technical Report of Information Processing Society of Japan, 99*(60), pp. 17-22.

Ohta, T., & Yamamoto, T. (1995). A Theory of Social Information Systems and its Basic Models. *Journal of the Japan Society for Management Information, 4*(2), 85-98.

Ohta, T., Kazunari, I., & Isamu, O. (2001). A Viable Cyber Commons: An Auto-Genesis World. *Proceedings of the 5th World Multiconference on Systemics, Cybernetics and Informatics (SCI 2001), VIII*, pp. 376-381.

Omand, D. (2010). *Securing the State.* London: Hurst & Co.

Oracle. (2010). *Sun OpenSSO Enterprise 8.0 Technical Overview > Part II Access Control Using OpenSSO Enterprise.* Retrieved May 10, 2011, from Sun OpenSSO Enterprise 8.0: http://download.oracle.com/docs/cd/E19681-01/820-3740/ggqxm/index.html

Orbe, M. P. (1998). *onstructing Co-Cultural Theory: An Explication of Culture, Power, and Communication.* London: Sage Publications, Inc.

Orlikowski, W. J., & Iacono, C. S. (2001). Research commentary: Desperately seeking "IT" in IT research - A call to theorizing the IT artifact., 12(2), 121. *Information Systems Research, 12*(2), 121.

Ostadzadeh, S. S., & Shams, F. (2011). An Architectural Framework for the Improvement of the Ultra-Large-Scale Systems Interoperability. *WORLDCOMP'11,The 2011 World Congress in Computer Science, Las Vagas, Nevada, 18-21 July 2011.* Tehran: Universal Conference Management Systems & Support (UCMSS).

Palaoro, H. F. (2010). Information Strategy: The Missing Link. *Joint Forces Quarterly, 59*(4), 83-85.

Palmisano, S. (2008). A Smarter Planet Instrumented, Interconnected and Intelligent. *IBM Business Leadership Forum, Istanbul, Turkey, 12 November, 2008.* IBM.

Pamulai, J., Ammann, P., Jajodia, S., & Ritchey, R. (2006). A Framework for Establishing, Assessing, and Managing Trust in Inter–Organizational Relationships. *Pamula, J., Ammann, P., Jajodia, S. and Ritchey, R. (2006). "A Framework for Establishing, Assessing, and MProceedings of the 3rd ACM workshop on Secure web services SWS'06, Alexandria, Virginia, 3 November 2006* (pp. 23-32). ACM.

Papadaki, M. (2008). Social Engineering: How vulnerable are we? *Special Financial Investigation Service for Electronic Trade & Electronic Crime (YPEE), Ministry of Economy and Finance, Athens, Greece, 31 March 2008.* YPEE.

Paquet, C., & Saxe, W. (2005). *The Business Case for Network Security: Advocay, Governance and ROI* (Vols. Network Business Series, CISCO Systems). Indianapolis, IN : CISCO Press.

Paquette, S., Jaeger, P. T., & Wilson, S. C. (2010, July). Identifying the security risks associated with governmental use of cloud computing. *Government Information Quarterly, 27*(3), 245-253.

Parmet, J. (2008, January 30). *Bloom's Taxonomy*. Retrieved July 15, 2010, from Portfolio of Janene Parmet: www.jparmet.com/masters

Pattee, P. G. (2008, Spring). Network-Centric Operations: A Need for Adaptation and Efficiency. *Air and Space Power Journal*.

Paul, C. (2008). *Information Operations: Doctrine and Practice* (Vols. Contemporary Military, Strategic and Security Issues). Westport CT: Praeger Security International.

Peltier, T. (2005). *Information Security Risk Analysis* (2nd Ed ed.). London: Auerbach Publications, Taylor & Francis Group, Informa plc.

Peltier, T. R., Peltier, J., & Blackley, J. (2005). *Information Security Fundamentals.* London: Auerbach Publications, Taylor & Francis Group, Informa plc.

Pentland, A., & Liu, A. (1999). Modeling and Prediction of Human Behavior. *Neural Computation, 11*, 229–242.

Perlo-Freeman, S., Cooper, J., Ismail, O., Sköns, E., & Solmirano, C. (2011). Chapter 4. Military Expenditure. In SIPRI, *Stockholm International Peace Research Institute Yearbook 2011* (42nd ed., pp. 158-229). Stockholm, Sweden: Oxford University Press.

Perrone, L. F., Aburdene, M., & Meng, X. (2005). Approaches to Undergraduate Instruction in Computer Security. *Proceedings of the American Society for Engineering Education Annual Conference & Exposition.* American Society for Engineering Education.

Perry, W., Signori, D., & Boon, J. (2004). *Exploring Information Superiority: A Methodology for Measuring the Quality of Information and its Impact on Shared Awareness.* National Defense Research Institute. Santa Monica, CA: RAND Corporation.

Pfitzmann, A. (2006). Multilateral Security: Enabling Technologies and their Evaluation. In G. Muller, *Emerging Trends in Information and Communication Security* (pp. 1-13). Berlin: Springer-Verlag.

Phillips, C. E., Ting, T. C., & Demurjian, S. A. (2002). *Information Sharing and Security in Dynamic Coalitions.* Storrs, CT: The University of Connecticut.

Phillips, J. C., Ting, T. C., & Dem, S. A. (2002). Information sharing and security in dynamic coalitions. *Proceedings of the seventh ACM symposium on Access control models and technologies* (pp. 87-96). New York: Association for Computing Machinery (ACM).

Piepenbrock , T. F. (2004). *Enterprise design for dynamic complexity : architecting & engineering organizations using system & structural dynamics.* Sloan School of Management, Dept. of Civil and Environmental Engineering. Cambridge, MA: Massachusetts Institute of Technology.

