Economic Information Warfare

Analysis of the relationship between the protection of Financial Information Infrastructure and Australia's National Security

By

Robert Luke Deakin

Bachelor of Business *(QUT)* – 1992

Graduate Certificate *(QUT)* – 1993

Principal Supervisor:

Professor William Caelli

Thesis submitted in accordance with the regulations for Degree of Master of Information Technology

Information Security Research Centre
Faculty of Information Technology
Queensland University of Technology

June 2003

Contents

List of Figures

Declaration

The work contained in this thesis has not been previously submitted for a degree or diploma at any higher education institution. To the best of my knowledge and belief, the thesis contains no material previously published or written by another person except where due reference is made.

Signed: . . . . . **Date:** . . . . . .

Acknowledgments

This work would have been unattainable were it not for the guidance, support and encouragement of my principal supervisor, Professor Bill Caelli. I would like to acknowledge Bill for his inspiration: it has been an honour to work with him.

I would like to thank the Australian information security community for the time and co-operation I have received. The time they have generously shared has given me a further insight into the contemporary workings and problems in protection of our National Information Infrastructure.

Special thanks must go to my close friends, for their understanding, suggestions and assistance during the extended period I have been focusing on this thesis, instead of focusing on them. I wish to thank my family and especially my parents for their support throughout the many years of education, which preceded this work.

Finally, I wish to express my deepest gratitude to my wife, Colleen, for her incredible patience, devotion and loving encouragement, especially over the many weekends I have been exiled in the study, researching and writing this thesis.

Abstract

The thesis presents an argument for the re-alignment of Australia's National Security efforts so that they mirror the changes occurring in our economy and society. Specifically, it seeks outcomes that can focus our efforts in protecting the critical infrastructure including our financial information infrastructure, from new and emerging threats.

The thesis presents a definition of security as it applies to the Nation-State and provides the evidence of the changes in conflict and global security. It outlines the changes in the National Security environment and identifies emerging forms of conflict that effect national economic systems, and financial information infrastructures. It shows how the traditional view of National Security is being eroded by the Information Age. To support this argument a view of the key forces that are changing weapons, warfare, and approaches to National Security are provided. The thesis presents a view of the unconventional threats to economic systems. In particular, it describes the targeting of critical national information infrastructures including energy, banking and finance, transportation, vital human services, and telecommunications.

The thesis outlines concern regarding the vulnerability of developed nations' social structures through increasing dependence on information and communications technology (ICT) systems, and the small population of specialist that support and protect it. The thesis argues that this dependency exposes national and global economies to new threats and forms of attack.

The thesis consists of an overview of the evolution National Security approaches. In particular, it examines collective security and security concepts as they relates to the Nation-State. It identifies a number of drivers, which outline the changing nature of the global security environment. The thesis describes asymmetric warfare and discusses Information Warfare (IW), describing its elements and goals. An analysis of offensive and defensive information warfare, strategies, and operations is provided. This is then related to economic systems and how they have featured in conflicts between nations throughout history. The information and communications technology (ICT) that underpin the financial environment (in particular payment systems) are reviewed and the thesis closes by focusing on the elements of economic infrastructure assets and types of attacks from which they require protection.

We conclude that the challenges for Critical Infrastructure protection in Australia are daunting and a number of recommendations are made that should be considered in light of the rapidly changing security environment. The challenges of Information Warfare will stretch Australia's resources, require re-conceptualising of our national defence forces, greater participation of the private sector, and changes in our daily lives.

Chapter 1. **Introduction**

"If man does not give thought to problems which are still distant, he will be worried by them when they come nearer".

Confucius

Chapter Overview

This chapter provides a statement of the thesis objectives. We provide a brief background to the topic of the thesis and then describe the structure of the document. This chapter serves to orient readers to the dimensions of the topic and give them a high level understanding of the arguments within each chapter.

1.1 Thesis objective

This thesis presents an argument for the re-alignment of Australia's National Security efforts so that they mirror the changes occurring in our economy and society. Specifically, we seek to recommend outcomes that can focus our efforts in protecting the critical infrastructure including our financial information infrastructure, from new and emerging threats.

1.2 Australia's Security

At this time, Australia stands as one of the healthiest, most knowledgeable and richest places on earth, according to the United Nations[1]. The United Nations view serves to remind us that abstract economic growth figures are a poor measure unless they translated into individual well-being and the quality of people's lives.

Our current standing reminds Australians of the sacrifices that our predecessors have made: to understand our place in the world and to appreciate the gains this nation has achieved in our short history. The development of Australian society cannot be taken for granted and requires all citizens to play their part in enhancing it further and securing the wealth, we have built.

To preserve and enhance the security of our Nation we are wise to prepare for (and where possible pre-empt) the challenges and opportunities of the future. History provides us with many valuable lessons from which we can learn when we come to face new threats. We should recognise that our society and our conceptualisation of security are evolving driven by the "Information Age"[2] and the age's unprecedented threats.

In this thesis we will consider one area of concern that is changing rapidly and has the potential to change the effectiveness of our current National Security efforts. Our area of study focuses on the changing dynamics amongst economic systems, financial infrastructures, and emerging forms of conflict. Within this dynamic, we will consider how traditional views of National Security are being undermined as the Information Age takes hold.

This thesis provides a description of some of the key forces that are changing weapons, warfare, and National Security approaches. We explore unconventional threats to our economic systems, in particular the targeting of critical national information infrastructures. These critical infrastructures include energy, banking and finance, transportation, vital human services, and telecommunications.

---

[1] Human Development Index (HDI) is published in the United Nations Development Program's - Human Development Report that has been published every year since 1990. By analysing 162 nations, it identifies the World's most desirable countries to live. In 2001, Australia was surpassed only by Norway, with Canada in third place, followed by Sweden, Belgium and then the U.S.A.. The HDI index is made up of three components - health, measured by life expectancy: education, measured by literacy and enrolment levels: and income measured by GDP per capita. Australia was ranked fifth in terms of life expectancy (78.8 years), enjoys a 99% literacy rate and the highest combined primary, secondary and tertiary gross enrolment ratio in the world, and the 12th highest GDP per capita income ($US 24,574). See http://www.undp.org

[2] The Term Information Age was described by Toffler, A., The Third Wave, New York: Bantam, 1980, describing a new age that is replacing that of the Industrial Age. The Information Age is described in more detail in section 3.2 Third Wave War on page 3-23

Australia's critical information infrastructure is highly complex. This can be seen in Figure 1, which is an illustration of the major telecommunications networks and other strategic resources[3] within Australia. This illustration depicts the scale of the infrastructure, especially its vast geographic footprint. Devising a strategy to manage vulnerabilities in such a complex system presents our national security planners with a significant challenge.

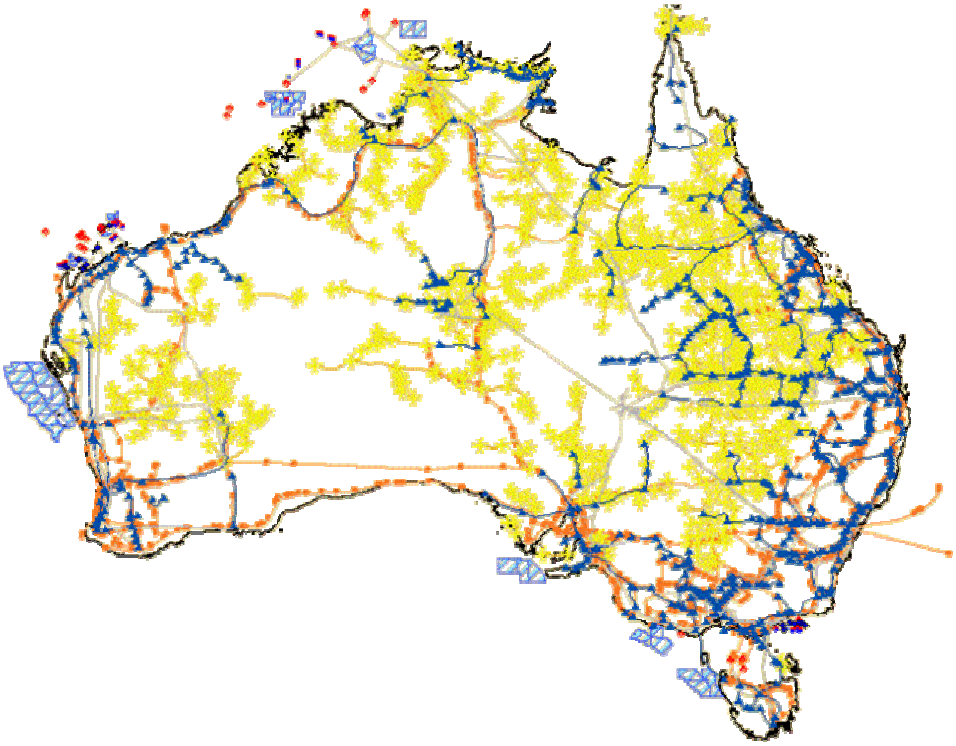


Figure 1 Australia's National Information Infrastructure[3]

The analysis in this thesis has resulted in a re-thinking of the way that information supports our social structures, in particular how critical information is conveyed through pricing of goods and services. The information conveyed by price quantifies and represents effort, value and a host of other signals, which contribute to efficient economies and social welfare. Price is most often settled with the exchange of money, which again we contend is a much

[3] This illustration was exported from a ArcInfo GIS (Geographic Information System) map assembled by the Author using GIS Data & Imagery from a number of sources. These include; AUSLIG (now Geoscience Australia), Australian Communications Authority Radiocommunications Record of Licences (RRL) Database, Street Directories and Government Mapping Agencies

more fundamental instrument than the paper or electronic forms that are used in its payment systems. Money can be seen as a representation used to convey the critical information, that of price and value. In the new information economy, money and price are no more than information, and it is the use of information itself which we view as the source of power: the power of the information age that fundamentally impacts our social structures and National Security.

It should be a concern to all developed nations that the vulnerabilities of our social structures are increasing through our dependence on information and communications technology (ICT) systems, and the small population of specialists that support and protect it. This dependency exposes our national and global economies to new threats and forms of attack.

1.3 Structure of the thesis

In the first sections of the thesis, the reader is provided with the background to the National Security by providing an overview of the fundamentals of security. In Chapter 2, National Security Background, the views of security as it relates to individuals within a community are defined. From this we expand our argument to define the various security functions that a Nation-State (or any interest group) may provide to its citizens. In particular, we examine collective security and the concept of security as it relates to the Nation-State. From these fundamental functions, we can focus on one aspect of security by charting the evolution of the conceptual frameworks used in the study of Nation-State relations.

Following the background provided on national security, we use Chapter 3, Analysis of Conflict, to demonstrate the events that occur when relationships between communities breakdown. These breakdowns may then escalate to periods of warfare. We will then show that the very nature of conflicts are changing, and we present our view of the dimensions of this change. These dimensions consist of a collection of forces, trends, problems, actors and other influences. We argue that these dimensions are the origins of our most significant contemporary vulnerabilities and dramatically impact our collective security. Therefore, we argue that they should be central to future security planning. A number of drivers are identified which outline the changing nature of the global environment and the risks that security resources must be aligned with. Concepts of future forms of war and weapons are then developed, including the increasing focus on asymmetric tactics to circumvent conventional security efforts. This includes introducing the central war form discussed in this thesis, information warfare.

In Chapter 4, Taxonomy of Information Warfare, we describe the elements of information warfare and its goals. We provide an analysis of offensive and defensive information warfare, strategies, and operations. We identify the elements and goals of information warfare so that it is clear how this form of war may impact on economic systems during conflicts. We present the significant contemporary taxonomies of information war, seeking to extract the key offensive and defensive strategies, tactics and operations. Based on this analysis we argue that this increasingly important form of war will require a re-alignment and focusing of our counter-measures and security structures.

To show how Governments are responding to the security dimensions we described earlier, Chapter 5, Review of Policy, details examples of government policy responses, particularly the threats to information systems. We demonstrate the high level of concern that developed nations (especially the United States) have about scenarios that involve in attacks on information infrastructure and Information Warfare. We detail the initiatives and policy that attempt to protect critical infrastructures from cyber attack both in Australia and in other nations.

Chapter 6, Analysis of Financial Information Infrastructure components, provides our framework for understanding the properties of economic systems that information warriors may seek to strike or shield. This analysis of financial information infrastructures supports our view of the relationships between economic processes, security and war. In particular, an outline if provided of how a community may achieve security through an efficient financial information infrastructure. This analysis focuses on the support and advancement that economic systems gives a society and dissects economic models to identify supporting infrastructures, such as flows of information and use of money. We show how economic systems give large communities, Nation-States and other interest-groups, the much needed capability to acquire resources, improve efficiency, and the maximising opportunities for future wealth creation. This wealth in turn enables the communities to protect and promote its religious, ideological, political and ethnic interests. Conversely, it is demonstrated how the weaknesses or collapse of economic infrastructure can precipitate uncertainty, difficulty and undermine the national interest.

Chapter 7, Analysis of Economic Information Warfare, provides our analysis of the strategy, operations and tactics that threaten critical economic systems of the Nation-State. We outline the broad range of activities that we believe exist on the spectrum of Economic War. In our argument, we assert that interference with economic effectiveness and efficiency of the adversaries' economic processes should be considered in the same light as conventional military strikes. In conjunction, we identify the need to protect our economic system with the same discipline and vigilance that we apply to traditional defence area such as border protection. We have identified eight hazards that impact the

security of financial infrastructure. Each of the hazards identified are inherent or systemic in nature, resulting from the processes that money and payment infrastructure play within a large-scale economy.

In the context of National Security and economic warfare, we argue that adversaries can seek to manipulate, leverage and multiply these hazards to support their objectives and interests. We then provide examples of how economic systems have been a feature of conflict between nations throughout history. Having identified the objectives hazards of the information warfare, we provide our categorisation of economic warfare tactics and the three realms; physical, information infrastructure and perceptual within which economic wars are fought. We then outline the capabilities required for mounting a comprehensive Economic Information War within the context of each realm (or battle space). We further consider how these elements may be attacked both directly and indirectly. The destabilisation, disruption, or collapse of financial systems has the potential to directly affect our level of National Security through the flow-on impacts on government, business, and the individual. We note that the private sector provides the majority of the critical systems that enable households, businesses and governments to efficiently exchange goods and services across our various markets. We also consider the changing market pressures and the potential for conflicts between corporations, regulators, and the public. ***Confidence*** in these systems is a fundamental element in the success of Australia's Economy.

In the final chapters, we provide recommendations and a summary of our conclusions for protection the Financial Information Infrastructure in Australia. Our conclusions provide a number of recommendations to address the rapidly changing security environment described in earlier chapters. We recap the challenges of Information Warfare that will stretch Australia's resources, requiring re-conceptualisation of our national defence forces, greater participation of the private sector, and changes in our daily lives.

Chapter 2. National Security Background

Chapter Overview

This chapter outlines the nature of security and the issues that we believe will play the dominant role in national security in the near future. The first section of this chapter outlines our view on the nature of security. We describe the origins of the term and how we see security within the context of societies. We expand this concept to the economic relationships that exist between the individual and the collective and ultimately the nation-state.

These security relationships are then presented in a framework of security functions that the Nation-State provides. This theoretical framework serves as a reference as we present our view on the evolution and alternative viewpoints in National Security thinking. These viewpoints help illustrate our argument by providing historical examples of failure and success that resulted for the alternative ways of aligning a Nation-States security efforts.

2.1 Defining Security

Security comes from a Latin noun "*securitas*", referring to a person's inner composure or tranquillity of spirit. As a social animal, humans find themselves at birth delivered into the smallest of communities with tacit obligations being the provision of security for the interests[1] of its members (i.e. blood relatives). In this context, security means the protection from real and perceived dangers and a general reduction in uncertainty, anxiety, or apprehension.

The security provided by the community is not free. Numerous community obligations (e.g. taxation) are part of social relationships. The individual's membership in a group has its own costs, exposing the individual to additional threats. The key economic question for individuals (and sub-groups) to decide if

[1] Maslow's hierarchy of needs describes these needs (physiological, safety and security needs, love and belonging, self-esteem, and self-actualisation). As one level is met the next level is sought see A. H. Maslow, Motivation and Personality, Harper & Row, New York, 1970

remaining within the protection of the community will provide an acceptable return on investment (ROI) in meeting the individual's needs.

Alone the individual finds it very difficult to provide adequate protection. Communal protection is sought because this provides the individual with the opportunity to participate in an efficient protective systems (e.g. sharing guard duties). Each individual chooses between production, self-protection (of their own production), and contributing to a collective security (e.g. community service or through taxation). Increasing the amount of time spent on self-protection reduces the productivity and/or collective security.

The less time an individual needs to spend on security the more time they have available to produce, coexist and benefit from the cooperation of others. Key to the efficiency of community security are the impacts of specialisation and technology being able to reduce the amount of time an individual has to spend on the production of security (for themselves and the collective).

Deciding how much effort to spend on self-protection and how much to spend on collective efforts are complex decisions even in simple economies[5]. Where an individual or group undertakes an activity with special risks, they and the community must make decisions about the allocation of private vs. public (shared) effort on security measures. As new activities are initiated and the security environment changes the security needs change. They may even act as a catalyst for the formation of different types of communities of increasing size, architecture and complexity; including villages, tribes, caravans, cities, banking systems, nation-states, military alliances, trading blocks and the United Nations.

2.2 Security Functions

In considering an investment in security and obligations, individuals are faced with many natural dangers and threats. Of great concern to individuals are the aggression and theft by others who choose to take production without adequate payment. The presence of bandits and villains are a basic drivers for individuals to seek collective protection. Consequently, the sophistication, resilience, efficiency, and power of very large communities are attractive attributes to individuals and sub-groups.

In the last two centuries, the collapse of religious and ancestral empires has seen the rise in dominance of the Nation-State as the largest community within which an individual concedes to mutual obligations or 'social contract' with the collective's government. A consequence of seeking the benefits and protection

[5] Wilhite A., *Seeking Protection and the Origin of the State*, Department of Economics and Finance, University of Alabama in Huntsville, 2001

of a Nation-State is the exposure of the individual to a number of risks. Both the States and the individual (and other non-state actors) are not passive parties: as well as being affected by threats and risks, they can be the sources of risk to each other.

Participation in a Nation-State or other communities of interest by individuals results in the creation of four specific security tasks; Defence, Constitutional, Authority and Protective[6], illustrated in Figure 2 Security Functions of the State. These functions are resourced by collective efforts. Each function deals with the different nature of threats to the state or non-state actors (esp. citizens) from other states and non-state actors. The four functions are described as follows;

- Defence function to secure the state from threat arising from other states i.e. inter-state war. This may include providing external protection of its jurisdiction against existential and other threats from states.
- Constitutional function to secure the rule of law within its jurisdiction to safeguard the individual against threats by the State(s). Including preventing the individuals from being harmed by the activity of their own state e.g. corruption, state based terror, human rights violations.
- Authority function to secure the legitimate monopoly of force within a jurisdiction. The authority function enables the state to act as the peak referent on community decisions. The function protects the state against those that seek to impose their will, through domestic terrorism, revolt or intra-state (civil) war.
- Protective function to secure the safety of individuals against the risk of harm by the actions of non-state actors e.g. crime, pollution, consumer rights

Over time and with changing economic conditions, the resources available for the total security spending on these functions vary. Further, the share of resources that each security function receives will be driven by priorities of the community or it leadership. It is important to note that the jurisdiction claimed by the Nation-State may not extend to all aspects of an individuals life. For example many western-liberal democracies permits various organisation to co-exist as the peak referent on religious matters.

[6] Adapted from Zangl, B. and Zürn, M. , The Effects of Denationalization on Security in the OECD World, Occasional Paper #15:OP:2 The Joan B. Kroc Institute for International Peace Studies, December 1998

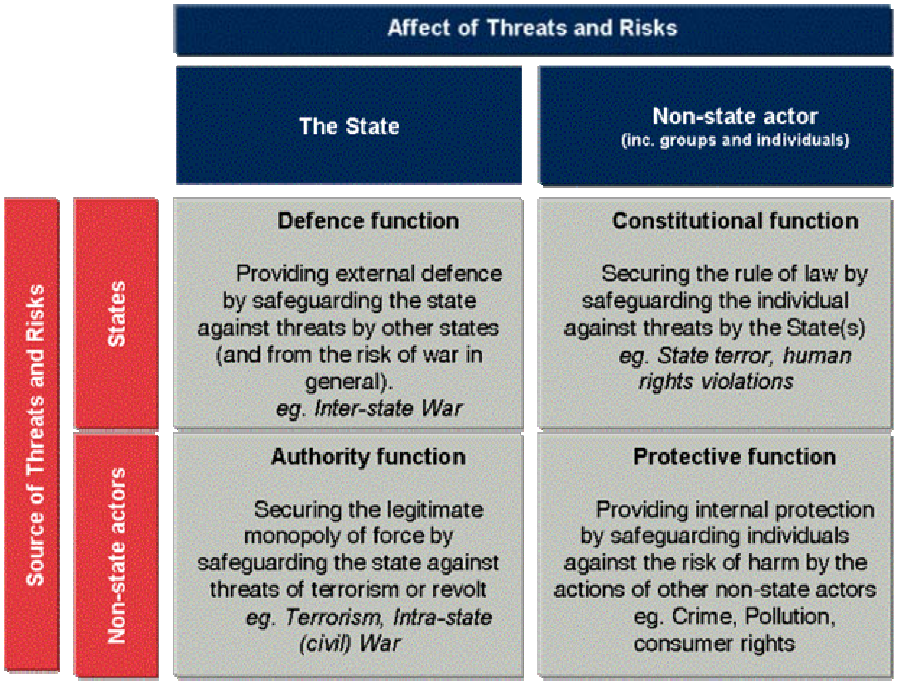


Figure 2 Security Functions of the State[1]

In its classical form, security commonly refers to the ability of a Community to defend itself from armed attack and military invasion. This remains a traditional function of governments. The other commonly understood area of security is the policing or protective function over life and enforcement of property rights. However, protection is not solely a public issue, as individuals and groups also undertake varying degrees of defence of their own life, property and protection of their own "rights".

Dispute over the importance of various risks may lead to breakdown of security obligation. If the investment in protection is not perceived as reasonable or beneficial to one or more parties, this breakdown can happen at any level of society, from the micro level within small groups like a family through to the macro level amongst Nation-States. The priority in resourcing security functions balances many factors, including immediate concerns for protection of life and property, existing production and current stores of wealth (a.k.a. savings). A Nation may perceive forces that threaten its interest in numerous dimensions beyond the physical assets and geographic borders (see 3.4 Contemporary Forces Shaping National Security). In addition to direct existential threats (e.g. countering invasion), Nations' or sub-national groups' security are threatened by other forces, for example religious, ideological, political and ethnic pressures. These "national interests" will also include

[1] Adapted from Zangl, B. and Zürn, M., The Effects of Denationalization on Security in the OECD World, Occasional Paper #15:OP:2 The Joan B. Kroc Institute for International Peace Studies, December 1998

economic outcomes. These include the capability to acquire resources, improve efficiency, and the maximising opportunities for future wealth creation. Large communities like Nation-States must consider longer range and complex strategic environments in order to plan adequately to manage the threats to their security and well-being.

2.3 Concepts of National Security

> *"As a nation we may take pride in the fact that we are soft-hearted: but we cannot afford to be soft-headed".*
>
> *Franklin D. Roosevelt*[8]

The relationships and dynamics amongst Nations, including National-Security, fall within an area of study known as international affairs. The definition, theories, and debates around concepts of National-Security are complex and continue to evolve. As civilisation has developed, there has been an increasing study of diplomatic history (esp. associated with the world wars) leading to review of the classical approach to National Security. Wing[9] described the major trends as contributing to the development of international politics and the approaches to National Security. These overlapping trends can include the following perspectives on security:

- "Classical realism"
- "Idealist" promotion of international law and organisation (between the great wars)
- 'Political realism' viewpoint (after WW II) focusing on power politics
- "Neo-realism" view of the balance of power
- "World system theory" of global interdependence and the international political economy
- Study of the "world order" to provide for human values

It is important to highlight that these approaches are not clear segmentations of the field, since they mainly differ in the approach to the analysis, the nature, and priorities of issues, and the way events and trends are reviewed.

---

[8] From *The Four Freedoms* speech delivered to 77th Congress of the United States by Franklin Delano Roosevelt, on January 6, 1941

[9] Wing, LTCOL I. G. R,. *Refocusing concepts of security: the convergence of military and non-military tasks*. Working paper no. 111, Land Warfare Studies Centre, Australia. November 2000. pg 4

2.3.1 Classical Realism

"War is merely the continuation of policy by other means'

Karl von Clausewitz[10]

Although it has been present since ancient times, the concept of the Nation-State as the paramount security community was established through the Peace of Westphalia as a result of the Thirty Years War (1648). Since this time, the sovereign Nation-State has been seen as the main actors (or referent) in international affairs. Nation-States have the right to manage their own domestic affairs. Historically, the military have either ruled or been very close to the ruling class. An army and navy became intrinsic component parts of the Nation-State supporting imperialism, nationalism, and militarism.

National Security theory followed the system of 'classical realism', which was concerned with the preservation of the existence of Nation-States and enabling these entities to grow and prosper. In classical realism, beyond the boundary of the state, no moral obligations existed. Inter-state relationships took on a selfish posture, with warfare as a calculated element of policy. This policy is not to say that morality was lost in inter-state relations. Many rulers and Governments followed the classical tradition of "jus ad bellum" and "jus in bello"[11]. These twin principles of "jus ad bellum" (the rights of states to resort to war) and "jus in bello" (the law regulating combat or the waging of war[12]) formed the basis of morals and ethics surrounding armed conflict. Leaders would consider the justness of sacrificing human lives in a war and the ways in which a war was conducted, such as whether the lives were lost in fair battle. This tradition tried to determine whether the warfare techniques and accompanying collateral damage was morally proportionate to the good that could be achieved.

Others such as Karl von Clausewitz considered a moderated balance with a concession to rules in war but the removal of ethical dimensions. His school of thought is illustrated by his quote on the use of war as one segment of the political spectrum.

---

[10] von Clausewitz, C. *On War*, (Ed/Trans) Howard M., Paret P. Princeton University Press, Princeton, NJ, 1976.

[11] Walzer, M., *Just and unjust wars: A moral argument with historical illustrations*, 2nd ed., New York, 1992

[12] Jus in bello in a broader sense also refers to the rights and obligations of neutral parties as well.

2.3.2 *Idealism and 'Political Realism'*

Institutional efforts to avoid armed conflicts and especially peace congresses[13] before World War I were not uncommon. However, international relations changed significantly though the shocks of the world war. The reaction to the catastrophes resulted in a search for peace and the rise of an optimistic National Security approach known as 'idealism' in international relations. The League of Nations was established after World War I at the Paris Peace Conference in 1919, providing renewed hope. The League was based on a Covenant of 26 articles that was included in peace treaties and in the Treaty of Versailles. It included the great powers: Great Britain, France, Italy, Japan, and later Germany and the USSR. The idealist sought to de-emphasise the drive for power and power-based relationships. Instead, they sought to balance the pre-eminence of the state against other considerations such as law, ethics, and morals. This movement was characterised by a belief in democracy and the rule of law to create a peaceful world.

The optimism viewpoint was challenged by the political turmoil in Europe and the Far East in the 1930s the rise of fascist dictators. Although it had early successes, the League of Nations was shown to be impotent. These events contributed to feelings of despair and cynicism among scholars with World War II shattering the dreams of many "idealist". Disillusioned academics such as Morgenthau[14] concluded that individuals were not perfectible and human behaviour would seek to maximise power: there is no role for morality in international relations: institutions cannot be reformed and war cannot be eliminated. This view is referred to as 'political realism' and it emerged (or reappeared) with power as the fundamental approach of National Security. Power, identified with military strength, was considered the absolute in relations between Nation-States. A strong military power created deterrence to aggression, and force (i.e. violence) was neither immoral nor irrational and it could (i.e. should) be legitimately used in the service of the national interest. For example, the use of British Sea Power to expand the British Empire around the globe, and protect Britain's economic interests.

In 1945, after World War II, the United Nations (UN) replaced the League of Nations, providing some hope of balance between idealism and realism in

[13] An International peace congress was first held in First in London 1843. A Second Universal Peace Congress in Brussels in 1848, a series of meetings in Paris 1849, Frankfurt 1850 and London in 1851. Other meetings included the International League of Peace and Liberty Geneva 1867 and after the Franco-Prussian War (1870–71) in Brussels 1873, also the first Pan-American Conference 1889–90, the Universal Peace Congress Chicago 1893, Hague Conferences 1899 and the Second Hague Conference 1907

[14] see Morgenthau, Prof. H. J, *Politics Among Nations*: the struggle for power and peace. New York, A. A. Knopf. 1948

international affairs. When founded the UN had 51 members, which has since grown to 189 nations.

The debate between realism and idealism continues in modern times with many theories on National-Security that have been put forward. As a counter-point to power politics, some theorists choose to focus on aspects other than power and re-examined broader influences on states (inc. scientific, sociological, anthropological, philosophical and structural). The systemic properties of the international political system are studied using "systems theory". This approach considered the characteristics of the whole system, identifying conflict at a particular time, the operation of power blocs, and the distribution of wealth and resources. There are still many different views about the relative importance of economic and political factors in determining the distribution of "rewards" (i.e. wealth) in the international system. There are a number of viewpoints at present ranging from neo-realism, through liberal institutionalism to world system analysis.

2.3.3 Neo-realism

An approach accredited to Waltz referred to as 'structural realism' or 'neo-realism' sought to explore how the system's overall structure, defined in terms of the distribution of power, influences political outcomes. It balances the importance of human behaviours, forces acting within the state, and systems and structures operating within and between states. However, neo-realism retained the state as the primary actor within the study of international relations. These actors rely on 'self-help' to maximise their power within systems and structure, influenced by forces that could be identified and understood. The viewpoint emphasises that power has always been distributed unequally and that the balance and distribution of power in the system are the key focus. Hegemony is seen as the most important historical force in international relations. This is the drive by the most powerful state(s) to establish, maintain, and defend its political dominance over the entire system. The interaction of the most powerful states each trying to maximize their national interests within the system determines the general characteristics of international relations at a particular time. When the power distribution changes, the system changes.

The neo-realists do acknowledge the increasing importance of interdependence and economic questions in world politics, but they argue that states' policy in all areas continues to be determined by a desire to maximize their relative power. Therefore, this viewpoint concludes that international regimes can only be established through the efforts of an effective hegemony. International regimes will reflect the hegemony's interests and regimes will decline when the hegemony's influence in the system declines.

During the Cold War, the study of National Security was largely focused on the bi-polar conflict[15] between the United States of America (U.S.A.) and the Soviet Union. This approach is called 'strategic studies' and it considers conflict in terms of the use of force and particularly the strategic nuclear standoff that existed between the superpowers. A dominant concept of the period was the doctrine of Mutually Assured Destruction (MAD)[16]. The MAD philosophy saw the survival of the Nation-State as paramount. Any attack (a.k.a. first strike) on the Nation-State would result in catastrophic retaliation, without regard for survival of any nations or the biosphere.

To enable the doctrine to work a credible nuclear deterrent needed to exist, along with the will to use it. The strategic gridlock created 'the long peace'[17] a period of relative global stability with few major regional wars. However at lower levels many small inter-state and sub-state conflicts occurred. Proxy wars were often fuelled by the major powers, as part of the broader ideological conflict between capitalist (democratic) liberalism and communist (authoritarian) socialism. Until the end of the Cold War, American intervention around the world was justified by the need to contain international communism.

2.3.4 World Systems Theory

Since the 1970s, international relations increasingly emphasised global interdependence and the changing role of the Nation-State[18]. The global "agenda" has seen a renaissance of "international political economy" considering the terms of international cooperation, and the dramatic change in priorities of social and economic issues rather than focus on military and diplomatic issues.

World systems theory[19] also emphasises the idea of hegemony, but dominance is established through economic superiority in agriculture, industry, and commerce. The theory takes the viewpoint of economic determinism, reversing the neo-realists causal link between politics and economics. The state

---

[15] Jacobsen, C. G., *Strategic Power: USA/USSR*. New York: St. Martin's Press, 1990. Numerous books, reports and journals detail the bi-polar struggle. Selected references include; Allison, G., and Treverton, G. F., eds. *Rethinking America's Security: Beyond the Cold War to the New World Order*. New York: Norton, 1992., Chafe, W. H., and Sitkoff, H., eds. *A History of Our Time: Readings on Postwar America*. 2d ed. New York: Oxford University Press, 1987

[16] _,The Origins of Massive Retaliation, Political Science Quarterly (spring 1981) and Gaddis, J. L. Strategies of Containment: A Critical Appraisal of Postwar American National Security, Oxford University Press, February 1982

[17] Gaddis, J. L. *The Long Peace*, Oxford University Press, Oxford, 1987

[18] Wallerstein, I. M., The End of the World As We Know It: Social Science for the Twenty-First Century , University of Minnesota Press , February 2001

[19] Wallerstein, I. M., *The Essential Wallerstein*, New Press, May 2000

is seen as an actor in an international capitalist economy. The politics between Nation-States are directly associated with effects on world economy. A state's priorities are the maintenance of its legitimacy and the accumulation of capital within its economy.

There are several parallels between neo-realism and world system theory as they both conclude that conflict and instability are inherent in an anarchical international system. Despite conceptual differences, both conclude that history demonstrates that hegemonies are relatively short-lived.

2.3.5 Liberal Institutionalisms and World Order Studies

In contrast to both neo-realism and world system approaches, Liberal institutionalists argue that due to the increasing interdependence (eg. technological, economic) states are compelled to work together to more efficiently coordinate their policies to maximise their national interests[20]. However, because of the diversity of national agendas, institutionalists look to a variety of "international regimes" for cooperative arrangements that involve principles, norms, rules, and decision-making procedures. Among states, there should be formal or informal institutions for collective decision-making and collective action in issue areas.

An approach called "world order studies" has evolved in parallel to the other viewpoints discussed above. This approach reviews the capability of the international political system to serve the individual's needs. World order theorists assess the way systems can be modified to better maximise the individuals values. The individual hierarchy of needs and well being in key areas are considered, including:

- Participation in real decision-making,
- Freedom from violence,
- Ecologically sound development and
- Self-realisation.

Therefore, security is part of the social contract between the people (citizens) and their community (Nation-State). Viewed through this perspective the changing nature of societies and new threats to individual security are critical in understanding the state interests and its security functions.

[20] *Walker, R. B. J., Political Theory and the Transformation of World Politics*, Princeton, NJ: Princeton University, Center of International Studies, World Order Studies Programm, Occasional Paper No. 8, 1980

2.4 Multiple Dimensions of Security

The meaning of 'security' has been described above, showing how it has changed and broadened the meaning of 'National Security'. In the new millennium, the concept of National Security has moved well beyond a traditional focus on inter-state military confrontation. Nation-States are now faced by a complex and uncertain future, for which the traditional military perspective and approaches to understanding National Security are no longer sufficient. Wing[21] highlights the diversity in the theoretical re-conceptualisation of approaches to security, across numerous dimensions. Several frameworks now exist upon which individuals, organisations and states measure their security. Some of those frameworks identified by Wing[21] include the following:

- Traditional Security
- Collective Security
- Regional Security
- Common Security
- Non-offensive Defence Security
- Comprehensive Security
- Environmental Security,
- Cooperative Security
- Societal Security
- Economic Security
- Non-gendered Security
- Global Security
- Human Security

An individual's view of security and therefore their security ROI calculation (i.e. the Return on Investment from their State) may be influenced to varying degrees across many (or all) of these dimensions. The traditional views of National-Security limited to state existential issues are now less relevant, giving way to a more complex view of what constitutes a secure nation. As the world has changed, so has the significance of the forces influencing the welfare of its people. If the Nation-State is unable to offer its citizen's adequate security or 'freedom from care, anxiety or apprehension' in the dimensions they value, the Nation-State will not survive as the peak referent for security.

To provide a balanced approach to National-Security, relevant to modern societies, the Nation-State should continuously monitor its various security

[21] Wing, LTCOL I. G. R,. *Refocusing concepts of security: the convergence of military and non-military tasks*. Working paper no. 111, Land Warfare Studies Centre, Australia. November 2000. See also Wing's paper War and anti-war and its implications for the ADF, working paper 1/97 land warfare studies centre, land warfare studies centre, australia. 1997

functions for relevance. These functions (i.e. Defence, Constitutional, Authority and Protective) need to be integrated in the National security policy and plans so that the States citizens can see the benefits of community participation and the relevance of the social contract for them. Failure to demonstrate clear value to citizens will result in deferring sovereignty to sub (or pan) national actors and forces.

2.4.1 Chapter Conclusions

In this chapter, we outlined the nature of security and the issues that we believe will play the dominant role in national security in the near future. This included our view on the nature of security. We expanded this concept to the economic relationships that exist between the individual and the collective and ultimately the nation-state.

We detailed the framework of security functions that the Nation-State outlined the evolution of National Security thinking. We argue that the evolution in thinking helps illustrate our argument of the changing nature of the security environment.

Chapter 3. **Analysis of Conflict**

Chapter Overview

Having considered the frameworks for developing a National-Security strategy we then introduce contemporary dimensions of the challenge. Firstly, we provide our analysis of conflict and war to illustrate our argument that the types and nature of war has changed as society has evolved. We provide an analysis of modern conflicts and identify the types of changes occurring.

We then argue that the very nature of conflicts are changing, within a set of security dimensions. We have used the term "security dimensions" to outline a collection of forces, trends, problems, actors and other influences that we have identified and believe will most significantly effect national security planning. We argue that the dimensions identified in this chapter are the origins of our societies most significant vulnerabilities. The resulting risks from these vulnerabilities dictate the alignment of our security efforts if we wish to ensure appropriate peace of mind. We have created a list of scenarios for National Security Planning that should be used to review the alignment of our security efforts.

3.1 Escalation to War

A Nation-States influence and security are ultimately the utility of economic strength. We argue that the strengths of Australia's international relationships are not the romantic result of cultural heritage or taking the high moral ground on issues. Our relationships now and particularly during conflicts are largely influenced by economic relationships and our capacity to afford a credible military force. The Security of a State can be degraded or enhanced by Wars.

Rethinking the notion of National-Security and its relationships to Economics and Information Warfare requires us to have an understanding of changes in warfare over history. War has been a feature of history since primitive times and is conceived as a community enterprise (rather than as individual action). The popular view of war focuses on attributes of armed or violent conflict

between nations or states (international or inter-state war) or between factions within a state (civil or intra-state war).

War also includes other types of intense conflicts resulting from the failure of diplomatic activities (e.g. failure of negotiation, arbitration and mediation). War is a name given to the highest level of conflict between humans: it is particularly applied where groups believe at a point in time that each other's interests (or objectives) are incompatible. No compromises are seen as practical in resolving difference in interests and objectives. In such a situation, each group seeks to use an appropriate "force intensity" (or compelling techniques) to protect its interests and make opponents submit to its will.

Conflicts achieve the status of "war"[22] when the previously legitimate activities and competitive relationships that are *limited or constrained in some manner* are transformed through the use of actions (usually violence) and intensity outside accepted limits. The dividing lines between a limited conflicts and true wars are unclear and open to interpretation. This is a point we do not attempt to resolve. The point of transition to war is affected by many factors. The factors may include cultural norms, legal structures, moral viewpoint, religious canon, or ethical values. The differences in legitimate activities constitute warfare activities versus reasonable competitive efforts. Even when a conflict transitions to what one society's individuals considers war, limits and constraints may still exist[23] that differentiate the level of hostility e.g. from limited to unlimited or total warfare. Further following from the legitimacy of the conflict are the issues of legitimacy of the techniques used by adversaries. Although a war may be considered morally justified, it may be fought using illegitimate or unjust techniques. Conversely, an immoral war can be fought according mutually respected rules and norms.

Because of the blurred boundary between legitimate competition and war, it is vital that Nation-States consider what potential adversary considers legitimate competitive behaviour. In the context of personal conflicts between individuals, Australia does not accept the use of deadly force by citizens as a legitimate behaviour to resolve every-day domestic conflicts. Instead, we have created social structures that include laws and law enforcement to independently deal with these conflict situations. With this structure in place, the legitimacy of certain behaviours has been changed. In this context, we now

---

[22] Moseley, A., *The Philosophy of War*, Internet Encyclopedia of Philosophy, www.utm.edu/research/iep/w/war.htm

[23] Warfare may have its own cultural rituals as in the case of ancients Aztec and contemporary New Guinea highlanders. Each side may respect certain seasonal or logistics factors – e.g. Japanese Medieval warfare avoiding fighting during winter or allowing the opponent army to deploy on the battlefield. Legal Agreements may be respected by combatants – such as the Geneva Convention or Strategic Arms Limitation Treaties (SALT) see Major International Instruments on Disarmament and Related Issues at http://www.unog.ch/frames/disarm/distreat/warfare.htm.

consider it legitimate behaviour for other citizens (eg police) to use the deadly force to resolve our conflicts[24]. In the same way, conflicts between large multi-national organisations and Nation-States may apply varying standards as to what are considered legitimate competitive activities within the bounds of the "game". For example, a mandate from the United Nations may make previously illegitimate tactics legitimate or visa versa[25].