Pilgermann, M., Vidalis, S., Morakis, E., & Blyth, A. (2005, December). Security in Heterogeneous Large Scale Environments Using GRID Technology. (P. Shi, & J.-S. Pan, Eds.) *International Journal for Innovative Computing, Information and Control (IJICIC), 1*(4), 715—725.

Pironti, J. (2006, May). Key Elements of a Threat and Vulnerability Management Program . *ISACA Journal, 3*.

Police National Accreditor. (2009). *IAM Code of Connection.* Police PKI Policy Management Authority (P3MA). London: National Policing Improvement Agency.

Pollock, N. (2002). *Knowledge Management and Information Technology.* Belvoir, VA: Defense Acquisition University Press.

Porter, B. (2007). Approaching Zero: A Study in Zero-Day Exploits, Origins, Cases, and Trends. *Norwich*

University Journal of Information Assurance, 3(1), 1-28.

Porter, M. E. (2001). Strategy and the Internet. *Havard Business Review*, 63-78.

Portnoy, M., & Goodman, S. (2009). The International Landscape of Cyber Security. In M. Portnoy, K. Minor, A. Howard, W. Lee, R. Givens, I. Liscano, et al., M. Portnoy, & S. Goodman (Eds.), *Global Initiatives to Secure Cyberspace* (Vol. 42, pp. 1-3). New York, NY: Springer Science+Business Media, LLC.

Potgieser, P. (2012, March 13). *Financial services messaging - Business benefits boosted by interoperability*. Retrieved June 10, 2012, from International Organization for Standardization: http://www.iso.org/iso/home/news_index/news_archive/news.htm?refid=Ref1536

Powell, A. L. (2009). *Is Cyberspace a source of Global Insecurity and is a reaction-based strategy really able to harness it for greater effect?* Royal College of Defence Studies. HMSO.

Powell, R. (1990). *Nuclear Deterrence Theory: The Search for Credibility.* Cambridge: Cambridge University Press.

Powell, T., & Dent-Micallef, A. (1997, May). Information technology as competitive advantage: The role of human, business, and technology resources. *Strategic Management Journal, 18*(5), 375-405.

Poynter, K. (2008). *Review of information security at HM Revenue and Customs -Final report.* London: Her Majesty's Stationery Office.

Price, R. D., Beltz, T. W., & McKinnon, N. (2006). Automating command post and battle staff operations at the USAF 45th space wing. *MILCOM'06 Proceedings of the 2006 IEEE Conference on Military Communications* (pp. 3544-3550). Piscataway, NJ: IEEE Press.

Price, S. M. (2008, September). Extending the McCumber Cube to Model Network Defence. *ISSA Journal, 9*, 14-18.

PricewaterhouseCoopers LLP (UK). (2010). *Revolution or evolution? Information Security 2020.* London: Technology Strategy Board.

Proctor, R. W., & Van Zandt, T. (2008). *Human Factors in Simple and Complex Systems.* Washington D.C.: CRC Press, Taylor and Francis Group.

Provos, N., & Holz, T. (2008). *Virtual Honeypots: From Botnet Tracking to Intrusion Detection.* Addison-Wesley, Pearson Education.

Puran, R. (2003). *Beyond Convential Terrorism...Cyber Assualt.* The SANS Institute. Bethesda, MD: SANS GIAC.

Qian, Y., Joshi, J., Tipper, D., & Krishnamurthy, P. (2008). Information Assurance. In Y. Qian, J. Joshi, D. Tipper, & P. Krishnamurthy, *Information Assurance: Dependability and Security in Network Systems* (pp. 1-14). Burlington: Morgan Kaufmann Publishers.

Ragsdale, D. J., Lathrop, S. D., & Dodge, R. C. (2003). Enhancing Information Warfare Education Through the Use of Virtual and Isolated Networks. *Journal of Information Warfare, 2*(3).

Raines, G. (2009). *Service-Oriented Architecture (SOA) Series: Cloud Computing and SOA.* System Engineering. MITRE.

Rannenberg, K. (2001). *Multilateral Security: A concept and examples for balanced security.* Cambridge, UK: Microsoft Research.

Rathmell, A. (2003). Controlling Computer Network Operations. *Studies in Conflict & Terrorism, 26*(3), 215-232.

Rattray, G. (2001). *Strategic Warfare in Cyberspace.* Cambridge, MA: The MIT Press.

Rattray, G. J. (2001). *Strategic Warfare in Cyberspace.* Cambridge, MA: The MIT Press.

Rawlinson, D. (2005). *Ministry of Defence Information Assurance Review.* London: Director General Information, MoD. (Restricted).

Raymond, J. C., & Campbell, D. E. (2003). *Building a Global Information Assurance Program.* Auerbach Publications, Taylor & Francis Group, Informa plc.

Redman, J., Warren, M. J., & Hutchinson, W. (2005). System survivability: a critical security problem. (S. M. Furnell, Ed.) *Information Management & Computer Security, 13*(3), 182-188.

Richards, G. (2010). Let Battle Connect. *Engineering & Technology, IET, 5(6)*, 36-39.

Richards, G. (2010a). Let Battle Connect. *Engineering and Technology, 5*(6), 36-38.

Richardson, C. J. (2007). Security: a necessary compromise? *NATO Conference, Bletchley Park, 26 June 2007.* Telindus.

Richardson, C. J. (2008). Bridging an IA Capability Gap. *Realising Network Enabled Capability (RNEC'08), NECTICE, Leeds, UK, 13 October 2008.* NECTISE Loughbourgh University.

Richardson, C. J. (2008). *Managing Information Security and its Assurance.* Blandford Forum: Defence College of Communications & Information Systems (DCCIS).

Richardson, C. J. (2008). *The IA Professional Framework - Draft White Paper.* Defence College of Communication and Information Systems (DCCIS), ICT Faculty. Blandford Forum: Cabinet Office.

Richardson, C. J. (2008b, October 20). Cyber Situational Awareness: The Assurance of Information Operations. *CISM MSc Lecture*. Blandford Forum, Dorset, UK: Defence College of CIS (DCCIS).

Richardson, C. J. (2009). A Holistic Approach to Effective Information Assurance Education. *Military Information Assurance and Security Symposium, MoD Abbey Wood, 16 April 2009.* Cobham Technical Services.

Richardson, C. J. (2009b, November 10). Computer Network Operations: Military Cyber Operations in Theatre. *CISM MSc Lecture*. Blandford Forum, Dorset, UK: Defence College of CIS (DCCIS).

Richardson, C. J. (2011). Cyberspace: The 5th Domain. *Cyber Security 2011, Brussels, Beliguim, 31 May- 1 June 2011.* IQPC.

Richardson, C. J. (2012, June 5). The Assurance of Socio-Technical Enterprise Operations. *MSc Information Assurance Module 2*. London, UK.

Rickards, D. A. (2010). *NO AIR: Cyber Dependency and the Doctrine Gap.* Naval War College, Joint Military Operations. Newport, RI: Defense Technical Information Center (DTIC).

Rid, T. R., & McBurney, P. (2012). Cyber-Weapons. *The RUSI Journal, 157*(1), 6-13.

Riechmann, T., & Hauck, F. J. (1998). Meta objects for access control: a formal model for role-based principals. *Proceedings of the 1998 ACM Workshop on New Security Paradigms* (pp. 30-38). Charlottesvillie, Virginia: Association for Computer Machinery (ACM).

Riggs, C. (2003). *Network Perimeter Security: Building Defence-In-Depth.* Auerbach Publications, Taylor & Francis Group, Informa plc.

Robb, J. (2007). *Brave New World.* John Wiley.

Robinson, C. L., Hughes, K. J., Staniforth, I., & Wiseman, S. (2003). *Classes of Security Functions for use with an Infosec Architecture Model.* Malvern, UK: QinetiQ,.

Robinson, M. (2012, June 26). Cyber terror threat to the UK. *DailyMail.co.uk/news*. London: The Daily Mail Online. Retrieved June 26, 2012, from http://www.dailymail.co.uk/news/article-2164780/Cyber-terror-threat-UK-industrial-scale--says-MI5-chief-reveals-company-lost-800-MILLION-result-state-sponsored-espionage.html

Rogers, J. (1997). *Sixteen Personality Types at Work in Organisations.* Management Futures Ltd.

Rogers, R. (1995). The psychological contract of trust – part II. *Executive Development, 8*(2), 7 - 15.

Rogers, R., & Devost, M. G. (2005). *Hacking a Terror Network: The Silent Threat of Covert Channels.* Syngress.

Ross, J. W., Weill, P., & Robertson, D. (2006). *Enterprise Architecture As Strategy: Creating a Foundation for Business Execution.* Cambridge, MA: Harvard Business School Press.

Rossel, P., & Finger, M. (2007). Conceptualizing e-Governance. In T. Janowski, & T. A. Pardo (Ed.), *Proceedings of the 1st International Conference on Theory and Practice of Electronic Governance* (pp. 399-407). Macao, China: ACM.

Rowley, B. (1995, April). *The Future Is Not What It Used To Be.* Retrieved March 15, 2011, from USAF Center for Strategy and Technology: http://www.au.af.mil/au/awc/awcgate/awc-ofut.htm

Rowlingson, R. (2005). Inside and out? The Information Security Threat From Insiders. *4th European Conference on Information Warfare and Security, University of Glamorgan, UK, 11-12 July 2005* (pp. 293-302). Academic Conferences Limited, Reading, UK.

Rubel, T. (2010, September). *Charting the Course of Government Transformation.* Retrieved April 18, 2011, from IDC Government Insights: http://www.emc.com/collateral/analyst-reports/10547-idc-charting-course-govt-trans-ar.pdf

Rubin, E. (2010). The Hidden Costs of Internal Clouds. (V. Vasquez, Ed.) *Cloudbook: The Cloud Computing & SaaS Information Resource, 1*(4).

Russell, G., & Russell, N. (1999). Cyberspace and School Education. *International Journal of Research & Method in Education, 22*(1), 7-17.

Salmela, H. (1997). From information systems quality to sustainable business quality. *Information and Software Technology, 39*(12), 819-825.

Sandhu, R. (2000). Engineering authority and trust in cyberspace: the OM-AM and RBAC way. *RBAC '00 Proceedings of the fifth ACM workshop on Role-based access control* (pp. 111 - 119). New York, NY: Association for Computing Machinery (ACM).

Sanes, K. (2008). *The Age of Stimulation.* Retrieved January 12, 2009, from Transparency now: http://www.transparencynow.com/

Savola, R. (2007). Towards a taxonomy for information security metrics. *Proceedings of the 2007 ACM workshop on Quality of protection* (pp. 28-30). ACM.

Saydjari, O. S. (2004, March). Cyber Defence: Art to Science. *Communications of the ACM, 47*(3), 53-57.

Scheffran, J. (2008). The complexity of security. *Complexity, 14*(1), 13-21.

Schiller, C. A., Binkley, J., Harley, D., & Evron, G. (2007). *Botnets: the Killer Web App.* Syngress Publishing, Inc., Elsevier.

Schiller, C. A., Binkley, J., Harley, D., Evron, G., Bradley, T., Willems, C., et al. (2007). *Botnets: The Killer Web App.* (C. A. Schiller, & J. Binkley, Eds.) Burlington, MA, USA: Syngress Publishing, Inc. Elsevier.

Schjolberg, S. (2005a). Law Comes to Cyberspace. *Proceedings Eleventh United Nations Congress on Crime Prevention and Criminal Justice, Bangkok, Thailand, 18-25 April, 2005.* United Nations Office on Drugs and Crime.