Of particular note are attempts in several theatres of war where combatants have attempted to create boundaries around acceptable warfare activities and intensity through either tacit or formal agreement. Clearly very dangerous and unpredictable condition occurs where the bounds of the legitimate competition differ between parties. A tactic, which is considered as a reasonable competitive action by one party, may cause an outrage for another party, resulting in an escalation in the intensity of a conflict.

When searching back through history and propaganda that surrounds conflicts, researchers are faced with significant problems in defining exactly what has constituted a war. Several data set have been identified by Collier and Hoeffler [26] that chart human conflicts, each with alternative data treatments on accurately and reporting of conflict.. The Conflict Catalogue prepared by Brecke contains wide criteria from inclusions of data covering the last 600 years and identifies 3516[27] violent conflicts of various sizes. This analysis shows that the number of violent conflicts decreases markedly starting in the mid-1600s remaining at a reduced level for almost a century and then rises sharply in the 19th and 20th centuries. Brecke notes that the "worst" decades in terms of new conflicts are the 1890s, 1910s, and 1960's with between 110 and 120 new conflicts for each of those decades as illustrated in Figure 3.

Different regions show markedly different trends, with Europe for example experiencing a general decline while Africa's experience was that of a slow increase until European imperial expansion in the 1890s creating a sharp peak with a second, smaller spike in the 1960s.

---

[24] Ryan, E., Righteous Bullets: Just War Tradition and the Use of Deadly Force by Police, Institute of Criminology, University of Melbourne, 2000

[25] Buti, A., and Parke, M., International Law Obligations to Provide Reparations for Human Rights Abuses, Murdoch University Electronic Journal of Law, Volume 6, Number 4,Murdoch University School of Law, December 1999

[26] Collier, P. and Hoeffler A., *Data Issues in the Study of Conflict First draft*: June 6, 2001 Paper prepared for the Conference on "Data Collection on Armed Conflict", Uppsala 8-9 June 2001 see http://www.pcr.uu.se/workpapers.html

[27] Brecke prepared a Conflict Catalog, a listing of all recorded violent conflicts that meet Richardson's magnitude 1.5 or higher criterion (32 or more deaths) in his paper. See Brecke, P. *The Long-Term Patterns of Violent Conflict in Different Regions of the World*, The Sam Nunn School of International Affairs, Georgia Institute of Technology Atlanta, GA Paper prepared for the Uppsala Conflict Data Conference on 8-9 June 2001 in Uppsala, Sweden

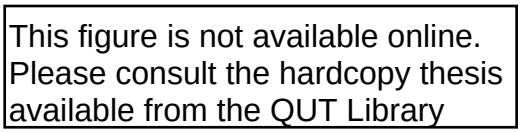


Figure 3 Violent conflicts over the last 600 years[28]

Looking more closely at the conflicts in the period after the end of World War II, we can produce highly detailed analysis. However, the definitions and criteria used in identifying conflicts are a source of debate. The leading data set for war analysis is the Correlates of War (COW) project[28] by Small and Singer, which requires a minimum of 1,000 battle-deaths for a conflict to qualify as a war. However, as lower level conflicts form a significant part of the modern security environment, researchers have expanded analysis to smaller conflicts.

The Department of Peace and Conflict Research (PCR) at Uppsala University with the International Peace Research Institute, Oslo (PRIO) has produced a data set[29] on armed conflicts for the period 1946–99. They define an armed conflict as "a contested incompatibility that concerns government or territory or both where the use of armed force between two parties results in at least 25 battle-related deaths. Of these two parties, at least one is the government of a state".

---

[28] Singer, J. David & Melvin Small, *Correlates of War Project: International and Civil War Data,* 1816–1992. ICPSR 9905, Ann Arbor, MI. 1994. see also www.umich.edu/~cowproj /.

[29] Gleditsch, N. P. Strand, H. Eriksson M., Sollenberg M. and Wallensteen, P. *Armed Conflict 1946–99: A New Dataset,* a paper prepared for 'Identifying Wars: Systematic Conflict Research and Its Utility in Conflict Resolution and Prevention', a Conference Co-sponsored by International Peace Research Institute, Oslo (PRIO), Department of Peace and Conflict Research, Uppsala University & World Bank, Development Economics Research Group (DECRG), Uppsala, 8-9 June 2001.

This study has identified 261 conflicts occurring after World War II[30]. This included 180 intra-state conflicts, 21 intra-state conflicts with external participation, 19 extra-systemic conflicts, and 41 inter-state conflicts. These figures confirm that throughout the period intra-state conflicts are the dominant form of conflict. However, the inter-state conflicts remain significant in terms of casualties. The researchers identified some inter-state conflicts, such as the Korean War, the Vietnam War, and the Iran-Iraq War claiming more than one million battle casualties each.

Of note are the two years (1994–95) during which no inter-state armed conflicts occur and they also note that there have not been no very large inter-state wars after 1988[31].

3.2 Third Wave War

Modern war has been increasingly been influenced by machine based warfare, industrial, scientific and especially electronic developments. The destructive capability and scope of wars reached truly global scale during the 20th century, compelling all nations to re-consider their strategy for "National Security".

The world's are transitioning from an industrial age to an information age. This transition is often referred to as the Third Wave[32] because of the work of popular futurists Alvin Toffler and his wife Heidi. Over two decades ago, Alvin Toffler introduced the notion that a titanic shift in the modes of production (wealth) reshaped civilization.

Toffler described how history could be described in terms of three distinct transitions (waves) during which civilizations' activists have radically changed. Each of these waves has seen the entire basis for wealth (production) and power (the potential for destruction) overturned. These waves saw a change in the

[30] Although war has been pervasive part of the 20th century, very few people in the Western world have actually seen a battle or been in one. Instead their view of war comes either from commercial films or more recently from television, leaving societies poorly prepared to participate in public policy debates about future wars. Michael Evans, the author of Serpent's Eye: The Cinema of 20th-Century Combat states that in World War II only 6 per cent of U.S.A. troops (700 000 out of 11 million) were in the infantry. In Vietnam only 14 per cent of U.S.A. troops ever saw action. Where significant number of civilians have been harmed it has been a result of direct urban attack (e.g. Strategic bombing), genocide or disease and starvation because of social infrastructure failures

[31] Several hugely destructive conflicts have occurred during these periods that do not meet the technical criteria for very large inter-state war. These wars included the Gulf War 1991 (a multilateral state/UN conflict), disintegration of Yugoslavia resulting in Croatia and in Bosnia-Herzegovina Wars in 1992-1995, the Secessionist conflict in Chechnya and the wars in Algeria, Liberia, Sierra Leone and Rwanda.

[32] Toffler, A., *The Third Wave*, New York: Bantam, 1980

central resource of wealth production and the use of new technologies that disturbed economic and military status quo.

The agricultural revolution of 10,000 years ago led to the transition from hunting, gathering, and foraging to the great peasant societies. The first of Toffler's waves broke around 8,000 B.C. and was called the Agricultural wave, with agricultural being the central factor in wealth. During this period, warfare was based on manpower, however it generally was poorly organized, poorly equipped, and poorly led armies. The wars typically consisted of seasonal fighting between rulers competing for territory. First-wave civilizations engaged in this form of war range from classical Greece and feudal Europe to those of ancient China. During this wave, some civilizations (e.g. Roman) where able to make significant conquests by developing armies which more efficiently used manpower.

The Industrial revolution approximately 300 years ago triggered a move to a factory-centred civilization. This wave is still spreading in some parts of the world as hundreds of millions of peasants, from China to Europe, flood into the cities searching for minimal-skill jobs on factory assembly lines. Toffler points to 1690 A.D. as the start of this second Industrial wave. Warfare is based on mass armies using standardized weaponry engaging in conflicts of attrition led by Officers produced from military academies. Physical attrition and manoeuvre warfare concepts dominate in military thinking due to careful studies of conflicts such as Karl von Clausewitz's classic military treatise, On War[33]. The technologies produced through industrial assembly lines included better weapons such as reliable firearms and new modes of transport result in new tactics. War during this period war may be considered as a contest between the capacity of each Nation-State to produce and utilise the greatest inventories of men, material and machines.

Currently we have entered the information age[32] with knowledge as the central resource. Global competition and other forces have driven advanced nations to move from an industrial assembly line to an economy fuelled by information, media and knowledge as the basis of power. Warfare is based on information-driven de-massification and niche capabilities. Information innovation permits combatants to deploy precision-guided weapons, non-lethal technology, psychological operations, directed-energy weaponry, malicious software and cyber war. Conflict now occur between subscribers to ideology and ownership of information assets.

Although the Tofflers' framework of theories on waves has been popularised and widely referenced, it is not alone and should not be acknowledged as the authoritative work on military, economic, and political change. Particularly in

[33] von Clausewitz, C., *On War*, New York: Viking Press, 1983

the area of theories on future warfare, the "Third Wave" view point exists alongside two other dominant theories: that of "Fourth-Generation Warfare"[34] and "Fourth-Epoch War"[35]. We acknowledge this debate, however a critic of futurist theory is not the focus of this thesis, and we shall persist with the Tofflerian viewpoint. Readers with specific interest in futurist theories on economic and military change are recommended to contrast Toffler's theories against variants and alternatives[36]. In their subsequent works, Powershift[37] and War and Anti-War[38], the Tofflers refined and explored in more detail the economic and military impacts of waves to further illustrate the transition to the information age. This third wave of change would impact individuals, organisations and Nation-States in a number of areas of change identified by Toffler[38] which are detailed below.

- Acceleration of processes - With increased speed and quality of information applied to problems, the process loops within processes become increasingly rapid. "Just-in-time" and "on-demand" delivery with real or near-time control becomes the norm.
- Continuous change - A wide base of information provides the opportunity to understand, continuously improve, and innovate. Learning organisations are able to transform to benefit for information-intensive environment[39].
- De-massification - Tasks including intelligence collection, processing, and targeting become highly customised and used with precision rather than treated as "one-size fits all". Rather than mass marketing and mass destruction, organisations move to "markets of one" and "one-round-one-kill" operation.
- Infrastructure - Information infrastructures are of prime importance with physical infrastructures taking a secondary support role

---

[34] Lind, W. S. Nightengale, Col K. M. USA: Schmitt, Capt J USMCR: Sutton, Col J. W. USA: and Wilson, Lt Col G I. USMCR published this theory in Marine Corps Gazette and Military Review. October Issue 1989, , p. 23

[35] Bunker, Dr R. J. *Generations, Waves, and Epochs Modes Of Warfare And The RPMA*, Airpower Journal - Spring 1996, see Col Owen E. Jensen, USAF, entitled Information Warfare: Principles of Third-Wave War Airpower Journal, Winter 1994 see also Moore, T. L. The Structure of War, The Claremont Graduate School, Claremont, California., 1989, 1–33 1989

[36] Numerous alternative frameworks exist that rival or compliment the Tofflers work. For further reading on futurist theories we suggested the following readings: Peter F. Drucker, Post-Capitalist Society, 1993, Mary C. Fitzgerald, "The Russian Military's Strategy for `Sixth Generation' Warfare," Orbis, Summer 1994: Andrew F. Krepinevich, "Cavalry to Computer: The Pattern of Military Revolutions," The National Interest, Fall 1994, Robert J. Bunker, "The Transition to Fourth Epoch War," Marine Corps Gazette, September 1994, Col Thomas X. Hammes, "The Evolution of War: The Fourth Generation," Marine Corps Gazette, September 1994: Martin van Creveld in The Transformation of War1991 New York: Free Press, Steven Metz, "A Wake for Clausewitz: Toward a Philosophy of 21st-Century Warfare," Parameters 24, no. 4 (Winter 1994–95)

[37] Toffler, A., *Powershift,* New York: Bantam, 1990

[38] Toffler, A., and H. Toffler, *War and Anti-War, Boston*: Little, Brown and Company, 1993.

[39] Senge, P. M., *The Fifth Discipline: The Art and Practice of the Learning Organization*, New York: Doubleday, 1990

- Intangible values - Wealth becomes based on intangible information assets rather than physical or property assets.
- Management - Hierarchical paternal management become superseded by flexible inter-disciplinary teams with flat structures that are able to take on management of organisations when solving specific problems.
- Organization - Organisations with information networks will transition from hierarchical structure (information flows up and down) toward networks where information flows throughout the organization. Military units will gain flexibility and field autonomy.
- Production - Competitive advantage becomes based on proficiency at production of knowledge that allows mastery of information intensive environment including: intelligence gathering, selecting directions, dissemination of instructions, precision targeting and supply chain logistics.
- Scale of operations - Organisational team sizes shrink to become more nimble with integrated process capabilities to deliver complex sophisticated solutions.
- Worker specialization - Labour becomes increasingly specialised requiring increased training and commitment to niche skills and knowledge

Each wave has also re-partitioned the world along lines according to the wave attributes they display. The Nation-States of the world are now trisected into nations within each of the three wave categories. A few nations have been unable to move beyond an economy based on agricultural capabilities (first wave), while most have made the transition to some form of modern industrial capabilities (second wave). Enlightened Governments understand the fundamental nature of the Third wave and are now racing to transition industrial age societies to information-based societies. A fortunate number of developed nations (including USA, Japan, Australia) now demonstrate the information-based capabilities that characterise them as "post-modern" information age states (third wave nations).

3.3 Transitioning Economies and Interests

The transformation from one economy to another is characterised by a gradual process of structural change. In the initial stages, the share of agriculture in total economic value added declines. A decline occurs in agricultural employment and the manufacturing sector grows as economies industrialise. In recent years, many OECD economies have experienced a decline in the share of manufacturing in overall economic activity[40]. By the end of the 1990s, services (including the public sector) accounted for 69% of OECD

[40] OECD *Science, Technology and Industry Scoreboard 2001* - Towards a knowledge-based economy see at http://www1.oecd.org/publications/e-book/92-2001-04-1-2987/

economic value added, while manufacturing accounted for about 19% and agriculture accounting for less than 3%. Conversely, high and medium-high-technology manufacturing accounted for about 9% of the total, and the knowledge-based[41]"market" services accounted for 18%. Australia however gets the best of both worlds in that industries predominantly involved in the extraction, processing and supply of fuel and energy goods produced the highest value added per labour unit. These industries were more than twice as productive as the average industry. They account for about 5% of total OECD value added and are typically highly capital-intensive.

We have already seen a direct and significant impact of ICT in Australia, that has seen a positive impact on productivity and growth[42] in conjunction with micro-economic reforms. The use of new technologies in Australian business has increased very rapidly in this last decade. Between 1997/98 and 1999/00, the proportion of businesses with Internet access has almost doubled (29% to 56%) and the use of the Internet to facilitate business processes is high[42]. The Commonwealth Government is highly focused on the transition to an Information economy, establishing a dedicated agency in the National Office for the Information Economy. The Information Policy Advisory Council[43] identified in its August 1997 report identified a number of Australia's comparative information economy strengths:

- Australia's well-established legal and institutional structures make it a safe and supportive environment for commerce.
- We have a world-class telecommunications network and cable rollout, including a leading edge hybrid fiberoptic/coaxial cable (HFC) network, providing a strong domestic market for online content and services.
- Australia has a tradition of rapid technology uptake—including one of the highest personal computer penetration rates in the world—and our consumer markets are sophisticated and enthusiastic about new information products and services.
- We are close to Asian markets, trade strongly in the region already, and have a body of business and trade knowledge that will be critical as the information economy expands in the Asia Pacific.

---

[41] OECD Division 64: Post and telecommunications, Divisions 65-67: Finance and insurance, Divisions 71-74: Business activities (not including real estate). see at http://www1.oecd.org/publications/e-book/92-2001-04-1-2987/D.5.htm

[42] Colecchia, A. and Schreyer, P. *ICT Investment And Economic Growth In The 1990s*: Is The United States A Unique Case? A Comparative Study Of Nine OECD Countries, STI Working paper 2001/7, Directorate for Science, Technology and Industry, OECD, 25 October 2001

[43] A national policy framework for structural adjustment within the new Commonwealth of Information, Information Policy Advisory Council, August, 1997 see at http://web.archive.org/web/19980118041011/www.ipac.gov.au/report2/index.html

- Because we lie in a different time zone to Europe and North America, an Australian base allows for global continuity of workflows and efficient handover of activities, for firms servicing markets in two hemispheres.
- Australian businesses and households are among the most advanced and sophisticated users of information and communications technologies in the world.
- As an English-speaking country, with great multilingual diversity, Australia has a natural advantage as a regional base for firms looking to build their business in the global information economy.
- Australia offers a well-educated and highly skilled workforce for new information businesses.
- Our climate, way of life and environment are attractive to international enterprises.
- Australian life is characterised by creativity and openness.

In 1998 Australia made up 1.2 per cent of global GDP, but about 2.3 per cent of global activity in information industries. In 1999, 82.7% of all businesses were connected to the Internet with 48% having a website[44]. We are good at information economy activities and we consistently occupy top ratings in adoption and use of information and communications technology. We are internationally well-regarded as having an innovative approach to the information economy.

For many Nations and those Non-Government Organisation's (NGO's) with industrial interests the transition is problematic, as increasingly wealth and power moves away from traditional to information assets. Those that can create custom knowledge products or acquire it and maintain ownership are likely to prosper at the expense of the previous power brokers. As a result of the these third wave economic re-alignments, tensions are created as the tradional power-bases are eroded, which can precipitate intense conflicts. Such a turbulent environment creates potential for worldwide multi-dimensional competitions in an information centric domain (a.k.a. "info-sphere"), amongst the tradional industrial power brokers and emerging information-centric interest groups.

[44] 95% used the website to promote products & services: 65% used the website for customer services: 53.7% used the website to receive orders: and 40.8% used the website for online advertising to promote their own business. Australian Bureau of Statistics, Commonwealth of Australia, 2000

These Information Age conflicts should not be envisaged as limited[45] or ad-hoc events derived simply from the utility of a new item of information technology. The conflicts upon which we focus are a result of multiple forces being unleased re-shaping the world by the increasing utility of information. We argue that these pressures will influence the broad social spectrum, affecting the social and political structure of nations, ideologies and economies and result in new dimensions of war.

3.4 Contemporary Forces Shaping National Security

A review of national strategic studies[46] at the global level outlines drivers and trends that are spawning contemporary and emerging threats that are shaping our security environment. Over the next decades, these forces outline the environment within which national security policy, strategy, and investments decision will need to take place. These shaping forces[46] include many credible points of instability and conflict for Australia and its allies, these include:

- (Re-) Emergence of rivals to the USA,
- Erosion of state sovereignty especially through globalisation,
- Population pressures,
- Health crisis,
- Management of natural resources,
- Energy consumption,
- Technology dependencies and
- Trans-national crime.

Taken together, these drivers and trends identify (with varying degrees of confidence) the security scenarios and uncertainties of strategic importance that we may confront in the next 10 to 15 years. The following section provides an

---

[45] Events such as strong sales of a software title, success in brand marketing, implementation of a successful online-payment service, developments of a new sensor or high-energy weapon are what we call limited (or small w) wealth and warfare advances. We differentiate these from "global" (or big W) wealth and warfare advances such are greater access to alternative information sources, less reliance on traditional social structures, different urban development patterns, invasion of privacy or neutralisation of contemporary military advantages

[46] Reference reviewed to identify these views included; Tangredi, S. J., *All Possible Wars? Toward a Consensus View of the Future Security Environment, 2001–2025* Mcnair Paper 63 Institute For National Strategic Studies, National Defense University Washington, D.C. 2000,__,*MAJOR THEMES AND IMPLICATIONS The Phase I Report on the Emerging Global Security Environment for the First Quarter of the 21st Century*,The United States Commission on National Security / 21st Century, http://www.nssg.gov/Reports/NWC.pdf, September 1999, Hammond, A., *Which World? Scenarios for the 21st Century*, Washington, D.C. Island Press/Shearwater Books, 1998

overview of these drivers and trends identified in strategic studies[46], and suggests how they relate to Infrastructure warfare.

3.4.1 New World Order (or Hegemony)

As in past millennia, one of the most significant drivers for the future has been the reshaping of the global superpower relationships. The bipolar world structure changed with the collapse[47] of the Soviet Union, as it was unable to match U.S.A. military strength and economic power. The Russian republic that emerged from the USSR was no longer a superpower able to rival the U.S.A., ending the Cold War status quo. Immediately after the collapse, the U.S.A. was seen as the unchallenged global superpower, with many declaring that the world had entered a 'unipolar' age.

The end of the Cold War reduced the scale of ideological conflict between communism and liberal capitalism. It led to optimism within the new international order and hope of an historic period of co-operation between states. The idealism is understandable, given that for 45 years hundreds of millions of people had grown up in fear of a nuclear holocaust, which at times seemed imminent (e.g. Cuban missile crisis of 1962).

In 1991 U.S.A. President George Bush elaborated on his concept of the "New World Order" in the context of U.S.A. leadership of the UN in conflict with Iraq:

[47] The end of the Cold War can be seen with the fall of the Berlin Wall in October 1989 and the reunification of Germany in 1990. The dismantling of the Warsaw Pact and the fall of the `Iron Curtain' across Eastern European countries. The Soviet Union was dismantled in 1991 with the Republic of Russia assumed the leading position in the newly formed Commonwealth of Independent States (CIS).

"Halfway around the world, we are engaged in a great struggle in the skies and on the seas and sands. We know why we're there: We are Americans, part of something larger than ourselves. For two centuries, we've done the hard work of freedom. And tonight, we lead the world in facing down a threat to decency and humanity.

What is at stake is more than one small country: it is a big idea: a new world order, where diverse nations are drawn together in common cause to achieve the universal aspirations of mankind—peace and security, freedom, and the rule of law. Such is a world worthy of our struggle and worthy of our children's future" [48].

The New World Order is considered by some commentators to be a euphemism for U.S.A. hegemony[49]. This identifies a contest between a unipolar and multipolar world. The unipolarity of the New World Order has not yet imposed the hegemony of one superpower (i.e. the USA), but rather it has seen the supremacy of a system of values including capitalist liberal democracy and focus on human rights. The counter point implies many centres of influence, including United Kingdom, Russia, China, India, Japan, and European Union (especially Germany). These actors have an interest in challenging the unipolar world, replacing it with a multipolar world. The U.S.A. faces a paradigm of great power competition with near peers, who are not considering military confrontations on a global scale. The paramount superpower now faces the limitations of its position and must consider how it will operate it a world with no-military peers.

The collapse of the Soviet Union compelled the U.S.A. (Bush and Clinton administrations) to review future international relations. In 1993, Anthony Lake[50], Assistant to the President for National Security Affairs provided a clear picture on the U.S.A. attitude towards national security:

[48] Bush, G. U.S.A. President, State of the Union Address, House Chamber, Washington, DC January 29, 1991

[49] O'Brien, K. P. and Clesse, A. *Two Hegemonies: Britain 1846-1914 and the United States 1941-2001,* Aldershot, U.K Asghate, 2002, Bryce, S. *Russia vs. New World Order*, New Dawn No. 64, www.newdawnmagazine.com.au, January-February 2001, Moore, R. K., *America and the New World Order*, New Dawn, March-April 1997

[50] Remarks of Anthony Lake, Assistant to the President for National Security Affairs *From Containment to Enlargement* Johns Hopkins University School of Advanced International Studies Washington, D.C.September 21, 1993

"…there is now no near-term threat to America's existence. Serious threats remain: terrorism, proliferating weapons of mass destruction, ethnic conflicts and the degradation of our global environment. Above all, we are threatened by sluggish economic growth, which undermines the security of our people as well as that of allies and friends abroad. Yet none of these threats holds the same immediate dangers for us as did Nazi conquest or Soviet expansionism."[50]

In describing a new foreign policy direction he stated:

"The successor to a doctrine of containment must be a strategy of enlargement—enlargement of the world's free community of market democracies."[50]

Trade and economic considerations through the promotion of democracy and increasing market size would henceforth dominate military and political factors in guiding foreign policy. The strategy is based on a core of liberal democracies that help foster and consolidate newly created capitalist liberal democracies. The superpower's priority is to counter aggression from states hostile to these liberal democracies, by isolating them through various means: diplomatic, military, economic, and technological.

3.4.2 Pressure of Globalisation

The last two decades have seen an extension of boundaries of social transactions beyond national borders and with an increased number of actors involved. These social transactions fall into three broad categories of welfare, signs, and threats. The increase in these transactions has eroded the state's claim to exclusive jurisdiction over its territory and its ability to deal with its problems unilaterally.

Many of these transactions fall into a category called welfare: this includes goods, services, capital, and labour. This globalisation has seen an intensification of international trade relations, the emergence of offshore financial markets, and the increased significance of direct investments by external actors. A global market now exists that dictates the value of national currencies and makes judgements on State policy. The international pressure can override the States 'economic sovereignty', forcing deregulation of national economies, changes in monetary policy or trade terms.

However, the growing economic interdependence has considerably reduced the probability of physical violence between states, with the 'new world order' not permitting the forcible annexation of territory. Economic interdependence

also drives the creation of economic institutional networks set up to deal with conflicts and common problems, again improving peace and stability[51].

Economic interdependence also drives the growth in relationships between the economic elites of different States, who see direct military solutions as inappropriate for achieving mutual economic goals. Further, Governments that are economically dependent on each other find it difficult to resort to military means due to mutual economic impacts of conflicts. The consequences of increasingly complex economic and other interdependencies between nations provide opportunities for enduring peace between states.

Other types of social transactions have also formed part of the Globalisation trends including communications. An increasing flow of information between states eliminates uncertainties about each other's intentions and increases transparency reducing mutual suspicion as well as the risk of misperceptions. Technology including, telephones, fax, television, e-mail and especially the Internet have all acted to accelerate the flow of information between societies. States have found it unfeasible to effectively control the flows of communications and information that are accessible by their citizens (although many try). In the face of these flows of information the State loses "cultural sovereignty' over its citizens. Nations now fear losing their role as cultural and moral guardians to the dominance of Western[52] culture and thought. As with economic interdependency, communication drives the creation of forums in which societal interests are articulated on a trans-national rather than on a national basis.

The consequences of Globalisation provide many benefits, but it also has a complementary cost. Many risks and threats can no longer be restricted regionally, temporally, or socially. These threats circumvent the existing security apparatus of the Nation-State, which in turn undermines its legitimacy as the provider of security functions. Although inter-state and state-induced threats and risks are being reduced in the developed world, globalisation has led to non-state (societal) threats and risks, increasingly overtaxing the state's ability to provide security. Citizens can choose to build social structures that are 'semi-detached' from state using advanced technologies across normal Nation-State boundaries.

Although the Nation-State is likely in the near term to remain the single most important of political, economic, and security organising units, its authority will be repeatedly challenged by increasingly powerful global non-state actors (both profit and non-profit). In particular, the Nation-State will have to deal increasingly with private sector actors (inc. trans-national corporations, media

---

[51] Rittberger, V (Ed.), *International Regimes in East-West Politics*, London Pinter, 1990

[52] Fukuyama, F. *The End of History and the Last Man*, Penguin Books, London, 1992.

conglomerates). One key challenge for the State is its ability to balance and manage the powers of multinational organisations including the World Trade Organisation (W.T.O.), International Monetary Fund (I.M.F.) and the United Nations (U.N.)

3.4.3 Population Demographics and Urbanisation

The worlds population by 2015 is estimated to reach 7.2 billion people with more than 95 % of the increase in world population in developing countries, nearly all in rapidly expanding urban areas[46]. In the near future more than half of the world's population is predicted to be urbanised, testing the capacity of governments to stimulate the investment required to generate jobs and to provide the services, infrastructure, and social supports necessary to sustain liveable and stable environments. It is expected that there will be a doubling of the number of people living in mega-cities[53]. Increasing urbanisation will provide many countries with the opportunity to tap the information revolution and other technological advances, but also exposes these populations to a tighter dependency on technology.

Largely urbanised populations and especially super-cities create inherent vulnerabilities through centralisation of critical (non-military) infrastructures. In these modern environments, millions of citizens can be impacted by low intensity warfare tactics used against fragile and combustible business infrastructures, such as power, water and health facilities. Today our urban infrastructures are not designed to resist professional attacks in the same way the walled cities of history were.

In higher intensity conflicts, the ability to use the combat power of police and military counter-terrorist organisation are further frustrated by the difficulty in identifying targets within the urban environment. Further, the Nation-States desires to increase surveillance and intelligence gathering (business and personal) to assist counter-terrorist organisation are expensive and is resisted on privacy grounds.

In this environment, the destabilisation of populations through conflicts or disasters will cause large internal displacements, refugee flows, humanitarian emergencies, that can quickly cascade and overload urban infrastructure.

3.4.4 Developments in Health and Biotechnology

For those Nations that can afford it, biotechnology may provide dramatic improvements in health, however gaps will persist and widen between

[53] A mega-city is currently defined as containing more than 10 million inhabitants. Mega-cities are expect to include - Mexico City, Sao Paulo, Buenos Aires, Lagos, Cairo, Karachi, Mumbai, Calcutta, Dhaka, Beijing, Shanghai, and Tokyo

countries, particularly the least developed[46]. While developed countries benefit from generous health spending and major medical advances, developing countries are likely to experience a surge in both infectious and non-infectious diseases and in general will have inadequate health care capacities and spending. Tuberculosis (TB), malaria, hepatitis, and especially AIDS will continue to increase rapidly[54]. These diseases will have a destructive impact on families and society, reducing average life spans by as much as 30 to 40 years, generating more than 40 million orphans and contributing to poverty, crime, and instability (especially in Africa).

The biotechnology revolution, including biomedical engineering, genomic profiling and genetic modification, will begin to have a major impact on the options for combating disease, increasing food production, reducing pollution, and enhancing the quality of life in wealthy segments of societies. However, the use of biotechnology will be controversial and face political, cultural, moral, and religious barriers.

3.4.5 Equity of Natural Resources and Environment

Driven by advances in agricultural technologies, world grain production, and stocks will be adequate to meet the needs of a growing world population, however distribution and availability will remain a problem[46]. The number of chronically malnourished people will increase by more than 20 % over the next 15 years with half the world's population living in "water-stressed " countries[55]. As in the past, water sharing disputes can lead to serious conflicts especially if they occur in combination with other sources of serious tension (eg religious). For example, Turkey is building new dams and irrigation projects on rivers that will affect flows into Syria and Iraq, and Egypt is proceeding with a major diversion of water from the Nile, which flows from Ethiopia and Sudan.

Environmental problems will persist and in many instances get worse. This will include substantially increased greenhouse gas emissions, intensive land use, significant degradation of arable land, depletion of tropical forests and other species-rich habitats increasing large losses of biological species. In the developed world environmental issues will become mainstream political issues however, progress in dealing with them will be inconsistent.

---

[54] AIDS and TB together are likely to account for the majority of deaths in most developing countries. AIDS will affect economic growth by up to 1 % of GDP per year and consume more than 50 % of health budgets in the hardest-hit countries.

[55] Less than 1,700 cubic meters of water per capita per year.

3.4.6 Increased Energy Needs

Meeting the increase in demand for energy, will neither pose a major supply challenge nor lead to substantial price increases in real terms, especially with the global economy being driven to greater energy efficiency[46]. Estimates of the world's total supplies of oil has steadily increased as technological progress in extracting oil from remote sources has enabled new discoveries and efficient productions[56]. North America will be replaced by Asia as the leading energy consumption region and accounting for more than half of the world's total increase in demand. China, and to a lesser extent India, will see especially dramatic increases in energy consumption.

3.4.7 Distribution of Science and Technology

The many new IT-enabled devices and services will be rapidly diffused across the globe through decreasing equipment costs and increased demand[46]. Communications systems will be pervasive with global networks, universal wireless connectivity via hand-held devices and large numbers of low-cost, low-altitude satellites. Breakthroughs in materials and nano-technology technology will generate widely available products that are smart, multifunctional, environmentally compatible, more survivable, and customisable. These will contribute to the growing information and biotechnology revolutions. Some advances will generate dramatic breakthroughs including agriculture, health, and communication. In these cases, we will see "leap-frog" applications, such as universal wireless cellular communications networking developing countries that never had landlines.

3.4.8 Growth of Criminal and Extremists

Trans-national organisations will become increasingly adept at exploiting the global diffusion of sophisticated information, financial, and transportation networks[46]. Terrorists, criminal, and non-government organisations have adapted to use available technology just as well, if not faster than businesses and consumers. For example:

[56] Recent estimates indicate that 80% of the world's available oil still remains in the ground, as does 95% of the world's natural gas.

"Terrorists have seized upon the worldwide practice of using information technology (IT) in daily life. They embrace IT for several reasons: it improves communication and aids organization, allows members to coordinate quickly with large numbers of followers, and provides a platform for propaganda. The Internet also allows terrorists to reach a wide audience of potential donors and recruits who may be located over a large geographic area.

In addition, terrorists are taking note of the proliferation of hacking and the use of the computer as a weapon. Extremists routinely post messages to widely accessible Web sites that call for defacing Western Internet sites and disrupting online service, for example. The widespread availability of hacking software and its anonymous and increasingly automated design make it likely that terrorists will more frequently incorporate these tools into their online activity. The appeal of such tools may increase as news media continue to sensationalize hacking"[57].

Criminal organisations and networks based in North America, Western Europe, China, Colombia, Israel, Japan, Mexico, Nigeria, and Russia will expand the scale and scope of their activities. They will form loose alliances with one another, with smaller criminal entrepreneurs, and with insurgent movements for specific operations.

Criminal organisations will corrupt leaders of unstable, economically fragile or failing states, insinuate themselves into troubled banks and businesses, and cooperate with insurgent political movements to control substantial geographic areas.

Criminal organisation will obtain their income from narcotics trafficking: alien smuggling: trafficking in women and children: smuggling toxic materials, hazardous wastes, illicit arms, military technologies, and other contra-band: financial fraud: and racketeering.

3.5 Scenarios for Future "wars"

Recent events focus us on the types of negative events that Nation-States must now consider as part of it National Security response and policy. These have included the Asian economic crisis, assertiveness by Iraq and North Korea, tension between the U.S.A. and China, failed reforms in Russia, nuclear tests and missile tests in South Asia, war in the Balkans and Global Terrorism (especially 9/11). These events are indicators of the underlying military,

[57] *Patterns of Global Terrorism 2000 and 2001*, U.S. Department of State USA, http://www.state.gov/s/ct/rls/pgtrpt/2001/

political, societal, economic, and ecological threats[58] that are driving international relationships.

The futures discussed by commentators[59] contain numerous and problematic sources of conflict amongst sub-national forces, other states, and supranational forces. These pressures on security roles threaten to compromise the Nation-State's integrity, reducing its effectiveness in protecting its citizens, corrupting institutions, and challenging it legitimacy and authority.

A broad range of forces have been outlined above, cross many disciplines and Security practitioners may be limited in their understanding of how these forces interact. Security practitioners should seek to understand global forces, deeper and broader security dimensions, and the resulting convergence of contemporary concepts of security. Otherwise, the State will not adequately meet its citizen's needs.

In considering how to develop a National Security policy and plan, the modern security practitioner needs to consider the potential destabilising effects of a range of threats and dangers[60]. Our research has identified the dimensions changing national security environment and from this we have developed numerous scenarios that may lead to future wars. The National Security Scenarios that we have identified are consolidation from common elements of significant reports [46] [57] [58] [60] as the basis for more detail planning by Australian policy makers are outlined below;

- Increase in Organised crime (esp. illicit drug trafficking, money laundering)
- Unchecked international migration, and large-scale movements of refugees
- Epidemics (HIV/AIDS[61], ebola, TB, Tuberculosis, malaria, hepatitis)

---

[58] Buzan B., *People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era,* London: Harvester Wheatsheaf 1991

[59] Tangredi S.J., *All Possible Wars? Toward a Consensus View of the Future Security Environment, 2001–2025* Mcnair Paper 63 Institute For National Strategic Studies, National Defence University Washington, D.C. 2000 see at http://www.ndu.edu/inss/macnair/mcnair63/m63cvr.html, Hammes, *The Evolution of War: The Fourth Generation,* LtCol T. X., Marine Corps Gazette, September 1994

[60] Top threats and dangers complied by authors from several forward-looking national assessments. Significant works contributing to this list include: STRATEGIC ASSESSMENT 1999, Priorities for a Turbulent World, Institute for National Strategic Studies, National Defense University, U.S. Government Printing Office, Washington, DC. and REGIONAL SECURITY OUTLOOK 2001, ARF (ASEAN Regional Forum), Australian Department of Foreign Affairs and Trade, Australia.

[61] For example, AIDS Is Declared Threat to U.S.A. National Security "Convinced that the global spread of AIDS is reaching catastrophic dimensions, the Clinton administration has formally designated the disease for the first time as a threat to U.S. national security that could topple foreign governments, touch off ethnic wars and undo decades of work in building free-market democracies abroad" Washington Post, April 30, 2000

- Clashes over resources, pollution and degradation of the environment (fresh water supplies, fisheries, good agricultural land, removal of forests, greenhouse-induced climate change, and stratospheric ozone depletion)
- Accelerating proliferation of weapons of mass destruction (WMD), missiles and dangerous technologies
- Globalisation of terrorism
- Increasing ethnic warfare[62] and violence from and within failed states, (inc ethnic cleansing)
- Aggression by current rogues, and emergence of new rogues
- Regional or Global economic collapses
- Military developments that erode status-quo of superiority and permit regional aggression
- Authoritarian rule in major countries, coupled with militarism and imperialism
- An effective anti-Western coalition of rogues and malcontents
- Emergence of a strong alliance in the Greater Middle East that seriously challenges Western interests
- Disintegration of Western Alliance systems and renewed nationalism.
- Geopolitical conflicts amongst emerging peers i.e. EU, China, Russia, India and/or the United States

We conclude that from our analysis of security dimensions and scenarios, we are re-entering a period of limited wars such as existed in Europe during the seventeenth and eighteenth centuries, with frequent small-scale internal conflicts stemming from state repression, religious, ethnic, migration pressures, as well as significant economic or political disputes. These conflicts are likely to occur most frequently in Sub-Saharan Africa, the Caucasus and Central Asia, and parts of South and Southeast Asia, Central America and the Andean region.

Van Creveld[63] describes future wars between sub-national groupings fighting for ethnic and religious causes where security depends on power wielded at the lowest levels of conflict, rather than rational national states using advanced Military forces.

Less frequent will be regional inter-state wars, although the risks of war among developed countries are still considered low. However, it is likely that

---

[62] This includes countless micro regional-ethic groups and macro cultural groupings of Western, Latin American, African, Islamic, Sinic, Hindu, Orthodox, Buddhist and Japanese (adapted from Huntington, S.P. *The Clash of Civilizations and the Remaking of World Order*, Touchstone Books, February, 1998).

[63] van Creveld, M., *The Transformation of War*, The Free Press, Sydney, 1991

Special Forces and special weapons will figure heavily in advanced country's' offensive operations. In addition to the Middle East and pursuit of terrorism, there is also the potential for large-scale inter-state conflict in Asia, particularly India-Pakistan, China-Taiwan, and in the South China Sea. It is likely that availability of Weapons if Mass Destruction, longer-range missile delivery systems, and other dangerous technologies will play a role in these conflicts.

3.6 Chapter Conclusions

In this, we have presented our views on the contemporary dimensions of the security challenge and demonstrated the changes in warfare as society has evolved. We showed that the very nature of conflicts are changing, within a set of security dimensions. These dimension where shown to be broader than traditional national security approaches and highlight vulnerabilities in our security strategy. In particular, we highlighted the central role of economies in defining security and the concerns that our financial information infrastructures are at risk.

The catastrophic impact of systematic destruction of the Global Financial Information Infrastructure (GFII) will continuously demand analysis and monitoring. However, we believe that it is highly unlikely that an attack at a global level would be successful. Although the evidence of the seriousness with which failures are seen can be seen in the work of numerous international organisations (inc. Bank of International Settlements and the United Nations).

- From our analysis we have however, identified conditions (see 3.5) that could escalate to encompass a campaign targeting financial hubs and links. This would have collateral impact on Australia's FII. In examining these strategic threats, we found no Australian centric conflict that was likely to result in an adversary attacking the entire GFII, however there are strategic scenarios (out to 2025) that have the remote possibility to threaten the entire GFII (and therefore Australia). The strategic scenarios that we have identified and categorised are listed below:
- **Collaterale hazards from Global Ideological War:** A broad unrestricted war between global power blocks over ideological issues such as values, culture, religion, philosophies etc. has the potential to destabilise Global economy.
- **Collaterale hazards from a war against the U.S.A.:** Of particular concern for Australia is the possibility of a conflict between a well-resourced third party (another Nation-State or pan-national group) and the U.S.A. Such a conflict could include targeting American FIIs. This presents a threat because there are high concentrations of globally significant information infrastructure (not just finance and banking) in the U.S.A. that makes it a lynch pin in the Global economy. Few Nations currently have the capacity to undertake a direct attack on the U.S.A, however the Hegemony may be unable to counter a campaign of

attacks including covert entry and use of WMD and other asymmetric methods including information war. Successful detonation of a small nuclear device (1-5kt) may disrupt key USA based nodes, expose many other economies, and destabilise the world economy. Without doubt, attacks on these systems would have grave consequences for Australia and our trading partners.