Schmidt, H. A. (2008). *Emerging Cyber Threats Report for 2009.* Georgia Tech Information Security Center.

Schneider, F. (1998). *Trust in Cyberspace.* Washington D.C.: National Academy Press .

Schneier, B. (1994). *Applied Cryptography.* John Wiley & Sons.

Schneier, B. (1996). *Applied Cryptography: Protocols, Algorithms and Source Code in C J* (2nd ed.). ohn Wiley and Sons.

Schneier, B. (2000). *Secrets and Lies: Digital Security in a Networked World.* John Wiley & Sons.

Schneier, B. (2006). *Beyond Fear:Thinking Sensibly About Security in an Uncertain World.* Springer Science.

Schneier, B. (2008). *Schneier on Security.* John Wiley & Sons.

Schneier, B., & Banisar, D. (1997). *The Electronic Privacy Papers.* John Wiley & Sons.

Schoder, D. (1999). *Navigation in Cyberspace -Using Multi-Dimensional Scaling to create three-dimensional navigational maps.* Institute for Information and Gesellschaft (IIG). Freiburg, Germany: University of Freiburg.

Schou, C. D., Kuehl, D., & Armistead, E. L. (2005). Information Operations Education: Lessons Learned from Information Assurance. *4th European Conference on Information Warfare and Security, University of Glamorgan, UK, 11-12 July 2005* (pp. 325-334). Academic Conferences Limited, Reading, UK.

Schuler, D., & Day, P. (2004). *Shaping the network society: the new role of civil society in cyberspace.* Cambridge, MA: The MIT Press.

Schwartau, W. (1996a). *Chaos on the Electronic Superhighway: Information Warfare.* New York, NY: Thunder's Mouth, Press.

Schwolow, S., & Jungfalk, M. (2010). *The Information Value Chain: Strategic Information Management for Competitive Advantage.* Copenhagen, Denmark: Copenhagen Business School.

Senge, P. (1990). *The Fifth Discipline: The Art & Practice of the Learning Organisation.* New York: Doubleday.

Senge, P. M., Kleiner, A., Roberts, C., Ross, R. B., & Smith, B. J. (1994). *The Fifth Discipline Fieldbook: Strategies and Tools for Building a Learning Organisation.* London: Nicholas Breadley Publishing.

Senge, P., Kleiner, A., Roberts, C., Ross, R., & Smith, B. (1994). *The Fifth Discipline: Strategies and tools for building a learning organization.* London: Brealey.

SFIA. (2010). *The Skills Framework for the Information Age, Version 4G.* London: SFIA Foundation .

Shannon, C. (1948, July & October). A Mathematical Theory of Communication. *Bell System Technical Journal, 27*(3 & 4), 379–423 & 623–656.

Sharma, D. (2010, April). Integrated Network Electronic Warfare: China's new concept of Information Warfare. (N. S. Sisodia, Ed.) *Journal of Defence Studies, 4*(2), 36-49.

Sharma, D. (2010b). Integrated Network Electronic Warfare: China’s New Concept of Information Warfare. (N. S. Sisodia, Ed.) *Journal of Defence Studies, 4*(2), 36-49.

Shatchman, N. (2010, June 21). *Darpa Taking Fire for Its Cyberwar Range*. Retrieved May 10, 2012, from Wired: http://www.wired.com/dangerroom/2010/06/darpa-taking-fire-for-its-cyberwar-range/

Shedroff, N. (1999). Information Interaction Design: Unified Theory of Design. In R. Jacobson, *Information Design* (pp. 267-292). Cambridge, MA: The MIT Press.

Shelton, C., & Darling, J. (2003). From Chaos to Order: Exploring New Frontiers in Conflict Management. *(Presented at the Midwest Academy of Management Conference, Kansas City* (pp. 1-17). Midwest Academy.

Shinder, D. (2011, February 28). *Cybercrime: Why it's the new growth industry*. Retrieved February 28, 2011, from TechRepublic: http://www.techrepublic.com/blog/security/cybercrime-why-its-the-new-growth-industry/5131

Sikich, G. W. (2003). *Integrated business continuity: maintaining resilience in uncertain times.* Tulsa: PennWell Corporation.

Singel, R. (2010, March 4). *White House Cyber Czar: ‘There Is No Cyberwar’*. Retrieved March 5, 2010, from Wired: http://www.wired.com/threatlevel/2010/03/schmidt-cyberwar/

Skoudis, E. (2002). *Counter Hack: A step-by-step Guide to Computer Attacks and Effective Defenses.* Prentice Hall series in Computer Networking and Distributed Systems, Prentice Hall PTR.

Sledge, C. (2006). *Information Assurance: Building Educational Capacity.* The Software Engineering Institute. Pittsburgh, PA: Carnegie Mellon University.

Smart, P. R., & Shadbolt, N. R. (2007). The Semantic Battlespace Infosphere: A Knowledge Infrastructure for Improved Coalition Interoperability. *International Conference on Integration of Knowledge Intensive Multi-Agent Systems, KIMAS 2007, 30 April- 3 May, 2007* (pp. 390-395). Waltham, Massachusetts: IEEE.

Smith, D. B. (2005). *Introducing a Guide to Interoperability.* Software Engineering Institute. Pittsburg: Carnegie Mellon University.

Smith, E. (2003). *Effects Based Operations: Applying Network Centric Warfare in Peace, Crisis, and War.* Office of the Assistant Secretary of Defense. Washington DC.: Command and Control Research Program (CCRP), DoD.

Snyder, R. (2006). Ethical hacking and password cracking: a pattern for individualized security exercises. *Proceedings of the 3rd annual conference on Information security curriculum development. Kennesaw, Georgia, 22-23 September, 2006* (pp. 13--18). ACM.

Söderström, E. (2009). Trust Types: An Overview. In G. Dhillon (Ed.), *Proceedings of the 8th Annual Security Conference Discourses in Security Assurance & Privacy Las Vegas, NV, USA, 15-16 April, 2009. 12*, pp. 1-14. Virginia Commonwealth University.

Sogge, D. (2011). New organisational frameworks: the importance of joint action. *Coordinadora de ONG para el Desarrollo-España, 17-18 May*, (pp. 1-10). Madrid.

Soliman, K. S., & Janz, B. D. (2004, July). An exploratory study to identify the critical factors affecting the decision to establish Internet-based interorganizational information systems. *Information & Management, 41*(6), 697-706.

Solomon, M. G., & Chapple, M. (2005). *Information Security Illuminated.* Jones and Bartlett Illuminated Series, Jones and Bartlett Publishers, Inc.

Sommer, P., & Brown, I. (2011). *Reducing Systemic Cybersecurity Risk.* Paris, France: The Organisation for Economic Co-operation and Development.

Spar, D. (1999). The Public Face of Cyberspace. In I. Kaul, I. Grunberg, & M. A. Stern (Eds.), *Global Public Goods - International Cooperation in the 21st Century* (pp. 344-353). Oxford, UK: The Oxford University Press.

Spivack, N. (2007). *Making Sense of the Semantic Web. 2007-10-21).* Retrieved June 10, 2009, from 2009-10-20 http://novaspivack. typepad. com/nova_spivacks_weblog/files/nova_spivack_semantic_web_talk. ppt.

Srimoolanathan, B. (2011). *Cyber Security – From Luxury to Necessity.* London: Frost & Sullivan.

Stahl, B. C. (2005). Chapter X: Responsibility for Information Assurance and Privacy. In M. A. Mahmood, *Advanced Topics in End User Computing* (Vol. 4, pp. 186-207). London, UK: Idea Group Publishing.

Stallings, W. (2000a). *Business Data Communications* (5th ed.). Prentice Hall, Pearson Education, Inc.

Stallings, W. (2000b). *Local and Metropolitan Area Networks* (6th ed.). Prentice Hall, Pearson Education, Inc.

Stallings, W. (2001). *High-Speed Networks and Internets* (2nd ed.). Prentice Hall, Pearson Education, Inc.

Stallings, W. (2003). *Computer Networks with Internet Protocols and Technology.* Prentice Hall, Pearson Education, Inc.

Stallings, W. (2004). *Wireless Communications and Networks* (2nd ed.). Prentice Hall, Pearson Education, Inc.

Stallings, W. (2005). *Computer Organisations and Architecture* (7th ed.). Prentice Hall, Pearson Education, Inc.

Stallings, W. (2006a). *Cryptography and Network Security: Principles and Practices* (4th ed.). Prentice Hall, Pearson Education, Inc.

Stallings, W. (2006b). *Network Security Essentials* (2nd ed.). Prentice Hall, Pearson Education, Inc.

Stallings, W. (2007). *Operating Systems* (5th ed.). Prentice Hall, Pearson Education, Inc.

Stallings, W. (2010). *Data and Computer Communications* (9th ed.). Prentice Hall, Pearson Education, Inc.

Starr, S. (2008). Towards a Preliminary Theory of Cyberpower. In F. D. Kramer, S. H. Starr, & L. Wentz (Ed.), *Proceedings International Command and Control Research and Technology Symposia (ICCRTS 2008), Seattle, WA., 17-19 June, 2008* (pp. 43-90). National Defence University and Potomac Books.

Starr, S. H. (2009). *Toward a Preliminary Theory of Cyberpower.* (F. D. Kramer, S. H. Starr, & L. K. Wentz, Eds.) Washington D.C.: National Defense University Press and Potomac Books.

Stavridis, J. G., & Parker, E. C. (2012, April). *Sailing the Cyber Sea*. Retrieved May 15, 2012, from Joint Forces Quarterly: http://www.ndu.edu/press/jfq-65.html

Steane, A. (1998). Reports on Progress in Physics. *Quantum Computing*, 119.

Steele, R. D. (2006, February). *Information Operations: Putting the "I" back into DIME.* U.S. Army War College, Strategic Studies Institute. Carlisle, PA: The Strategic Studies Institute.

Steinberg, A. N., Bowman, C. L., & White, F. E. (1999). *Revisions to the JDL Data Fusion Model.* Arlington, VA: Environmental Research Inst of Michigan.

Sterner, E. (2011, Spring). Retaliatory Deterrence in Cyberspace. *Strategic Studies Quarterly, 5*(1), 62-80.

Sterner, E. (2011). *Wikileaks and Cyberspace Cultures in Conflict.* The George C. Marshall Institute, Arlington, VA.

Stevens, T. (2009). Cyberspace and Security: Issues and Concerns. *World Defence Systems*, 248-251.

Strang, T., & Linnhoff-Popien, C. (2004). A Context Modeling Survey. In D. De Roure, & J. Indulska (Ed.), *1st Int. Workshop on Advanced Context Modelling, Reasoning and Management, Nottingham, UK, 7-8 September 2004.*

Stvilia, B., Twidale, M. B., & Smith, L. C. (2006). *Assessing information quality of a community-based encyclopedia.* Champaign, IL: University of Illinois.

Suler, J. (2004, June). The Online Disinhibition Effect. (B. K. Wiederhold, Ed.) *CyberPsychology and Behavior, 7*(3), 321-326.

Suri, N., Benincasa, G., Formaggi, S., Winkler, R., Choy, S., Kovach, J., et al. (2008). DisService: A Peer to Peer Information Dissemination Service for Tactical Environments. *Proceedings of the 2008 Meeting of the Military Sensing Symposia (MSS), Nellis AFB, NV, February, 2008.* Speciality Group on Battlespace Accoustic and Seismic Sensing (BAMS 2008).