- **Collaterale hazards from war within the U.S.A.:** Although it extremely unlikely, an intrastate conflict within America may threaten the Global economy if it encompassed targeting enough of the U.S.A. elements of the GFII. Such a conflict may result from migration pressures, ideological groups, religious extremist, corrupt governments, criminal enterprises or significant class conflicts

We have identified a handful of nations that provide the provide the major hub nodes and links of the GFII that are interlinked with Australia's FII. The strategic scenarios that we have identified and categorised that threaten these sub-components and therefore Australia's FII include:

- **Collaterale hazards from attacks on Coalition partner's:** Within the context of large-scale conflicts we are likely to see other nations working as a member of a Colation force, (such as those we have contributed to United Nations missions). Such involvement may cause FII in multiple nations targeted by a well-resourced adversary (or its allies).
- **Collaterale hazards from foreign conflicts involving key Nations**: In addition to the U.S.A., regional or internal conflict in United Kingdom, European Union, and Japan FII may see targeting of key sub-components of the GFII.

The strategic scenarios that we have identified and categorised that directly threaten Australia's FII include:

- **Direct targeting due to foreign operations in Australia:** Australia's FII supports the operations of a number of foreign operations (e.g. Pine Gap, Diplomatic Missions, Branches of Multinationals, NGO fund raising, education of Foreign Students) that may be embroiled in a foreign conflict. The FII may be targeted to disrupt these operations. If a conflict occurred between major powers (e.g. between U.S.A. and China), our FII would face one of the extreme sets of threats.
- **Direct targeting due to Australia's membership of a Coalition:** Australia's choice to be a member of a Colation force may cause our FII to be specifically targeted by the Coalitions adversary. The FII may be targeted to punish Australia's involvement or disrupt the effectiveness of the Coalition.

The more likely strategic scenarios that will cause attacks on our FII will result directly (or as blow back) from the increasing number of non-conventional conflicts described earlier (see 3.5). The strategic scenarios that we have identified and categorised that directly threaten sub-components of Australia's FII:

- **Direct targeting due to Australia's involvement in low-intensity conflicts**: Intrastate wars, counter-insurgency and counter-narcotic campaigns, prolonged low-intensity conflicts, military operations in urban terrain, and peacekeeping operations all have potential for Australia's FII to be targeted. Australian involvement in various types conflicts (e.g. Bougainville, Solomon Island, Timor), outlaw motorcycle gangs and organised crime, issue motivated groups) may be prompt target sub-components of Australia's FII.

Given the change in the international order, a financial attack on Australia or one of its international dependencies now seem more likely than a decade ago.

Chapter 4. **Taxonomy of Information Warfare**

"What enables the wise sovereign and the good general to strike and conquer, and achieve things beyond the reach of ordinary men, is foreknowledge."

Sun Tzu[64]

Chapter Overview

In this chapter, we identify the elements and goals of information warfare to understand how this form of war may impact on economic systems during conflicts. One of the issues we face in alignment of our security efforts, is the rise of our dependency on critical infrastructures and the increasing use of Asymmetric Warfare. In particular, we focus on the change in strategies from a nuclear stalemate to post-cold war security and the threats arising from Information Warfare (IW). We present the significant contemporary taxonomies of information war, seeking to extract the key offensive and defensive strategies, tactics and operations. Based the analysis we argue that this increasingly important form of war will require a re-alignment and focusing of our counter-measures and security structures.

[64] Sun Tzu is a legendary Chinese military strategist who wrote his often-quoted text on warfare "Art of War" in the sixth century B.C. Several translations of the text are available are available: Sun Tzu "*The Art of War*" Cleary, T. (Translator), Shambhala Publications: Reprint edition May 1991. A public available translation is available at http://all.net/books/tzu/tzu.html

4.1 Dominance of Asymmetric Warfare

4.1.1 Dichotomy of New Weapons

In June 326 BC Alexander was arguably forced to fight one of his most demanding battle at Hydaspes against King Porus in India[65]. This battle marked the first real encounter with war elephants – a new "technology" on the battle field. The 200 war elephants terrified many of the Macedonians and their cavalry horses were afraid of them. Alexander's legendary phalanx was smashed by charging elephants. The battle raged for eight hours and the Macedonians suffered more than in any other campaign (a toll of almost 75% killed and wounded of the foot companions according to writings of Diodorus). However King Poru's "new weapons technology" was turned against him by Alexanders versatile light infantry, who targeted elephants drivers and hamstrung the beasts with axes, The battle turned against the Indian's as their elephants stampeded into their own infantry, collapsing the army, which then fled with many Indians being killed in the pursuit. From the victory, Alexander's army captured 80 war elephants, which he put to good use.

The battle at Hydaspes is an historical example that illustrates the dichotomy of new strategies: tactics, technology, and weapons, through which we can gain tremendous, benefit and at the same time expose us to additional risks. The result in warfare can be legendary victories and defeats or in business breathtaking profits or catastrophic losses.

As States reconsider their understanding of security, they too are re-considering other fundamentals, such as the definition of warfare, the readiness of their security forces and requirements for weapons. One key concept that has re-emerged is the fundamental re-assessment of how current weapons assist the state achieve a desired "end-state" in a conflict.

We see a theme emerging , which challenges the focus of requirement for weapons programs. This theme promotes the view that weapons are not exclusively designed to destroy[66] military targets. Rather a weapon's requirement is to compel others to submit to the users will. This may require a wide range of outcomes, only one of which is the destruction of military targets. Weapons also include limited strike capability to damage or neutralize military and non-military targets, through to actions that affect, change, modify, or

[65] Bosworth, A. B., *Alexander and the East: The Tragedy of Triumph*, Clarendon Press, Oxford, 1996

[66] We consider the pursuit of destruction for its own sake to be "evil". This is distinguished from destruction caused in the pursuit of a goal which one side may consider illegitimate or immoral.

impede activities or behaviours. The threatened or actual use of such weapons must be able (by force, constraint or coercion) to predicably impose your will on others[67] (a.k.a. the enemy, rivals or adversary).

Preceding civilisations used the crudest forms of weapons to force a rival to concede. Simply they took a very direct approach to physically destroying things of value (such as human life and property), until the rival decided that the most logical act was surrender and/or a negotiated cessation of hostilities. It has been an approach based on killing and destruction of a few to influence others (survivors). This style of military behaviour has largely been based around scenarios where one side "killed" another military force with the assumption that the unprotected civilian population would then concede[68] to the will of the victor. The extension of the strategy of destruction can be seen on the grandest scale throughout the Cold War. Global nuclear weapon systems were designed and created to influence the behaviour of the enemy through its threatened use, "no-one wins" posture.

4.2 Post-war Nuclear Stalemate

From the early 1950s, people around the world were forced to deal with a fundamental change in their sense of security. The east-west nuclear tensions threatened industries, institutions, and the existence of many nations. Whole generations across the globe grew up fearing nuclear attack, learning to "duck and cover" at school, and building bomb shelters in back yards. New weapons such as long-range bombers, huge aircraft carriers, missile submarines and intercontinental ballistic missiles striped away geographic protection (e.g. oceans). In that time Hackers[69] were heroes who pioneered the new electronic technology revolution, not a menace to sensitive systems. The early 1950s prevailing military strategy (in the west) was centred on an inflexible "massive retaliation" to counter a small air nuclear Soviet threat with limited warning. As the Soviets increased capabilities in the late 1960s, a new strategy was adopted: appropriately named "MAD" or Mutually Assured Destruction to counter inevitable parity in ballistic missile and other strategic forces. This strategy emphasised a western ability to absorb a first strike and retaliate with certainty of a lose-lose end-state.

---

[67] This supports Clausewitz requirement that warfare must have a purpose.

[68] However, in some cases the objective behind a military operation has not been the concession of an enemy population. Instead, in attempting to influence an audience within the community, solely destruction force has been used on "outsiders". This can lead to genocide (a.k.a. ethnic cleansing) as a States objective in war

[69] In the 1950s "hacker" was first used to describe researcher and programmers working on computer because they were incessantly adjusting and experimenting with the new technology Levy, S. *Hackers: Heroes of the Computer Revolution*, New York: Dell Publishing, 1984

The west attempted to contain the Soviets geographically and economically. Control of strategic (ocean) supply routes and foreign markets became a key element in a Cold War. In the 1960s, East Asian economies had enormous economic success, growing faster than any other region's, and poverty (in absolute terms) declined significantly. However, in regional economies, in particular financial sectors formed a weak link in national development strategies as they reeled under the impact of Cold War manoeuvres and distortions. As this Cold War dragged on, the adversary's forces matured their system through the 1970s and into the early 1980s. Much-improved sensors, satellites, and other early warning capabilities to indicate and warn of attacks bloomed on both sides. Intelligence capability on both sides reached sophisticated heights, contributing to more sensitive and flexible options being added to the MAD strategy, such as enabling counter force targeting, greater force endurance and flexible command and control strategy that was previously unimaginable. This Strategy becomes known as the Countervailing Strategy (CVS)

With the increase in the lethality of conventional forces and the proliferation of nuclear and other weapons of mass destruction (WMD) capacity, conduct of global or continental warfare was largely dissuaded or at least a stalemate occurred. This appeared to bring an apparent stability to some relationships between rivals. In particular, during the post-war period, the capability and willingness of the West and East to wage nuclear war seems to have acted as a strategic deterrent to seizure of rival's homelands[70]. During the extended bipolar stand off during the Cold War[15], WMD were useful due to the "mass" of the targets threatened with destruction (i.e. naval fleets, large land forces, large urban and industrial clusters and entire nation infrastructures). However, as the political system has become more liberal and open, political pressure has increasingly reduced the acceptable or legitimate use of such systems. Some even consider WMD systems as WMI or "Weapons of Mass Irrelevances"[71] in the current strategic environment. They argue that a major power cannot use these weapons in most cases because they will not be politically or practically useful. These highly lethal weapons have low utility to influence the morale of many contemporary adversaries, especially in numerous situations where there are no mass targets, eg terrorist targets distributed amongst friendly populations.

In a different dimension, contemporary populations with different ethics and standards, now place heavy pressure political and military leaders to seek "softer" or a more measured use of force. Highly desirable requirements for

[70] Ultimately these weapons systems only provided a stalemate and it was the "weapons" of economic power that resulted in the final victory

[71] For more detail discussion on weapons see Leonard, R. R., *Principles of War for the Information Age*, Presidio Press, CA, 1998

new weapons include being less bloody, more targeted, and especially morally easy to digest: yet still enabling the ability to enforce political will over rivals. Civilian populations have come to expect their armed forces limit both civilian and military casualties on both sides. The Iraqis in 1991 and the Serbs during Allied Force used this fact, using politically sensitive structures such as hospitals, religious and historic sites, and residential neighbourhoods to "morally harden" military targets.

In our time the rapid development of electronic technology and its application to business and war are reshaping notions of weaponry. Electronic technology's pervasive usage and dependence in the developed world make new kinds of weapons that use or target electronic equipment and electronic information systems an attractive alternative for those who wish to destabilise the status quo.

4.2.1 Revolution in Military Affairs

> *"A military revolution, in the fullest sense, occurs only when a new civilization arises to challenge the old, when an entire society transforms itself, forcing its armed services to change at every level simultaneously—from technology and culture to organization, tactics, training, doctrine, and logistics. When this happens, the relationship of the military to the economy and society is transformed, and the balance of power on earth is shattered"*
>
> *Alvin and Heidi Toffler.*[72]

The response (in part) by several nations to the changing strategic security environment is a program (although they have their own unique nomenclatures,) that we will categorise as a "Revolution in Military Affairs" (RMA)[73]. The various national RMA programs are attempts at addressing fundamental changes in the nature of war. RMA recognises the need to address the changes occurring in organisation, military doctrine, economic, social, political factors, and technology[74] around the globe. Although it seems to have

---

[72] Toffler, A. and Toffler, H., *War and Anti-War: Survival at the Dawn of the 21st Century*, New York: Little, Brown and Co., 1993

[73] See Butler, R., *West Meets East: Chinese and Western Researchers Exchange Views on the Revolution in Military Affairs,* The Historical Evaluation & Research Organization, 1999. Malik, Lt Col Z., *A new form of warfare*. Defence Journal. Karachi, Pakistan, July 2000. See www.defencejournal.com, Cordesman, A. H., *The Revolution in Military Affairs and Developments in the Gulf,* Center for Strategic and International Studies, Washington, DC, July 1999, Metz, S. *Armed Conflict In The 21st Century:The Information Revolution And Post-Modern Warfare*, Strategic Studies Institute, U.S. Army War College, Carlisle, PA, March 2000

[74] This definition is derived from that in use in the Department of History at the United States Military Academy and was the joint creation of several officers and historians. Baseman, R. L. *Digital War, A View from the Front Lines*, provides a good overview.

many variations and interpretations, RMA is a powerful theme within military theory circles. United States is credited as leading the "revolution" and the debate that has spawned debates around intelligence networks and precision weapons, and on broader issues such as fundamental macroeconomics, technology education, and social change. This revolution has prompted reassessments of current definitions about war and military affairs including "what is a weapon?" not only the Americans but by authors from other major powers including France, UK, China, and Russia.

Military now define the concept of armed conflict in terms of high, medium, low intensity and a range of other activities that fall short of a declared war but have "an absence of peace". The United States have developed concepts called Operations Other Than War (OOTW) and a subset Military Operations Other Than War (MOOTW) which poses intriguing contradictions and irony considering the historical views of the military and war fighting.

4.2.2 Asymmetric Warfare

"Kill with a Borrowed Sword"

The 3rd of the 36 Strategies of Ancient China [75]

The prohibitive costs, destructive effects and uncertainty of outcomes of head-to-head conventional and nuclear military confrontation have resulted in an increased interest in the development of asymmetric warfare strategies, tactics, and weapons. Asymmetric warfare aims at circumventing or minimising strengths while exploiting perceived weaknesses in security strategies. Development in this kind of warfare seeks to avoid direct engagements with military and other security forces. Instead, asymmetric warfare seeks to identify "sideways" combinations of numerous tactics to undermine the rival's security strategy. Asymmetric warfare is not new[76], it only has a renewed emphasis, as leaders have always sought to counter opponents advantages.

The rise in asymmetric strategy and tactics stems from the recognition that it will not be feasible for one party to impose its will on another through a restricted set of warfare techniques. Instead one or more parties will use a "cocktail" of tactics possible including one or more of the following examples:

---

[75] Brahm, L. J., *Negotiating in China: 36 Strategies*. Singapore, Reed Academic Publishing Asia, 1995.The 3rd of the 36 Strategies of Ancient China - When you do not have the means to attack your enemy directly, then attack using the strength of another. Trick an ally into attacking him, bribe an official to turn traitor, or use the enemy's own strength against him. For further reading

[76] Goulding, V. J., *Back to the Future with Asymmetric Warfare*, Parameters, Winter 2000-01, pp. 21-30

espionage, terrorism, weapons of mass destruction (including nuclear, biological and chemical weapons), non-violent resistances, propaganda, and information warfare

Where one party attempts to resist the domination of significantly larger and more capable opponent, asymmetric strategy may be the only viable option. In the current environment where a dominant state processes vastly superior economic, information or military advantages (esp. the USA), small states and non-state adversaries, (particularly politically-motivated groups and organised criminals) are unsurprisingly attracted to asymmetric strategies, tactics, technology and weapons. For states under pressure from asymmetric warfare, the development of counter-measures (where feasible) becomes the dominant characteristic in addressing threats to National Security[77].

In considering the new dimension and global forces effecting security we see that traditional weapons, structures, and approaches are increasingly dysfunctional. Van Creveld[78] exhaustively analysed the twentieth century influences of technology and the limits of technology in future physical and ideological low intensity conflicts. He with others concludes that they lack capabilities to protect the National Interest that are relevant to our time. Rather than resulting in new and innovative doctrines and weapons, in many developed countries forces increasingly seek higher technology weapons systems to address symmetric threats, rather than developing effective systems for low intensity conflicts.

Weapons must be useful in a range of conflicts that are focused on new national security scenarios, rather than traditional 'existential threats' to national survival (i.e. invasion). In low intensity (and even no intensity) conflicts an advanced military force has destructive power available that far exceeds its needs, yet it is constrained by broader morale, social and political costs associated with direct destructive attacks, a factor that will be maximised by asymmetric opponents. Planning to use force on an opponent must now acknowledge that there are restrictive Rules of Engagement (ROE), pervasive media (i.e. the CNN factor), and political involvement in the targeting process, propaganda assessments and public expectation for low (or no) "collateral" damage or friendly fire. Modern conflict and the potential escalation to unrestricted warfare present fundamental challenges to traditional symmetric military approaches and their weapons designers.

In 1996, the U.S.A.'s publicly articulated[79] "information superiority" in its Joint Vision 2010 as the key-enabling element of twenty-first century warfare.

The Joint Vision 2010 outlined the use of information superiority to integrate and amplify four essential operational components:

- Dominant manoeuvre: to apply speed, precision, and mobility to engage targets from widely dispersed units:
- Precision engagement: of targets by high-fidelity acquisition, prioritisation of targets, and joint force command and control:
- Focused logistics to achieve efficient support of forces by integrating information about needs, available transportation, and resources:
- Full-dimension protection: of systems processes and forces through awareness and assessment of threats in all dimensions (physical, information, perception).

The superiority in the information domain was seen as enabled by command and control, fused all-source intelligence, dominant battle space awareness, and both offensive and defensive information warfare.

4.3 Information@War

The desire of war fighters for quality information has been a feature of warfare since ancient times. Military texts both old[80] and new ponder the ways and means of gaining the information advantage: seeking the intelligence and security that will achieve victory. Little has changed in the fundamental value of information to the warrior, what has changed are the technologies and ways that we acquire process and disseminate information.

The technical meaning of information term encompasses three levels of abstraction, distinguished by information as both content and process. The lowest level requires observations of the physical world, which are collected and reported. Data consists of individual observations, measurements, and primitive messages forming the lowest level. Human communication, text messages, electronic queries, or scientific instruments that sense phenomena are the major sources of data.

Once filtered, transformed, and organized, data sets become information. The organizational process may include sorting, classifying, or indexing and linking

---

[77] de Somer, LTCOL G., *The Implications of the United States Army's Army-After-Next Concepts for the Australian Army*, Land Warfare Studies Centre, Working Paper No. 104, June 1999

[78] van Creveld, M., " The Transformation of War, New York: Free Press, 1991

[79] "Joint Vision 2010," U.S. Joint Chiefs of Staff, US Department of Defence, 1996

[80] "The Art of War" stresses the key role that information in war. Other texts for contrast include Bakshi, G.D., "*The Indian Art of War* : *The Mahabharata Paradigm (Quest for an Indian Strategic Culture)"* Delhi, Sharada, 2002, *The Book of Isaiah* (ca. 8th - 2nd centuries B.C.). The reader may also find interest in Johnson J.T., *Just war and Jihad: Historical and theoretical perspectives on war and peace in Western and Islamic tradition*, New York/London, 1991

data to place data elements in relational context for subsequent searching and analysis.

Information once analysed and understood, is knowledge. Understanding of information provides a degree of comprehension of both the static and dynamic relationships of the objects of data and the ability to model structure and past (and future) behaviour of those objects. Knowledge includes both static content and dynamic processes. In the military context, this level of understanding is referred to as intelligence.

From ancient early drums and flag, through semaphore, Morse code, enigma ciphers, undersea cables, remote imaging satellites communication, Global Positioning Systems (GPS) and unmanned aerial vehicles (UAVs) there has been a purposeful adoption of systems that have improved the quality of information that combatants have at their disposal. The qualities[81] of information that adversaries seek are as follows;

- Relevance - Whether the information addresses the user's needs
- Accuracy - Whether the information reflects the underlying reality
- Timeliness - Whether the information is current
- Completeness - All necessary information is available: necessary information is not hidden by extraneous details
- Coherence - How well the information hangs together and is internally consistent
- Format - How the information is presented to the user
- Accessibility – That it can be obtained when needed
- Compatibility -Whether it can be combined with other information
- Security - Protected from unauthorised access and use
- Validity – That it can be verified as being true.

Quality information can be applied to improvements in: firepower and lethality, manoeuvrability, command and control, interoperability of forces, and precision application of forces.

The role of information and the conduct of warfare has been increasingly revolutionized through the adoption of use of new information technologies. Our military and commercial information systems now collect, process, and communicate information in a quantity and quality unimaginable to ancient commanders. In particular, electronic collection and management of information at all levels has increased to become a central focus in both military

[81] These popular definition are derived from Miller, H. The multiple dimensions of information quality. *Information Systems Management*, *13*(2), Auerbach Publishers: New York , Spring 1996, pp. 79-82.

and commercial affairs. The electronic transmission and processing of information content has expanded both the scope and speed of warfare and business processes.

In the last decade of this century, electronic communications and processing technologies have accelerated the role of the information to become the very essence and manifestation of competition, conflict, and war. This shift has seen development of significant advantages in a number of areas of warfare including improvements in range, tempo, and precision[82]. Range refers to how forces can be detected, selected, tracked, observed and targeted, at increased ranges. Intelligence surveillance and reconnaissance (ISR) technologies are extending the scope of engagements across time and distance.

Tempo refers to how commanders can now receive quality information from diverse sensors that permit operational command and control at increased tempo. Decisions maker using sophisticated electronic decisions support systems can achieve increased (real time) knowledge of their battle space and quickly select optimal courses of actions. The decisions can be rapidly communicated to subordinates, peers, and superiors to co ordinate complex activities.

Precision refers to how highly integrated information systems provide increased precision and accuracy, minimising the waste, increasing effective lethality, and facilitating new tactics. Precision reduces the mission's planner's need to over provision weapons to increase the probability of success to acceptable levels. The precision provided by information system reduce time required in the targeting/delivery cycle and allows "one round one kill" weapons

Along with the increased use of electronic systems, we have seen a corresponding growth in electronic warfare as a specialist field of combat, accelerated during World War II, it matured during the early years of the Cold War fuelled by the espionage, interception and deception integral to the East-West struggle. Through conflicts in Korea, Indo-China, North Africa, the Middle East and Latin America commanders learnt lessons[83] on how new information technologies could provide better communication and tactical intelligence and also assist in deceiving and disrupting the adversary's intelligence and targeting capabilities.

---

[82] HENRY, R. and PEARTREE, C. E., *Military Theory and Information Warfare*, Center for Strategic & International Studies, Parameters, Autumn 1998, pp. 121-35

[83] Evans, M., *Forward From The Past: The Development Of Australian Army Doctrine, 1972–Present*, Land Warfare Studies Centre, Working Paper No. 301, September 1999

4.4 Taxonomies of Information Warfare

"We may realize that our true potential as a nation, and by extension that of our military, lies not in the fact that we have the most main battle tanks, but in the fact that we have 45 million children who are perfectly comfortable using 700 Mhz computers to play games"

Robert Bateman [84]

In the early nineties, there was a growth in public research and publications around "information warfare". Authors such as Beyerchen, Arquilla, and Ronfeldt began open discussions around potential new war forms[85]. These discussions are mirrored around the world including France, Russia, and China. The use of information technologies, has been widely referenced, as evidence of the stages in transformation of warfare by many authors including the Tofflers, however this is not the only view of the changes in warfare.[86] A broad group of changes are often referred to as being part of "information warfare" strategies: conversely, "information warfare" is also used at the micro level to describe very specific tactics associated with particular weapons systems.

In modern times, the concepts and operations of warfare based around information can be traced to (at the time secret) work done the 1970s, with Tom Rona[87] credited with the term "Information Warfare". Warfare at the information level can take on several possible forms "war forms" that describe operations at different phases during a conflict. These forms of conflict may be viewed as sequential and overlapping when mapped against an escalation of

---

[84] Bateman, R. *Hacking Our Way to Victory, An American weapon for the 21st century*, Armor March-April Issue 2001, pp 18-22

[85] Beyerchen, Al. *Clausewitz, Nonlinearity, and the Unpredictability of War.* International Security, Winter 1992/93: pp 59-90. Arquilla, J. and Ronfeldt. D. *Cyberwar is Coming.* Comparative Strategy. Vol. 12, 1993 pp141-165: Arquilla, J. *The Strategic Implications of Information Dominance.* Strategic Review. Vol 22 #3 Summer 1994 pp. 24-30; also Fitzgerald, M. *Russian Views on Electronic Signals and Information Warfare* American Intelligence Journal 15, Spring-Summer 1994 pp 81-87

[86] See, for example, Lind, W, S. et al., *The Changing Face of War: Into the Fourth Generation,* Marine Corps Gazette, Oct. 1989, pp 22-26. In this article, four generations of warfare types are enumerated: (1) massed manpower warfare, (2) massed firepower warfare, (3) manoeuvre warfare, and (4) terrorism-like warfare, This concept was refined by Hammes to modify the fourth category to be net warfare. See Hammes, T , X., *The Evolution of War: The Fourth Generation*, Marine Corps Gazette, Sept. 1994, p, 35.

[87] Rona Dr. T. P. is often credited with first applying the term "information warfare" while performing research for the U.S. DoD throughout the mid 1990s on the historical, theoretical, and operational concepts of IW. See his article, *From Scorched Earth to Information Warfare" in Cyberwar: Security, Strategy and Conflict in the Information Age*, pp 9 Fairfax, VA: AFCEA Press

hostilities timeline[88] as illustrated in Figure 4. However, the precise definitions of each of the war forms that combine to make up Information Warfare (IW) are still under development.

This figure is not available online. Please consult the hardcopy thesis available from the QUT Library

Figure 4 Information Conflict Timeline[88]

The American's lead the way by publishing many[89] documents (eg. regulations, directives, manuals, handbooks, and instructions), which relate either directly or indirectly to information warfare including US DoD Directive TS3600.1, Information Warfare. TS3600 established information warfare policy and assigns responsibilities to the Assistant Secretary of Defence, as the primary point of contact for information warfare, NSA for information purposes in matters relating to technology and system development: and to the DISA, for the protection of the Defence Information Infrastructure (DII). The U.S.A.'s military doctrine is the most obviously advanced in development of IW

[88] _,*Joint Doctrine for Information Operations,* Joint Pub 3-13, Joint Doctrine Branch, US Dept of Defence, October 1998

[89] Joint Publication 1, Joint Warfare, refers to the "information differential." CJCS MOP 30, Command and Control Warfare (C2W) provides joint policy and guidance for both offensive and defensive aspects of C2W. Joint Staff publications CJCSI 3210.01, *Joint Information Warfare Policy* (U), January 1996, and CJCSI 6510.01A, *Defensive Information Warfare Implementation*, 31 May 1996. DA Pam 525-69, Information Operations: Army C2 Protect Library: *FM 100-6, Information Operations*: OPNAVINST 3430.26, Implementing Instruction for Information Warfare/Command and Control Warfare (IW/C2W): and AFI 33-207, Information Protection Operations.

doctrine, having placed volumes of information into the public domain. We assume that other nations have similar doctrine, but are less willing to share their approach. Numerous authors have envisioned possible models of future information warfare at all levels of society.

John Arquilla and David Ronfeldt are the authors of the influential RAND paper "Cyber war is Coming!"[90] This widely referenced work distinguished four basic categories of information warfare; Net War, Political, Economic and Cyber war, based on the information infrastructures. The war forms are organized as descending levels of abstract ideological conflict and ascending levels in the conventional conflict time line.

The Net warfare[91] (net war) form is information-related conflict waged against Nation-States or societies at the highest level, with the objective of disrupting, damaging, or modifying what the target population knows about itself or the world around it. While the target of net war may be a nation state, the attacker need not be. The network empowers attackers that may have no physical force, enabling them to mount an effective attack in the network domain, although their force is "asymmetric" relative to the target. The weapons of net war include diplomacy, propaganda and psychological campaigns, political and cultural subversion, deception or interference with the local media, infiltration of computer databases, and efforts to promote dissident or opposition movements across computer networks. The conflict is conducted over global information infrastructures (networks). Some have categorized net warfare actions as weapons of mass destruction used by terrorists, predicting that terrorism will adopt higher technology means to augment physical destruction.

Political warfare is through the institution of national policy, along with diplomacy, and threats to move to more intense war forms. While Economic warfare are conflicts that target economic performance through actions to influence economic factors (trade, technology, trust) of a nation. This intensifies warfare from the political level to a more tangible level. Cyber war or Command and control warfare[90] (C2W) is the most intense level that target opponent's military command and control. This military strategy implements Information Warfare on the battlefield and integrates it with physical destruction. Its objective is to decapitate the enemy's command structure from its body of command forces.

---

[90] Arquilla, J., and D. F. Ronfeldt, "Cyberwar is Coming!," J. Comparative Strategy Vol. 12, No.2, Apr.-June, 1993

[91] Arquilla, J. and Ronfeldt, D. F., The Advent of Netwar, National Defense Research Institute, RAND, Santa Monica, CA, 1996

Martin Libicki taxonomy consists of seven categories of information warfare that identify specific type of operations[92]. T Libicki's categories are as follows;

- Command and control warfare - Attacks on command and control systems to separate command from forces:
- Intelligence based warfare - The collection, exploitation, and protection of information by systems to support attacks in other warfare forms:
- Electronic warfare - Communications combat in the realms of the physical transfer of information (radio electronic) and the abstract formats of information (cryptographic):
- Psychological warfare - Combat against the human mind:
- Hacker warfare - Combat at all levels over the global information infrastructure
- Economic information warfare - Control of economics via control, information by blockade or imperialistic controls:
- Cyber warfare - Futuristic abstract forms of terrorism, fully simulated combat, and reality control are combined in this warfare category and are considered by Libicki to be relevant to national security only in the far term.

Robert Steele's taxonomy uses two dimensions to distinguish levels of technology and the nature of the combatant involved in them[93]. The first dimension is the means of applying technology in the conduct of the conflict. High-technology means includes the use of electronic information-based networks, computers, and data communications, while low-technology means includes telephone voice, newsprint, and paper-based information. The second dimension is the type of conflict: is either abstract conflict (influencing knowledge and perception) or physical combat. From these two dimensions, Steele defines four national-level domains of combatant all with the same objective of changing human perception and decision-making. The combatants that Steele defines are high-tech brutes, low-tech brutes, high-tech seers and low-tech seers described as follows;

- High Tech Brutes rely on money and capital, physical stealth of equipment, and precision targeting by highly technical munitions. Their vulnerabilities include command & control links, and especially commercial communications paths, and financial databases. Their capabilities are unsuited for combat

---

[92] Libicki, M., "What Is Information Warfare?", Center for Advanced Concepts and Technology, National Defense University, 1995, p.7.

[93] Steele, R. D., (USMCR), "The Transformation of War and the Role of the Future of the Corps," USMC document approved for public release, April 28, 1992. For a refined presentation of the concept, see "Creating a Smart Nation: Information Strategy, Virtual Intelligence, and Information Warfare" in Cyberwar: Security, Strategy and Conflict in the Information Age, Fairfax, VA: AFCEA Press

against low-tech single and mobile targets, or the mass movements of non-combatants.

- Low Tech Brutes rely on "low slow singleton" invisibility, which creates a "needle in the haystack" problem for high-tech brutes. So they can use the randomness of route and of objective to frustrate preplanned physical surveillance. Their capabilities match their goals and they are relatively invulnerable as a class due to high profits available (e.g. drugs) and leverage the high availability of expendable individuals.
- High Tech Seers rely on knowledge (inc. cyber-stealth that allows invisible access to knowledge bases). They are vulnerable as a class to high tech attack such as electromagnetic strikes which "melts down" entire communications and computing infrastructures. Single individuals are relatively invulnerable to detection and control, but are unable to deal with low- tech seers or low-tech brutes.
- Low Tech Seers rely on ideological appeal to masses. Impervious to high-tech brute attack if latter pulls punches and fails to take the ideo-cultural high ground. They are oblivious to terrorism, and insensitive to knowledge or profit pressures. Can only be defeated by a comprehensive ideological and cultural campaign which wins away its grass roots support.

Steele states that in a conflict an adversary may choose to conduct all four categories of warfare, orchestrated to achieve a common information objective.

Winn Schwartau[94] explained the broader threat to global information networks and extended the terminology of information warfare to apply to three domains of society: personal, corporate (or institutional), and national (or global). Schwartau domains are as follows;

- Class I – Privacy, includes the attack against an individual's electronic privacy, digital records, files, or other portions of a person's electronic essence.
- Class II – Espionage, includes industrial and economic espionage, the study and analysis of financial information (restricted and open source), means of putting a company's information systems out of commission, "denial of service", stealing secrets, eavesdropping on faxes, or reading computer screens, HERF Guns.
- Class III- Terrorism, is waged against industries, political spheres of influence, global economic forces, or even against entire countries. It is the use of technology against technology: it is about secrets and the theft of secrets: it is about turning information against its owners: it is about denying an enemy the ability to use both his technology and his information: waged across the global network by computers everywhere against computers everywhere.

[94] Schwartau, W., Information Warfare: Chaos on the Information Superhighway, New York: Thunder's Mouth Press, 1994.

These are not mutually exclusive domains within a conflict. Rather they exist for reference only. For example, Schwartau notes that an individual may attempt an attack on a nation or a corporation.

4.5 Early Information Wars

Information and information systems have moved from a secondary role in operations to increasingly becoming a target for operations in it own right. Modern warfare has seen a dramatic rise in the use and capabilities of systems and tactics that target the use information from disrupting an opponent's forces (e.g. jamming communications) through to undermining their will to resist (eg propaganda). Military (and business) analysts recognized the significant shift in approaches occurring from the rapid rise in use of electronic information technology since the middle of the 20th Century.

The Gulf war of 1991 between Iraq and American allies is popularly described as the first information war[95], which demonstrated the multiplier effect of information superiority. Technical reports[96] have provided detail analysis of the information-based strategy of the Gulf War, concluding that the Coalitions information infrastructure provided the "information differential" in terms of deception, manoeuvre, and speed. One of the starkest demonstrations of changes in thinking revealed through the Gulf War was the shift from physical weapons and targets as the central resource of the conflict to Information-based warfare (IBW) that accentuated information to gain advantage rather than physical weapons.

The objectives of the campaign were to subdue the aggressor's will, so that it resulted in the withdrawal of the forces that had annexed Kuwait. Coalition forces applied combinations of physical and non-physical actions against the Iraqi centres of gravity to subdue the will of Iraqi leaders, causing them to act in accordance with the coalition objectives.

The strategy included a strategic air campaign, which not only achieved traditional attrition of units but also aggressively hunted for command and control nodes. As the campaign continued air and ground units conducted

---

[95] The conflict occurred in the desolate "real-world" battle space, rather than an abstract info-sphere. Although Iraq was able to counter some information strategies the adversaries had such disparity in information power that the engagement was largely an information campaign for the Coalition, which allowed multiplication of the conventional combat power and the use of innovative technologies, as such it was an information based war (IBW) rather than a pure information war (IW).

[96] Campen's "The First Information War" described the C4I component systems employed in the Gulf War See Campen, A., *The First Information War*, Fairfax, VA: AFCEA International Press, 1992. Munro provided specific details focusing on the essentials of electronic warfare and its impact on command and control. See Munro, N., *The Quick and the Dead: Electronic Combat and Modern Warfare*, New York: St. Martin's Press, 1991.

relentless physical and electronic attacks on nodes, links and sensors. The strikes of the information infrastructure was a deliberate attack on Iraqi perceptions in order to disrupt the ability of Iraqi command to maintain awareness of Coalition actions and their own forces dispositions and status. The Coalition forces also applied an overwhelming military intelligence, which tracked precisely, identified Iraqi ground units that could be targeted with messages to impact on their psychological perception of the battle space. Deceptive operations were undertaken to influence Iraqi perception that the Coalition strategy included a major amphibious assault and that the U.S. would respond in kind (i.e. use Nuclear weapons) if Iraqi employed chemical-biological weapons[97].

This change in thinking is moving the object of conflict from physical assets to information assets, with the battle space moving from the material geographic plain to abstract info-sphere. While conflict in the material realm allows description of targets in terms of physical space and point in time, defining conflict boundaries in the info-sphere are more problematic. The Info-sphere blurs boundaries between civilian and military weapons and targets, for example much of the worlds military traffic is carried over civil communication infrastructure. The lack of clear boundaries necessitates caution to ensure that targeting and defence are effective. In protecting the National Interest, the State is faced with a complex battle space, which does not equate to its traditional physical or temporal boundaries. A Nation-States economic and military info-sphere certainly has domains within the physical realm of other states. Further, each Nation-States diverse interest further blur boundaries occur between times of peace and escalation to conflict. Whereas overt physical acts can be identified as the start of a phase of physical conflict, conflict in the info-sphere is inherently covert and less easily distinguishable from its legitimate use.

The information technology and information strategies that enhanced the IBW campaign could be seen at all levels of the conflict: from sensors used in night fighting, UAVs, command and control system, strategic deception and media management. The "all-ways" integration of information tactics into the concept of operations resulted in a transition from mass destruction of physical assets toward precision attack (eg. cruise missiles) and defence (eg. patriot) and even non-physical destruction-information warfare.

---

[97] Statements by U.S. secretary of state indicating in-kind response to weapons of mass ' destruction are presumed to be an influencing factor in Iraqi command withholding available chemical-biological weapons. Due to weapons conventions, the United States does not maintain chemical-biological weaponry, but considers nuclear forces as mass destruction weapons, implying the threat of a nuclear response to chemical-biological attacks. See Baker, J. A III, and T. M. DeFrank, The Politics of Diplomacy: Revolution, War and Peace, 1989-1992, New York: G. P. Putnam's Sons, 1995, p. 359.

4.6 Information Infrastructure Battle space

A battle space is the environment, factors, and conditions that must be understood to successfully apply combat power, protect friendly force, and complete the mission. In conventional warfare the Battle space includes the air, land, sea, space, the enemy and friendly forces, fixed and mobile facilities:, weather, terrain, the electromagnetic spectrum, and the information environment within the operational areas and areas of interest. Those who pose a potential threat to include hackers, disgruntled employees and contractors, criminals including organised crime groups, commercial competitors, issue motivated groups (IMGs), terrorists and terrorist organisations, and foreign forces including "hostile" States.

The new aspect to information warfare is the expansion of the battle space beyond the traditional military realm. Information targets and weapons can be drawn from both civil and commercial infrastructure of a nation, allies, or the entire global info-sphere. In the IW battle space the military is not restricted to the use of military style weapons. In addition, the Nation-State is not restricted to only using the Military to wage War.

Depending the objectives of the campaign, action can be undertaken exclusively against elements of the Defence Information Infrastructure (DII) or in wider information infrastructures. The DII are those systems most tightly linked to each Nation's military forces operations, normally specifically created for war fighting. Beyond a weapon's tactical information systems, even middle powers posses sophisticated command and control systems. These are integrated into command and intelligence systems that enable voice, data imagery to be delivered to commanders in the field. The DII may also interconnect with mission support networks and computers to provide a wider range of operational information (e.g. real time video) and then extend further into combat support services, such logistics and on into more civil functions such as payrolls.

The DII may depend on a broad range of civilian infrastructures such as public and private high-speed networks that offer narrow and broadband communications. The II that support the defense and intelligence functions of the Nation-State overlap with those that provide its other essential function and private sector infrastructure. The public and private sector information systems form a National Information Infrastructure (NII) that links individuals, organizations and the Governments together. It includes both large and small systems from satellites and ground stations and fiber optic bearers down to corporate databases, television, personal computer and consumer electronics. These and numerous other components support business of all kinds, and especially financial infrastructures.

The Banking and finance community has quickly moved to realise the potential of information and communication technologies (ICT). Banks worked hard through the 80s to grow new systems of Electronic Funds Transfer (EFT). These systems operated on private networks enabled new business models and extended the Financial Information Infrastructure (FII) deeply into retail and business environments. At that point in time, the Banks wisely recognised the need to protect the transactions following through these essentially untrusted links and nodes. The potential vulnerability of the infrastructure has been demonstrated on a number of occasions, for example in 1994, a group hacked into a major financial service company's cash management system and attempted transfers totalling $10 million[98].

Great efforts in Australia[99] and worldwide were undertaken to develop security standards which enable EFT to rapidly be adopted. These standards allow banking systems greater interaction with each other, further expanding the FII.

Infrastructures are often found to be under private sector control, and the joint public and private sector responsibility to defend these non-public (and non-military) assets becomes a problematic. It is especially acute problem where the NII supports the critical Nation-States operations (electricity generation, health care etc.) To complicate this responsibility, each NII is interconnected to the vast global communications networks, computers, and databases, into a web of global information infrastructures. Significant disruption (including destruction) in one area or grouping could cascade widely across many other groupings or areas of the NII. Besides the direct or indirect impact of the above on any particular government service, the political, strategic, economic and societal implications of this, where the disruptions are very widespread and serious, raises the fundamental issue of the challenge to government to continue to effectively manage national affairs in such a crisis situation. When considered at its broadest manifestation this is the global information Infrastructure (GII).

The GII today is largely seen as the interconnection of various public and private information systems much of which has its origins in the work of the

---

[98] Statement for the Record, Deputy Assistant Director and Chief, National Infrastructure Protection Center, Federal Bureau of Investigation, before the Congressional Joint Economic Committee, March 24, 1998

[99] In the mid 1980s numerous banking standards are developed including: AS 2805.4-1985 Electronic funds transfer - Requirements for interfaces - Message authentication, AS 2805.7-1986 Electronic funds transfer - Requirements for interfaces - POS message content, AS 2805.8-1986 Electronic funds transfer - Requirements for interfaces - Financial institution message content, AS 3521-1988 Identification cards - Physical characteristics, AS 3522 (parts 1 to 5) 1988 Identification cards - Recording technique (Embossing, Magnetic stripe, Location of embossed characters on ID-1 cards, Location of read-only magnetic tracks - Tracks 1 and 2, Location of read-write magnetic track - Track 3), AS 3524-1988 Identification cards - Financial transaction cards, AS 3525-1988 Bank cards - Magnetic stripe data content for Track 3,

U.S.A. Advanced Research Projects Agency[100] (ARPA) work. Under the post war threat of U.S.A. networks being attacked, ARPA looked at how to build resilient computer networks that could survive physical attacks[101] or malfunctions, resulting in the design of the "Internet" in 1968. A network was created linking academic institutions undertaking related research

The widespread interconnectivity of the GII also creates new challenges and risks to computer systems and, more importantly, to the critical operations and infrastructures they support, such as telecommunications: power distribution: national defence, including the military's war fighting capability: law enforcement: government services: and emergency services.

During the early 1990s the Internet usage exploded out of the research community to change the way advanced the world communicate and conduct business. Business is expected to be 24-hour-a-day operation, and electronic mail, Internet websites, and computer bulletin boards allow communication quickly and easily with large numbers of other individuals and groups across the GII. During 1991, the Banking industry continued to develop secure messaging systems and standards to support EFT[102]. The types of technical Standards [103] being delivered also reflect a wider more global "systems of systems".

The GII is the complex mesh that interconnects individuals, groups, and nations. It is practically boundless and is expanding as interconnection deepens through the continuous application of technology. IW makes all information sources and processes legitimate targets and potential weapons.

The information domain is the realm where a defender observes the world, monitors and measures the conflicts status, and communicates with its defence forces. We categorise it into three battle spaces[104] ;

- Physical - Physical items may be attacked (e.g., destruction or theft of computers destruction of facilities, communication nodes or lines, or databases) as a means to influence information. These are often referred to as "hard" attacks

---

[100] ARPA is now the Defense Advanced Research Projects Agency (DARPA)

[101] Anderson, R. H., and A. C. Hearn, "An Exploration of Cyberspace Security R&D Investment Strategies for DARPA: The Day After... in Cyberspace II, MR-797-DARPA," Santa Monica, CA, RAND, 1996.

[102] AS 2805.5.1/2/3/6 -1992 Electronic funds transfer - Requirements for interfaces - Ciphers - Data encipherment algorithm 1 (DEA 1), Modes of operation for an n-bit block cipher algorithm, Data encipherment algorithm 2 (DEA 2), Key management - TCU initialization – Asymmetric

[103] AS 3659-1989 Securities - International Securities Identification Numbering system (ISIN) and AS 3759-1990 Codes for the representation of currencies and funds

[104] Waltz, E. Information Warfare Principles and Operations, Artech House, August 1998

- Information infrastructure - Information content or processes may be attacked electronically (through electromagnetic transmission or over accessible networks, by breaching information security protections) to directly influence the information process or content without a physical impact on the target. These approaches have been distinguished as indirect or "soft" attacks.
- Perceptual - Finally, attacks may be directly targeted on the human mind through electronic, printed, or oral transmission paths. Propaganda, brainwashing, and misinformation techniques are examples of attacks in this realm

While the military is assumed to protect private sector assets (e.g. critical NII) in times of war, it does not have this mandate in peacetime. Yet, in contrast to industrial era warfare, it is unlikely that the transition from times of peace, to war will be clear. In addition, as the battle space described above is not defined in terms of a geo-spatial area of operations conventional description and legal frameworks do not apply well. A Joint Security Commission (JSC) was convened in the U.S.A. in 1993 to examine the processes used to formulate and implement security policy in the DoD and the Intelligence Community[105]. The Commission is highly critical of the condition of policy;

> *"the policies and standards upon which the Defence and Intelligence Communities base information systems security services were developed when computers were physically and electronically isolated".*

They conclude that the resulting policies and standards are not suitable for the networked world of today. Further they did not deal effectively with information systems security as part of a balanced mix of security countermeasures, were not flexible enough to address the wide variations among systems used or dynamically evolving information technology, did not differentiate between the security countermeasures needed in different environments and where information moved between networks of different security levels.

During 1994 many concepts surrounding the National Information Infrastructure (NII) were discussed by academics in papers[106] especially interoperability, as fundamental to issue realizing the potential of a NII. In February, the Joint Security Commission (JSC) published a report for the

---

[105] _,*Redefining Security A Report To The Secretary Of Defense And The Director Of Central Intelligence*, Joint Security Commission, Washington, D.C ,February 1994

[106] For example: In February the Computer Systems Policy Project identified critical interfaces in the NII, a June a workshop held by NIST (Technology Policy Working Group) looked at the need for NII interoperability and later a National Research Council Report[106] was issued, Harvard also addresses the broader challenge of standards policy for the NII. Also a Cross-Industry Working Team's report, "An Architectural Framework for the National Information Infrastructure", Several bills are before Congress in an attempt to address NII interoperability.

Secretary of Defence and the Director of Central Intelligence: "Redefining Security". [107] The report recommends, "using risk management as the underlying basis for security decision making". The report warned that computer networks are "a battlefield of the future" and that the risk was not limited to military systems. The Commission stated that, if an enemy attacked the unprotected civilian infrastructure, the economic and other results could be disastrous.

The GII as a battle space makes it difficult to distinguish between crime, industrial espionage, military reconnaissance and strikes[108]. This is especially the case where the technology of the information environment may enable anonymity or make it impossible to determine if the activity is domestic or foreign [109] In the Late 70s and early 80s, the impacts of the NII and GII caused Government concerns on many fronts. In Australia the Commonwealth passed new pieces of legislation in an attempt to better deal with Australia as an information centric environment: these included Australian Security Intelligence Organization Act 1979, Telecommunications (Interception) Act 1979, National Crime Authority Act 1984 and Freedom of Information Act 1982. In 1980 the OECD established Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.

IW attacks can occur anywhere within the GII, in particular, they may occur simultaneously, in multiple realms, using various attack vectors. The only criteria are that such an attack would allow an advantage to be obtained. Within the physical domain are workforces, resources, weapons, communication infrastructure, and leadership that provided the opponent with the capacity to react.

Physical force is the basic device of intimidation and the traditional vector for warfare by attrition. Physical attack will normally use heat, blast, fragmentation or other techniques to strike at assets in the physical domain and attacking the physical capacity of defender to respond. Targets will include military weapons, forces, bridges, roads, bases, communications lines, industrial capacity, economic centres, and other resources. Attacks are designed to disable the capacity to observe, to orient, to command, react with force or to destroy. Physical attacks on observation (sensors, communications) or orientation

---

[107] _,*Redefining Security*, A Report to the Secretary of Defense and the Director of Central Intelligence from the Joint Security Commission, Redefining Security: Joint Security Commission Report, Feb.1994, also see "Report of the Defense Science Board Summer Study Task Force on Information Architecture for the Battlefield," Defense Science Board, Office of Secretary of Defense, October 1994

[108] Hundley, R. O., and R. H. Anderson, "*Emerging Challenge: Security and Safety in Cyberspace,"* RAND/DRR-1382-CMS, RAND Corp., 1996.

[109] Molander, R. C., A. S. Riddle, and P. A. Wilson, "*Strategic Information Warfare: A New Face of War*," MR-661-0SD, RAND Corp., 1996

processes (command nodes) deny valuable information or otherwise corrupt the perception of decision makers.

Deceptive actions achieve a degree of surprise in attacks and seducing defender to orient to the attacker's advantage. The orientation may cause the defender to undertake ineffective and vulnerable actions. Deception enhances the effectiveness of all other attacks by reducing defender's effectiveness in both defence and offence.

While deception wishes to induce specific behaviours, psychological operations (PSYOPS)[110] are aimed at overall ability to perceive – causing a desired **disorientation** rather than a desired orientation by defender. Attacks at human perception seek to manage (or at least influence) the perception of defender about the circumstances of the conflict or action.

Electronic information vectors target the electronic processes and content of the information infrastructure (sensors, communication links, and processing networks) that provides observation and orientation to defender's decision makers. These attacks have the prospect to directly affect the ability and effectiveness of defender to perceive the conflict situation. Information attacks may directly attack the observation and orientation processes, contrasting with deception and psychological operations that must pass through the sensors etc. They do have the potential of inserting messages (inc. deception or psychological messages), disrupting or even destroying observation and orientation processes. Information attacks may have certain effects that cascade back into the physical domain, too. Attacks on computers or links controlling physical processes, such as power plants, pipelines, and machinery, can cause destruction in the physical domain. Here, we are focusing only on the means to influence the observation and orientation behaviour of defender, without examining all of the causal relationships between domains in the model.

4.7 OODA loop

The functional model[111] illustrated in Figure 5 depicts a blue force IW attack on red force in which society (population, private sector interests, economies): command authorities (political infrastructure and public sector): and media all come under attack in addition to the direct attack on red's DII.

[110] JP 3-53, Doctrine for Joint Psychological Operations, Joint Doctrine Branch, US Dept of Defence JULY 1996

This figure is not available online.
Please consult the hardcopy thesis
available from the QUT Library

Figure 5 Information Warfare Functional Model[111]

Both the DII and the NII are concurrent targets of a structured IW attack, which influences the OODA loop as well as the national objective of the "decide" element of the loop.

4.7.1 Observe and Orient

From a functional perspective an information war occurs within the adversaries observe, orient, decide, act (OODA) loop[111]. The objective of attacker is to cause the defender to act in a way that will aid in the attacker achieving it's objective. The defender must determine how to react to the actions of the attacker. The objective of each combatant is to cause their opponent/s to make mistakes, fail to achieve desired outcomes, surrender or withdraw from the conflict.

As actors grapple with Information Warfare, the OODA loop[111] describes how opposing forces attempt to influence each other in various ways. In early phases of competitive activities, parties try to learn about their opponent. Observations are made of the Battle space, which is known as intelligence preparation of the

[111] The OODA loop was developed by Col. John Boyd (USAF) in a classic briefing presented at Maxwell AFB entitled "*A Discourse on Winning and Losing*," in Aug. 1987. The concept is described in Orr, G. E., Combat Operations C3I: Fundamentals and Introductions, Maxwell AFB, AL: Air University Press.

battle space. Factors such as network topologies, identification of opposing, and other forces (a.k.a. orders of battle) modelling (political, economic, physical, and military) structures and processes. Should vulnerability be identified, attacker forces may be oriented to exploit it. This may represent a tactical advantage measured in seconds or a strategic weakness where orientation takes years. The defender may also observe vulnerabilities or deduce them from the orientation of the attacker and orient to counter threats.

4.7.2 Incident Detection and Response

The speed at which the GII could be exploited was illustrated in the major Internet security incident known as the Morris Worm[112]. The incident resulted in the creation of first Computer Emergency Response Team (CERT) being established in 1988 by ARPA within the Carnegie - Mellon University in Pittsburgh. Similarly the UK's Unified Incident Reporting and Alert Scheme (UNIRAS) was established in 1990 to centralise reporting of all detected IT security incidents occurring in the UK government departments and executive agencies[113].

Australia's AUSCERT was established in 1993 at the University of Queensland: by three Brisbane based universities in direct response to increased intrusions into their computers. As the only publicly accessible CERT in Australia it acts as both a central point of contact to the public and private sectors on computer security issues, and a range of advisory services including vulnerability assessments and defensive strategies. In the same year, that AUSCERT is established the Carnegie-Mellon University's CERT Coordination Centre reports that it has handled 1,334 reported incidents. Theses centres provide individuals, organisations and Nations with enhanced "observe" and "orient" capability. This capability enables coordination and communication amongst experts in order to limit the damage associated with, and respond to, incidents and building awareness of security issues across the Internet community.

A study done for the Commission by Carnegie-Mellon University's Computer Emergency Response Team (CERT) in 1997 confirmed, "Because the ties between critical infrastructures and the Internet will continue to become stronger and more intricate, the impact of an Internet attack could be devastating." CERT report to the Commission, January 1997, networking is increased exposure of data and systems to unauthorized and anonymous

---

[112] _,Virus Highlights Need for improved Internet Management, Report to the Chairman, Subcommittee on Telecommunications and Finance, Committee on Energy and Commerce GAO/IMTEC-89-57, GAO June 1989

[113] By the mid 90s there is an increasing number of statistics on the misuse of information systems. Such as the 1995/96 annual report by the UK's UNIRAS reporting 20% of all security incidents involved hacking.

access. By 1997 over 60 incident response and security teams spanning 16 countries were members of the Forum of Incident Response and Security Teams (FIRST). At least sixteen other countries have, or are in the process of establishing, a response team. The teams range from national coverage to specific government, academic and corporate coverage. Some corporate teams operate on a multinational basis. In general CERTs are either non-profit organisations, sometimes self-funded, or fully funded elements of other organisations. While individual CERTs' roles may vary, they generally receive reports of incidents, assist sites in recovery, develop solutions to identified vulnerabilities, and issue alerts and advisory notices on preventative measures. In some cases they undertake research, security training and consultancy services. In the case of a widespread attack it is not unusual for a number of CERTs to work together to address the problem.

These "observe" and "orient" processes are now dominated by the electronic systems; from the tactical weapon system to computerised stock market analysis. The defender's "observe" and "orient" processes provide Information Warriors with an additional set of targets that can influence options available and the outcomes of alternative actions.

4.7.3 Decide and Act

Opponents make decision regarding their courses of actions based on their perceived situation via these electronic systems. Three major factors influence defender's decisions resulting from attacks. These are the capacity, will, and perception[111] of the defender and are described as follws;

- **Capacity** - Attack on this capacity impacts the ability of defender to respond through physical force. This is measured in terms of capability to command and strength of force. Attrition warfare is based on the premise that the degradation of defender's war-fighting capacity will ultimately cause defender to make decisions that succumb to the attacker's objectives. Capacity is not measured in a single magnitude and is defined in many components, including mass, "centres of gravity" strategic characteristics, capabilities, or localities from which a military force derives its freedom of action, physical strength, or will to fight.
- **Will** - The will is a human factor that is a measure of the resolve or determination of the human decision maker(s) and their inclination toward alternative actions. This element is the most difficult for the attacker to measure, model, or directly influence. The strength of will to take actions to achieve a stated objective or purpose may transcend "objective" decision criteria. Confronted with certain military or economic defeat, the will of a decision maker may press on, no matter how great the risk. In this way the action may even appear irrational (in military or economic terms).

- **Perception** - Perception is the understanding of the situation from the perspective of defender. It is an abstract information factor, measured in terms such as accuracy, completeness, confidence or uncertainty, and timeliness. The decisions that defender makes are determined by the perception of the situation (attacker's attacks on defender) and the perception of defender's own capacity to act. Based on these perceptions, the perceived alternative actions available and their likely outcomes, and the human willpower of decision makers, defender responds.

In the perceptual realm, we confront the complexity of waging war in the information battle space or Info-sphere. Attacks on those factors that influence defender's decisions (capacity, will, and perception) are valid targets in Information Warfare. Psychological attacks result in one party never fully realising the significance of the actions of the opponents information warriors or even that an information war is occurring. Such careful management of the other party's perception blinds the opponents and as Sun Tzu suggested "break the enemy's resistance without fighting". Such skill would represent the highest level of information conflict. However, we are not of the opinion that such capability is likely in the near future[114].

4.8 Chapter Conclusions

In this chapter, we identified the elements and goals of information warfare to understand how this form of war impacts on economic systems during conflicts. We outlined the revolution in military affairs and the shift in approaches to conducting future wars. Our review of contemporary taxonomies established the nature of doctrine under which information warriors will fight.

We found no evidence that any foreign or domestic organisation was deliberately developing a specific capability to attack the Australia's FII. However, it would be unlikely that any adversaries would flag their intent or contingencies openly. Many Nations are known to have developed some level of information warfare capability[115].

We established the techniques that allow small groups to create asymmetric impact on a large power through targeting critical infrastructures. Based on our

[114] The "fight less" or "bloodless" war suggested by some authors is conceptually problematic in that one party must at least commit some effort to the conflict. Even if such a conflict is unconscious and bloodless for the opponent, it does not mean that no effort has been expended to achieve victory. This effort represents the substitution of physical activity and mortal risks for some other intangible activity and risks resources. If this substitution is investment in carefully planning an information operation or simply outthinking the opponent, these then must be considered weapons that harm the opponent interests.

[115] At least 30 Nations are known to have begun developing some capability for information warfare. See Waitzman, W. *In a World Without Frontiers, Every Battle Can Hit Home*, *Barron's*, March 1996

analysis we argue that this form of war is more accessible. The wide discussion of asymmetric warfare makes it highly likely that large numbers of adversaries will have considered the vulnerabilities of their opponents. It is naïve to believe that combatants have not analysed the vulnerabilities of their opponents to economic information warfare and considered strategies for targeting the global or local FII.

Contemporary conflicts (inc. Iraq, Israel, Kosivo, Chechnya, Afghanistan) have shown how different tactics, equipment, training, and skills are being used in modern warfare, including Information Warfare. Although several large-scale conflicts may occur, numerous conflicts are unlikely to be able to utilise divisions of troops or clearly defined battle space in geographic terms over a limited period.

Numerous offensive and defensive contingencies require capabilities, which involve small organic units operating in urban terrain over long periods (years), using new weapons and asymmetric techniques. Nation-States are attempting to re-orient and improve their mass armies to non-conventional and special forces. While they attempt to change to face the new operating environment, their more nimble adversaries already take this form. Stateless actors, separatist and fringe independence movements, organised crime, ideological extremists, and other potential actors (e.g. hackers, corrupt executives) have become networked organisations and adapted to a more insidious type conflict. "Terrorist style" tactics are both evolving from the inability for groups and Nations to undertake open conventional warfare. These capabilities are also devolving, spreading outside traditional military structures and it constrains.

These actors (inc aggressive states) desire the capability to infiltrate environments, exploit Weapons of Mass Destruction (WMD), Information Warfare (IW), and other unconventional threats. Some of these will provide the capability to maintain a degree of anonymity. Aggressors have already discovered that business infrastructure and economic targets are safer targets and highly effective in disrupting the opponents operations. Being able to create general civic breakdown and unrest (e.g. riot) may be more easily achieved by a wide-scale disruption economic activity rather than direct attack on military or government targets. Using terror and low intensity warfare tactics against civic or economic targets enables the aggressors to leverage the fragility of large urban infrastructure, which do not have the same protection and resilience as military environments. Adversaries are also likely to maximise diverse and differing vectors to overcome opponents, so that conventional attacks would be conducted in conjunction with multiple infrastructure attacks.

As we have seen, in some regions (e.g. Colombia, Pakistan, Burma, Soviet Union) there is the potential for capability to be resourced by wealthy foreign government or corporate sponsors. Extralegal or "mafia" corporations that

attempt to infiltrate or subvert legitimate business, benefit from the disruption of competitors and destabilization of uncooperative governments. It must be remembered that the drug and crime driven "underground economy" in some nations rivals that of official legitimate economy. Not only does this sponsorship create a direct threats, it allow capabilities to "leak" to splinter and extremist groups who may put them to different use than originally envisaged by the sponsor.

The unintentional vulnerabilities introduced by new and emerging technologies have reduced the cost of acquiring information warfare capabilities. Especially in the case of commonly used commercial grade information and communication technology, damaging techniques are rapidly distributed amongst loose networks of hackers and easily acquired by aggressors. Many of these commercial grade systems and their accompanying vulnerabilities are finding their way into high security environments and national information infrastructures exposing these environments to aggressor's capabilities.

Those that can cause harm to our FII are not limited to external threat. Significant damage may also result from the insider threat. Attacks pre-armed with the information, opportunity and skill present an extreme threat. The motivations for insider attacks may come from disgruntled (e.g. financially) or disturbed (e.g. stressed) employees, activist, subverted (e.g. traitors) or compromised staff (e.g. drugs, gambling, blackmail).

We conclude this chapter by asserting that the changes in vulnerabilities and rising capabilities of adversaries require focusing our counter-measures and security structures on economic information warfare.

Chapter 5. **Review of Policy**

"The crisis in the Persian Gulf offers a rare opportunity to move toward an historic period of cooperation. Out of these troubled times, a new world order can emerge in which the nations of the world, east and west, north and south can prosper and live in harmony. Today the world is struggling to be born"
George Bush[116].

Ten years later to the day, terrorists struck the World Trade Centre and the Pentagon.

Chapter Overview

In this chapter we show how the Governments are responding to the security dimensions described earlier and in particular the threats to information systems. We demonstrate the high level of concern that developed nations (especially the United States) have about scenarios that involve in attacks on information infrastructure and Information Warfare. In particularly we highlight the initiatives and policy that attempt to protect critical infrastructures from cyber attack both in Australia and in other nations.

5.1 President's Commission on Critical Infrastructure Protection

5.1.1 Heightened Awareness

The Tofflers' War and Anti-War works heightened the awareness and study of the implications of information warfare at a popular level. At the technical and operational levels, a number of publications, conferences, and formal studies by the U.S.A. DoD Defence Science Board increased awareness. They have also increased the legitimacy of calls to prepare for information threats to national security in the United States, UK, Australia, and other nations with high information technology dependencies.

[116] Bush, President G. H. W., President's Address to Congress, September 11, 1991

In September of 1994, U.S.A. Presidential Decision Directive 29 (PDD 29)[117] was made stating that a new security process is required and that the process should be based on sound threat analysis and risk management practices[118]. The U.S.A. GAO increasingly raises concerns about the U.S.A. Federal agencies computer security weaknesses and makes scores of related recommendations. Agencies are having difficulty in determining how to incorporate risk management into its current processes as it confronts a "risk avoidance" culture that developed and matured during the "Cold War". Reports also highlighted a need for uniformity in skills and knowledge taught security professionals to build a common understanding and implementation of security policies and procedures.

In response to bombing of the Murrah Federal Building in Oklahoma City in 1995 (April 19), the U.S.A. Attorney General created the Critical Infrastructure Working Group (CIWG) which conducted limited examination of threats and vulnerabilities of critical national infrastructures, marking a rise in the awareness in the area of Critical Infrastructure Protection (CIP).

In June 1995, U.S.A. Presidential Decision Directive 39 (PDD 39)[119] was issued, enumerating responsibilities for federal agencies in combating terrorism, including domestic terrorism. Recognizing the vulnerability of the United States to various forms of terrorism, Other U.S.A. federal agencies, including those in FEMA: the Departments of Justice, Health and Human Services, and Energy: and the Environmental Protection Agency, also developed programs to assist state and local governments in preparing for terrorist events. The OTA published an update of their 1994 report entitled "Information Security and Privacy in Network Environments" which provided useful summaries of the privacy and security background and issues associated with computer networks. U.S.A. Defence Science Board Task Force also reported on Information Warfare[120] and the Director of Central Intelligence stated that there is evidence that "a number of countries are developing the doctrine, strategies, and tools to conduct information attacks" and that "international terrorists groups clearly have the capability to attack the information infrastructure of the

---

[117] _, *Security Policy Coordination*, Presidential Decision Directive/Nsc – 29, The White House, Washington, September 1994

[118] Also supported by Director Central Intelligence Directive (DCID) 1/7, "Security Controls on Dissemination of Intelligence Information," Central Intelligence Agency April 1995

[119] _, *Counterterrorism Policy*, Presidential Decision Directive/Nsc – 39, The White House, Washington, June 1995

[120] Information Warfare: Defense - providing independent advice to the Secretary of Defense related to defensive information warfare capabilities.

United States."[121] The U.S.A. NII Security Forum released the report on the NII Security.[122]

On May 20, 1996, the Interagency Working Group on Cryptographic Policy issued a draft report: "Enabling Privacy, Commerce, Security and Public Safety in the Global Information Infrastructure"[123]. The report presents a vision for developing a cryptographic infrastructure that will protect valuable information on national and international networks. Further, the report outlines a course of action for developing an infrastructure that will protect valuable national information resources on national and international networks. It concludes that Government and industry must work together to create a security management infrastructure and attendant products that incorporate robust cryptography without undermining national security and public safety.

In the same year, the Information Science and Technology (ISAT) office of DARPA's commissioned a Study on Survivable Distributed Information Systems[124]. The purpose of the study was to determine whether the nation's critical information infrastructure could be hardened to improve survivability against a wide range of possible intentional and accidental threats. The study found the following:

- The systems that matter are often complex and unstructured with multiple legacy and commercial off-the-shelf components.
- The process of hardening complex systems is poorly understood.
- Laboratory successes are not impacting the nationally critical technologies.
- There is a requirement for a practical technology for selectively hardening complex systems to achieve high confidence solutions.

The greatest concern was that hackers, terrorists, or other nations could use information warfare techniques as part of a coordinated attack to seriously disrupt electric power distribution, air traffic control, or financial sectors. Not ignoring non-cyber threats the U.S.A. Congress passed the Defence against Weapons of Mass Destruction Act of 1996 (also known as the Nunn-Lugar-Domenici program) to train and equip state and local emergency services personnel who would likely be the first responders to a domestic terrorist event.

---

[121] _, Statement for the Record by the Director of Central Intelligence to the U.S. Senate Committee on Governmental Affairs, Permanent Subcommittee on Investigations, *Foreign Information Warfare Programs and Capabilities*, June 25, 1996

[122] _, NII Security: *The Federal Role - a report by the NII Security Issues Forum articulating information assurance expectations for the NII*, NII Security Issues Forum, 1995

[123] _, *Enabling Privacy, Commerce, Security and Public Safety in the Global Information Infrastructure*, US Interagency Working Group on Cryptographic Policy, May 1996

[124] _, Survivable Distributed Information Systems, ISAT Defensive Information Warfare Summer Study. ARPA, 1995

5.1.2 Critical Infrastructure Working Group

On 6 February 1996, the Critical Infrastructure Working Group (CIWG)[125] issued a report recommending the creation of two organizations to address current and future threats and vulnerabilities. Subsequently the U.S.A. President Clinton signed Executive Order 13010 on 15 July 1996[126]. Executive Order 13010 establishes the Infrastructure Protection Task Force (IPTF) as an interim coordinating measure for the short term and the "President's Commission on Critical Infrastructure Protection" (PCCIP) for the long term. The Task Force was created within the Department of Justice as an immediate measure because threats were considered authentic and impending and to increase the:

> *"coordination of existing infrastructure protection efforts in order to better address, and prevent, crises that would have a debilitating regional or national impact."*

The critical infrastructures are defined as those whose incapacity or destruction would have a debilitating impact on the defence or economic security of the USA. There are eight particular infrastructures considered the backbone of the nation's defence and economic strength. The Executive Order 13010 detailed these eight categories of critical infrastructures PCCIP was to recommend a national protection and assurance policy to ensure their continued operation. These are as follows;

- Electrical power systems - Consists of generation, transmission, and distribution systems that are essential to all other infrastructures and every aspect of the economy.
- Gas and oil storage and distribution - Fuels transportation services, manufacturing operations and home utilities that serve as a vital part in the readiness of armed forces and sustainment of operations overseas.
- Telecommunications - Consists of the transmission of signals and information that are essential to all other infrastructures and every aspect of the economy.
- Banking and finance - Manages trillions of dollars, from deposit of individual payments to the transfer of huge amounts in support of major global enterprises.

---

[125] Gorelick, J., U.S. Deputy Attorney General; Statement Before the Senate Committee on Governmental Affairs Permanent Subcommittee on Investigations, July 16, 1996.

[126] _, *Executive Order 13010 of July 15, 1996",* Executive Order 13010—Critical Infrastructure Protection, The White House, Presidential Documents, Federal Register, Vol. 61, No. 138, Wednesday, July 17, 1996

- Transportation - That moves goods and people within and beyond borders, and makes it possible for the United States to play a leading role in the global economy.
- Water supply systems - That assures a steady flow of water for agriculture, industry (including various manufacturing processes, power generation, and cooling), business, fire fighting, and our homes.
- Emergency services - In communities across the country responds (including medical, police, fire, rescue) to our urgent needs, saving lives and preserving property.
- Continuity of government - Federal, state and local agencies that provide essential services to the public, promoting the general welfare.

The Executive Order acknowledged that many of these critical infrastructures are owned and operated by the private sector and it stated that:

> *"it is essential that the government and private sector work together to develop a strategy for protecting them and assuring their continued operation"*[126]

The Commission was chaired by retired Air Force General Robert T. Marsh and was comprised of members of the federal government and industry. A Steering Committee of senior government officials and an Advisory Committee of key industry leaders guided its work. The Commission was chartered to conduct a comprehensive review of infrastructure because

> *"Certain national infrastructures are so vital that their incapacity or destruction {by either physical or cyber attack} would have debilitating impact on the defence or economic security of the United States."*[126]

The RAND Corporation was asked in 1996, to provide and exercise[127] to test the plausibility of strategic attack via information warfare tactics against the United States vital interests. Senior members of the national security community, telecommunications, and information systems industries were involved in the exercise. The basic conclusion was that key national military strategy assumptions are obsolescent and inadequate for confronting cyber threats that could possibly be cyber-terrorism.

Across the U.S.A. Federal Government, a CIO Council was established through the requirement in the Clinger-Cohen Act of 1996. GAO September

---

[127] Molander, R. C., *Strategic Information Warfare: A New Face of War*, (Santa Monica, CA: National Defense Research Institute, 1996)

report again concludes that more effective actions were needed at the government wide level. The GAO continues to issues reports[128] that provided a view of security problems and the need for concerted improvement efforts. In February 1997, in another series of reports to the Congress, GAO designated information security as a new government-wide high-risk area[129]. .These reports concluded that in the U.S.A. that poor information security was a widespread Federal problem with potentially devastating consequences. It recommends that the Office of Management and Budget (OMB) play a more proactive role in overseeing agency practices and managing improvements.

Vulnerability to an adversary using "cyber" tools was examined during a military exercise[130] conducted in 1997. The scenario featured "scripted" attacks on the energy and telecommunications infrastructures (controllers injected incidents into the scenario: military commands and government agencies reacted as though the reported incidents were real). Companies providing electrical power in selected cities were subjected to scripted attack by cyber means, over time, in a way that made the resulting simulated outages appear to be random and unrelated. Concurrently, a "Red Team" used hacker techniques available on the Internet to attempt to penetrate Department of Defence (DoD) computers. With no insider information, and constrained by U.S.A. law, the team spent three months probing the vulnerabilities of several hundred unclassified computer networks. They were able to penetrate many of these networks, and even gained system administrator level privileges in some. In addition IDA produced a National Strategies and Structures for Infrastructure Protection in 1997 examining critical infrastructure vulnerabilities and threats, with particular emphasis on the newly emerging dangers associated with "cyber attacks". Audit reports by the U.S.A. GAO in 1998 still show that largest U.S.A. federal agencies have significant computer security weaknesses[131]

5.2 Australia's Response

In November 1996, Australia's Defence Signals Directorate (DSD) advised the Secretaries Committee on National Security in its annual report on Australian

---

[128] The GAO reported in September 1996, that since September 1994, serious weaknesses had been reported for 10 of the largest 15 federal agencies Information Security: Opportunities for Improved OMB Oversight of Agency Practices (_, GAO/AIMD-96-110, September 24, 1996). that since September 1994, serious weaknesses had been reported for 10 of the largest 15 federal agencies. Information Security: Opportunities for Improved OMB Oversight of Agency Practices (_, GAO/AIMD-96-110, September 24, 1996).

[129] _,GAO *High Risk Series:* Information Management and Technology (GAO/HR-97-9, February 1997)

[130] _,U.S.A. Chairman of the Joint Chiefs of Staff Exercise *Eligible Receiver* 1997

[131] _, *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk*, GAO/AIMD-98-92, September 23

Government Electronic Security that it would be publishing in early 1997 a major report on threats and vulnerabilities to Australia's national information infrastructure (NII).

The first official DOD definition of IW[132] was published in 1996. The Australian Defence Force (ADF) adopts the working definitions IW used by U.S.A. (and the UK). This redefined some elements previously included in the IW concept as now being part of 'information operations'. These new definitions are:

- Information Operations (IO): Actions taken to affect adversary information and information systems, while defending one's own information and information systems, and
- Information Warfare (IW): IO conducted during times of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.

The pivotal year ends with the U.S.A. National Institute of Standards and Technology releasing An Introduction to Computer Security Handbook [133] in December

In February 1997, the Defence Signals Directorate (DSD) published the classified report on Australia's National Information Infrastructure: Threats and Vulnerabilities. The contribution of DSD, and especially that of Ian Dudgeon, the consultant who did the original work in this area, could not be credited publicly until this point. The unclassified version[134] of the report was also published with a number of recommendations. These recommendations were:

- Establishment of a formal structure involving both Government and the private sector to coordinate and implement national policy for protection of the NII.
- That insufficient information is available about the actual threats to our NII. There is a need to put in place, within government, procedures to detect, collate, and assess IT security incidents,
- To increase IT security generally through improved awareness and other programs.
- No formal structure exists for the coordination and implementation of a national policy for protecting and assuring the continued operation of critical elements of the NII in peace or during hostilities. It concluded that a structure should be established that includes private sector participation.

---

[132] _, U.S.A. DOD *Directive S-3600*.1, 9 December 1996,

[133] _, *An Introduction to Computer Security: The NIST Handbook*, Special Publication 800-12, National Institute of Standards and Technology, December 1995

[134] _, *Australia's National Information Infrastructure: Threats and Vulnerabilities*, Defence Signals Directorate, February 1997. http://www.asio.gov.au/Work/Content/niireport/niirpt.htm

In forming its recommendations, the report considered developments in the United States, the United Kingdom and Canada however, Australia's difference size and circumstances necessitated adjustments.

The key industry (or functional) groupings emerged out of the three areas mirrored the U.S.A. approach. The DSD defined the NII as encompassing three areas that impacted on the political and socio-economic well being of the Australia. These three sectors were described as National security community, civil government, and the Private sector. Each sector can be described as follows;

- National security community - This sector includes the Defence Forces, the intelligence and security agencies, law enforcement and emergency services, and DFAT's diplomatic missions abroad. Information within this community is mostly classified, stored and processed in restricted-access databases and transported with encryption protection over wide area networks (WANs) within or between agencies and departments.

- Civil government - This sector includes those areas that deal with other "sensitive" information unrelated to national security but which is vital for good government and the national well-being such as Treasury, Finance, Social Security and Taxation as well as statutory authorities or Government Business Enterprises (GBEs) involving banking (the Reserve Bank), transportation (Air Traffic Management), telecommunications, broadcast radio and TV (Radio Australia, ABC), and electricity and water. This area includes the data bases, control and communications systems central to the functioning of government departments

- Private sector - This sector includes those that provide key services of national interest, some of which parallel the functions of GBEs. These include banking and finance, the Stock Exchange, the economic market place generally, telecommunications (Optus), and non-State transportation and information (radio, TV, the Internet). The security measures to protect key aspects of information or information systems within the private sector range from very high to very low.

While the issue of information assurance applies to the individual networks and systems within each of the above areas and groupings, also of importance is the very high level of interdependence amongst these areas and groupings.

The Secretaries' Committee on National Security (SCNS) considered the DSD Report on 18 August 1997[134]. The SCNS accepted the recommendations and tasked the Attorney-General's Department with establishing an interdepartmental committee (IDC) to examine measures to implement the recommendations for protecting the NII and report back by the end of 1998.

The IDC consulted relevant stakeholders in both the Commonwealth, banking and finance, communications, energy and utilities and transport sectors, establishing an interim Consultative Industry Forum (CIF). The CIF involved experts and industry peak bodies representing the private sector owners or operators of the NII. The SCNS continued the Industry Forum to provide industry input to policy development and facilitate the development of industry responses to Government policy. The CIF met quarterly and has agreed with the general approach proposed. The SCNS also recommended the continuation of the existing IDC as a Standing Interdepartmental Committee for Protection of the National Information Infrastructure (SIDC) responsible to SCNS.

5.3 Critical Foundations Report

The President's Commission on Critical Infrastructure Protection released its landmark report "Critical Foundations: Protecting America's Infrastructures"[135] on 13 October 1997. The report found no evidence of an impending cyber attack that could have a debilitating effect on the Nation's critical infrastructures. However, it did conclude that all critical infrastructures are increasingly vulnerable to attack. Some of the findings included:

- Both the capability for harm and the vulnerability of our [USA] infrastructures are serious risks:
- Neither the warning capability nor a nation-wide analytic capability exists to protect infrastructures from a concerted attack.
- Neither government nor industry are prepared to deal with these types of threats, nor do they share the relevant information that might give warning of a cyber attack.
- Finally, R&D efforts are not sufficient to address the cyber threat.

Although the threat of an Internet attack at the time appeared small, the prospect for such attacks in the future was found to be significant

The Commission Chairman[136] testified "the nation's critical infrastructures—telecommunications, water supply, electric power, banking and others—have substantial vulnerabilities that can be exploited by terrorists and foreign powers". Deputy Secretary of Defence (John Hamre,) likened the scenario to an

---

[135] _,: _, *"Critical Foundations: Protecting America's Infrastructures The Report of the President's Commission on Critical Infrastructure Protection*, President's Commission on Critical Infrastructure Protection, United States Government Printing Office, October 1997.

[136] In testimony by General Robert T. Marsh before the Senate Judiciary Subcommittee on Technology and Terrorism,

electronic Pearl Harbour, and warned, "there will be an electronic attack sometime in our future."

The "Critical Foundations" identified potential threats as including insiders, recreational and institutional hackers, organized criminals, industrial competitors, terrorists, and states. Because the nation's critical infrastructures are mainly privately owned and operated, the Commission concluded that "critical infrastructure assurance is a shared responsibility of the public and private sectors", and the only sure way to protect infrastructures is through a real partnership between infrastructure owners and the government.

From the Report, several critical infrastructures had been identified specifically as strategic targets that could be disrupted by "cyber" terrorism and information warfare operations based on the 1996 Executive Order 13010. The emphasis on these targets resulted from their integrated roles serving the vital interests and defence posture of the United States. Serious and cascading effects on the U.S. national security operations and private industry would likely to result if these targets were disrupted or destroyed.

The significance of these finding resulted in a Presidential Directive (PPD-63) to establish within the United States, a national centre and coordinator to warn of and respond to information warfare and cyber terror attacks. The creation of this agency acknowledged the degree of threat posed by terrorism and information warfare may degrade military and civilian operations can, and may indeed, be a strategic threat to U.S. vital interests.

In June 1998 (again in February 1999), the Director for Central Intelligence testified[137] that several nations recognize that cyber attacks against civilian computer systems represent an option they could use to "level the playing field" during an armed crisis against the United States, and they are developing information warfare capabilities. He added that terrorists and others were beginning to recognize that information warfare offers them "low cost, easily hidden tools to support their causes".

5.4 Activity in Australian

In December 1998 as required by the Secretaries' Committee on National Security (SCNS), interdepartmental committee (IDC) reported[138] on its review of measures to implement the recommendations for protecting the Australian NII.

---

[137] Testimony by Director for Central Intelligence before the Senate Committee on Governmental Affairs, June 24, 1998

[138] _, *Protecting Australia's National Information Infrastructure*, Report Of The Interdepartmental Committee On Protection Of The National Information Infrastructure, Attorney-General's Department, Canberra December 1998 www.asio.gov.au/Work/Content/niireport/niirpt.htm

Because of security planning made under Australia's National Anti-Terrorist Plan for the 2000 Olympics, major changes or agency mergers to address the issue were not suggested. Instead a coordinating body was created, the National Information Infrastructure Protection Secretariat (NIIPS) within the Protective Security Coordination Centre of the Attorney-General's Department (PSCC).

The technical response capability was to be the primary responsibility of DSD with expansion of the role of DSD's National Computer Security Authority (NCSA) to deal with damage to, or disruption of, data and systems, including those in the private sector. DSD also had its role expanded to provide increased analysis, threat assessment and protective security capabilities for ASIO.

The roles of AFP and the Information and Security Law Division of Attorney-General's Department were also expanded. In developing the framework the IDC was conscious of the role of the Australian Computer Emergency Response Team (AusCERT) as being complementary to DSD's NCSA. AusCERT has expressed concerns that the establishment of the proposed national framework may have some short-term impact on the viability of AusCERT.

The Australian National Audit Office conducted a review[139] of Internet Security Management in 1997-1998 within the Commonwealth public sector and to provide better practice guidance for managing an Internet connection. The results of the audit were that most agencies had some of the core elements required for effective Internet management: however, improvement was required in several key areas: and a small number of agencies were operating and managing their Internet facilities at or near identified better practice. In May 1998, the Australian Government also announced the publication of the Gatekeeper Report, which outlined the strategy for the use of Public Key Technology for securing electronic transactions in Commonwealth agencies.