Sushil, J., Liu, P., Swarup, V., & Wang, C. (2010). Overview of Cyber Situational Awareness. *Cyber Situational Awareness: Advances in Information Security, 46*, 15-35.

Suzić, R., & Yi, C.-h. (2008). Information Exchange Requirements (IER) and Information Exchange Models (IEM). In J.-P. Bourey, & R. G. Seguer (Ed.), *Proceedings of MDISIS, Montpellier, France, 16 June 2008. 340*, pp. 31-45. CEUR Workshop Proceedings.

Swanson, M., & Guttman, B. (1996). *NIST SP 800-14: Generally Accepted Principles and Practices for Securing Information Technology Systems.* National Institute of Standards and Technology Technology Administration, U.S. Department of Commerce. Gaithersburg, MD: NISP.

Tait, A. (2010). *G-Cloud Founding Principles.* London: Cabinet Office.

Talevski, A., Chang, E., & Dillon, T. S. (2005, May). Reconfigurable Web service integration in the extended logistics enterprise. *Industrial Informatics, 1*(2).

Tapscott, D., Williams, A. D., & Herman, D. (2008, January). *Government 2.0: Transforming Government and Governance for the Twenty-First Century.* Retrieved March 15, 2011, from Google Academia: http://google.academia.edu/DanHerman/Papers/378095/Government_2.0_Transforming_Government_and_Governance_for_the_Twenty-First_Century

Task Force on National Security in the Information Age. (2002). *ProtectingAmerica's Freedom in the Information Age.* New York, NY: The Markle Foundation.

Taylor, B., & Azadegan, S. (2006). Threading secure coding principles and risk analysis into the undergraduate computer science and information systems curriculum. *Proceedings of the 3rd annual conference on Information Security Curriculum Development (InfoSecCD). Kennesaw, Georgia, USA, 22-23 September, 2006* (pp. 24-29). ACM.

The Economist. (2010, July 1). *Cyberwar: It is time for countries to start talking about arms control on the internet*. Retrieved July 15, 2010, from The Economist: http://www.economist.com/node/16481504?story_id=16481504&source=features_box1

The US National Security Council. (2008). *The Comprehensive National Cybersecurity Initiative.* Washington, D.C.: The White House.

The US National Security Council. (2011). *The International Strategy for Cyberspace.* Washington, D.C.: The White House.

The White House. (2011). *The Strategy to Combat Transnational Organised Crime: Addressing Converging Threats to National Security.* Washington, DC: The White House.

Thomas, S. (2009a). *Collaboration without Boundaries, Cross-Domain Solutions for Network-Centric Operations.* Fairfax, VA: Trident Systems Inc.

Thomson, K. (2009). Information Security Conscience: a precondition to an Information Security Culture? In G. Dhillon (Ed.), *Security, Assurance and Privacy: Organizational Challenges Proceedings of the 8th Annual Security Conference Discourses in Security*

Assurance & Privacy Las Vegas, NV, USA April 15-16, 2009.

Tipton, H. F., & Krause, M. (2008). *Information Security Management Handbook* (6th ed.). Auerbach Publications, Taylor & Francis Group, Informa plc.

Toffler, A., & Toffler, H. (1980). *The Third Wave.* New York: William Morrow and Co.

Tolk, A. (2001). Computer Generated Forces –Integration into the Operational Environment. *Simulation of and for Military Decision Making, Rome, Italy, 15-16 October 2001. 9*, pp. 1-18. NATO Research and Technologies Organisation.

Tolk, A. (2003). Beyond Technical Interoperability – Introducing a Reference Model for Measures of Merit for Coalition Interoperability. *Proceedings of the 8th International Command and Control Research and Technology Symposium, National Defense University, Washington, DC, 17-19 June, 2003.* (pp. 1-24). DoD CCRP.

Tolk, A. (2003). Beyond Technical Interoperability – Introducing a Reference Model for Measures of Merit for Coalition Interoperability. *8th International Command and Control Research and Technology Symposium, National Defense University. Washington, 17-19 June, 2003* (pp. 1-47). Defense Technical Information Center (DTiC).

Tolk, A. (2003). Beyond Technical Interoperability: Introducing a Reference Model for Measures of Merit for Coalition Interoperability. *Proceedings of the Command and Control Research and Technology Symposium (CCRTS).* Washington, DC: CCRP Press.

Tolk, A., & Kunde, D. (2010, November 25). Decision Support Systems - Technical Prerequisites and Military Requirements. *Computing Research Repository (CoRR).*

Tolk, A., & Muguira, J. (2003). The Levels of Conceptual Interoperability Model (LCIM). *Proceedings IEEE Fall Simulation Interoperability Workshop.* Orlando, Fl.: IEEE CS Press.

Tremaine, R. L. (2010, August). Demonstrating Cyberspace Superiority in an Acquisition World. (N. Sage, Ed.) *High Frontier: The Journal for Space & Missile Professionals, 6*(4), 62-65.

Trist, E. (1981). The Sociotechnical Perspective: The Evolution of Sociotechnical Systems as a Conceptua Framework and as an Action Research Program. In A. H. Van de Ven, & W. F. Joyce, *Perspectives on organization design and behavior* (pp. 19-75). New York: John Wiley & Son.

Trost, R. (2010). *Practical Intrusion Analysis: Prevention and Detection for the Twenty-First Century.* Addison-Wesley, Pearson Education, Inc.

Tudor, J. (200). *Information security architecture: An integrated approach to security in the organisation.* Auerbach Publications, Taylor & Francis Group, Informa plc.

Tullao, T. S. (2003). *Education & Globalization.* Makati City, Philippines: Philippine Institute for Development Studies (PIDS).