The 1998 explosion at Esso's Longford gas plant and Victoria's gas crisis [140] and the Sydney's water supply contamination[141] highlighted the potential vulnerability, social disruption and exposed the vulnerability of some of Australia's infrastructure. Within the emergency management community, the term 'community lifelines' or 'infrastructure lifelines' are used to describe systems or networks that provide for the circulation of people, goods and services and information upon which health, safety and comfort and economic activity depend. In 1998 the EMA an agency within the Department of Defence

---

[139] _, Australian Government Audit Office, *Internet Security Management 1997/1998* (Tabled: 27/11/1997) Financial Control and Administration Audit Report No. 15

[140] _,Longford Royal Commission Report Longford Royal Commission, Information Victoria, Melbourne, June 1999, In New Zealand, Auckland's power crisis also occurred in the same period, providing an example of infrastructure failure that had a devastating economic effect.

[141] Korzy, M., Water Boiling For 3 More Days At Least – Health Department, AAP, Sydney Aug. 27 1998

advised that the value of this infrastructure is estimated to be of the order of $400 billion with around 10 to 25% of business input costs being infrastructure related. EMA also reports that much of Australia's infrastructure is ageing, lacks robustness, has little redundancy, and is costly to maintain. Due to high cost, owners are reluctant to replace it until forced to do so by an event that brings the service provided into public focus.

Following on the initiatives identified in the National Information Infrastructure: Threats and Vulnerabilities Report, the Australian Commonwealth Government makes commitments to expand the Australian Federal Police[142] with additional Computer Crime Teams and training program targeting AFP investigators in computer search and evidence recovery procedures for routine matters. The Government has difficulty retaining these AFP experts, whose expertise is sought after in the private sector, offering significantly higher salaries.

Several committees and events have occurred with parties attempting to address the complex issues that span commercial-government and inter-agency responsibilities. There has been little in the way of resources or authority to do anything material for NII protection. Government agencies with traditional information security focus (e.g. AG's PSCC, AFP, DSD, ASIO) still struggled to engage with the Australian Business who are cautious and suspicious of what outcomes can be achieved. However, in the past few years we have seen some positive trends.

- Executive-level understanding of information security is improving, through increased coverage in business publications and requirements to manage operational risks.
- Coordination of individual and collective agency efforts are becoming more focused, through the efforts of NOIE and the Attorney Generals department.
- Awareness of technical threats is more widely understood in the community and ICT circles. Increasing use of the Internet in Australia has fuelled discussion of information system vulnerabilities more common in the popular and trade press. Some incidents such as large-scale virus events have even made front-page news.
- Agency discussions are beginning to result in budget and policy changes. Recent budget announcements clarify responsibilities and direction for NII

[142] At the time, the Australian Federal Police had computer crime teams in Sydney, Melbourne, and Perth, with an Electronic Forensic Support Team located in Canberra. The teams provide technical assistance and advice to operational elements of the AFP in circumstances where computer technology has been used to commit an offence, where evidence of criminal activity may be located on electronic storage devices, or where specific technical skills are required to investigate computer crimes such as computer intrusion. AFP teams also provide a forensic collection and analysis service for other Commonwealth and State agencies when required. New teams where planned for Canberra and Brisbane during 1998/99 and 1999/2000 respectively.

protection. The Federal departments and agencies have initiated coordinating activities.

- The Department of Defence is moving aggressively to incorporate information, tools, and support for information warfare concepts and initiatives in all services. The services all recognise the priority to integrate network with strong security management functions.
- The Commonwealth is moving to leverage the commercial operations of AusCERT, possibly by significant endorsement or funding.
- Working groups conducted National-level threat assessment processes.

A number of technical committees and other forums provide cross industry co-ordination within Australia. Some of these may provide a focus for co-ordinating FII protection. Unfortunately, many of the forums are limited to specific product or system lines (eg. securities, superannuation, insurance, payment streams). We suggest that co-ordinating FII protection be clearly made the responsibility of the RBA (under Section 10.(2).(c)) of Bank's charter. This section already states that the RBA contribute to "…the economic prosperity and welfare of the people of Australia".

Further, the RBA also has responsibilities in applying the Core Principles for Systemically Important Payment Systems (CPSIPS), from the Bank for International Settlements (BIS). These principles were established in January 2001 and define central Banks responsibility. This includes the Banks responsibility to "cooperate with other central banks and with any other relevant domestic or foreign authorities". Principles number VII. states, "The system should ensure a high degree of security and operational reliability and should have contingency arrangements for timely completion of daily processing." which clearly aligns with FII protection objectives. The RBA should chair a Systemically Important Economic Systems (SIES) forum which includes APRA, ASIC, Austrac, Treasury, ABA, APCA, and direct representative from major Australian financial business (inc. NAB, ANZ, CBA, WBC, AMP) should establish forum to advise the government. The forum should establish working parties to deal with various issues including: legislation changes (in conjunction with AG's and Legal Associations), international relations, telecommunication services (in conjunction with ATUG), technical measures (in conjunction with existing Australian Standards IT12/4 committees). The Forum should also make representatives available to inter-industry task forces on issues such as incident reporting and management (in conjunction with existing AusCERT, AFP, ADF initiatives).

5.5 Development of Global Frameworks

Canada's approach to NII protection is to expand existing protective security arrangements rather than establish new agencies. The Department of National Defence is to support civil agencies in the same way as it does in other areas (such as natural disasters) responding to emergencies. The level of threat to Canadian information infrastructure is considered generally low but not so low that it can be ignored.

In the United Kingdom, the assessment is that the threat from electronic attack on its critical infrastructure is also currently low, but is likely to increase. The UK had a long history of protection of critical national infrastructures against terrorist physical attacks, and within government, there is a well-established and comprehensive approach to all aspects of security. This experience provides a strong platform on which to build arrangements for ensuring the adequate protection of key systems in both the public and private sectors. The UK is also emphasising the need to raise standards of information security more generally. The British Standard on Information Security Management, BS 7799 [143] and its accreditation scheme (known as "c:cure") are seen as providing the way forward and their benefits are being promoted among senior corporate decision-makers and information specialists.

The FBI established the National Infrastructure Protection Centre, in 1998, to facilitate and coordinate the federal government's investigation and response to attacks on critical infrastructures. However, these efforts are not yet being coordinated under a comprehensive plan. As a result, there is a risk that these efforts will be unfocused, inefficient, and ineffective. For example, the CIO Council Security Committee and a recently established working group both have efforts underway to identify standards and best practices that could improve federal agency efforts. While such efforts are generally laudable, it is unclear how the guidance that may result from them will relate to guidance issued by NIST and policies issued by OMB, two organizations that have statutory responsibilities in these areas

The "Solar Sunrise" attacks, on Department of Defence (DOD) and other computers in early 1998 illustrated the United States government's susceptibility to malicious actions. According to the DOD, Solar Sunrise was a series of attacks during February that targeted its servers by exploiting a well-known vulnerability in the Solaris operating system. The attacks were widespread and systematic and showed a pattern that indicated they might be the preparation for a coordinated attack on DoD's information infrastructure. They were of particular concern because they targeted key parts of DoD's

[143] BS 7799 was issued in Australia as AS/NZS 4444 and later as AS/NZS 7799

networks at a time when it was preparing for possible military operations against Iraq.

In March 1998 the Chief of the U.S.A. National Infrastructure Protection Centre (NIPC), Federal Bureau of Investigation, testified that "transnational criminals are rapidly becoming aware of and exploiting the power of cyber tools" and that recent computer crimes illustrate "the growing problem of cyber crime, the international dimension of the problem, and the increasing threat to our critical infrastructure". To make matter s worse the GOA reports [144] in March that there are widespread and serious computer control weaknesses. These weaknesses place enormous amounts of federal assets at risk of fraud and misuse, financial data at risk of unauthorized modification or destruction, sensitive information at risk of inappropriate disclosure, and critical operations at risk of disruption.

The CIP Research and Development Interagency Working Group was established in March to develop and sustain a roadmap on what technologies should be pursued to reduce vulnerabilities of and counter threats to our critical infrastructures.

5.6 Presidential Decision Directive 63

In May 1998, Presidential Decision Directive 63 (PDD 63)[145] recognized that addressing computer-based risks to the United State's critical infrastructures requires a new approach that involves coordination and cooperation across federal agencies and among public and private sector entities and other nations. PDD 63 created several new entities for developing and implementing a strategy for critical infrastructure protection. In addition, it tasked federal agencies with developing critical infrastructure protection plans and establishing related links with private industry sectors.

PDD 63 called for a range of actions intended to improve federal agency security programs, establish a partnership between the government and the private sector, and improve the U.S.A.'s ability to detect and respond to serious attacks. The program to accomplish this objective included designation of the following entities:

- Critical Infrastructure Assurance Office (CIAO), an interagency office housed in the Department of Commerce, which was established to develop a national plan for CIP on the basis of infrastructure plans developed by the private sector and federal agencies.

---

[144] _, Financial Audit: 1997 Consolidated Financial Statements of the United States Government GAO/AIMD-98-127, March 31, 1998. see www.gao.gov/archive/1998/ai98127.pdf

[145] _, Information Systems Protection, Presidential Decision Directive/NSC – 63, The White House, Washington, May 22, 1998

- National Infrastructure Protection Centre (NIPC), an organization within the FBI, which was expanded to address national-level threat assessment, warning, vulnerability, and law enforcement investigation and response.
- National Infrastructure Assurance Council, which was established to enhance the partnership of the public and private sectors in protecting critical infrastructures.

A "National Infrastructure Assurance Plan" is a central requirement of PDD 63. Industry sectors and federal agencies that are important to critical infrastructure protection required a more detailed analysis to determine the risks, systems and interdependencies, and to create a prioritised lists for action. The U.S.A. Government wanted to lead by example, showing how infrastructure assurance is best achieved. It designated lead agencies to work with private sector and government organizations.

PDD 63 also established CIP as a national goal and stated that, by the close of 2000, the United States was to have achieved an initial operating capability to protect the nation's critical infrastructures from intentional destructive acts and, no later than 2003, an enhanced capability[146].

The Directive also redefined the critical infrastructure by describing it in terms of eight industry sectors and five special functions[147]. For each of the infrastructures and functions, the directive designated lead federal agencies and required that the sector liaison and coordinator work with each other and the private sector to address problems. In particular sector liaison and coordinator were required develop and implement a vulnerability awareness and education program. They were also required to assist in the National Infrastructure Assurance Plan by:

- Assessing the vulnerabilities of the sector to cyber or physical attacks
- Recommending a plan to eliminate significant vulnerabilities
- Proposing a system for identifying and preventing major attacks
- Developing a plan for alerting, containing, and rebuffing an attack in progress
- Coordination with the Federal Emergency Management Agency as appropriate, rapidly reconstitute minimum essential capabilities in the aftermath of an attack.

[146] Shades of "by the end of the decade we will put a man on the moon".

[147] The infrastructures are information and communications: banking and finance: water supply: aviation, highway, mass transit, pipelines, rail, and waterborne commerce: emergency law enforcement: emergency fire services and continuity of government: electric power and oil and gas production and storage: and public health services. The special functions are law enforcement and internal security, intelligence, foreign affairs, national defense, and research and development.

The Government Agencies had 180 days to assess vulnerabilities and 180 days, to develop a plan for remedial action. In parallel the directive required a "Vulnerability Awareness and Education Programs" within government and the private sector. In September, GAO audit report made it clear how massive this objective was. It reported[148] that due to weaknesses in every major federal agency's critical federal operations were at risk of disruption, fraud, and inappropriate disclosure

5.7 Chapter Conclusions

In this chapter, we discussed how certain Governments are responding to the security dimensions, asymmetric threats and information warfare. We have found that in the last few years' progress has been made in awareness, understanding, coordination, and resolution of many of the challenges around NII protection (see Chapter 5). Globally the U.S.A. has led the way on opening community discussion of the issue in the early 1990s. The Commonwealth Government has been proactive in addressing the challenges, but is limited in its capacity when compared to the United States and also by private sector ownership of the majority of infrastructure.

During the late 1990s, the Commonwealth took steps to better understand the threats and improve awareness in public and private sectors. The Commonwealth Attorney-General (Darrel Williams) in particular, appeared to have place a high priority on addressing the issue. A number of Australian organisations realised the pressing importance of information infrastructure security for their business. In parallel with the NII concerns, fixing the Year 2000 bug and preparing for the 2000 Olympics, provided many organisations with a much needed (and overdue) focus on information systems security.

We conclude that there is a high level of concern in the developed nations and especially the United States about attacks on critical information infrastructure and Information Warfare. This provides an opportunity for these nations to work together to improve the stability of the many-shared infrastructures.

[148] _,Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk (GAO/AIMD-98-92, September 23, 1998.

Chapter 6. Analysis of Financial Information Infrastructure components

"Military power in the final analysis is based on economic power"

General Fu Quanyou[149]

Chapter Overview

In this chapter, we provide framework for understanding the properties of economic systems that information warriors may seek to strike or shield. An analysis of financial information infrastructure is required in order to establish the relationship between economic processes, security and war. This analysis focuses on the support and advancement that an economic system gives a society. In particular, we outline how a community may achieve security through an efficient financial information infrastructure. We show how economic systems give large communities, Nation-States and other interest-groups, the much needed capability to acquire resources, improve efficiency, and the maximising of opportunities for future wealth creation. This wealth in turn enables the communities to protect and promote its religious, ideological, political and ethnic interests. Conversely, we demonstrate how weaknesses or collapse of economic infrastructure can precipitate uncertainty, difficulty and undermine the "national-interests".

[149] General Fu Quanyou is Director of the General Staff Department and former Director of the General Logistics Department, People's Liberation Army. General Fu Quanyou , *Future Logistics Modernization*, China Military Science Spring 1994.

6.1 Targeting Economic Infrastructures

Banking and Finance systems are consistently identified as critical social infrastructures. It is no surprise that the histories of economics and warfare have been intertwined throughout the development (and destruction) of civilisations[150]. However, economic power and its development is an unyielding everyday force, which in less dramatic ways improves productivity, enhances social welfare, and improves quality of life to humanity. The study of economic history is mandatory for those that wish to critic security strategy and seek ways to improve social wellfare. This chapter introduces elements that when assembled constitute the global banking and finance systems within the context of Information Warfare and the protection of Information Infrastructures. We do not intend within this thesis to provide more than an overview of economic systems. However, by providing an analysis of the various basic elements of economic systems, it is hoped that the readers will consider the threats posed by information warfare to the national infrastructure on a broader strategic basis.

Supporting a rival's economy is its critical financial infrastructure consisting of some form of monetary infrastructure (or alternative system of exchange) with associated payment infrastructure. Affecting this financial infrastructure may be highly desirable in the lead up and during conventional engagement. Taking a defensive strategy a well protected economic infrastructure in tandem with possessing capability and willingness to attack a rival's economic infrastructure may provide a strategic deterrent against aggression, possibly more so than traditional direct force against military forces. For those who can master it, attacking a rival Nation's economy through its financial infrastructure appears to be an elegant strategy in the information age.

Degrading, disrupting, or destroying an adversary's infrastructures may be required in support of diplomatic and military activities. Alternatively a campaign of economic warfare may be undertaken, as an activity in it own right, to weaken[151] another Nation economy or economic progress. In order to protect the Nations interests it is essential for national security agencies and defence forces to protect critical economic interests, such as its resources, physical and information infrastructures.

Modern economic warfare requires much more sophisticated tactics and indirect application of power commensurate with the size and sophistication of

---

[150] Economics systems (inc. banking, finance and associated payment systems) can boast inventions equal those of medicine and military technology, but it is fair to say that they do not capture the historic drama or attention we associate with other events in history. Medicine, military and other areas provide many with interesting areas of to study: plagues, vaccines, trench warfare, and nuclear weapons.

[151] The restriction of access to energy products and advanced technologies could be interpreted as part of an economic of economic war between haves and have-nots.

the target infrastructure. In the short term, indirect action inevitably meant less efficient use of resources, than "open" warfare, which has been aimed at direct action (usually destruction of opposing military forces). However, economic warfare may offer alternative approaches to meeting many of the requirements for new weapons, especially management of public perceptions and the ability to strike asymmetrically. Although deployed tactical military capability is unlikely to be impacted in the short term by the loss of a financial infrastructure outside its area of operations, it may quickly inhibit operations and strategically influence the rival's military power and will.

Knowledge of economics is particularly important in the National Security context of globalisation and the changing role of economic roles of Nation-states. Consideration must be given to joint understanding economic, technology, and military history. In particularly within defence forces the vital contribution of institutions and individual financers, bankers, insurers, and entrepreneurs should be understood in the context of the security of Nations. A practical business focused posture must be encouraged within information age forces. Conversely, in an effort to a avoid (fanatical) pre-occupation with daily micro-mechanics, financial institutions must understand the broad social, institutional, and national security impacts of their work and decisions. The financial sector should also understand their role as both targets and weapons in the information age security struggle. The lessons to be learned from a balanced military and financial history, should assist strategist avoid myopic views of national security.

6.1.1 Conceptualising Economic Systems

While simple economic systems may not be difficult to conceptualise, consider the economic systems required to support the envisage, engineer, manufacturing and assembling the 1,000,000 plus physical parts that make up an America space shuttle. Such economic systems represent the principle of contemporary economic development. Such sophistication provides the host Nation with great opportunities for wealth creation, which maintains high levels of economic security. Today's financial infrastructure has evolved numerous countermeasures in response to the crisis that have occurred throughout history. Some would argue that the risk of past systemic failures could not now occur again, because of the various technical controls in place. At a global level the global financial infrastructure (GFI) may be considered robust, however few will claim it is invulnerable. As we have identified earlier, the trends towards new forms of warfare, it is likely that adversaries will seek out different targets and use asymmetric attacks that are difficult to predict or counter. The key in learning from our past and recent experiences (in our rapidly changing environment) is that we cannot be complacent – knowing that history may not repeat itself – but it sure does rhyme.

Since our federation the Commonwealth of Australia, and other advanced nations, have seen dramatic changes in our financial infrastructure and supporting information infrastructures. We now face accelerated changes in the face of globalisation and technology trends. Such change implies the need to examine the existing paradigms for protection of the stability, integrity and efficiency of the financial system.

At a micro level, money and an associated payments infrastructure exist to provide certainty around the exchange of value in the exchange of goods and services. The particular resource that fuels wealth creation varies from place-to-place and time-to-time, but at a macro level our economic systems are vital engines for growth. When working properly these engines efficiently and effectively transport value and other economic messages between buyers and sellers. The dynamic movement of value allows the economy to find equilibriums resulting in maximising of productivity of the individuals and their Nation.

In re-thinking the relationship between economics, information infrastructure, and National Security, we must understand this new battle space. Attacking and defending an economy will requires a comprehensive understanding of the wide variety of societies, economic structures, money, payment systems and related elements of the economy of interest.

An economy, like a market or a single transaction, relates to the exchange of goods, services, and resources. However, the economy refers to an aggregated set of production and consumption activities, consisting of the workings of a large and complex number of distinct markets for goods, services, and resources. An economy has traditionally been associated with a city-state, region, or nation usually under common governance or legal system.

Within these economies, a highly complex serries of transaction occur underpinned by some form of payment system. The basic circular flow model positions the various actors within an economy to demonstrate their interactions.

6.1.2 Economic Specialisation

The specialised labour economy has been the predominant and fundamental structure of economies since pre-historic human societies. Some specialisation of labour existed even within pre-tribal family groups. Individuals[152] and

[152] In modern times, there appears to be a heroic portrayal of some societies consisting of "rugged individualists". This romantic dysfunctional conception rarely considers how economically dependent such groups are on highly specialised labour (eg for weapons, money, medicines). True "rugged individualists" have likely never existed. However, it is important to note that some individuals are less dependent and some individual seek to minimise dependence upon specialist's skills, economic infrastructures or the Nation.

groups that acceptance of specialisation implying that the security and advantage of such specialisation outweighs the disadvantages and risks.

Society exists along a continuum (in term of economics) between individualists who consume ONLY that which they themselves produce and one that consists of individuals who are ALL specialised labour and produce only one component of goods and services.

Specialisation of labour refers to different units of labour being used differently in the production processes. In other words, some types of labour might be used to produce only one particular type of good while others are used to produce a different good. In fact, as labour becomes more specialised then a labourer might become so specialised as to produce only one part of one good or service in long supply chains: making only cartwheels, guarding a facility, writing computer programs, or piloting a space shuttle

Together communities are able to obtain essential security improvements by specialisation of its labour, not only sharing costs of protection of their output, they may also be able to create economies of scale through trading enhanced opportunities (adding value), knowledge, use of technology and better management of risks through supply chains. One key improvement as civilisation developed, was that labour could be divided on functional basis to aid the communities interests and economic growth. This specialisation enabled the creation of roles that could improve production and protection of individual and communal wealth.

Some economies could afford the growth of specialists, who did not convert any primary resource into products. Government and merchants specialists created the early services sectors. In even more advanced economies, roles such as bankers and financial agents improved efficient allocation of labour and productive investment of wealth. Where resources, stores of wealth and supply chains, existed roles were needed such as guards, law enforcement and soldiers[153] to counter theft enforce contacts and prevent numerous opportunities to misuse of resources. If protection was found to be insufficient, a host of Thieves, Bandits, Embezzlers, and other Nations could acquire the assets. Conversely, a strong defensive force could be re-invented as an offensive function to undertake attacks on other group's resource and sources of wealth.

[153] The ancient relationship between economics and warfare is curiously demonstrated in the origin of word "soldier". In between the years 306-337AD the Emperor Constantine adopted Christianity and amassed vast wealth after confiscating pagan treasures. He issued a new gold coin called the Solidus, which remained in production, unchanged in purity and weight, throughout the eastern Roman Empire for the next 700 years. Centuries later, in 1159, having suffered the disastrous fall in the quality of England's silver currency during the reign of Henry I (1100-1135), Henry II restored England's financial prestige and introduced a new tax. He commuted their annual 40 days military service, allowing cash payment instead. With the wealth gained through this taxation, he was able to recruit men-at-arms (and mercenaries) creating a regular army. These professionals became known from the Solidus coins they where paid as "soldiers".

Note that the resources or assets being contested could be anything. As the sources of wealth have changed over time, so has the roles, they have become more specialised and sophisticated (see the section on the Third Wave and Information Age). Although contemporary contest may still be fought over water rights or farmland, the dynamic outlined above is equally applied to battles for talented individuals, software, patents, innovations, market share, and ideas.

Specialisation advantage[154] is that labour productivity increases (as observed by economist Adam Smith) increasing total economic output. The presence of warriors, bankers, and numerous others roles within an economy allowed the development of sophisticated civilization. This specialisation continues today within our financial information infrastructure. Banking, litigation, telecommunications, law enforcement, and many other individuals with highly specialist skills, build and maintain our economic infrastructure.

As societies produce advanced goods and services, they bear the cost and risks of more sophisticated supply chains and infrastructures to produce and support the creation of specialised skills, (eg teachers, pilots, communications experts). Increasing sophistication and specialisation results in advanced skills and experience, on which a Nation becomes highly dependent, being placed in the hands of an increasingly smaller number [155] of persons (i.e. world experts).

6.1.3 Protection of Supply Chains

The risk of reliance upon others is that in the case of a breakdown in the supply chain it becomes difficult or impossible to obtain vital goods and services. The temporary break down in the exchange of good and service, such as an industrial strike of coal miners, airline or nursing staff causes significant disruption for consumers. However, a prolonged or permanent loss of strategic specialists may have a devastating impact on the Nation's sense of security: from the capture of intelligence agents, defection of key citizens, or assignation of political leadership. In a less tangible sense, a breakdown in the value of the exchange system (e.g. money) or infrastructure may have a similar impact on the availability of specialist skills. Some examples include: loss of contact with markets, inability to set prices, unacceptable transaction risk

---

[154] The individualist society has as its main advantage a system where individuals do not need to rely upon others for their sustenance and security. Infrastructure may still be built, but through cooperation of non-specialised labour. Its main disadvantage is the decreased efficiency and resultant lowered standard of living (judged by goods and services).

[155] Consider the potential outcomes, if during the World War II the 3,000 people (approx 500 where killed) who confronted the Luftwaffe during the Battle of Britain had not prevailed. This relatively small group of the nations-sates specialist "the few", especially the very small number of experienced fighter pilots, where noted in Churchill's speech 20th August 1940 "Never in the field of human conflict was so much owed by so many to so few".

A highly specialised labour society has the major vulnerability of high reliance on other individuals to make the supply chains and society function, such as rulers, soldiers, merchants, peasants. With advanced goods and services, the methods of exchange also require highly complex supply chains, consisting of communications and logistics support for delivery (inc transportation) over large distances and in great quantities. The management of complex supply chains has radically changed in recent decades such that they are collaborative and highly optimised to deliver maximum productivity.

Risk is created through investing and supporting others to develop specialisation and sharing supply chains. However, the economic benefits achieved have in general outweighed the vulnerabilities to which the Nation is exposed.

The Nation's dependence on these individuals raises moral and ethical questions for the nation-state[156]. Another risk is that the investments may not be realised or the loss of talented and key specialist (eg leaders, scientists, military specialists) cannot be quickly replaced. Worst yet a specialist ceases to co-operate with others and the non-specialist is unable to acquire specialised skill quickly enough to avert disaster. For example, the lighthouse keeper refuses to operate the light, the pilot unwilling to take off, or the surgeon not operating. Most specialists will have situations where their skills and our dependence are time-critical and other situations where they are not. This dependence on specialists is critical in considering infrastructure protection, as these specialists are legitimate targets in war. (see 4.6 Information Infrastructure).

6.2 Financial Infrastructure

The following section provides an overview of money, and economic models essential in understanding the vulnerabilities of economic systems. It includes a basic introduction of clearing and settlement process for modern payment services. These components form the basis of the financial infrastructure in the same way, power stations, telephone exchanges, and hospitals form the basis of other critical infrastructures.

Throughout history, there have been countless permutations of economic systems each with its own money, rules, customs, markets, exchanges, regulators, taxes, payment systems, and other key elements. Much of an economic system can be very simple or a complex combination of the basic forms of exchange: Quantitative forms (metrics, counting), Barter forms (swaps, offsets, promises) and Qualitative forms (beliefs).

[156] Example -Should DNA screening for mental diseases be required before society invests in critical knowledge in its specialists.

Qualitative forms of exchange provide certainty of valuation based on social value structures (obligations, rights, duties, prestige) where the value metrics of goods and services exchanged are intangible or subjective[157] outside the social value structure. These systems fall within fields of study of religion, marketing (inc propaganda) and especially politics, rather within quantitative universe of accounting, banking, and finance.

The architecture of a system of exchange varies widely, and may be unrecognisable in one scheme even though the same payment instrument is used. The actual payment architecture may consist of a complex combination of swaps, offsets, promises, physical transfer of cash (banknotes and coins), updating of accounting records, communication protocols, triggers (inc. time, authorisation) and risk management techniques.

6.2.1 Types of Economies

The specialised labour society requires some method of exchange between individuals for goods and services. Exchange normally refers to the process by which specialised individuals give up goods and services that they produce in return for those they wish to consume. However, in a specialised society the type of economic system in place drives the need for exchanges at any given time.

There are a number of possible economic systems of which drive production and consumption and the nature of exchanges: including: force, tradition, planned, market and mixed economies[158]. These are illustrated in Figure 6 and explained below.

A force based economy consists of the use of threat, fear, coercion, intimidation and violence to determine ownership (i.e. control) of resources, outputs and consumption. This system can be very efficient (for the aggressor) as it does not require many of the processes and structures needed for other forms of exchange (eg value negotiation, payment instruments etc.). However force required commitment of resources to the processes and structures to deliver the exchange by force to the individuals, it also requires resources to ensure that rivals do not undermine this system (eg. standing up to the bully, escape form the system). This system, although often illegal, remains widely used at all levels from individuals to nations

[157] For example sacrifice of a family member to the sun god in exchange for better weather.

[158] Byrns, R. T. and Stone, G. W. *Economics* (6th Edition), Addison-Wesley Pub Co; January 1997

A traditional economy does not need to resort to force as specialisation of labour using structures such as social classes or castes. In tribal, and with increasing sophistication in feudal societies of the Middle Ages, the class, caste, status or family in which an individual was born determined entitlements and what was to be produced and who received output. A practical component of this system was that some specialist provided protection against the force from rivals groups. Although this provided efficiency when some flexibility is built into the system, societies with especially rigid classes and traditions undermined efficient allocation of labour.

Planned economies have some legitimated authority (all or some of the society), who plans the allocation of labour needed and what production will occur. With a small society, this may be a plan for production over a short period, such as details of the next hunt (eg who goes and where). As an economy expands, the society expands the complexity of planning. Plans become extensive, detailed and must cover longer periods as well as more complex economic interactions. Communist systems are associated with planned economies, however this is not to imply that they are identical[159]. For example, some central planning does occur within non-communist societies. The Soviet Union, which collapsed in 1991, is a modern example of an extensive planned economy.

[159] Kapstein, E., *Governing the Global Economy: International Finance and the State*. Cambridge MA: Harvard University Press, 1996

This figure is not available online.
Please consult the hardcopy thesis
available from the QUT Library

Figure 6 Types of Economic Systems[158]

A market system seeks to support individuals deciding for themselves on what they will specialise, produce and then exchange with others[160]. A producer selects the goods and services they create based on their own preferences, abilities, and resources and then seek others who want to consume their output. Some producers will find that the market will not exchange on acceptable terms. These producers will be forced to select other goods and services to produce. A "free market economy" enables the balance between production and consumption to find a natural equilibrium.

Mixed economies are the most common economy and can be seen in nations and diverse as China, Australian and the US where various combinations of force, tradition, plan and market forces determine allocation of labour. In a mixed economy, the focus is often on the balance between the level of the plan and the market systems. As parents do in the home, the government may

[160] Friedman,. M. *Capitalism and Freedom*, (2nd edition), University of Chicago Press; February 1963

prohibit some market activities and regulates many others for the benefit of society. Other economic systems may play different roles throughout the economy in exchanges of particular goods and services: such as force within criminal economy and tradition in charity activities.

6.2.2 Circular Flow Model

The circular flow model[161] illustrated in Figure 7 show in a simplistic way the flow goods and services, for resources, and payments. Even at this high level, there are numerous types of payments apart from payments required in the direct exchange of goods and services. These include payments to store savings wealth, taxation, investments, wages, income, loans, and interest. In addition to payments within the economy, the communities may need to trade with external communities (foreign) where they do not have the specialisation of labour internally.

People (inc shareholders) who live in some kind of household own all the resources (that are privately owned) that are available to use in production activities. The household sector is the consumer of goods and services, which they buy in product market. The business sector is the producers of goods and services, which they sell in the market place to households. The business sector uses the payments from such transactions to buy the resources in factor markets necessary to produce goods and services In order to obtain the necessary money for such purchases, households exchange resources in factor markets. This series of exchanges creates a circular flow of money between sectors and markets.

[161] Byrns, R. T. and Stone, G. W. Economics (6th Edition), Addison-Wesley Pub Co; January 1997

This figure is not available online.
Please consult the hardcopy thesis
available from the QUT Library

Figure 7 Circular flow of money[161]

Within the economic systems, the interference of the Government system alters the market price for goods and services between buyers and sellers[162]. Its position in the system is tolerated because it gathers taxes from both households and businesses to be used for community (shared) benefit. Taxes are used to buy resources and transfers of wealth (such as welfare and subsidies) to both households and business. The community needs the Government to provide goods and service that they cannot effectively or efficiently provided by other

[162] von Mises, L., *Human Action, (4th Edition)1996 Online www.mises.org/humanaction.asp*

means. A constant debate (in open societies) occurs in taxed communities as to the level, fairness, and effective allocation of taxes to solve current problems. One of the other main roles of Government is to review the system as a whole to determine threats and opportunities that affect the entire community. The Government faces debate over future threats and opportunities to the community, especially in strategic arena where cause, effect, likelihood, and impact are difficult to determine. It assists through the provision of numerous mechanisms (eg tax concessions) to improve systems and invests tax dollars in the protection of critical parts of the economic system.

In going about its role a Government purchases resources (eg. public servants) from the factor market and produces some monopoly public goods and services. With its special powers, it is able to impose rules within markets. These public goods and services exist along the continuum from being provided directly to businesses and households (such as emergency services) or sold in competition with firms through the product markets[162]. Other government goods and services may be provided on a user pays basis, mandated payments (fines) or be indirectly paid for in goods and services produced by the Business sector.

With the co-operation of Governments, increased trade has been flowing between national economies[162]. Multinational economies and trading blocks are now common, mostly through attempts to create a common legal system between geographically or historically close countries. An example of a multinational economy is the European Union (EU), which was formally created on November 1, 1993. With the globalisation of trade, production and consumption activities are now being measured without regard for national boundaries or legal framework.

6.3 Money Infrastructure

> *"…no duty is more imperative on the Government, than the duty it owes the people, of furnishing them a sound and uniform currency"*
>
> *Abraham Lincoln* [163]

In all but the most primitive economies, the flow of money facilitates the efficient exchanges of goods and services. In this scene, money is the primary economic infrastructure of an economy. However, money in this context does not equate to the coin and notes issued by Governments or the electronic

[163] Lincoln, A., "*Many Free Countries Have Lost Their Liberty*," A Speech on the Subtreasury, Springfield, Illinois, December 26, 1839.

numbers recorded within computer systems. Money has a greater and more fundamental meaning when viewed as infrastructure of civilisation. In our experience, the role of "money" as stabilising and civilizing driver is rarely described in terms of the security that it provides a civilisation. A broad understanding of monies (and payment systems) are vital in understanding economics, warfare and security. We consider money as anything that is widely used for making payments and accounting for obligations (eg debts and credits)

Consider what a producer or merchants will accept as money. Most modern Nation's governments issue currency in the form of coins and banknotes. Within Australia, merchants willingly accept Australian Government's cash as a form of money with little thought. However, even in the most advanced economies, merchants may not accept personal cheques and certainly become suspicious should you wish to pay with currency from unknown Governments or unfamiliar payment instruments. Conversely, merchants in countries with much larger economies than Australia's, reject payment with currency issued by their own Government[164].

6.3.1 Acceptance

One of the most important improvements over the simplest forms of early barter was use of a small number of standard items rather than numerous individual items. Artefacts and items originally accepted for one purpose were often found to be useful for other non-economic purposes and, because of their wide acceptability began to be used for general trading supplementing or replacing barter. Items that made good money were accepted because of their efficiency characteristics in acting as media of exchange. Certain commodities were chosen as preferred barter items for a number of characteristics[165]. including:

- Security of storage
- Portability
- High value densities
- Durability and integrity
- Cultural convenience (within and across communities)
- Easy acceptance with new trading partners

Any commodities that were widely desired and could meet some or all of the above characteristics would be easy to exchange and could become accepted as

[164] _, *Russian Economic Trends* (1995-1999). Blackwell Publishers. Many Russian merchants prefer or exclusively use US dollars.

[165] Davies, G. (1996), *A History of Money from Ancient Times to the Present Day*, (rev. ed.), University of Wales Press, Cardiff.

money. In some cases one community's view of these money characteristics widely differed from their trading partners. For example, slaves and livestock were used as money. Coming to a common form of money, such as certain precious metals, is a significant factor in improving macro-economic infrastructures efficiency and productivity.

One can see why many societies gravitated towards more efficient media of exchange especially precious metals. Precious metals have had ornamental uses throughout history and that could be one reason why they were widely adopted for use as money within and between many communities. One form of precious metal based money has dominated human history for several centuries – gold[166].

In our time, the preferred form of money (by value) is computer based using electronic signals sent across telecommunications networks and numbers recorded on computer systems hard disks. These electronic values now exceed the value of all the gold on the planet.

6.3.2 Functions of Money

It is almost inadequate to define money as physical artefacts and items: rather any definition is best based on its economic functions[167]. The function of each instance of money may not include all functions and may change over time. The specific functions of money are mostly micro-economic and are of primary importance to the individuals (buyers and sellers) in an economy. The specific micro-economic functions include:

- Unit of account (abstract)
- Medium of exchange (concrete)
- Means of payment and settlement (concrete)
- Store of value (concrete)
- Standard for deferred payments (abstract)
- Common measure of value (abstract)

The more general functions of money are mostly macro-economic and abstract function. These functions are of primary importance to society (especially the Government) as a whole. Davis[167] described these as:

---

[166] The combination of gold's aesthetics and its resistance to corrosion led to its use for monetary transactions for millennia. It was only in relatively recent 1970s where the last vestiges of the Gold Standard linking currency to the metal disappeared. However, people around the globe still seem to prefer some of their wealth to be stored in the form of gold rather than in inflation-prone currencies.

[167] Davies, G. (1996), *A History of Money from Ancient Times to the Present Day*, (rev. ed.), University of Wales Press, Cardiff.

- Liquid asset
- Framework of the market allocative system (prices)
- A causative factor in the economy
- Controller of the economy

6.4 Payment Infrastructure

"Payment and settlement systems are to economic activity what roads are to traffic: necessary but typically taken for granted unless they cause an accident or bottlenecks develop."

Gregor Heinrich, BIS [168]

The core information infrastructure of the modern business world is its payments system. It would be highly unusual for business transactions to occur without the use of a monetary payment system[169]. Transactions, which are not paid in cash, require some mechanism for transferring funds from the buyer's bank account to the seller's bank account. In this section, we provide the conceptual architecture of payment infrastructures. Payment processes can be divided into a number of more detailed steps, which can vary according to the type of payment instruments used. The "payments system" refers to the ways in which these counter parties call for and move value between each other. These systems include differing forms of payment instruments - such as cowries shells, currency (cash), cheques and electronic funds transfers - and the supporting technology processes involved in transferring value from one party to another.

6.5 Black markets and Alternative economies

Co-existing and interacting with the "legitimate" national economic infrastructure, are several alternative economies, which place alternative values on goods and services. Such economies exist at many levels and scales, often structured in radially different ways to the broader economy. Elements of the "legitimate" economy may be used eg Cash, but different rules and conditions may be applied (eg not charging interest) that distort prices or place alternative

[168] Heinrich, G., Head of the CPSS Secretariat, Bank for International Settlements, in his paper on the *CPSS Core Principles Bank for International Settlements*, 64th BIS Annual Report (1994)

[169] Outside the business world there are some cases where goods and services are exchanged willingly without the use of a monetary payment system : such as in the case of charity, military assistance, humanitarian aid or disaster relief.

values on some good and services. These alternative economies can vary from: the trading of favours within small communities: swaps or bartering within particular industries, closed group economies (eg within prison), trading pirate software, religious or traditional custom, through to large scale criminal black-markets or terrorist financing operating on a global scale. In each of the examples listed above, the participants will relate to the wider economy in various manners. For example, they can consider themselves as excluded or independent to the economy of the Nation. Alternatively, the national economy can be seen as a trading peer for specific goods and services, operating through certain channels. These channels function exchanges for good and services, converting value amongst different systems. Like the national economy, these alternative economies may have trading partners in other regions and states.

The official measures of aggregated production and consumption activities within alternative economy may be able to be measured for some or all of it activities. However, some economies are invisible to the broader Nation-State with little or no data about its activities and operations. To measure these "black-markets" special deductions or surveillance may be required. The effectiveness of these measures are dependent on the Government agency's capabilities to track the delivery of illegal goods & services and identify payments (eg drugs, corruption, money laundering). The existence, emergence, and operation of alternative economic structures are an important consideration in the boundary of an economy and therefore its security. The alternative economy may be the main factor identifying "us and them" in an economic information war.

6.6 Chapter Conclusions

In this chapter, a framework was described highlighting the properties of economic systems that information warriors may seek to strike or shield. This analysis of financial information infrastructures established the relationship between economic processes, security and war. We focused our analysis on the support and advancement that an economic system gives a society. In particular, we outlined how a community may achieve security through an efficient financial information infrastructure.

We argued that economic systems give large communities, Nation-States and other interest-groups, the capability to acquire resources, improve efficiency, and maximise opportunities for future wealth creation. This wealth in turn enables the communities to protect and promote its religious, ideological, political and ethnic interests. Conversely, we demonstrated how weaknesses or collapse of economic infrastructure could precipitate uncertainty, difficulty and undermine the "national-interests".

Chapter 7. Analysis of Economic Information Warfare

"economic sanctions are means of destruction like nuclear weapons"

Taleeban[170].