Twitchell, D. P. (2006). Social engineering in information assurance curricula. *Proceedings of the 3rd annual conference on Information security curriculum development, Kennesaw, Georgia, 23-24 September 2006* (pp. 191--193). ACM.

UKAS. (2002). *UKAS Guidance for bodies operating certification of Trust Service Providers seeking approval under tScheme.* London: The United Kingdom Accreditation Service (UKAS).

UN. (2004). *A more secure world: Our shared responsibility.* United Nations, International Coalition for the Responsibility to Protect. New York: United Nations Department of Public Information.

United Nations. (2004). *A More Secure World: Our Shared Responsibility.* New York, NY: UN.

United Nations. (2010). *Cyber security: emerging threats and challenges, ECOSOC General Segment briefing.* New York, NY: UN.

US Congress. (2012). *Cyber Security.* Congressional Record, US Senate, Washington, DC.

USAF. (2008). *Air Force Doctrine Document 2-11: Cyberspace Operations.* Air Force Doctrine Center. Maxwell AFB, AL: Air University Press.

USN. (2010). *Computer Network Defense .* Proactive Computer Network Defense and Information Assurance (CND/IA) Programme, Department of the Navy: Science and Technology. Arlington, VA: Office of Naval Research.

VADM Brown, N. E. (2009, May). Difficulties encountered as we evolve the Cyber Landscape for the military. (N. Sage, Ed.) *High Frontier: The Journal for Space & Missile Professionals, 5*(3), 6-8.

van den Berg, R. (2010). The 21st Century Battlespace: The Danger of Technological Ethnocentrism. (D. Bashow, Ed.) *Canadian Military, 10*(4).

Van Grembergen, W. (2004). *Strategies for information technology governance.* London: Idea Group Inc.

Van Grembergen, W., & Dehaes, S. (2007). *Implementing Information Technology Governance: Models, Practices and Cases.* Hershey, PA: IGI Publishing.

Van Oranje-Nassau, C., Krapels, J., Botterman, M., & Cave, J. (2009). *The Future of the Internet Economy.* Cambridge: RAND Europe.

van Swaay, M. (1992). How shall we manage cyberspace and its growing population? *CSC '92 Proceedings of the 1992 ACM annual conference on Communications* (pp. 559--). Kansas City, Missouri: The Association for Computing Machinery (ACM).

VanVactor, J. D., & Gill, T. (2010, March). Comparing military and civilian critical thinking and information processes in operational risk management: What are the lessons? *Journal of Business Continuity & Emergency Planning, 4*(2), 97-112.

Vatis, M. (2001). *Cyber Attacks During the War on Terrorism: A Predictive Analysis.* Institute for Security and, Technology Studies. Dartmouth College.

Vego, M. N. (2006). Effects Based Approach. (M. E. Krause, Ed.) *Joint Force Quarterly (JFQ), 2*(41), 51-57.

Vego, M. N. (2006). Effects Based Operations: A critique. *Joint Forces Quarterly, 41*, 51-57.

Verkhovsky, B. (2008). Information assurance protocols: Efficiency analysis and implementation for secure communication. *Journal of Information*

Assurance and Security, Dynamic Publishers Inc.

Vice Adm. Cebrowski, A., & Gartska, J. (1998, January). Net-Centric Warfare: Its Origin and Future. *Proceedings Magazine, 124*(1), pp. 28-35.

Vidalis, S., Jones, A., Blyth, A., & Thomas, P. (2004). Assessing Cyber Threats in the Information Environment. *Journal of Network Security, 11*, 10-11.

Vidanage, H. (2009). The Sri-Lankan Case. In A. Karatzogianni (Ed.), *Cyber-Conflict and Global Politics:* (pp. 146-161). Abingdon, Oxon, UK: Routledge.

Vietmeyer, R. (2004). Net-centric Enterprise Services. *Boundaryless Information Flow Conference.* Boston, MA: DoD DISA.

Wacker, A., Schiele, G., Schuster, S., & Weis, T. (2008, December). Towards an authentication service for Peer-to-Peer based Massively Multiuser Virtual Environments . *Int. J. Adv. Media Commun., 2*(4), 364--379.

Waltz, E. (1999). *Information Warfare: Principles and Operations.* Artech House Publishers.

Wang, R. Y. (2005a). *Information Quality (Advances in Management Information Systems).* (R. Wang, E. Pierce, S. Madnick, & C. Fisher, Eds.) M.E. Sharpe.

Wang, Y. D., & Emurian, H. (2005). An overview of online trust: Concepts, elements, and implications. *Computers in Human Behaviour, 21*, 105-125.

Watts, B. (2008). *What are today's social evils?* York: Joseph Rowntree Foundation.

Weaver, N., Paxson, V., Staniford, S., & Cunningham, R. (2003). A Taxonomy of Computer Worms. *Proceedings of the 2003 ACM Workshop on Rapid Malcode (WORM), Washington DC, 27 October 2003* (pp. 11-18). ACM.

Weckert, J. (2005). Five: Trust in Cyberspace. In R. J. Cavalier, *The impact of the Internet on our moral lives* (pp. 95-120). Albany, NY: State of University New York Press.

Wentz, L. K., Barry, C. L., & Starr, S. H. (2009). *Military Perspectives on Cyber Power.* Washington, DC: Center for Technology and National Security Policy at the National Defense University.

WFS. (2009). The Erice Declaration on Principles for Cyber Stability and Cyber Peace. *42nd Session of the International Seminars on Planetary Emergencies, Erice, Sicily, 20 August,2009.* Permanent Monitoring Panel on Information Security of the World Federation of Scientists.

Wheatley, M. J. (2006). *Leadership and the new science: discovering order in a chaotic world.* San Francisco, CA: Berrett-Koehler.

Wheatley, M. J. (2006a). *Leadership and the New Science: Discovering Order in a Chaotic World* (3rd ed.). Berrett-Koehler Publishers, Inc.

Whitaker, A., Evans, K., & Voth, J. B. (2009). *Chained Exploits: Advanced Hacking Attacks from Start to Finish.* Addison-Wesley, Pearson Education, Inc.

Whitman, M. E. (2004). In defense of the realm: understanding the threats to information security. (P. Hills, Ed.) *International Journal of Information Management, 24*(1), 43-45.

Whitman, M. E., & Mattord, H. J. (2006). *Hands-on Information Security Lab Manual* (2nd ed.). Course Technology, Cengage Learning.

Whitman, M. E., & Mattord, H. J. (2006). *Readings and Cases in the Management of Information Security.* Course Technology, Cengage Learning.

Whitman, M. E., & Mattord, H. J. (2008). *Management of Information Security* (2nd ed.). Course Technology, Cengage Learning.

Whitman, M. E., & Mattord, H. J. (2009). *Principles of Information Security* (3rd ed.). Course Technology, Cengage Learning.

Wikipedia. (2011, May 5). *Information Technology Infrastructure Library*. Retrieved May 10, 2011, from Wikipedia: http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library

Wiles, J. (2007). *Techno Security's Guide to E-Discovery and Digital Forensics.* Syngress Publishing, Inc., Elsevier.

Willett, K. D. (2008). *Information Assurance Architecture.* Boca Raton, FL: CRC Press, Taylor & Francis Group.

Williams, B. T. (2002). *Effects-Based Operations:Theory, Application and the Role of Airpower.* USAWC Strategy Research Project. Carlisle Barrack, PA: U.S. Army War College.

Williams, D. G. (1969). Official Secrecy in England. *Federal Law Review , 3*(1).

Wilson, C. (2006). *Information Operations and Cyberwar: Capabilities and Related Policy Issues.* The Library of Congress. Washington, DC: Congressional Research Service.

Wilson, C. (2007). *Network Centric Operations: Background and Oversight Issues for Congress.* Congressional Research Services, Technology and National Security, Foreign Affairs, Defense, and Trade Division. Washington D.C.: US House of Congress.

Wilson, C. (2007). *Network Centric Operations: Background and Oversight Issues for Congress.* Congressional Research Services, Technology and National Security, Foreign Affairs, Defense, and Trade Division. Washington D.C.: US House of Congress.

Wilson, T. D. (2002a). *Strangers to Ourselves: Discovering the Adaptive Unconscious.* Cambridge, MA: Belknap Press.

Winkler, V. J. (2011). Operating a Cloud. *Securing the cloud*, 253-277.

Winn, J. K. (1997). Open Systems, Free Markets, and Regulation of Internet Commerce. *Tulane Law Review, 72*, 1177.

World Economic Forum. (2012). *Global Risks 2012 - Seventh Edition.* Geneva: The World Economic Forum.

Wray, S. (2011). *Tyrants and Hackers.* Bournemouth, UK.

Wu, B., Wu, J., Fernandez, E. B., & Magliveras, S. (2005). Secure and Efficient Key Management in Mobile Ad Hoc Networks. *roceedings of the 19th IEEE International Parallel and Distributed Processing Symposium (IPDPS'05) - Workshop 17. 18*, pp. 288.1-. Washington D.C.: IEEE Computer Society.

Wylder, J. (2004). *Strategic Information Security.* Auerbach Publications, Taylor & Francis Group, Informa plc.

Yeung, R. W. (2002). *A First Course in Information Theory.* (J. K. Wolf, Ed.) New York, NY: Kluwer Academic, Springer.

YÖN, H., & Aydinli, E. (2011). Transgovernmentalism Meets Security: Police Liaison Officers, Terrorism, and Statist Transnationalism. *Governance, 24*(1), 55-84.

Zachman, J. (2002). *The Zachman Framework™: The Official Concise Definition.* Zachman International.

Zack, M. H. (1999, Summer). Managing Codified Knowledge. *MIT Sloan Management Review, 40*(4), 45-58.

Zakaria, O. (2005). Information Security Culture and Leadership. *4th European Conference on Information Warfare and Security, University of Glamorgan, UK, 11-12 July 2005* (pp. 415-). Academic Conferences Limited, Reading, UK.

Zegura, E., Calvert, K., & Bhatta, S. (1996). How to Model an Internetwork. *Proceedings IEEE INFOCOM '96, The Conference on Computer Communications, Fifteenth Annual Joint Conference of the IEEE Computer and Communications Societies, Networking the Next Generation, San Francisco, CA, 24-28 March, 1996. 2*, pp. 594--602. IEEE.

Zeilinger, A. (2002, March 25). *Zeilinger, A. (2002), "Why the Quantum? It from Bit? A Participatory Universe?," The Global Spiral, Metanexus Online, March 25, 2002, p.3.* (J. Levine, Ed.) Retrieved November 15, 2010, from Information Realism: Quantum Bit in the Cyber space: http://www.digicult.it/digimag/article.asp?id=1852

Zimet, E., Barry, C. L., Smith, J. G., Brown, M. A., Hare, F. B., Zimmerman, G., et al. (2009). *Military Perspectives on Cyberpower.* (L. K. Wentz, C. L. Barry, & S. H. Starr, Eds.) Washington, D.C.: Institute for National Strategic Studies (INSS).

Zittrain, J. (2008). *The Future of the Internet—And How To Stop It.* London: Allen Lane.

Zohar, D. (1997). *Rewiring the Corporate Brain: Using the New Science to Rethink How We Structure and Lead Organizations* (1st ed.). Berrett-Koehler Publishers.

Zohar, D., & Marshall, I. N. (1990). *The Quantum Self - Human Nature And Consciousness Defined By The New Physics.* William Morrow & Co, Inc.

Zorz, Z. (2011, April 21). Why do governments have trouble retaining cyber warriors? *Help Net Security*.