Chapter Overview

In this chapter, an analysis of the strategy, operations and tactics that threaten critical economic systems of the Nation-State is provided. Firstly, we revisit Australia's economic and security history and changes in alignment of the National Security Strategy. We outline the broad range of activities that we believe exist on the spectrum of Economic War. In our argument, we assert that interference with economic effectiveness and efficiency of the adversaries' economic processes should be considered in the same light as conventional military strikes. In conjunction, we identify the need to protect our economic system with the same discipline and vigilance that we apply to traditional defence area such as border protection. We have identified eight hazards that impact the security of financial infrastructure. Each of the hazards identified are inherent or systemic in nature, resulting from the processes that money and payment infrastructure play within a large-scale economy. In the context of National Security and economic warfare, the adversaries seek to manipulate, leverage and multiply these hazards to support their objectives and interests. Having identified the objectives hazards of the information warfare, we provide our categorisation of economic warfare tactics. As we argued in section 3.1, the dividing lines between acceptable business and economic warfare are open to interpretation by adversaries. Therefore, we present a spectrum of tactics to which we attach no ethical or moral significance. Following on from our categorisation tactics, we present our view on the three realms; physical, information infrastructure and perceptual within which economic wars are fought. The capabilities required for mounting a comprehensive Economic

[170] Taleban slam UN economic sanctions as human rights violations 20/11/2000 Business Recorder Copyright (C) 2000 Business Recorder: Source: World Reporter (TM) ISLAMABAD :

Information War are described within the context of each realm (or battle space). We then discuss the different demands nations faces when they are subjected to an economic information war, including the gaps in private sector contingency plans.

7.1 Securing the National-Economic Base

Failure to protect our economic base, by commercial, diplomatic, and military means, creates the prospect that we will be dominated by aggressors. In the past Australia's economy was largely based on, and prospered through, its vast agricultural and minerals wealth: an attribute linked to geography. Australia's wealth was protected from turmoil by its geographical isolation and the natural defences provided by the Air-Sea gap and our alliance with powerful nations. Our relative isolation (also referred to as the "tyranny of distance") underlies a popular belief that directed attack on our economy or invasion would be a logistical nightmare for an aggressor, who would then be confronted by our powerful protector. However, periods of fear and panic in Australia have been accompanied by perceptions isolation and that aggressors could approach our shores undetected[171]. Coupled with a relatively small population our National Security strategy has always sought to try counter threats at sea (and later in the air) before they could threaten the mainland. For the most of its history, Australia's security was imagined in a framework of alliances and treaties with major power protectors. Before World War II, Australia's defence relationship with Britain was instinctive, with the Nation considered almost exclusively tied to the "mother country". The expectation was that both nations had absolute duty to defend the British Empire.

This belief in British protection was shattered with the fall of Malaya and Singapore, early in World War II. This resuledt in a deep shock to the nation self-confidence and caused Australia to re-evaluate its dependence on Britain for national security. Australia then turned towards the U.S.A. for protection during World War II. America's Asian presence and influence increased with the defeat and rebuilding of Japan, and conflicts with communist in the Philippines, Korea and Vietnam. The emergence of the U.S.S.R as a peer competitor to the U.S.A. made national security relationships event closer. Again, Australia's sense of security was shaken when in 1969 U.S.A. President Nixon announced (the Guam Doctrine) although the U.S.A was prepared to

[171] For example, Russian Panic was caused news of British participation in the Crimean war (1854). Before this France and America had been thought of as real enemies of Australian colonies. They imported canon and built fortifications against the French, who they perceived as threatening them their "stronghold" in New Caledonia. Australian's of the time also feared raids from American privateers (capers). "The Russian Fear" however was the strongest and most persistent fear, and planners considered which cities would be attacked first and how, would they destroy cities, occupy or just seize gold in banks.

honour its treaty commitments, direct United States intervention and military assistance to allies would only be predicated based on an external nuclear threat. In short, U.S.A. allies were expected to take greater stake in their own defence. These experiences created a new and powerful principle that would dominate all subsequent national security thinking.

The Australian Government Policy Information Paper - The Defence of Australia in 1987[172] outlined three fundamental principles: the need for self-reliance, the development of effective regional cooperation, and strong international alliances. The priorities presented in "Defence White Paper 1994 - Defending Australia" (DWP94) amended some terms used in DOA87 to make it more politically correct to our neighbours, and largely kept the themes of self-reliance, technologically superior forces and alliances.

Our natural bastion, coupled with our access to comparative technological advantages that limited maritime power-projection of our neighbours, has lead us even in recent times to declare that 'Australia is one of the most secure countries in the world.'[173] For two centuries, Australian National security has (correctly) focused on the protection of our agricultural and industrial assets[174], and being able to protect our direct (maritime) approaches and trade routes[175].

These defence declarations and objectives are still relevant, as physical assets still represent significant income, and no neighbours currently could sustain a military campaign based on physical invasion. However, in the last decade we have seen the dramatic changes in the economy, technology, and the nature of threats, which have neutered the protection previously provided by the tyranny of distance[176]. Security concerns are many and varied: some require the conventional use of military force and others are in the realm of diplomacy. Our new security strategy must address a wide range of concerns including information attacks, organised crime, money laundering, terrorism, illegal immigration, the drug trade, illegal fishing, piracy and quarantine infringements.

---

[172] _, *The Defence of Australia* (DOA87), Department of Defence, AGPS, Canberra, 1987.

[173] Dibb, P., *Review of Australia's Defence Capabilities,* 1986

[174] These include live stock: fishing zones, orchards: wheat, cotton and other fields: gold, opal, pearl and precious metals deposits: bauxite, iron and mineral deposits: oil, gas and coal energy reserves

[175] O'Neill, R. and Horner, D. (Eds), *Australian Defence Policy for the 1980s*, University of Queensland, St Lucia, 1982, and _, Australian Defence, Department of Defence, Australian Government Publishing Service, Canberra, 1976.

[176] _, *Defence Review 2000 – Our Future Defence Force*. A Public Discussion, Paper, Department of Defence, Defence Publishing Service, Canberra, 2000

7.1.1 Alignment of Our National Security strategy

The new strategic security environment no longer allows protection solely based on a concept of geography. The environment requires us to operate a balance across three realms: physical, information infrastructure and perceptual. Australia's current critical dependence on information infrastructure and our future dependence on the Information economy demands urgent attention be paid to ensuring that our National Security strategy is oriented to protecting our sources of wealth. Ten broad National priorities for realising the benefits of the information economy have been identified[177] by the Government. The ten priorities are as follows;

- Maximise opportunities for all Australians to benefit from the information economy.
- Deliver the education and skills Australians need to participate in the information economy.
- Advance the growth of a world-class infrastructure for the information economy.
- Increase significantly the use of electronic commerce by Australian business.
- Develop a legal and regulatory framework to facilitate electronic commerce.
- Promote the integrity and growth of Australian content and culture in the information economy.
- Develop the Australian information industries.
- Unlock the potential of the health sector.
- Influence the emerging international rules and conventions for electronic commerce.
- Implement a world-class model for delivery of all appropriate government services online.

The objectives in these priority areas and the structures that support achieving them will increasingly become the core assets of Australia. In addition the stronger, more secure and survivable our Australia's information-base becomes - the more attractive our Nation will become to investors seeking a safe and reliable environment within which to conduct their business, resulting in still more opportunities for Australia to increase its wealth.

[177] _, A Strategic Framework For The Information Economy Identified Priority Areas For The Nation To Focus On, *Identifying Priorities For Action*, NOIE December 1998

7.2 Economic Security

Markets in general, are quite effective at producing safe, efficient, and welfare-enhancing outcomes; this proposition is the foundation stone of the market economy[178]. However, when an economic or other contest does arise between States, it is an unpleasant affair[179]. Failure of the Nation to protect and enhance its economic prosperity results in destabilisation of communities, undermining of choice and freedom, erosion of the quality of life and ultimately the collapse or extinction of the Nation itself (i.e. it becomes a failed state).

Its economic capacity and capabilities are a fundamental component of the Nation's power and specifically provide its ability to resource the security functions of the state (Figure 2 Security Functions of the State) described earlier. These security functions, including conventional military power, have always been tightly linked to a Nation's economic strength and visa versa. The relative strengths of a Nation's security functions and its economies, are especially important when a governments attempts to influence the will of another Nation[180].

This intimate relationship between national security and economics was made painfully obvious during the Asian Economic Crisis. This financial crisis and others precipitated massive social upheaval and escalated intrastate political, ethnic, and religious conflicts. The hotspots of strife in Asia, Middle East, Africa, and Latin America have all suffered significant hardships. The acquisition of high-technology military systems from (i.e. hard-currency foreign) suppliers was significantly impeded by these crises. In some ways, this applied a welcome brake on a dangerous pattern that some analyst called the Asian Arms race. Governments had to defer or cancel acquisition of sophisticated weaponry or equipment, either because they did not have the capital or would be unable to afford service maintenance and upgrades. From an Australia's regional security perspective, this was a benefit of the crisis, as it permitted, Australian defence forces maintain a modest technology 'edge' over its neighbours.

7.2.1 Economic Security Strategy

Should a Nation wish to impose on or oppose other Nation's will, it becomes increasingly critical that its security structures and practices are properly

---

[178] Carmichael, J., (Chairman APRA), *Financial Regulation in the Twenty-First Century*, Speech at the PACAP-FMA Conference in Melbourne 6 July 2000

[179] For example the impact on Chile people from the USA's economic war. See National Security Decision Memorandum (NSDM) 93 issued in early Nov. 1970.

[180] Kapstein E. B., T*he Political Economy of National Security, A Global Perspective*, McGraw-Hill, New York, 1992

aligned with the economy, so that it can not only counter a rival'ss conventional military forces but also its asymmetric, economic and other attacks.

Economic security concepts have emerged as an increasingly important area in international relation studies[181]. The factors shaping the new millennium should force Nations to re-align economic security issues across all of its Defence, Authority, Constitutional and Protective functions. This is not a call to review politics of departmental budgets and funding of existing conventional security programs: rather we seek to have national security as strongly associated with the economic well being of each of the Nations citizens, as national security is associated with border protection, military intelligence and conventional defence forces. Aligning and encapsulating an economic security strategy within the traditional national security agenda and agency frameworks creates a dilemma'[182]. This requires our national security planners to balance the Nation's agenda in the economic security spectrum between a vision of co-operation and domination:

- Co-operation - Seeking collective security through integrating trading systems, co-operating to grow markets and sharing benefits of growth (i.e. 'non-zero-sum' or win-win strategy).
- Domination (or confrontation) - Seeking to maximize the protection of the Nation's economic interests, counter the economic leverage of others, including developing the capabilities to strike at another actors economic power and to detect and defend against attacks on the Nation's own economy

The first vision of co-operation accepts weakening the positions of the Nation, deferring to transnational economic actors, in order to allow positive effects of the global economy to flow to the Nation's citizens. This may be viewed as an "idealist" view (see 2.3.2 Idealism and 'Political Realism') of economic security, however the benefits of globalisation are a moot point in this thesis. The alternative confrontational vision sees geo-economic warfare[183] where Nations seek to develop new weapons and defences to maintain or create a dominant position in economic and international affairs.

---

[181] Luttwak E. N., '*The Coming Global War for Economic Power'*, The International Economy, 1993

[182] An example of this dilemma' was described by Beverly Crawford in an often quoted chapter "*Hawks, Doves, but No Owls: International Economic Interdependence and the Construction of a New Security Dilemma*" from On Security (Lipschutz R.D., ed. On Security, New York: Columbia University Press, 1995). Crawford makes the case that decreasing the dominance of the Nation reduces military threats, however this same process increases the military vulnerability through dependence on commercial markets for military technology outside the Nations control.

[183] Luttwak described geo-economics as the "dominant phenomenon in the central arena of world affairs'. See Luttwak E. N., '*The Coming Global War for Economic Power', The International Economy*, September/October 1993

7.2.2 Economic Crisis Scenarios

Economic and security commentators[184] forecast that Nations in the Caucasus, Central Asia, Sub-Saharan Africa, Middle East and some in Latin America Nations will suffer economically. These nations tend to include poorly diversified economies with existing conflicts. Other crisis areas see new economic superpowers that emerge to rival US economic hegemony (eg the European Union, China and/or India). However, Nations of all economic strengths that do not manage all of the new millenniums drivers[185] face the prospect of financial instability, crisis, and failure.

In parallel to the changing fortunes of Nations, the gaps in the standard of living may increase dramatically as economic benefits flow to only limited segments of the global population: fuelling ethnic, class and regional (geographic) tension both internally and externally. Unlike previous periods of economic growth, the media of the information revolution makes a person's poverty (or wealth) more transparent to themselves and others; in addition, it makes suffering (or greed) more difficult to disguise, further fuelling tensions. Those tensions can now extend to new transnationals economic classes.

Even for the well-placed economies, such as Australia, sustaining positive economic growth will depend upon managing through the economic conditions that influence the global economy. The increasing interdependence of markets and financial systems has seen financial shocks[186] rapidly flowing over borders and creating instability and crisis in other (innocent) Nations.

The Nation must ensure adequate protection against combinations of economic instability and crisis that may result from a number of crisis scenarios such as;

- Disruption of the flow of energy products (i.e. blockade or wars)
- The sustained downturn US economy (beyond a cyclic recession)
- Failure to address structural risk arising from changing demographic in large economies (eg EU and Japan)
- China and/or India's economic growth stagnates or fails to meet high growth expectations

---

[184] For example Tenet, G. J., (Director of Central Intelligence), *Worldwide Threat 2001: National Security in a Changing World*, Central Intelligence Agency, Statement before the Senate Select Committee on Intelligence on February 7, 2001, STRATFOR.COM *Global Intelligence Update*, January 3, 2000 www.stratfor.com, berghof Handbook for conflict Transformation, berghof Research Center for constructive conflict management, 2001, www.berghof-handbook.net

[185] These include: emerging rivals to the USA, globalisation eroding the Nations sovereignty, population pressures, heath crisis, management of natural resources, energy consumption, technology dependencies and trans-national crime. See page section 1.4 for more details

[186] For example the 1998 Asian financial crisis.

- Government and financial institutions in Nations targeted as emerging market allow weak governance and/or do not reform to meet minium global requirements

Many organisations, central banks and in particular the Bank of International Settlements (BIS) focus efforts on international protocols to improve safety and stability of the global financial system, especially to prevent systemic shocks. Against the background of the global economy, individual Nations and trading collectives search for national economic security.

Major sources of tensions and conflicts among world powers are the accelerating economic interdependence and international competition for wealth. In previous eras, it was possible for powerful Nations to seize domains with the aim of profiting from any resources acquired as spoils of victory. In resource rich domains[187] where opponents had inadequate defences, Nations with dominant military power quickly brought it to bear to dismantle incumbent or native control, extract resources and open new markets. In the event that a campaign failed, another military investment could be made again or elsewhere, which was hoped would make up for previous losses. To capitalise on domains acquired the Nation provided special access and patronage to its own trading groups and supplied various security forces. So long as these forces could be employed to exploit colonial holdings, economic problems at home could be addressed.

Competition for economic control and the freedom to exploit economic resources in new domains would quickly grow between rivals with symmetric military power. In addition to military forces, a Nation may have also conducted crude forms of economic war, targeting non-military assets of the rival Nation[188]. Historically economic warfare has been relatively blunt and direct. It consisted of attempts to overtly starve rivals of economic resources, or influencing resource use, over time causing the rival to choose between economically bleeding to death or submitting to the attackers will.

Increasingly material desires place political pressure on all Nations to improve their relative standard of living. Emerging powers (esp. India, China), developing economies, and poor countries (i.e. have-nots) search for whatever means available to enhance their economic security to the developed levels. Conversely, developed countries (i.e. haves) are eager to maintain their

[187] Examples are found in Medieval Middle East, America Indian Nations, Australian settlement, and Chinese Opium wars.

[188] Dombrowski, P., *Alternative Futures in War and Conflict, Implications for U.S. National Security in the Next Century*, Strategic Research Department, Center for Naval Warfare Studies, Naval War College, Newport RI, April 2000 and Gumahadii, A. T., *The Profession of Arms in the Information Age* ,Joint Force Quarterly, Institute for National Strategic Studies, National Defense University(USA), Spring 1997

standards of living, grow market share and especially not loose any of their (relative) economic power to peers and emerging rivals.

7.3 Financial Infrastructure Hazards

> *"In flying I have learned that carelessness and overconfidence are usually far more dangerous than deliberately accepted risks"*
>
> *Wilbur Wright*[189]

Having considered the vital place that financial infrastructure (esp. money, payment systems and financial information systems) play in security, we now turn our attention to the threats, vulnerabilities and risks faced by individuals, communities or Nations and the global economy.

In addition to common fraud and other transactional problems, the use of money and payment system creates vulnerabilities resulting in several broad families of risk. These include tangible problems such as protecting confidentiality and dependency of transactions, through to social impacts of systemic failure. Our research has identified eight broad families of hazards that adversaries could seek to manipulate, leverage and multiply to support their objectives and interests as part of economic warfare. These hazards families must be understood so that they can be appropriately protected or exploited.

Firstly, we must distinguish the economy from its financial infrastructure. Financial systems risk management consist of the study of many individual threats, hazards, vulnerabilities, and resulting levels of risk. These risks exist at different "levels" and stages of a transaction. This thesis does not focus discussion on the classes of risks associated with the everyday quality of goods and services being exchanged or the particular risk issues associated with different markets (e.g. oil, bonds, securities, futures). Rather, we focus on what we call "below the waterline" vulnerabilities: those that counterparties are either unaware of, or expect are handled by other parties in the market. These hazards are inherent or a systemic in nature, resulting from the role that money and payment infrastructure plays, especially in the context of National Security.

7.3.1 Transaction Hazards

Threats to financial systems can take on many complex, technical, and theoretical forms, especially as transactions become more sophisticated in terms of time, number of parties and diversity of trading terms. At the heart of

189 Wilbur Wright in a letter to his father, September 1900.

transactions are a number of types of problems that are well known to experienced trading parties and systems designers. Commonly recognised threats in systems of exchange consist of one or more elements from the following families of malice.

Conversion and money laundering hazards whereby sellers misrepresent transaction in order to obtain payment instrument for insufficient value goods and services. For example, a buyer overpays the seller for stolen (dirty) goods in order for the seller to receive (clean) money via a third party payment systems provider

Forgery hazards whereby buyers create (or use) invalid payment instruments to misrepresent a source of value. For example, use counterfeit currency.

Insolvency hazards whereby buyers use a valid payment instrument to exchange value where no value exists. For example, a buyer writes a check or conduct offline card insufficient funds or credit exist (i.e. when not liquid in order to gain advantage before the payment claim can be verified.

Masquerade hazards whereby buyer uses a valid payment instrument to transfer a value that rightfully belongs to someone else. For example, use of a stolen credit card or identity theft[190].

As these examples indicate, traditional payments media such as currency, checks, and credit cards are not exempt from these threats. Currency fraud (counterfeiting), check fraud, and credit card fraud cost billions of dollars each year.

7.3.2 Operator Negligence Hazards

In addition to mundane transactional risks, the users of financial infrastructure become systemically vulnerable to the operation risks within that infrastructure (provided by a third party). No one actually "regulates" or manages these risks on a global level, although some organisations (e.g. BIS) provide focus points for co-operating states. Concerns over the vulnerability and stability of the financial infrastructure are very prominent in discussions taking place at the level of central banks, international regulators, and international financial institutions. National Security and Social welfare actors are seemly taking greater interest in payment systems risks as dependencies become clearer.

The financial information infrastructure providers naturally seek to operate profitable systems that can reduce risks more efficiently than the traders could manage themselves. However, the trading parties face the possibility that the

[190] Where a villain is able to create a passible personal signature they use a both masquerade and forgery techniques

third parties over engineer their controls or alternatively provide inadequate operational or strategic protections. The systemic exposure to a third party's risk management posture is illustrated in the extreme by the impact on citizens when the monopoly issued currency of their state collapses.

From the viewpoint of the traders, there are concerns that the third parties do not address the threats (or risk level) in a ways that are consistent with the traders expectations. For example robbery or embezzlement at a local bank (prior to regional banking chains), effectively undermining the entire communities store of wealth. A key dilemma for third parties is trying to balance the level of transparency they provide to users of their financial infrastructures, with the need to restrict knowledge of controls for operational security reasons. Fortunately, in most modern Nation-States, licensing of financial institutions is commonplace, which provides customers with a level of confidence in the adequacy of risk management approach. In addition, advanced nations pride themselves on the use of commercial forces to drive financial infrastructure providers toward the most appropriate risk management postures.

However, there are considerable opportunities for poor risk management where a third party has a monopoly, undue influence or cohesive power over the trading parties. In particular, where licensing requirements do not stay up-to-date with new threats, or regulators are unable to effectively enforce licensing, opportunity for inconsistent risk management can arise.

To provide payment certainty, a successful payments medium has to overcome various risks that are a natural part of the payments process. The key for risk managers is to find the optimal level of controls by balancing costs and benefits. A successful system does not attempt to eliminate payment risk however it aims to make losses predicable so those prices can be appropriately adjusted.

These are highly complex and demanding tasks, as the payment infrastructure continues to be assaulted by micro and macro risks identified by changing economic, organisational, social, political, and technology factors.

The significance of risks varies with the type of payment system, its architecture, and the nature of the risk managers. For example, in large-value systems the regulators are commonly focused on (wholesale) interbank counterparty risk esp. credit and liquidity, because failure of a bank may cause the failure of innocent others. Whereas a small merchant accepting cheques focuses on operational risks of signature verification, lest they face dishonours by their (retail) bank.

On a global scale, risks relate to the growth in a "system of systems" that transfers the many trillion (worth) of US dollars every day. System growth has occurred in the number payments (and related messages) and the value of

payments handled by payment systems – "many of which were originally ill equipped to handle the activity"[191].

Anxiety within the global payment's forums continues the real battle to reduce many types of payment risks because these risks pose such a significant threat to financial stability for so many. For example, we are witnessing the move away from netting architectures in large-value payments to replacement by Real Time Gross Settlement (RTGS) structures, along with improvement the relevant contractual and statutory factors.

7.3.3 Criminalisation Hazards

Actors (esp. money launderers), use covert techniques to infiltrate large legitimate businesses, undermine sectors and potentially subvert the legitimate governments roles. Rather than overt degrading or destruction of financial infrastructure, an underground or black economy[192] impacts effective regulation, collection of taxation, and productivity benefits of a Nation's own economy. A greater risks are that the entire Nation becomes criminalized to support the market manipulation and criminal activities. This creates a considerable risk to those in small states faced by the influence of large multinational organisations that are dependant on the state's financial infrastructure.

7.3.4 Surveillance Hazards

In advanced economies, purchases of goods typically involve a third party who is either the issuer of the community's fiat currency[193] or a provider of the payment systems. The great advantages of these systems are that they can address risk issues on a much broader front that any buyer or seller could hope to manage alone.

However, the involvement of third parties creates many fundamental hazards for the buyer and seller, resulting from the third party privileged position in transactions. With physical notes and coins the risks of third party involvements are largely logistical, currency strength and to a lesser extent

---

[191] Heinrich, G. (Head of the CPSS Secretariat) *The BIS Process And The CPPS Core Principles Bank For International Settlements, The Contribution Of Payment Systems To Financial Stability* Papers presented at a workshop on payment systems at CEMLA, Mexico City, May 2000

[192] For example in Pakistan, Colombia and the trends in parts of the former Soviet Union.

[193] In the event that you are exchanging goods and service directly for currency (not as a sale), with the currency providers or issuer (eg. chief, priest, king, government, EU) you are presumably bartering with that party as to the value of their money.

surveillance[194]. Attention tends to focus on the loss of the stored value via theft, destruction or devaluation of the money artefacts.

Within electronic financial infrastructure, surveillance becomes a major hazard for users. This is a major disadvantage in those exchanges where confidentiality is vital. These situations are numerous and include illegal exchanges and especially those that are "legal but sensitive" exchanges. Sensitive exchanges will vary across jurisdictions, however they can be described as transactions that are unethical, commercial-in-confidence, or socially embarrassing for the parties.

Further, because global criminal (and unethical) enterprises need to use global electronic payment systems they go to extraordinary lengths to avoid detection. As a result, payment system providers have legitimate reasons to build increasingly more sophisticated surveillance systems, with the common user being often unaware of the potential of these systems to be misused.

7.3.5 Erosion of Quality Hazards

When barter and unstructured promissory systems dominate primitive economic infrastructure: the risk management burden (esp. fraud prevention) and assessment of the quality of exchanged goods and services are largely placed on the trading parties. Parties must focus on the quality in the immediate transaction, with threats largely determined by the parties' (limited) experience, knowledge, and skills. However, in advanced economic environments fraud prevention must additionally focus on factors outside the trading parties direct influence or control. This includes the "quality" of monies and the "confidence" in payment systems and economy.

As we have seen, by using some form of money, an economy can function more efficiently by allowing parties a value system (count or measure) so that they can undertake transactions without the restriction of a double coincidence of needs/wants. In advanced economies the buyer can also offer to transfer to the seller an promise to pay later (eg an IOU) or an ability to make a payment claim on a 3rd party (eg the issuer of currency). This system creates great flexibility but incurs vulnerabilities related to the wider value of the money or system.

At one level, the issuers (or backers) of the money or system are rarely physically present to verify the quality or confidence of the claim at the place and time of the exchange. When a transfer from buyer to seller occurs, there are then always possibilities that the buyer may offer a fraudulent payment claim

[194] An example of indirect surveillance through currency occurs where governments regularly test notes (and coins) for the presents of various substances to determine trends in cash use or public health. For example some governments test cash for traces of illegal drugs to infer usage patterns.

or the seller passes goods and services at a fraudulent value[195] (i.e. for money laundering).

Beyond the single transaction, parties are at the mercy of many others within the economy who use the same money and payment systems. Various changes in the broader economy can result in the relative purchasing power of a currency chain. This can result in erosion in the quality (or confidence) of the money used. Savings and investments may then become worthless through no fault of their owners.

7.3.6 Panics (Runs and Liquidity Shocks) Hazards

One of the seemingly pervasive hazards that affect the stability of economies occurs through the asymmetric access to information about the state of a market. Where creditors become concerned that major organisations are insolvent, the organisation, its Banks and interrelated parties may experience a liquidity shocks. These shocks can flow through the rest of a sector, with other financial institutions being drawn into depressed equity prices and restrictions in credit. While sources of credit are restricted, organisations scramble for funding and call for tighter payment terms. In depressed times and insolvencies the total available credit may be limited, making its distribution even more critical for the functioning of a Nation's economy.

Initial liquidity shocks make investors (and bank depositors) uncertain about the accuracy and suitability of the risk management and underwriting techniques. The behaviour of the accurately informed and mis-informed actors may be indistinguishable to outside observers. Worse still third party analysts may make assessments leading to further uncertainty about the actual state of the market. Parties may be unable to target, gather, process, analyse and act on market information a sufficient speed to make correct judgements. Lack of sufficient transparency and independent reporting contributes to the "fog of the market" and permits rumours and speculation to be used for decision-making.

However, some will be better placed than others to understand the environment and can use this information to maximise opportunities or can

[195] This can also occur on simultaneously both sides of the transaction. For example, we could consider two "unethical (!)" parties who enter into and exchange. Party A may buys some illegal product, such as drugs from B using some form of cash as payment. Both parties then discover that they have been defrauded at different parts of the transaction. Party A holds may have been sold worthless drugs at an agreed value and B discovers that he has been given cash that is worthless (i.e. forged value). Both have committed fraud, but within different elements of the transaction. Either party may attempt to reverse the transaction (and bear associated risks) or they could attempt to transfer the problem onto other parties, in the hope that a future exchange will provide them with some form of "real" value.

charge a premium for data. The asymmetric information[196] across the various parties serves to amplify disturbances allowing dramatically different outcomes. The accelerated tempo during a crisis leaves all parties (inc the Government agencies) exposed to information gaps. Financial infrastructure that normally operates perfectly well becomes unable to serve the markets needs. Information becomes a premium and desperately sought by exposed parties, further compounding the cost of the crisis. In the absence of credible information, parties may flee the market or may choose to gamble funds without sufficient understanding of the environment.

The traders may take defensive positions (just in case) by moving substantial sums out of the organisation and its dependant parties. At this point in a crisis, it may become difficult for credit to be made available to perfectly healthy operations, because lenders become nervous, highly conservative, and uncertain about the way in which they can identify borrower solvency. For economies that have highly automated infrastructures and sophisticated markets, the shock can be transmitted quickly through the whole economy without human involvement. Organisations may only have hours within which they must be able to reassure investors, depositors and regulators of solvency.

Confronted with failure in a private credit market, the Nation may be able to provide some payment system stability. However, there are strong disincentives in market economies for the Nation to interfere in the operation of the financial sector, as in theory letting the market discipline rule will produce less-riskier more efficient banks. The state's interference in the financial operations may be required in order to protect it political and security interests above that of the private sector. The Nation also has unique powers or options to construct solution than are within the power of the private sector acting independently. Using its special position it may be able to obtain information that can be put to use in way that the private sectors cannot. The Nation can act as a lender of last resort (LLR) in cases where the national interest and national security requires extra-ordinary interference in the market. The Nation does not have to lend capital directly to the market in these cases. It can provide liquidity indirectly through a wide variety of mechanism from interest rate adjustments, special terms or trade and even tax relief. The Nation may provide liquidity to individual banks (which cannot fund themselves) to ensure that stability of the economies payment systems. In a crisis, this may mean that the Nation role is restricted to lending only to solvent, but non-liquid banks. Difficulties arise for the Nation, as the LLR if it does not have the specialist-lending framework or

[196] A change in monetary policy in early 1995 the practices of Russian bankers caused the paralysis of the banking system the August 1995. It became impossible to tell strong banks from weak because of a lack of publicly available truthful information. With inadequate information to access counterparty risk, Banks became nervous about interbank exposures and a crisis occurred as banks refusing to transact triggered only by mild signs of non-liquidity.

can not identify better solutions than the private sector specialists (i.e. banks). Further, the Nation itself may not have the capacity to provide the necessary funds to lend. This is particularly the case in the world's smaller economies that may be dominated by multi-national organisations.

7.3.7 Demonetising Hazards

In the event of failure of payment systems and the resulting shock, an economy may be forced away from certain types of payment system. In the some case, the payment system failure can spill over into a money failure (the community may reject some form of existing money). If prices, payment system, and money supply don't find a new equilibrium, the economy may be caught in the institutional trap of barter and become systemically demonetised. Without effective payment systems and institutions, an economic recovery from low-level equilibrium may become retarded.

The rapid growth of non-monetary transactions is one of the most striking features of Russia's transition to a market economy. Russian economy has become highly demonetised since the macroeconomic stabilisation of 1995[197]. Barter and promissory notes (a.k.a. vessels) have become a major payment system in Russia.

Some of the worst effects of demonetised economies are the potentials for local power brokers to focus only on economic building based on their local power over barter goods and services. For example, during the 1970s war in Lebanon[198], warlords entrenched themselves at major access and trading routes and added to the fragmentation of the economy and to transaction costs. This focuses local politicians, from these areas, to encourage barter as part of their power base. This puts them on a collision course with federal governments. The federal government has to bear the macro-economic impacts and cost of Government without an effect tax base of money circulation. Widespread barter reduces transparency in the economy that in turns leads to poor accounting and governance, lower tax base and enables greater corruption.

In order to reduce barter, governments are then forced to promote competition and fight the barter and promissory notes payment systems to try to re-introduce the Nation's currency. Except where there are double coincidences of needs, a barter system cannot deliver optimum production, and

---

[197] The broad money base (M2) has been only about 15 % of annual GDP, which is far below levels observed in OECD countries and other transition economies. See Russian Economic Trends (1995-1999). Blackwell Publishers. According to various sources, barter accounts for 30 to 80 % of inter-firm transactions. Data on promissory notes are scarce but some estimates indicate that they account for 10-20 % of inter-firm transactions with total volume being as large as 10 % GDP

[198]. Kubursi, A. A *Reconstructing The Economy Of Lebanon,* Arab Studies Quarterly, Winter99, Vol. 21 Issue 1

has high transaction costs. In addition, when in competition with Money based payment systems it is soft and slow to pass on price signals, resulting in the efficient firms not being rewarded.

7.3.8 Systemic Collapse Hazards

The global financial information infrastructure is an artefact of our evolution into a worldwide information civilization. When considered in terms of scope and value traded[199], financial infrastructures define the global market in its broadest sense; they are multi-time zone, multi-currency, multi-national, multi-lingual and multi-cultural. These infrastructures are some of the greatest users of high technology: highly network and highly information centric.

Our dependency on value exchanged as money via the electronic payment systems cannot be understated. The capability provided by money and financial systems allows individuals, organisations and nations to exchange goods and services, especially the innovation and ideas, allow all to progress.

A collapse of a currency or financial system not only impacts on the efficiency and effectiveness in that domain it has the potential to trigger systemic collapse. Widespread systemic failure of one or more system; from a catastrophic natural diasters or deliberate action, have painful consequences for domestic and global economies.

Countries denied the capacity to trade (buy) goods and services are at the mercy of the charity of other nations. Examples of the potential impacts on societies can be drawn form numerous economic sanctions used to punish rogue nations. The loss of the ability of a Nation to trade its internal sources wealth (e.g. oil, knowledge or even its tourism) for external goods and services (eg. food, water, medical or military systems) undermine its freedom and choice – therefore its security.

As has been painfully demonstrated in the Asian, Russian, Latin and September 11th financial crisis, the system is not "too big to fail" across a region. If the money stops going around, the effects could range from consumer inconvenience through to hellish nightmares of social or even civilisations collapse. We consider that few entities have the capacity to cause a global systemic collapse and consider this scenario unlikely. Such an attack would require systematic strikes on dozens of the core global system (e.g. SWIFT, FEDWIRE, TARGET, BOJ), nodes (eg New York, London, Tokyo) and associated fail-over facilities. Techniques to deliver such a strike are achievable by the major powers (eg USA, UK, France, Russia, India, China) using their various WMD (eg nuclear) capabilities. Scenarios that are more complex could

[199] Although barter and non-electronic systems account for significant volume of transaction, they are dwarfed by the value-transacted daily by international electronic systems.

be developed, such as using asymmetric information attacks. We however consider such a global level threat theoretical. Of greater likelihood is a deliberate attack on a specific nation or group in the context of an economic conflict. Such an attack may be aimed at collapsing a system for a limited period, or in the case of an ideological battle an attempt to destroy economic foundations.

7.4 White War in practice

Economic warfare, known as the `white war'[200] has developed along the same path as our economic development. Simple raids and theft was the common tactic in pre-industrial eras. Economic warfare developed through events such as scourced earth tactics, destruction of banks, naval blockades and the interception of contraband.

The ideas of economic warfare were seen in large scale in the Non-Importation Act of 1807[201] of the American Revolution prohibiting most British imports, the Embargo Act[202] against all foreign trade, and the Non-Intercourse Act[203] of 1809 banning trade only with France and Britain. The wars of the French Revolution and Empire further enhanced the strategy of coercion by denial of supply. As greater international trade developed, tactics included pressuring neutral countries from which the enemy obtained its supplies and to deny markets for goods. For example, Napoleon's 1806 Berlin Decrees and his Continental System to prevent European Nations from trading with the "nation of shop keepers" i.e. Britain.

In the large conventional arms conflicts between Nations in the 20th century it was often seen as critical to secure both control over primary economic resources (oil fields coal mines, wheat fields, rubber plantations, fresh water etc.) and the financial infrastructure within newly controlled areas. In these conflicts, economic warfare can also be used to ensure war reparations, rehabilitation or to ensure return of wealth to legal owners. For example the Safe haven program of WWII restricted the movement of German resources (inc. "enemy" capital and technicians), for a number of virtuous reasons, however the essential act made it economically unfeasible for Germany to start another war. In the wake of military victories, the new power needed to re-

[200] The term White War was first used by The Economist, May 1939

[201] _, *Importation Act,* House of Representatives, 9th Congress, 2nd Session, H.R. 59, Congressional Record, February 13, 1807

[202] _, *Embargo Act,* House of Representatives, 10th Congress, 1st Session, H.R. 20, Congressional Record, December 22, 1807

[203] _, *Non-Intercourse Act*, House of Representatives, 10th Congress, 2nd Session, H.R. 64, Congressional Record, February 11, 1809

establish a financial infrastructure that would ensure military return on the investment and further enforce its control.

Beyond imposing a tax, victors can seek to impose their own economic order by taking over business registers and collection of business information, restructuring supply for their benefit and most importantly controlling wealth flowing through the conquered economy (esp. to achieve popular compliance). Until the wide spread adoption of electronic system in the later parts of the century, this often meant targeting precious metals (Gold), gems (diamond) and especially national currencies.

This figure is not available online.
Please consult the hardcopy thesis
available from the QUT Library

Figure 8 Japanese "occupation money" (1942)[204]

For example during the WWII, the Japanese had specific economic plans for its newly acquired empire. Japanese economic experts, who had toured the world, had selected a plan based on the "English Model" of colonialism, before the start of the war, for what it called the Southern Region. The model can be seen in the decree was passed in 1942, during a liaison conference[204] between the Military and the Zaibatsu (powerful industrial business-families).

> *"The Southern Region will be, for the present, a source of raw materials and a market for our manufactured products. Measures will be taken to prevent industry in this area. Wages will be kept or as low as possible….*
>
> *…. A Southern Region Development Bank will be set up to milk all foreign assets and to supervise the introduction of a new currency."*[204]

[204] Mac Master, H., *The Brisbane Line*, Central Queensland University, Rockhampton

As part of this strategy millions of notes were printed to be used as "Occupation Money" and example of which is depicted in Figure 8. However, it was secretly agreed that the Japanese Yen (a back currency) would not back these occupation currency, making it essentially worthless outside the empire. Millions of these bank notes were printed using currency titles, denominations and style familiar in each conquered areas[205].

During WWII in the USA, the Executive Committee of Economic Foreign Policy (ECEFP) was established in April 1944, as an interdepartmental group, to function as the primary planning and coordinating body for economic policy[206]. The ECEFP studied issues involved in economic warfare, anticipated the economic programs connected with Germany in the post-war period, and took steps to initiate plans which would operate effectively after the defeat of the Axis. It considered from time to time such matters as modification of wartime financial controls over foreign assets. It had considered for example the possibility of continuing the Proclaimed List after the surrender of Germany as a method of economic supervision of Axis friends.

Economic warfare was refined after World War II as part of Cold War tactics to deny potential enemies goods and commercial knowledge that might contribute to war-making ability. One of the primary measures during this period was the embargos on specific goods or total embargoes on all goods. For example during the 1950s, the United States and other countries maintained strict embargos against the Soviet Union and Eastern Europe on a large list of broadly defined strategic goods (including encryption technology).

The major powers attempted to obscure much of the economic warfare they conducted during the Cold war. However, some time direct policy involvement in overt campaigns came to the attention of the public, such as in 1973 when Chilean economy came under heavy attack by the US[207]. The US cut exports leading to parts shortages, bilateral aid was cut, export-import bank credits were cut entirely, Inter-American Development Bank loans were slashed and the World Bank was pressured to give no loans to Chile.

With increasingly complex global operations and sophisticated technology, economic war fighters have a number of additional tactics at their disposal.

---

[205] For example: pounds and shillings where created for the South Pacific including Australia and New Zealand, dollars and cents in Singapore and Malaya, pesos and centavos for the Philippines, guilders and cents for Indonesia. As Australia and New Zealand resisted invasion few of the pound or shilling notes were circulated. Millions of these pound and shilling notes were discovered in Japanese warehouse after the war and destroyed.

[206] Records of the Economic Warfare Planning Committee, National Archives and Records Administration (NARA), www.archives.gov

[207] This policy is clearly stated in USA's National Security Decision Memorandum (NSDM) 93 issued in early Nov. 1970.

7.4.1 Contemporary Use of Economic warfare

Evidence of insurgent attacks on economic targets has been clearly demonstrated. Recently economic warfare has seen specific industries targeted simply for their economic value to a rival, not because of any associated military value. The tourism sector in Spain is a recent example of such an industry, where ETA conducted campaigns aimed at disruption. Numerous examples can be found in other countries including incidents in Greece (e.g. Banks, car dealership, and businesses), Colombia (eg. multiple oil pipeline bombings), India (e.g. attack on multiple commercial buildings in Bombay), Egypt (e.g. Tourism), and Sri Lanka[208] and of course battle weary Israel.

Economic sanctions have become a frequent tactic of economic warfare against rivals[209]. Where offence was taken by an alliance of states, multilateral actions could be taken with the added benefit of propaganda advantages. The idea of the League of Nations Union in 1918 was that the political mechanism of economic sanctions could convey to the people of the target Nation the disapproval of the world[210]. It was expected that an aroused public would compel their government to bow to the demand of the world community. The intent of the League of Nations and later the United Nations has been to develop economic sanctions as a coercive instrument, capable of forcing target governments into altering policies. As a coercive force, economic sanctions aim to create political pressure on in the rival Nation (esp. on leadership) to facilitate compliance. However, sanctions create propaganda and other dilemmas as the poor and vulnerable may be impacted [211] in a target Nation, leaving the real targets (eg leadership or business) virtually untouched. Before the war in Afghanistan, the ruling Taleeban condemned the economic sanctions on the war-ravaged country.

In addition, factions and government may strive to misuse sanction for profiteering or revenge. In June 1995, the Secretary-General of the United

---

[208] In one incident a military air base was attacked along with the international airport

[209] Littlefield, N., Self-Enforcement and Economic Sanctions: Obligation or Self Interest, Rationality or Ideology, Social Science 410, Andover Economics Project, Phillips Academy Andover, MA, November, 1998

[210] Kirshner, J. Political Economy in Security Studies after The Cold War, Occasional Paper #20, Peace Studies Program, Department of Government, Cornell University, Cornell University, April 1997

[211] Unicef's "The State of the World's Children" 1996 , report stated that several years of sanctions against Iraq reveals a minimum of political dividends as against a the price paid primarily by women and children. The food rationing system provides less than 60 per cent of the required daily calorie intake, the water and sanitation systems are in a Nation of collapse, and there is a critical shortage of life-saving drugs. In Haiti, too, sanctions are thought to have cost the lives of thousands of children

Nations recognised one of the dilemmas in the use of sanctions and described sanctions as a blunt instrument[212].

> *"They raise the ethical question of whether suffering inflicted on vulnerable groups in the target country is a legitimate means of exerting pressure on political leaders whose behaviour is unlikely to be affected by the plight of their subjects."*

Disapproval signalled by sanctioning Nation might not motivate people of the rival Nation into compelling their leadership to change position (in fact it may strengthen their leadership's resolve). However, the sanctions and economic warfare may still be a coercive force, where rival leadership comply for their own personal economic reasons without regard to their citizens. In planning to use this tactic of economic warfare, the coercive forces should be target on elements able to influence policy. The capability to target economic warfare tactics requires considerable sophistication on behalf of the attacker. As in other forms of warfare, information warfare is an increasingly important element to economic warfare.

7.4.2 Overt Attack

The tactics discussed above describe the range and nature of economic warfare, as we know it today. It is important to note that overt interference and attacks on business operations are already significant, with terrorist attacks capturing attention of policy makers. Businesses and its infrastructures are already the favourite targets of terrorism. These actors have discovered that the wide-scale fear and chaos they seek can be more efficiently achieved by attacks on infrastructure/economic targets rather attacking the Nation's security framework directly.

From the point of view of planning an operation, it is obviously more dangerous to attack a tank than a bank. A commercial bank branch is unlikely to be protected by a broad military security umbrella, armour, professionally trained military personnel and doesn't fire high-explosive rounds back at you.

Examples of overt economic attacks can be found in insurgent attacks on economic targets are found in places like Colombia (multiple oil pipeline bombings), India (attack on multiple commercial buildings in Bombay), and Sri Lanka (bank and commercial building attacks). Some evidence of rivals (esp. organised crime) supporting these operations are already in evidence in Colombia, Pakistan, Burma, and parts of the former Soviet Union.

---

[212] Annan, K., *Transcript Of Press Conference By Secretary-General Kofi Annan, At United Nations Office At Geneva On 30 January*, Press Release, Sg/Sm/6152, January 31, 1997. www.un.org/News/Press/docs/1997/19970131.sgsm6152.html

7.5 Tactics of Economic warfare

Broadly Economic Warfare can be defined as (Nationally) sanctioned, backed or tolerated economic activities that knowingly influences economic systems in order to force political will on to others (Nation-State or non-State actor). Economic warfare methods and tactics aim to interfere with the rivals economic interfaces (i.e. inputs and outputs) and interfere with economic effectiveness and efficiency of the adversaries' economic processes.

For some entities, economic warfare, and the supporting tactics used, may be considered a legitimate and reasonable operation (i.e. Japanese "business is war" philosophy) and even a good investment of a corporate or tax dollars. The assessment of legitimacy of using the tactics below is largely an ethical, moral, and political issue outside the scope of this thesis. What is significant is that the tactics selected for a conflict will be influenced by the viewpoints of the combatants and will change at different levels of hostilities. Many of the techniques of economic warfare require overlap with conventional and information warfare.

In review of tactics along the spectrum of economic warfare tactics, we have identified number of families of tactics[213]. The spectrums of families we have identified are as follows;

- Manage Trade Conditions - Effect/remove trade controls, duties and customs or facilitate escape of favoured trade
- Manage Market Liquidity - Supply or Withdraw Loans, Subsidises and Aid, Effect a foreign credit rating and availability focused on favourable outcomes
- Deny access to Markets - Embargos, Blockades, Quarantine, Black listing
- Exploit Market Intelligence - Supply/ Withdraw of economic intelligence and economic espionage assistance, economic and political sabotage,
- Exploit Specialist - Supply/ Withdraw of specialist financial, technical and other skills
- Exploit Local Interests - Providing assistance to allied elements or those that will cause economic problems, support for financial and other crimes, Organisation of a alternative or black markets, Buying votes and contracts
- Degrade Efficiency of Market - Assistance with various types of market manipulation, curtail investments, Slow delivery of goods, services and credit
- Exploit Third Party Local Conflicts - Manipulation or compromise of third party domestic actors or interest groups (eg. domestic trade organisations, regulators, law enforcement), create domestic strikes and industrial unrest, bribe and blackmail officials, assist NGO or interest groups

[213] This lists was complied and refined by the Author

- Manage Decision Information - Dissemination of mis-information and propaganda, support consumer boycotts, psywar (inc fear campaigns) directed at opinion-making sectors such as trade unions, farmer and peasants, student activists and media
- Manage Allied Liquidity - Enlist multinational cooperation, international financial institutions and private firms to tighten economic conditions
- Degrade Supply Chains - Seek local or multinationals suppliers to stop spare parts supply, and cause supply chain interruptions
- Degrade Foreign Markets - Manipulative trade agreements with 3rd party or neutral states, pre-emptive buying and exclusive trading
- Degrade Money Quality - Currency, credit and payment interference (eg strategic default, strategic forgery), Fuelling the black market with currency/credit.
- Exploit Terms of Trade - Pressure domestic savings, superannuation/pensions and loans
- Deny Liquidity - Cut off economic aid, cut off credits, Seek multinationals to stop provision of credit. Develop predominant position in (international) financial institutions to dry up flow of credit and other financial assistance, Cutting off aid and lines of international public and private financing, prevent renewing of credit
- Degrade Development - Retarding development (eg denying personnel and training, limiting energy supply and preventing technology transfer)
- Exploit Supporting Infrastructures - Infrastructure interference (eg power, shipping, air,) and Information systems interference (eg computers, communications)
- Degrade Supporting Infrastructures - Sabotage or covert attacks on rival assets (plant destruction, poisoning, biological agent release)
- Deny Supporting Infrastructure - Overt attacks on rivals assets to deny or destroy infrastructure (eg. terrorist, SF, air strike, or other conventional strike)
- Degrade Goods and Services - Deny or destroy the value of Goods and Services traded in the market (eg. destroy oil facilities, poison live stock, contaminate medicines, disable workforce, infringe copyright)

We must also be reminded that economic warfare is not limited in application to battles between great powers. With increasingly internal security issues including civil wars, domestic emergencies and other conflicts, an adversary may be a non-state actor. This may include organised crime (esp. criminal drug enterprises), separatist and fringe movements, terrorists, religious and political group, or even an internal provincial rebels of independence movements.

In addition to these tactics, counter tactics exist which may also assist in the economic campaign. For example one party may apply a blockade or sanctions on a third party's goods and services, while a rival may counter this by providing the third party with intelligence, techniques and equipment to circumvent the blockade or establish an alternative market.

7.5.1 Advanced Economic Warfare Strategies

The more elegant strategies of economic warfare go far beyond denial of supply (eg through sanctions) Even more sophisticated strategy include measures by one Nation to ensure the economic dependence of another, and thereby obtain political power over it. This may consists of creating an artificial dependence through a subsided market for the exports. In addition, the Nation can attempt to monopolise the supply of certain goods. Consider the historical dependence of states on oil or the contemporary situation with software or the dual effect of defence technology dependence. An ideal end-Nation sees the rival economy and tax base subordinated without corresponding responsibility taken for a rival's population – the economic death sentence for the rival.

Economic warfare is likely to be more effective in the short run when the rival is unprepared for attack and unaware of its systemic vulnerability in its economy. In the longer term a rival who survives the campaign will seek to develop defences and countermeasures, establishing alternative courses of action [214] such as new processes, finding substitutes goods or justification for renouncing debt or contracts[215]. The target may even benefit by strengthening economic independence and developing new trading with enemy or neutrals. In addition, poorly considered economic warfare can provide a propaganda harvest for the rival if attack patterns can be identified. The unintended creation of opposing cartels must be considered in waging economic warfare. As in combined arms and manoeuvre warfare, economic warfare planning must consider the reaction of the rival and make detailed contingencies to be effective in their destruction.

7.6 Conducting Economic Information Warfare

The Nation-State that engaging in Economic Information Warfare (EIW) requires a broad range of capabilities to ensure success. The effectiveness of any campaign will clearly depend on appropriate mix of capabilities compared to

[214] Numerous examples can be found in analysis of the Cold war era and contemporary examples in so-called "rogue" Nations such as North Korea, Cuba, Libya and Iraq.

[215] Olson contends that blockade were formative in Hitler's determination to destroy democracies and occupy the Ukrainian wheat lands.

the defenders. Below we present areas for future focus in the structuring our future National Security strategy.

Attacks on Financial Infrastructure may occur in three Information Warfare Realms that we categorise as physical, information infrastructure and perceptual. It is possible to conceive of campaign launched in isolation within one realm, however we believe that future conflicts are more likely to occur simultaneously across the full dimension of the battle space.

The key capabilities required for mounting a comprehensive Economic Information War are described below in context of each realm. These capabilities are not an exhaustive list; rather we have highlighted priorities areas that planners should consider as part of offensive and defensive programs. Note that we have not listed the counters as separate capabilities as these are not static and will evolve in parallel. The interaction between the various capabilities, their counters and realms is complex and non-linear. It requires the combatants to carefully model the effect of offensive and defensive programs to ensure that desired outcomes are being achieved that are aligned with the opponent own values.

Both the defence and offence of each opponent will contend with attempts at deception by each other. Deception will try to enhance the effectiveness off actions by achieving a degree of surprise in attacks, causing the opponent to take ineffective actions, or making the opponent more vulnerable to attack. Capabilities that aid or degrade deception actions are essential targets in their own right and will be aggressively targeted to enhance the effectiveness of defence and offence.

As highlighted previously, adversaries are not constrained by a shared view of ethical, moral, and political issues. Capabilities will be developed and used based on the viewpoints of the combatants. For example, we suggest that it is reasonable to assume that some adversaries will resort to sinister forms of interrogation and torture in an economic information war. Although we may not consider this as legitimate, our adversaries may be see this as a vulnerability and exploit our weaknesses.

7.6.1 Attacking the Physical Realm

Rather than relying soley on information attacks, physical elements within the FII may be attacked. We argue that it may be more effective to attack numerous points using "hard" attacks including heat, blast, or fragmentation effects. Physical forces and special weapons platforms are selected to attack the responders (staff and equipment), disable the capacity to observe (sensors and communication links), orient and control resources, deny availability of valuable information.

Information Infrastructure attacks in the physical realm may include targets such as financial data centres, telecommunications switches, media outlets, satellite control ground stations, CERTs, corporate head offices and executive residences.

The key physical attack capabilities[216] that we argue will require increased attention and priority in the new national security environment are as follows

- Anti-Satellite Capability (ASAT) - Capability to threaten, strike or interfere with satellites services (to fixed and mobile facilities in the battle space). This may include degrading temporarily or permanently systems such as the Global Positioning System (GPS), SPOT and LANDSAT imagery, communications and especially broadcast systems. ASAT requires sophisticated technologies such as space launch vehicles or high altitude missile launch platforms. This capability may only be available to major powers, with minor powers limited to capabilities that focused on terrestrial command nodes.
- Anti-Submarine Cable - Capability to threaten, strike, or degrade temporarily or permanently marine cable services. Typically, this capability is available to major powers that have specialist submersible recovery equipment. However, low-tech approaches such as trawling cable hooks can provide limited destructive capabilities to lessor combatants.
- Special Operations Forces (SOF) - Special operations forces and agents (including military and intelligence agencies) provide flexible personnel to initiate unconventional physical attacks, especially with urban environments. Working in solo or in small units size, their unique capabilities, and the self-reliance of SOF units make them well suited to indirect aggression required in Economic Information Warfare. Their deployment does not entail the degree of visibility, political liability or escalation risk that accompanies the use of larger conventional forces. Such forces augment the covert infiltration and extraction of key personnel or equipment, aid long-range intelligence gathering, targeting and destruction of facilities, and extraction of individuals and equipment. Special Operation Agents may conduct assassination of key subjects, undertake sabotage and destruction of facilities
- Covert Infiltration and Extraction - Where commercial or overt transport is not feasible into the area of operations then some form of covert land, airborne and surface assets are required to move personnel and equipment into and out of the areas of operation. The area of operations may include an internal jurisdiction undergoing unrest or tension, which may require special transportation to avoid detection, such as appropriately inconspicuous motor vehicles. Further, this capability may require the covert deployment of devices to support intelligence gathering or other operations.
- Energy Disruption Weapons – This capability includes the use of weapons specifically designed to attack oil, petroleum, gas, electricity infrastructures.

[216] This lists was complied and refined by the Author

This includes such weapons as the conductive filaments devices (eg carbon fibres) deployed across transmission lines and distribution points to cause a massive short circuit. The fibres must be removed from the environment to ensure that secondary short circuits do not occur. This weapon can be delivered by cruise missiles or from manned aircraft.

- Strike Co-ordination - C4I modernization and automation to support land, sea, air, space and other precision strike (conventional and non-conventional) capability on to degrade or destroy communications nodes key nodes, links, and personnel associated with critical telecommunication and financial information infrastructure. Platforms may include military strike systems such as: (land-attack cruise missiles (LACMs), Cruise and Surface-to-Surface Missiles, Long Range Aircraft and Artillery). However, the co-ordination should also enable co-ordination of insurgency method (car bombs, mortars) or through use of various industrial equipment (hijack, excavation equipment, explosives, chemical agents) and other asymmetric techniques.
- Physical Intelligence – The capabilities listed in the physical and other realms are interdependent on appropriate reconnaissance, surveillance and targeting capabilities. This includes platforms such as signals collection, real-time electro-optical imaging, high-resolution film-based photoreconnaissance, and meteorological satellite. Visual urban surveillance (incorporating reliable face recognition and automated vehicle recognition) and tracking systems drawing on geographic information system and CCTV Surveillance Networks and other Surveillance platforms (web, UAV etc).
- Directed Energy Weapons (DEW)[217] – High (gigawatts) energy Radio Frequency Weapons (HERF) guns and devices that directs high power radio energy at an electronic target, exploiting electronic circuits vulnerability to overload it temporarily, permanently and may be used trigger a catastrophic failure of supported system (e.g. telecommunication switching network). Weapons the size of a small briefcase must be placed very close to target system, like a computer at a desk. Low Energy Lasers can be used to damage the optical systems of human or electronics thus degrading data collection and processing. A less discriminatory Devices that generate Electro-Magnetic Pulse (EMP) to disable unshielded electronic systems. A development beam generator with a one gigawatt capacity could be used to develop a line of sight EMP which would knock-out most unshielded electronic devices within a radius measurable in tens to hundreds of metres, depending on the employment method. High power microwaves, communications, computers, navigation and data processing systems would be most affected by such weapons

[217] 1995 saw the first known use of HPM technology by subversives. Chechnyan rebels used HPM to defeat a Russian security system and gain access to a controlled area.

7.6.2 Attacking the Information Realm

The FII can be attacked without direct physical impact on the target. This category of indirect or "soft" attack uses communications network or the electromagnetic spectrum to influence the information process or content. It includes the use of bloodless techniques such as various types of software manipulation, manipulation of information process or content by specialists and sophisticated electronic warfare. Although the use of electronic warfare technology is classed with the Information Realm, it should be noted that the frequencies and energy used could be lethal or cause substantial physical destruction because of cascading systems failures (such as a plane crash) in the physical realm. The key information attack capabilities[218] that we argue will require increased attention and priority in the new national security environment are as follows;

- Counterfeit and forgery - Capabilities for creating, modifying, or injecting false or misleading artefacts into the target environment. Artefacts may include creation of passports, financial instruments and electronic files needed to manipulate system or people
- Data warehouses and decision support - Large scale databases to enable situation awareness of the Information Infrastructure under attack. Capability allows interference, aggregation searches, traffic analysis and data mining regards the targeted environment.
- Finance and Market Analysis - Highly qualified economists, market specialist, local advisors and insiders to devise effective strategies. These individuals are skilled to identify optimal financial targets, key supply chains, dependencies, and outcomes required. Specialist must be able to identify priority for intelligence collection and model alternative courses of action.
- Cryptographic Analysis - Sophisticated mathematical and applied engineering skills to break cryptographic protections. This may include breaking authorisation mechanisms via password, tokens and encryption protecting messages
- High end Cracking Facilities - Large computer decryption processing power to crack cipher encryption by brute force. Capability may be supplied by a dedicated large scale facilities furnished with mainframes or through massive parrel array of inexpensive processors.
- Software Development - Programming and design skills required to create various types of malicious programs (Malware) including Spy ware, Pest Programs, Virus, Trojan horse, Logic bombs suitable for use within a specific the target environment or on commercial of the shelf software (COTS)

[218] This lists was complied and refined by the Author

- Systems engineers – This includes professional staff to breach information security protections by using sophisticated vulnerabilities in target systems environment. These specialist software (hackers) and hardware (chippers) engineers identify errors, bypasses, backdoor, flaws, reverse engineer devices, inserts alternative microchips and source codes.
- Information Intelligence - Analysis capability for signals collected and capability for generating high volumes of legitimate traffic to saturate opponents processing capabilities. Capability may be supplied by a dedicated large scale facilities furnished with mainframes or through massive parrel array of inexpensive processors.
- Electronic jamming and deception - Jamming and other electromagnetic attack systems calibrated to impact opponent's devices such as saturate a device with a high volume of signals or broadcast false signals. This may include Low Energy Radio Frequency (LERF) or Ultra Wide Band (UWB) Jammers that generate attacks spread over a wide frequency spectrum to disrupting normal functioning of computers due to high probability that its wide spectrum contains frequencies matching resonance frequencies of critical components. LERF approach does not require time compression, nor does it utilize high-tech components. Capability to disguise or deceive adversaries electronic counter-measures.

These attacks target the processes and content of the information infrastructure to degrade the effectiveness of the defender to perceive the conflict situation. Such behaviour in a limited sense is common in normal competitive business, where opponents attempt to prevent others from perceiving each other projects and plans. However, in an Economic Information War additional techniques will be used to affect observation and orientation of the defender's decision makers. Information attacks may directly attack the observation and orientation processes by overloading or corrupting them to prevent the flow of messages. For example, the economic information warrior who has compromised the Supervisory Control and Data Acquisition (SCADA) system for a liquid natural gas (LNG) distribution's network may be able to choose between destroying the systems or injecting deceptive messages into it. In the case of destruction, the system may be instructed to create an explosive situation destroying the capacity to deliver LNG for export at a predetermined time. Alternatively, configuring message delay or deceptive reporting of data may provide the attacker with opportunities to either attack the efficiency of production (driving up costs) or manipulate the energy market and its derivatives over an extended period.

7.6.3 Attacking the Perceptual Realm

The humans and their mind's can be targeted directly or indirectly with capabilities in the perceptual realm. These capabilities cover a wide range of

techniques and tools, from primitive to leading edge technology. Attacks on human perception seek to influence the perception of defenders about the circumstances of the conflict. Note that deceptions are different to perceptual attacks described. Deception attempts to tempt a specific response from defenders i.e. desirable orientation. Perceptual attacks are subtler than deception, as they seek to cause a desired disorientation (inc. motivation, belief, view, opinion). These capabilities enable the attacker to influence the behaviour of defender, rather than targeting the content and process in the physical and information infrastructure domains.

Psychological operations (PSYOPS) are one of the most well known elements of attacks in this realm, however as detailed below there are numerous other techniques that apply to this domain. Security capabilities[219] that we argue will require increased attention and priority in the new national security environment are as follows;

- Psychological Operations (PSYOP) – These operations capture an audience, hold its attention, deliver messages, and foster a particular belief or behaviour. Reflexive control may be used to create pattern or providing partial information that causes an enemy to react in a predetermined fashion without realizing that they are being manipulated. PSYOPS aims at influencing command and control systems, economic decision makers, buyers and sellers and specific audiences (markets). A Psychological Operations group should consist of individuals that are oriented and trained in language skills, cultural awareness, and ethnicity. PSYOPS groups may be required to operate in internal or domestic environments to counter opponents PSYOPS or build domestic support. In particular, highly qualified linguists, local hires, and native-born speakers should be identified well before hostilities occur, to understand the target audiences behaviours, symbology, norms and values. PSYOPS includes the capability to deliver information using rallies, leaflets, printing presses, loudspeakers, radio and TV transmitters, billboards and posters. In environments with deeper information infrastructure the capabilities may extend further to autodial used with faxes and recorded messages to individuals via fixed or mobile telephones (eg. SMS and WAP messages), CB radio, direct broadcast aircraft and satellites, email, web sites, web casts and emerging broadcast technologies. PSYOP forces tailor the message so it is more effective to the extent to which its messages are culturally sound, linguistically perfect, and highly persuasive, that is, messages that resonate with and reinforce attitudes that can work to produce the desired behavioural results.
- Public affairs – This is the capability to manage relationships with civic leadership regulators, market analysts, and public (both friendly and hostile). Working with PSYOP, this may require the capability to manage the media

[219] This lists was complied and refined by the Author

and manipulating public opinions and a centre of gravity in the perception battle.

- Social engineers and special operations agents - This is the capability to persuade, influence, and impersonate specific individuals within the targeted environment in orders to obtain information or circumvents counter-measures using interpersonal and other "soft" skills. Subjects may include the likes of diplomats, politicians, technical specialists, key facilities staff and especially counter-intelligence or national security specialists. Working with special operations agents, they can assist in intelligence gathering and identify targets. Unarmed agents working solo or in small cells may be tasked to penetrate organisations or facilities to conduct intelligence gathering (a.k.a. spy), identify targets, and undertake espionage. Together with social engineers, the special operations agents provide the capability to use money, ideology, ego, sex, or any other techniques to recruit, compromise, blackmail or otherwise manipulate key subjects or groups. Working with PSYOPs and Public affairs this may include cultivating key subjects that are significant to the target audience. The subjects to be engineered may be used in many ways not solely to demonstrate positive support. Subjects may also be influenced to be neutral, independent or support an opponents cause in order to have a negative effect on their perception. These key subjects may include popular celebrities (e.g. film and music stars), interest group leaders, trendsetters, media commentators and other opinion makers.
- Human Interrogation – The capability to extract critical information from detained subjects within required timeframes. In recent times, sophisticated techniques have increased the speed in breaking down a subjects resistance, using technology and psychological methods that are palatable to open societies values. It must also be recognised that research and development have also devised ever more cruel and inhumane means of extracting obedience and information from reluctant subjects. Contingencies involving interrogation and torture should be considered and appropriate strategies put in place.
- Human Incapacitation Weapons – These include the promising technology of second-generation chemical, acoustic, optical-acoustic, kinetic, microwave systems that enable disabling and paralysing debilitating effects on humans. Such system can be used on internal populations, abduction of key individuals, assist in facility entry without having to resort to deadly force. Such technologies used at lower intensity results in modifications in behaviour patterns and can lead to temporary stupefaction, which can be continued for extended periods. At higher levels of output the rapid increase in body temperature and especially body organs because of microwave bombardment can be fatal.

- Psychiatric Modification – This is the capability to use psychiatric drugs, mind effecting substances and devices[220] to influence the behaviour of individual subjects or groups

7.7 "Hearts and Minds" in open societies

Winning the "hearts and minds" of targeted audiences is an essential part of most conflicts (see 7.6.3). We believe that deception and psychological operations (PSYOPS) will increasingly influence future conventional and information conflicts. Deception is generally well understood, however its cousin: PSYOPS seems poorly understood outside professional circles. PSYOPS activities are directed towards enemy, friendly and neutral audiences in order to influence attitudes/behaviour affecting the achievement of objectives. PSYOPS consists of a blend of disorienting tactics: such as the selected use of real information, disinformation, manipulation of the press, media management, propaganda and other methods that may be considered repugnant by our society. The audiences targeted may be the public, military units, selection panels, interest groups, NGOs, labour organisations, bureaucrats, sponsors and donors, business leaders, or even a specific individual. As in marketing and public relations, adversaries will seek to cause their audiences to conform to their interests. Successful PSYOPS can result in rational people to openly support an organization, ideas or undertake actions that others would consider abhorrent (e.g. smoking tobacco).

An example is the campaign by Sadam Hussien convincing various audiences that American did not beat him in the Gulf War (or that it resulted in stalemate/draw) and that he "defeated" WMD inspections. United Nations sanctions against Hussein have been undermined using a range of techniques including cultivating Arab, Russia, and French interest. Hussein was able to curb further attacks on his country and even obtain authorisation to sell oil to buy food and medicines. The American response to this campaign is to suggest that such a programs will only see funds diverted to rebuild palaces, and military assets. Western interest commonly accuses such "rogue" leaders of conducting propaganda campaigns as evidence of their villainy. Other popular targets have been the Khomeini, Castro, Arafat, Gidaffi and in the past various Soviet Governments and their "puppet" states.

Our analysis however reveals that spin-doctors and PYSOPS are in use by enemies and friends alike, making moral judgements on its use are naive.

[220] We have avoided listing the host of influencing devices speculated about by the conspiracy set and popular press. However the reader should note that that during the Cold War significant resources where committed by Governments to study effects on behaviours of certain technologies (e.g. magnetic effects, harmonic microwaves and electronic implant). Advances in neurology may yet prove to be some techniques useful.

However, a call for better counter-PSYOPS raises emotive concerns in western liberal democracies. We acknowledge that there are many reasonable and serious concerns about developing advanced PSYOPS capabilities, however we suggest that an enhanced capability be developed. Our political leadership should re-examine Australia's PSYOPS doctrines (Offence, Defence, Counters) from political, morale and operational viewpoint. Australia should not fear using PSYOPS capabilities when responding to the full spectrum of crises. The enhancement of our capabilities in this area must be appropriately constrained, with usage restrictions that preserve our National integrity and values.

7.8 National Emergency and Economic Information War

Most disasters and emergency incidents have a relatively short period and are contained when compared to the effects of an economic information war. The response plans for "normal" disasters and emergencies are based around a different paradigm to that of information wars. A non-IW incident occurs as a recognisable event within a disasters area, into which remedial, repair and other emergency workers are deployed. Spare parts are brought into the area to fix nodes and links, and temporary routing is established around the area, until the situation is restored and life goes back to normal. This paradigm contrasts with that of economic warfare or "white war" which aims to slowly drain the financial blood stream of an opponent. Such an attack may not be detected for months or years, it has a simultaneous and nation wide consequences and may corrupt system so that they cannot be restored.

An emergency response to economic attacks has little in common with "normal" disasters. Elements[221] of the plan may call for one or more of the following actions:

- Suspension or conditional trading
- Extra-ordinary transaction with "allied" exchanges and other Central Banks
- Dialogues with international bodies (inc. IMF, UN, WTO, rating agencies)
- Highly specialised financial assistance (e.g. world experts),
- Cancel or deferring payments
- Cancelling contracts, and changing terms of trade
- Arresting or detaining individuals
- Passing emergency legislation
- Confiscation of foreign assets (inc bond, stock, cash)

[221] This lists was complied and refined by the Author

- Seizing exports (grain, coal, steel) or plant (ships, planes) in Australian territory
- Seizing assets outside Australian territory
- One or more other economic warfare tactics (see 7.5)

One of the most complex issues is the jurisdiction and legal situation in the event of declaring an economic disaster. The authority to execute the emergency plan may include a "shut-down," of the Banking system in whole or part. Such a situation may force the roll back of one or more days of trading creating massive disruptions and distorting the entire market. Different types of attacks would require different emergency powers vested in the EMA, RBA, or the National Security Committee. Further Corporate Disaster Recovery Plans (DRP) are not scoped to cover extra-ordinary events like those discussed above. These plans should be updated in line with the Commonwealth approach to survive with an economic information infrastructure attack including the loss of payments systems – i.e. being unable to pay staff, sell and buy and determine liquidity.

7.9 Chapter Conclusions

In this chapter, we provided our analysis of the strategy, operations and tactics that threaten critical economic systems of the Nation-State. We outlined the broad range of activities that we believe exist on the spectrum of Economic War. In our argument, we asserted that interference with economic effectiveness and efficiency of the adversaries' economic processes should be considered in the same light as conventional military strikes. In conjunction, we identified the need to protect our economic system with the same discipline and vigilance that we apply to traditional defence area such as border protection.

We identified eight hazards that impact the security of financial infrastructure. Each of the hazards identified are inherent or systemic in nature, resulting from the processes that money and payment infrastructure play within a large-scale economy. In the context of National Security and economic warfare, the adversaries seek to manipulate, leverage and multiply these hazards to support their objectives and interests.

Having identified the hazards of the information warfare, we provided our categorisation of economic warfare tactics. We also argued that the dividing lines between acceptable business and economic warfare are open to interpretation by adversaries. Therefore, we presented a spectrum of tactics to and did not attach an ethical or moral significance.

Following on from our categorisation tactics, we presented our view on the three realms; physical, information infrastructure and perceptual within which

economic wars will be fought. The capabilities required for mounting a comprehensive Economic Information War where described within the context of each of these realm (or battle space).

Chapter 8. **Recommendations**

Chapter Overview

In this chapter, we provide a number of recommendations that address the rapidly changing security environments described in earlier chapters. Implemented in isolation the recommendations are underway in one form or another. However there is not a consistent or broad program that resources these areas with a view as to protection and assurance of our Financial Information Infrastructure.

8.1 Adopt a consistent information security approach

Across both the public and private sectors, information security is inconsistently approached and implemented. Commonwealth government has long recognised this difficulty and created guidelines (e.g. SECMAN) that should be followed in certain sensitive systems. However, across industries, regulations, codes and contracts there is scope for wide interpretation of security requirements, especially in the private sector. Some organisations have large centralised security teams staffed by experts in all aspects of security (risk management, physical, information, classification, communications, personnel, access administrative, etc.). Yet, within the same industries, we find poorly outsourced responsibilities, inadequate security policies, ineffective risk management, and a host of other inconsistent or naïve approaches. We are not suggesting that there is a one size fits all approach to security management in infrastructure owners and operators. However, the community and industry partners expect that certain minimum practices be met. For example, in the operation of community facilities such as hospitals and air transport, certain minium safety practices are mandated and consistently applied – failure to do so can result in severe impacts on the business.

What we are suggesting is that examination that is more careful be undertaken of what constitutes minimum-security practices for critical infrastructure owners and operators. We are seeing a precursor to this with

wider adoption of the ISO 17799 standard for security management. Increasing consistency through this and other measures should be encouraged.

8.2 Seek wider industry involvement

Before the impact of year 2000 bug, it was difficult to raise the profile of security with senior management. General security and in particular electronic security was viewed as an operational issue to be dealt with by technical managers. The profile started to slowly rise during the 1990s, in parallel to the increasing use of electronic commerce. Security has become a headline issue because of 9/11 events, however the national responses to the new threats have largely originated from an organizational traditional viewpoint. These perspectives come from at most a few hundred specialists - based on individual experience and constrained by organisational roles. The individuals with law enforcement, defence and intelligence agencies each have their different priorities and issues. Particular agency perspectives that must be open to challenge and review by the community. To its credit, the Government has tried to maximise the public availability of information on its first rounds initiative and attempted to engage with business on policy issues - with some success. Yet, the involvement of the body politic in a policy discourse has been limited. A comprehensive National Security strategy including a framework for information infrastructure protection policy should incorporate the following categories:

- Education, innovation, R&D and competitiveness policies
- Emergency services and defence force call out policies
- Encryption and Security Certification policies
- Government and State information resources management policies
- ICT and other crime policies
- Industry ICT policies
- Interception, FOI and Privacy policies
- Library and archives policies
- Media policies
- Official secrets, confidentiality and intellectual property policies
- Telecommunications, broadcasting, and satellite transmissions policies

As a future National Security strategy may result in a significant investment by the taxpayer and/or shareholder (hundreds of millions rather than the current few million), consultation must be wider and comprehensive to cover the complex social issues listed above.

8.3 Encourage Pro Bono Services

Leadership and role models are a key to a credible deterrence and defence against attacks on the FII. The entire nation: at all of the levels of government, businesses, academia, community groups, and individuals should understand the changes that are occurring in the welfare of Australia. Australian professionals in the various fields that constitute the National-Security elites have a citizen's duty to seek way to communicate, cooperate, and coordinate to confront the threats of asymmetric warfare. Within our communities, the legal profession provides a Pro Bono service to the disadvantaged, improving legal outcomes and enhancing general social welfare. Major Businesses and individual professionals should co-ordinate and implement a similar Pro Bono services to address the new threats. The call for assistance has already been answered by a number of visionary corporates and individual, who have volunteered their time to work with the government on Critical Infrastructure Protection committees and task forces. Australia does not have the resources of the major powers to address our disadvantaged and vulnerable information infrastructure, Australia needs all the assistance it can get.

8.4 Improve Financial Systems Literacy

An extensive set of skills is required to address the threats of information warfare on our financial information infrastructure. This includes training in areas as diverse as intelligence, ICT technology, business, legal, public relations, psychology, diplomacy, and politics. Very few individuals would possess all this knowledge. As a result, we must develop teams of professional that have the capability to apply these varied skills rapidly to NII challenges. Although some law enforcement, defence, intelligence and ICT staff possess training in a number of these fields, it is uncommon to find security professional trained in banking, finance, and economics. The absence of understanding of these fields, and detail knowledge of systems that support them, make the task of protecting the critical elements extremely difficult. This is compounded by the premium demand for individuals with this knowledge in the industry itself, which draw staff away from the security industry. Only a small number of analysts have considered strategic weaknesses and strengths in Australia's financial information infrastructure. Few of these also have experience and knowledge of RITS, RTGS, and other core systems. National Security planners must understand Australia's strengths and weaknesses in order to form an effective strategy. Therefore, training in finance, economics, and the various system discussed in this thesis should be a mandatory requirement framing policy.

8.5 Capitalise on the opportunity provided by demand for security goods and services

A comprehensive security policy for Australia will include both defensive protection and assurance elements. We should also look for opportunities to capitalise and exploit the situation. Australia has a well-educated population, a mature infrastructure, and political stability that can enable it to capitalise on the information age demands. A secure electronic commerce environment could be leveraged to multiply investment and provide new opportunities for wealth creation (in our region).

In the past, we have capitalised on its agricultural and mineral wealth during the transitions from agricultural to industrial ears. We should look for new sources on income with information communication technology and electronic commerce as a key strategy in future wealth creation. The rapid growth in these areas is driving the demand[222] for security goods and services. As an export industry, Australia can take advantage of this opportunity in time to offer differentiated information security goods and services – in a similar way, that other nation becomes have become net exporters of national security products. Work by the Mint, DSTO, software developers and others are already showing export promise. Strategically targeting electronic information security as a priority area, (similar to that which occurs within the biotechnology sectors) offers Australia a number of benefits:

- Develops core competency in a service that is growing in demand internationally
- Develop expert knowledge of offensive and defensive techniques
- Spread cost of developing solutions across larger customer base
- Enabling local organizations to access to quality goods and services
- Reduce dependency on foreign imported products and services

8.6 Reoriented R&D efforts to align with NII protection

We are not suggesting that current security work by DSTO, CSIRO and Universities is inappropriate. We do however see a lack of co-ordination of R&D directed addressing the threats to our infrastructure. Much of the investment in R&D still tends to address traditional defence and intelligence

[222] Frost and Sullivan said that the U.S. firewall market alone grew 59 % in 1999. It is predicted to grow at 38.7 % annually over the next few years. A 1999 Yankee Group study, said that security was one of the top two Internet concerns of small to medium businesses. IDC said that security consulting for large enterprises would reach $14.8 billion by 2003, up from $6.2 billion in 1999. A 1999 Ovum report said security services would grow from $74 million in 2000 to $40 billion in 2006 worldwide.

approaches. R&D investment is yet to demonstrate how it is oriented to deal with asymmetric and other threats our information infrastructure faces. Funding should be targeted at increasing efforts until it balances traditional "geographic" economic defence oriented research efforts with those of the information economy.

8.7 Assess the Financial Information Infrastructure dependancies

The functional dynamics of our dependency on NII is not understood in detail. To accurately assess our vulnerabilities and priority we must actively review our financial information infrastructure, especially dependencies on power, and ICT dimensions. This activity is undertaken regularly by owners of infrastructure to deal with natural threats (e.g. cyclones, bush fires, floods) and build in redundancy. On occasion the Commonwealth Disaster plan (i.e. DISPLAN) is updated because of such activity. The closest we have come to such an activity is the Predict exercise undertaken by the ADF looking at its logistics supply chain. However what is not assessed, at the national level, is how infrastructures complement and support each other. Further, such an analysis would need to be updated with the development of new infrastructure. This would include the following; key nodes and linkages, organisational structures, individuals that need to be identified in order to tailor protection, along with an assessment of the resilience of the infrastructure and preparations to handle emergency.

8.7.1 Assess potential aggressors

In parallel with this activity, we should be actively looking at developments, which improve the capability or incentives that may lead others to threaten the information economy. Such assessment would need to build on traditional systems, analytic and training techniques, but would need to develop new observables, indicators, sensors and expand existing data bases. Estimates would need to be made of the options available, triggers, various reaction times and responses.

8.7.2 Conduct exercises to assess preparedness

Once a reasonable picture of our targets and the various threats are articulated, exercise should be undertaken to test scenario assumptions and reactions. A team of appropriately skilled personnel would be charged with actively acting out attacks by adversaries (eg. the fictional Musorians) or organised crime, targeting vulnerabilities, and "attacking" financial information infrastructure. In this way, the defenders could learn lessons about the exposures and incorporate this into the security strategy.

8.8 Expand warning mechanisms

The Government has established a basic framework for National Security alerts and advice through the web and email. However, this system is limited in that it does not provide tailored infrastructure alerts. In conjunction with AusCERT, the existing PSCC warning mechanism should be expanded to include a broader base and provide a dynamic overview of the status information infrastructure. A model for this function is the service provided by the Bureau of Meteorology's issuing of weather reports for shipping and aircraft.

8.8.1 Provide additional resources to AusCERT

Australia does not have the resource to establish dedicated monitoring centres for each industry or sector. Instead, we should enhance what is already working. As AusCERT is already operating and receiving some Commonwealth funding it is an ideal candidate as a base upon which to build. We suggest that critical industries do not establish their own CERTs rather seek to fund AusCERT. Funds can be used to run an industry focused cell within the existing structures and develop appropriate technical interfaces. The Government can assist further with funding, seconding personnel to the centre, providing clearance, vetting services for staff, and providing expertise in operating such centres.

***8.8.2** Begin planning for a National Intrusion Detection system*

The defence and monitoring of our expansive geographic border is a difficult enough task on its own. We now have another border in our electronic perimeter. It is often argued that defending that perimeter is impossible, we disagree, and would rather seek to quantify the difficulty. China and other nations have endeavoured to build a comparable function, however we are only advocating monitoring, and not filtering or blocking. In should be noted that until very recently many nations were able to monitor most of the electronic traffic entering their Nations. In fact, the major powers have built global systems, not to monitor their own traffic, but the traffic of many other nations. Now the volume of traffic and cost of equipment are making it a very expensive exercise, which only a few nations can afford.

We believe that it is feasible to monitor a significant proportion of traffic entering our borders to detect some attacks. A parallel can be seen in the Intrusion Detection Systems (IDS) operated in large corporate networks, which although do not cover all attack vectors, do provide significant assistance in

focusing resources and managing incidents. Highly sophisticated attacks are unlikely to be easily or even unfeasible to detect. That is not the intention of such a system: instead, it is to detect overt penetration experiments, wide probing, and practicing and known patterns of misuse. It aids in deterring and detecting misuse of the network, raising the capabilities required to conduct attacks. We do not consider the creation of such a system as a trivial task: rather we see this as an enormous national project requiring broad co-operation, which can be approached in a number of ways. It will require the building of national data sets that can be used to characterize traffic and build warning systems. Although elements of this system already exist as part of the telecommunications and corporate management framework, monolithic issues need to be worked through to realise a National IDS. We should start planning this project as soon as possible as it might take a decade to realise.

Chapter 9. **Conclusion**

"'In the practical art of war, the best thing is to take the enemy's country whole and intact. Hence to fight and conquer in all your battles is not supreme excellence: supreme excellence consists in breaking the enemy's resistance without fighting."

Sun Tzu[223]

The challenges of Asymmetric threats and Information Warfare will stretch Australia's resources, and require re-conceptualisation of our national interests and security forces including, greater participation of the private sector, and changes in our daily lives. The new and emerging threats to our National Security have been met with predictable calls for more government funding on existing defence and intelligence capabilities. This thesis supports the request, but cautions that there is a need for a fundamental re-assessment of what National-Security means. We have highlighted capabilities that should be factored into an information age defence force that is charged with protection of the National Information Infrastructure. Corporations and individuals should acknowledge that public funds are very limited with only a few trained staff to address these strategic problems. Within our Commonwealth agencies only, a few individuals have a full time commitment to National Information Infrastructure protection[224]. Outside Australian Governments, few of our corporations have dedicated security teams. Many large corporate organisations have a sole security analyst/manager, with the majority relying on a small pool of external consultants and service providers (when they can afford it) for advice and assistance with security issues.

In response to the reality, that Australia, as a community of interest, does not have the resources of the major powers: we argue that significant commitments will be required from the private sector to address our changed security environment. Broadly, our view is that investments in Australian Infrastructure security is unlikely to be considered positive, unless a strategic view of National

[223] The Art of War" by Sun Tzu

[224] Parts of DSD, have a moderately sized full time commitments, but these are limited to technical security in specific ADF oriented areas.

economic welfare can be envisioned, communicated and then factored into ROI calculations.

The business case for investments requires security initiatives that can provide a positive return on investment within the scope of normal business operations. Normal (i.e. predictable) operational business costs and difficulties are avoided or mitigated by appropriate investment in safeguards. However, as we have discussed, business is also exposed to extra-ordinary operational risks. Diligent commercial organisations are considered to acting prudently, where they accept the risk of rare high impact events if it is prohibitively expensive (i.e. unprofitable) for the organisation to defend against the threat and remain competitive – i.e. they take the business risk. As shareholders we want business to make appropriate level of investments in security and will accept some remote catastrophic events occurring – in order to achieve an optimal - but not perfect, level of protection. However, in the context of the entire community the failure of certain (i.e. critical) business may have a catastrophic impact on the national economy.

As we have shown, the previous assumption about the likelihood and impact of Information Age conflict and information war has been challenged. The potential for catastrophic economic impacts on our National Security are no longer remote. A collective approach to National Security investments is required, which includes a re-conceptionalisation of the obligations and sacrifices of individuals, business and governments. Such an approach must be adopted in order to maximise the efficiency of solutions and enhance the productivity of the entire economy.

There are many physical, information and perceptual targets vulnerable to information warfare within Australia. Regardless of their form, a sub-set of support operations and industries which are critical to our National Security. Our infrastructures have been damaged by accidents and mistakes in the past, which have resulted in varying degrees of problems, from temporary inconveniences to significant community hardship. Both local and foreign, criminals and vandals have also sought out vulnerabilities in the NII to commit fraud or mischief.

Amongst the infrastructures that may be targeted are the financial telecommunications and energy networks, which underpin the Australian economy. These and other infrastructure have complex interdependencies and relationships, which if disturbed may cause cascading strategic impacts.

We assert that moderate level of effort is required to deliberately cause a significant disturbance to the infrastructure. Of note is that the level of effort creates exponential impacts. Where as in a less ICT based environment accidents and vandalism in the past have been limited or localised impacts. However, well-planned and resourced efforts have the potential to cause much

wider and more devastating outcomes. Several types of contemporary actors have been identified that have the capacity, motive, and skill to mount such attacks.

The Australian FIII is a highly distributed large-scale inter-network information infrastructure. Such systems represent one of the most complex systems that can be built. The protection of this infrastructure has focused on concepts of traditional security (confidentiality, integrity and availability) and "bounded-system thinking" that are typified by technologies such as Firewalls. It fundamentally ignores new strategic security environment which is no longer solely based on concept of geography (i.e. objects and places) but includes threats across three equally important realms: physical, information infrastructure and perceptual

Security, as it is currently used, attempts to increase the cost, feasibility or complexity to attackers until a state is achieve that gives us some comfort that attacker will be discouraged or attacks will be unsuccessful. This view does not align with the definition of security: a general reduction in uncertainty, anxiety, or apprehension, because we know that attackers will strive to reduce the cost of attack, seek more feasible vectors and unravel the complexity of our defences. We contend that our strategy is fundamentally flawed and must be changed to a strategy of "survivability". Survivability in terms of the information infrastructure, accepts the reality that no individual component of a system is immune to all attacks accidents, and failures. Survivability also recognizes the unbounded nature of real world and National Information Infrastructures. At the highest policy level this reality is acknowledged:[225]

> *"Of course we cannot guard against all possibilities or eliminate strategic risks" Defence 2000.*

We are not suggesting that existing best practices in security are irrelevant: in fact, they are highly relevant. A strategy of survivability incorporates as a core element security, but it is one of a number of elements including fault tolerance, safety, reliability, reuse, performance, verification, and testing. The focus of Survivability is preserving essential services in unbounded environments, even when systems in such environments are penetrated. From a defence point of view, the Defence Capability Plan in identified "information capabilities" as a separate AU$2.5 billion group, which covers intelligence and surveillance capabilities, communications, information warfare, command and headquarters systems, and logistics and business applications. Although there may be civilian spill over benefits of this investment, it is largely focused on operation of the Military Information Infrastructure (MII).

[225] Defence 2000: *Our Future Defence Force*, Commonwealth of Australia 2000

A National level plan should be created to ensure that the FII (and other critical infrastructure) has the capability to deliver essential services in the face of attack, failure, or accident. The approach to this plan should move beyond the Security paradigm and focus on Survivability as the core strategy. Survivability is defined the capability of a system to fulfil its mission, in a timely manner, in the presence of attacks, failures, or accidents. In practice, this means that the system must be subordinate to the mission, which can be simply put as "…the economic prosperity and welfare of the people of Australia". Such a plan requires prior negotiation between individual component stakeholders so that balance can be agreed amongst multiple attributes including: performance, security, reliability, availability, fault-tolerance, modifiability, and affordability. Australia's National Security Strategy should consist of the three building blocks to protect the Information Economy:

- **Resistance**: Resistance is the capability of the infrastructure to deter attacks such as firewalls, authentication, and encryption.
- **Recognition**: Recognition is the capability of the infrastructure to recognize attacks or the reconnaissance that precedes attacks such error-detection, logging, auditing, intrusion detection and investigations of anomaly
- **Recovery**: Recovery is the capability of the infrastructure to restore services after an attack has occurred. This may include elements such as replication of systems, fault-tolerance, backup systems, and transaction roll-back.

We suggest that methods such as the Survivable Network Analysis[226] (SNA) be urgently used to assess and improve the FII. We need to consider how we would operate "when" essential services are disrupted rather than claim that they cannot be disrupted.

Australia's has some inherent resilience to infrastructure disturbances because of its vast (geographic) size. This attribute has both opportunities and weaknesses for creating survivable infrastructures. The "normal" natural disasters and some types of attack are unlikely to be able to affect the entire continental infrastructure. Therefore, in some emergencies it may be possible to fallback operations to alternative sites. This is already a common practice with many organisations having one data centre in Sydney and another in Melbourne. However distributing critical nodes geographically is only one aspect of survivable systems. (e.g. Sydney and Melbourne are both serviced by the same electricity market).

Beyond the Survivability of our own information infrastructure we should seek to stabilise information infrastructure conflict elsewhere. This is consistent with the strategic changes that have occurred in our defence strategies. Since the

[226] See Ellison, R. J. , Linger, R. C., Longstaff, T., and Mead, N. R., *A Case Study in Survivable Network System Analysis*, Software Engineering Institute Technical Report No. CMU/SEI-98-TR-014, September 1998

release of Defence 2000, Australian defence strategy is based around five strategic objectives. The first of these builds on a well-established strategy: ensure the Defence of Australia and its Direct Approaches. However, we have steadily added a greater emphasis on foster neighbourhood and Global security. This focus now sees four of the five strategic objectives being related to fostering a peaceful environment: (i.e. Contributing to the Security of our Immediate Neighbourhood, Promote Stability and Cooperation in Southeast Asia, Support Strategic Stability in the Wider Asia Pacific Region and Support Global Security). This has been demonstrated through Australia's proactive approach[227] to humanitarian relief, evacuations, peacekeeping and peace-enforcement. We suggest that this list of traditional roles be extended to the GII and the NII of other disadvantaged and developing nations. Australia can undertake various operations to help stabilize NII's operating remotely or within other nations. "Information Peacekeeping" may consist of a wide variety of tasks: assisting organisations or governments with low levels of skills to connect to the GII and provide them with some level of protection against their adversaries. Our skills may be of value in countering threats from virus through to preventing the establishment of "information outlaw" communities. Such an effort may be requested outside Australia's traditional boundaries. A uni-lateral (rapid) response capability that can assist others with Resistance, Recognition and Recovery from information threats should be considered. In parallel to directly helping the disadvantaged, Australian agencies and individual volunteers should be supported when working with the UN, OECD, other Governments, Standard bodies and NGOs to help develop common approaches to managing technology risks and the survivability of the GII. Supporting information peacekeepers and volunteers is possibly the most important long-term strategic programme to improve the welfare of Australians and our neighbours in the Information Age.

[END OF THESIS}

[227] For example over the past decade the ADF has operated in Namibia, Somalia, Western Sahara, Rwanda, Middle East, Cambodia, the Solomon Islands, Papua New Guinea(Bougainville), Indonesia (drought relief in Irian Jaya) and East Timor.

Appendix A Evolution of Banking and Currency

Development of Money

Money evolved out of numerous social activities and deeply rooted customs, not just the inefficiencies of the barter systems. Many other significant factors caused the abstract leap to "money" including the following:

- Tribute and tax to rulers
- Compensation for blood and brides between families
- Ceremonial and religious rites for priests
- Ostentatious and ornamental displays of wealth

Many societies had laws requiring compensation in some form for crimes of violence, instead of the less that productive "an eye for an eye" approach. The word to "pay" is derived from the Latin "pacare" meaning originally to pacify, appease, or make peace with - through the appropriate unit of value customarily acceptable to both sides. A similarly widespread custom was payment for brides in order to compensate the head of the family for the loss of a daughter's economic services.

Rulers did not seek to barter with subjects for the payment of taxes and tribute, however they sought a store of wealth for central revenue purposes. Robing the possessions from their subjects only gave short-term benefit and impacted economic output. Developing a money system enabled the subjects to measure, compare, and value their tax at work. Religious obligations also worked in a similar fashion creating further drivers for some form of money.

What is it that makes some money accepted and other rejected? Over history, an enormous number of artefacts and items have been used to represent money for payments and accounting. Some forms of money arose out of primitive needs and evolved to support economic activity. For example, animals such as pigs had original function as a store of nutrients, but evolved to be used as a mechanism to settle debt. The abstract concept of a pig as a unit of account or standard of value should not be confused with its physical form. This de-coupling of utility from value can be seen in the Kirghiz of the Russian steppes who used horses as their main monetary unit, with sheep as a subsidiary unit and lambskins as further small change. The numerous forms of primitive money included: alcohol, amber, beads, drums, eggs, fabric, feathers, gongs,

ivory, jade, kettles, leather, mats, nails, livestock, quartz, rice, shells, salt, thimbles and weapons.

These primitive forms of money develop as distinct from a commodity traded for purely utilitarian or asthenic purposes. The balance between the secondary (i.e. utilitarian or asthenic) purposes of a form of money has change as communities evolved and interacted economically with other communities and new environments.

Ancient Money

Sometime before 3,000 B.C. the people of Sumerian city of Uruk (Iraq), began to use pictographic tablets of clay to record economic transactions[228]. Banking appears to have developed in Ancient Mesopotamia where royal palaces and temples provided secure places for the safekeeping of grain and other commodities. Receipts came to be used for transfers not only to the original depositors but also to third parties. Eventually private houses in Mesopotamia also got involved in these banking operations. The laws regulating banking were included in the code of the famous Babylonian king Hammurabi (1792-1750 B.C). The majority of records recovered from this time have been financial records. The records demonstrate a well-developed banking industry, which suggest the presence of a stable and reliable legal system, and the ability to contract over long periods (up to 30 years). One record even sets out classroom style questions on calculation of compound interest.

The development of ancient banking system in Egypt also occurred through Nation warehouses that held the wealth of the harvests. The warehouses were filled by owners whose crops had been deposited there for safety and convenience, or crops compulsorily deposited (a.k.a. tax) to the credit of the king. Written orders for the withdrawal of separate lots of grain became used as a general method of payment of debts to other persons including tax gatherers, priests and traders. Even after the introduction of coinage, these Egyptian grain banks served to modify the macroeconomics by reducing the need for precious metals money stock in the domestic economy. Precious metals currency was tended to be reserved for foreign purchases, particularly in connection with military activities.

Precious metals

Many primitive forms of money were counted just like coins. As early as the 16th Century BC (Shang Dynasty) the Chinese used cowrie shells as money. The cowrie is the longest used currency in human history. Many societies have used cowries as money, and even as recently as the middle of this century, cowries have been used in some parts of Africa.

---

[228] Goetzmann, W. N., *Financing Civilization*, viking.som.yale.edu/will/finciv/chapter1.htm

The Shang craftsmen in the city of Yanshi mixed tin and copper to produce the hard wearing and beautiful metal called bronze. This lead to the creation of imitations of bronze cowries, considered as some of the earliest forms of metal coins. In addition to these metal "cowries" the Chinese also produced "coins" in the form of other objects that had long been accepted in their society as money e.g. spades, hoes, and knives. The ancient Greeks used iron nails as coins. These quasi-coins were all easy to counterfeit and, being made of base metals, of low intrinsic worth and thus not convenient for expensive purchases. The ancient Britons used sword blades as coins at the time of Julius Caesar, however they had minted true coins before they were conquered by the Romans.

These early metal monies developed into primitive versions of round coins. Chinese coins were made out of base metals, often containing holes so they could be strung together like a chain. Outside of China, the first true coins developed as lumps of precious metals such as silver, bronze, and gold, which had more value that is inherent. Early coins were then made into round shapes, and were stamped with pictures of various gods or emperors to testify to their authenticity. These early coins first saw use soon after 650 BC by the Lydians (in modern Turkey). The King Croesus of Lydia (reigned c. 560–546 BC) produced a bimetallic system of pure gold and pure silver coins[229].

Precious metals, in weighed quantities, were a common form of money in ancient times. The transition to quantities that could be counted rather than weighed [230] came gradually. The basic unit of weight in the Greek-speaking world was the "drachma" meaning a handful of grain. However, the weight varied[231] considerably across the region. The "stater" was a standard form of currency in antiquity meaning literally "balancer" or "weigher". In the Bible, we hear of the "Talent" which was also a Greek unit of weight, about 60 pounds.

Ancient Economic Warfare

Coin production took hold and was quickly copied and refined by the various states of Greek, Persian, Macedonian, and later the Roman empires. Inflation and other currency problems that we see in modern forms also arose. In 407 BC, Sparta captured the Athenian silver mines at Laurion and released its slaves. In Athens, this caused a money supply problem in the following years. The ruler's reaction was the issues of more currency in the form of bronze coins with a thin plating of silver. Unfortunately, this backfired creating a further shortage, as the pure silver coins disappear from circulation. The people naturally kept the old coins and used only the new coins instead.

---

[229] The foundation deposit of the Artemisium (temple to Artemis) at Ephesus shows that electrum coins were in production before Croesus, possibly under King Gyges.

[230] The words "spend", "expenditure", and "pound" (as in the main British monetary unit) all come from the Latin "expendere" meaning "to weigh".

[231] Less than 3 grams in Corinth to more than 6 grams in Aegina.

The battle for currency superiority was fierce, especially for national economic prestige. The minting of coins was a way signalling political independence of City-states and wide acceptance of a currency provided economic leverage. Monetary union was not negotiated, but imposed by force. Athens forced Aegina to stop minting 'turtle' coinage in 456 BC and accept Athenian 'owls' which then lasted almost unchanged in design and purity for 600 years. Later Athens ordered all 'foreign' currency to be handed and compelling all her allies to use the standard of weights, measures and money. Alexander the Great later caused much of the known world into a degree of monetary uniformity through the monetisation and diffusion of the vast, relatively dormant gold and silver reserves of the Persian Empire.

The Greeks and Romans were especially fond of using money as a tool for propaganda, sending messages to the masses about victories, changes in leadership and the civilisation strength minted on coins.

Money Exchange and Credit Transfer

The great variety of coinages originally in use in the Hellenic world meant that money changing was the earliest and most common form of Greek banking. They would set up their infrastructure, trapezium-shaped tables, near temples, warehouse and other public buildings. The actual word bank comes from the Italian "banca" that means bench or counter.

Money changing was not the only form of early banking and finance infrastructure. One of the most important services was "bottomry" or lending to finance the carriage of freight by ships. Other business enterprises supported by the Greek bankers included mining and the construction of public buildings. When Egypt fell under the rule of a Greek dynasty, the Ptolemies (323-30 BC) old system of warehouse banking reached a new level of sophistication. The numerous scattered government granaries were transformed into a network of grain banks with what amounted to a central banking infrastructure in Alexandria where the main accounts from all the Nation granary banks were recorded. This banking infrastructure functioned as a "giro" system in which payments were effected by transfer from one account to another without moving the actual money. The barren offshore island of Delos also rose to prominence in trading and financial during the late second and third centuries BC. In Delos cash transactions were replaced by real credit receipts and payments made on simple instructions with accounts kept for each client. When Carthage and Corinth Banks were destroyed, the Romans adopted the Bank of Delos model. However, the Roman preference for coin transactions seems to have limited the importance and sophistication of Roman Banks.

Modern Money and Banking

After the fall of the Roman Empire banking was somewhat forgotten and had to wait to re-emerge in Europe at about the time of the Crusades. In Italian city-states such as Rome, Venice and Genoa, and in the fairs of medieval France, the need to transfer sums of money for trading purposes led to the development of financial services including bills of exchange.

It is thought that Bills may have been in use by the Arabs in the eighth century and the Jews in the tenth. However, definite evidence emerges in a contract issued in Genoa in 1156 detailing the reimbursement of a bank's agents in Constantinople.

The Crusades gave a great economic and military stimulus to banking because payments for supplies, equipment, allies, ransoms etc. required safe and speedy means of transferring and exchanging vast values efficiently. Consequently, the Knights of the Temple and the Hospitallers began to provide some banking services such as those already being developed in the more sophisticated Italian city-states. Banking again began to operate over vast distances and between states. One of the reasons for the rapid spread of the use of coins was their efficiency in exchange (esp. convenience) if both parties trusted the coin issuer (a trusted third party).

In situations where coins were generally acceptable at their nominal value, there was no need to weigh them and in everyday transactions were relatively small numbers were, involved counting was quicker and far more convenient than weighing. Coinage and Banking may have also helped reduce extortionate bartering conditions in outlying parts of the economies

Influence on Money Supply

At this time primitive macro-economic influence over the money supply occurred through the Kings and governments monopoly control of coin production (minting). By the Middle Ages monarchs were able to use this monopoly convenience as a source of profit from minting, known as "seigniorage". This occurred because the value of coins imposed by the King was higher than the value of their metal content. Recalling, melting down and then re-minting coins with less precious metal value could allow the King to make a profit (from the metal kept). Seigniorage allowed a King to make significant profit by regularly recalling coinage, especially where he could force all existing coins to be recalled and his new coins then adopted. The new coins had to be made clearly distinguishable by the authorities in order to prevent competition from earlier issues and frustrate counterfeiters. The confidence and acceptance by the public was fostered by an overly elaborate system of royal testing of coinage, with severe penalties. In England, these recoinage cycles were far more frequent than could be justified by wear and tear on the coins but

were important in supplementing the revenue that monarchs raised from the systems of taxation introduced by the Normans. Not until the rise of commercial banking and the widespread adoption of paper money was this minting monopoly broken, with profound consequences.

Paper Money

China was the first civilisation to develop paper money system. Paper money was developed by merchants, in response to the increasingly difficult task of transporting large sums of metal coins though out the region. They agreed to accept specially prepared paper slips from one another, and to replace the paper "vouchers" with hard currency within three years for the convenience of being able to travel light. In the beginning, this paper money system was run by ten of the more successful merchants of the day, but in 100 A.D., the printing of paper money became a government-run operation.

However, in the rest of the world it was not until the late 18th, starting in France and early 19th centuries that paper money and bank notes were in large-scale issue. The bulk of the money in use came to consist of fiduciary money—promises to pay specified amounts of gold and silver at some point. These promises to pay were originally made by individuals or companies as bank notes or as the transfer of book values, which came to be called deposits.

The fiduciary-money evolved into fiat-money when they became issued on the "fiat" of the King. This fiat money removed the links to the payee. A note was no longer a promise of payment to a person of with something else in future; instead, the note specified a legal tender value for circulation. French revolutionary government (rather than the King) issued paper money in the form of assignats from 1789 to 1796. Early mis-management of fiat money caused many problems. In the American colonies and Continental Congress bills of credit were issued that could be used in making payments. This money was over issued, and prices rose drastically until it became worthless or was redeemed in coinage at a small fraction of its initial value.

With the support of the Bank of England, the total quantity of paper money eventually overtook the quantity of commodity money during the 17th century. However, the quality of this paper money still rested upon a base of national precious metal reserves.

Disintegration of Specie-Backed Currency

The relationship between governments and populations over reliability and trust in currency has been often violated throughout history. To overcome manipulation and other problems communities tried to develop institutions and mechanisms aimed at limiting a government's ability to print money without due regard for systemic economic effects.

A common approach has been the use of specie-backed currency, which is convertible into a unit of a non-monetary commodity. Many countries between 1821 to 1973 intermittently used gold and silver "standards" to support currency values. The obligation to convert notes into gold at a fixed rate played a significant part in producing a remarkable degree of price stability and was copied by other nations including Germany, Japan, and the USA.

Before World War I, the United States dollar was defined as equal to 1/20 of an ounce of gold and therefore the currency that could be issued was equal to the national holdings of gold reserves. British pounds were similarly defined as equal to 5/20 of an ounce of gold, this fixed dollar/pound exchange rate of $5 per pound. If governments issued more money than would be consistent with maintaining its value in gold, it would lose gold reserves to the country with the more stable currency. This system underpinned the purchasing power of a nation's money and limited the manipulation of the currencies by governments.

A key weakness in specie currency is that it is only as stable as the value of the specie it is linked to. With relative stability of the gold supply during the 1870s and 1880s, money supply grew slowly, leading to a general deflation. However, when gold was discovered in Alaska and South Africa in the 1890s the specie backing of currencies changed dramatically with inflation up until World War I.

Unfortunately, during the development of modern currency the linking of specie money did not prevent governments from trying to manipulate events, especially during conflict. For example, the payment of gold for the outstanding bank notes was "suspended" by Great Britain during the Napoleonic Wars (1797–1815). As a result, gold coin and bullion became more expensive in terms of paper. Similarly, in the United States during the Civil War, convertibility of Union currency (greenbacks) into specie was suspended, and resumption did not occur until 1879. At its peak, in 1864, the greenback price of gold, nominally equivalent to $100, reached more than $250. Most notably, during the World War I (1914-1918) gold was withdrawn from many countries' internal circulation. In these and other situations, Governments interfered or redefined the value of their currencies, including suspending gold standards, without allowing appropriate foreign reserves to be transferred. However, this manipulation was largely countered by undermining effect it had on the country economy. Large scale speculative attacks ensued as investors sought to sell the currency leading to it being devalued.

Bretton Woods system

In modern times, the Bretton Woods system attempted to bring stability to the currency market. The system stipulated that the price of the U.S. dollar was fixed in terms of gold (initially at $35 per ounce) with other currencies pegged to the U.S. dollar. A countries balance of payments had to maintain the exchange rate through purchases or sales of U.S. dollars, as the reserve

currency. Also part of the Bretton Woods system was the creation of the World Bank and its affiliates to make longer-term loans to nations and the International Monetary Fund to provide temporary financial support to countries with balance of payments problems. The exchange rate could only be changed if the country developed a "fundamental disequilibrium" and obtained IMF approval to change the pegged value of its currency. One of the founders (Harry Dexter White) commented:

"The Fund is essential to winning and preserving peace. Currency warfare is the most destructive form of economic warfare. Economic warfare eventually brings war."

The destabilizing effects of speculation and the persistent U.S. balance-of-payments deficit were seen as the immediate causes of the system's demise. The breakdown of the exchange-rate system was catalysed by the U.S. government's decision in August 1971 not to supply gold to other nations' central banks at $35 per ounce. This abandonment of the system's nominal anchor naturally led other nations to be unwilling to continue to peg their currency values to the overvalued U.S. dollar, so the par-value arrangements disintegrated.

Because the U.S. dollar was the key reserve currency, the United States was reluctant to devalue despite persistent deficits. At the same time, surplus countries chose to add to their dollar holdings rather than to revalue. As U.S. deficits persisted, the stock of U.S. dollars held abroad ballooned relative to the need for a reserve currency. Some countries viewed the United States as abusing its privilege to issue reserve currency and as forcing other countries to finance persistent U.S. deficits. New par values were painfully established during the December 1971 meeting at the Smithsonian Institution, but after a new crisis, the system crumbled in March 1973. Eventual increases in the dollar price of gold and the refusal of Germany and Japan to revalue their currencies were the final blows.

The fundamental flaw in the system was that international liquidity considerations encouraged foreign central banks to hold U.S. dollars, but it also hindered other nations from revaluing their currencies to eliminate their balance-of-payments surpluses[232]. Ultimately, confidence in the dollar as a reserve currency had to suffer.

The resulting collapse of the gold standard post 1973 has seen highly competitive market forces providing pressure on countries to maintain the quality of their "money" in the way that competition forces companies to maintain the quality of their products.

---

[232] It is interesting to note that the US President Franklin Roosevelt said that the creation of the International Monetary Fund and the World Bank "spelled the difference between a world caught again in the maelstrom of panic and economic warfare, or a world in which nations strive for a better life through mutual trust, cooperation and assistance."

We now find that stable purchasing power of a nation's money is a competitive asset for its society (as it was to the Greeks), providing a fundamental base on which to build national security. Currency issuers (i.e. nations) that provide superior money are finding that other communities and markets prefer to import and use it money to support their own trade. Facing global currency competition, a nations that chooses to retain control its own currency must keep on improving the quality of their money, increase the value of products, possibility erect "trade barriers," or face exclusion from the global money market.

Appendix B Legal Regulatory Aspects

The legal environment for information warfare is determined in part by laws that are specific to the handling of information in these sectors but also, to a large extent, by laws of more general application. The legal position differs markedly in time of war. Laws prohibiting attacks against Australian interests include the following:

Crimes Act 1901

Crimes Act *1901 Parts II and VII* dealing with national security offences such as treason and espionage:

Crimes Act *1901 Part VIA* dealing with attacks against Commonwealth computers and attacks against any computer by using the Australian telecommunications system (or, more accurately, attacks by the use of 'a facility operated or provided by the Commonwealth or a carrier...'):

Telecommunications *(Interception) Act 1979*

Telecommunications *(Interception) Act 1979* prohibiting the interception of telecommunications (including data transmissions) within Australia except under warrant:

In addition there are provisions in the Telecommunications *Act 1997* requiring a carrier or carriage service provider to enter into an agreement with the Commonwealth about planning for network survivability or operational requirements in time of crisis and providing that a carrier licence condition or service provider rule may deal with compliance with a disaster plan.

Radio communications *Act1992*

Radio communications *Act1992* covering offences relating to radio emission including interference likely to prejudice the safe operation of aircraft or vessels: interference in relation to certain radio communications: and interference likely to endanger safety or cause loss or damage:

- State legislation dealing with particular aspects of the information infrastructure or of more general application: and
- Common law of civil liability for damage to property.

Payment Systems (Regulation) Act 1998

The Payment Systems (Regulation) Act 1998 gives the Reserve Bank powers to regulate the payments system and purchased payment facilities (such as travellers' cheques and stored-value cards). Its Payments System Board (PSB) that, under the Reserve Bank Act 1959, determines payments system policy exercises the Reserve Bank's powers under the Act. This policy is to be directed to: Controlling risk in the financial system, Promoting efficiency of the payments system and Promoting competition in the market for payment services, consistent with overall stability of the financial system.

The Payment Systems (Regulation) Act allows the Bank to designate a payments system where this is considered to be in the national interest. Designation enables the Bank to impose an access regime on a payments system, to determine standards to be complied with by participants in the system and to give directions to those participants. In addition, the Bank has the power to authorise parties, other than authorised deposit-taking institutions to act as the holder of the store of value for purchased payment facilities. It is expected that designation of a payments system and the imposition of requirements on it will generally occur only after substantial consultation with participants and after voluntary arrangements have been exhausted. Effectively, it is a reserve power.

Payment Systems and Netting Act 1998

The Payment Systems and Netting Act 1998 allows the Reserve Bank to exempt transactions in systems which settle on a RTGS basis from the potential application of the "zero-hour rule". Under this rule, a court-ordered liquidation is deemed to commence from the first moment of time on the day the court order was granted. The application of this rule would have resulted in payments made by a failed institution between midnight and the time the court order was made being declared invalid. This would have undermined the irrevocable nature of RTGS payments and may have created severe liquidity, and potentially systemic, problems in the payments system. The Reserve Bank has approved the Reserve Bank Information and Transfer System (RITS), which include all RTGS transactions, and Austraclear Ltd's FINTRACS, as systems exempted from this rule. This legislation also gives legal certainty to existing multilateral net settlement arrangements approved by the Reserve Bank, such as those for direct-entry and card-based payments. Other provisions in the Act give certainty to netting in financial markets: this will enable Australian banks to join multilateral netting schemes aimed at reducing foreign exchange settlement risk.

Cheques Act 1986

The Cheques Act 1986 is the principal piece of legislation dealing with paper payment instruments in Australia. It establishes the framework under which cheques are drawn, accepted and paid. The Act was amended in 1998 to allow non-bank deposit-taking institutions to issue cheques in their own right. As a result, the provisions relating to payment orders (cheque-like instruments drawn on non-bank financial intermediaries, such as building societies and credit unions) were deleted. The Act now also allows for the turn back or presumed dishonour of cheques for which a failed institution has not settled.

Financial Transaction Reports Act 1988

The Financial Transaction Reports Act 1988 aids law enforcement agencies in detecting money laundering, other financial crime and the recipients of the proceeds of crime. It obliges cash dealers (financial institutions, securities dealers, brokers, bullion dealers, cash carriers, gambling enterprises, etc.) to verify the identity of customers before opening accounts, and to report to the Australian Transaction Reports and Analysis Centre (AUSTRAC) all cash transactions of AUD10,000 and above, information about suspect transactions and all international funds transfers. The Act also requires the public to report cash transfers into and out of Australia of AUD$10, 000 or more or the foreign currency equivalent. AUSTRAC analyses the data, and provides information to law enforcement agencies and to the Australian Taxation Office.

Proceeds of Crime Act 1987

The Proceeds of Crime Act 1987 makes money laundering an offence and several supporting pieces of legislation provide for the confiscation of the proceeds of crime.

Commonwealth Trade Practices Act 1974

Provisions in the Commonwealth Trade Practices Act 1974 dealing with restrictive trade practices and consumer protection are relevant to the operation of the payments system. The Act prohibits, inter alia, conduct such as price agreements, boycotts and exclusive dealing with the purpose or effect of substantially lessening competition. However, the Australian Competition and Consumer Commission (ACCC) may authorise such conduct if it judges it to be in the public interest.

The regulations and procedures for three clearing streams operated by the Australian Payments Clearing Association Limited (APCA) have been authorised by this process: authorisation of a fourth stream is currently being sought. Should the Reserve Bank impose an access regime or standards on a payments system, the system and its members will not be at risk under the Trade Practices Act by complying with the Reserve Bank requirements. There

are also provisions in the Act giving the Australian Securities and Investment Commission (ASIC) consumer protection powers in relation to the finance sector.

Uniform Consumer Credit Code

A Uniform Consumer Credit Code covering the provision of credit was enacted by each of the State and Territory governments in November 1996. The Code focuses primarily on consumer protection. The Code was introduced following an extensive review of previous legislation, which varied widely between the States.

Appendix C Financial Infrastructure

Payment Arrangement

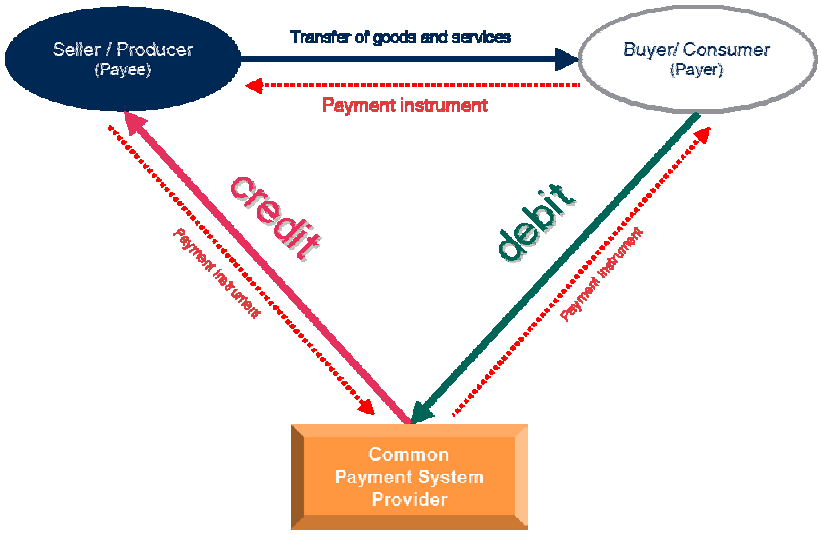
Non-trade-related financial transactions have shown significant growth through the deregulation and globalization of markets. Each of these transactions creates payment obligations that need to be settled through transfer of money in electronic large value payment systems. Since the 1960's there has been a major expansions in payment and settlement systems. These now handle payment volumes on a daily basis, which collectively dwarf economic output in the main industrial countries.

The settlement of payments requires an infrastructure arrangement with a number attributes, including:

- Ensuring the valid creation of payment instruments,
- Exchange of relevant information between payer and the payee, and
- Final exchange of funds between any financial institutions involved.

Often the structure of these infrastructure arrangements depends on whether or not the counterparties's financial institutions are the same. If both the buyer and seller have accounts with the same bank, this is a simple task as the bank debits the buyer's account and credits the seller's account. All phases in the clearing and settlement processes can occur within a single financial institution (in-house arrangements).

However it is common in the corporate world counterparties to have different financial institutions (or multiple banks, accounts and even currencies), therefore some payment system that is acceptable to all parties is needed to complete transactions. The payer's and the payee's financial institutions will have to interact to complete the payment process (inter-bank arrangements). A simple payments system can be though of as a bank's bank where all member banks of a payments system hold accounts of a central bank. Each member makes deposits in these accounts, which in turn can be debited and credited to enable the clearing balances within the system. Payments among member banks are settled by simultaneously debiting and crediting the respective accounts of paying and receiving banks.



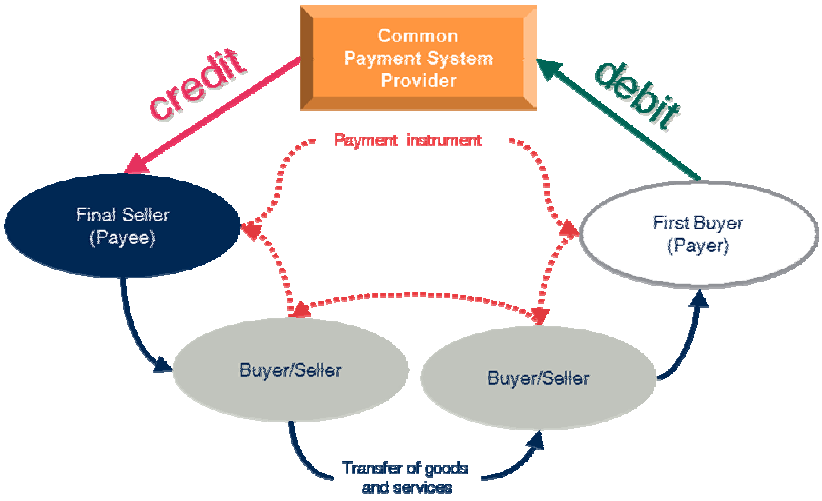
In general, there are four types of arrangements for the clearing of payment instructions. The first arrangement takes place within the same financial institution: the other three types require inter-bank arrangements, these are as follows;

- In House clearing- Accounts to be debited and credited are held in the same financial institution. The exchange of information and the calculation of balances that characterises the clearing process can be performed with in the single financial institution
- Bilateral arrangement - The sorting and processing of payments flowing between two financial institutions is handled by the institutions themselves
- Correspondent arrangements- A common 3rd party is used for clearing according to contracts that are negotiated bilaterally, with one or more institutions forwarding payment instructions to the correspondent for sorting and processing
- Multilateral (clearing house and association) - Arrangements are based on a set of procedures whereby financial institutions present and exchange data and/or documents relating to funds transfers to other financial institutions under a common set of rules

The multilateral clearinghouse arrangement operates a central facility and acts as a central counter-party in the settlement of the payment obligations under a multilateral netting arrangement. Alternatively, multilateral clearing association arrangements may be based on a coordinating body organising (eg. rules and membership) and facilitating clearing among institutions but which does not operate central processing facilities or act as a principal for settlement. Multilateral netting has been attractive because a small fraction of the gross values needed to be exchanged. The system or its designated agent will

compute from the total value of payment instructions exchanged, a net amount that represents the difference between what is owed by each participant to all other participants and what others owe that participant. Because of the arithmetic of multilateral netting, the multilateral net debits and credits may be a small fraction of the gross value of the original payment instruments subject to the netting.

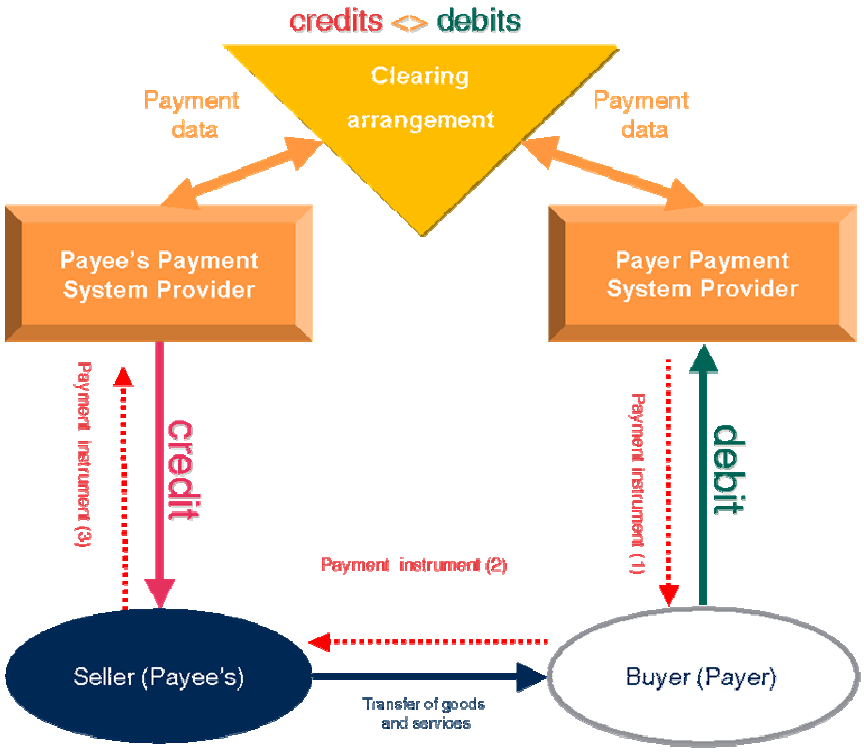
Various permutations are possible on top of these arrangements including cross-membership in clearing houses that has correspondents submitting payment instructions on behalf of its clients. Linkages between correspondents and clearing houses, and cross-membership or interchange agreements between clearing houses, creates the capability of an economy to service wider range buyers and sellers (counterparties).



A) CLEARING INFRASTRUCTURE

The following is a description of the flow of information and payment instructions for a "generic" payment among the counterparties (payer, payer's financial institution, payee, payee's financial institution) involved in a funds transfer payment.

If the payer uses a credit transfer, the payment instrument will go directly from the buyer (payer) to their payment system provider (arrow 1). If a debit instrument such as a cheque or payment card is used, the instrument will be submitted by the seller (payee) to their payment system provider (arrow 2) to ensure that it will accept the instrument (exchange value exists). The payment system provider may be reselling a payment systems scheme and has to also check with the scheme provider to validate the instrument.



At some point the payee's submit the payment to the clearing arrangement that both they and the payers payment system provider belongs too. Both instruments will then be exchanged between the two financial institutions via some type of clearing arrangement. Finally, the financial institutions involved in the transaction undertake interbank settlement (this part of the payment process is not shown in the chart).

From the buyer and sellers point of viewpoint, the process ends with the payer's account being debited and the payee's account being credited with the amount of the payment. Within a payment there are a number of process ensures the creation, validation and transmission of a payment, including.

- Verification of the identity of the involved parties,
- Validation of the payment instrument,
- Verification of the ability to pay,
- Authorisation of the transfer of the funds by both the payer and the payer's financial institution,
- Communication of the information by the payer's financial institution to the payee's financial institution, and
- Processing of the transaction.

The structure of such steps varies considerably with the type of payment instrument. Different procedures may be used for authenticating and authorising payments.

In practice, the various steps may not be performed sequentially. The payment procedure may optimise the execution of certain payments using that particular instruments based on a risk management approach. These procedures may be executed immediately (eg on-line) authenticating and authorisation by the payer's financial institution at the initiation of the payment transaction process. Alternatively, authentication and authorisation may be deferred (off-line) at the end of the transaction processes following the request of the payee's financial institution handling the payment information. Immediate authentication and authorisation generally occur in the case of credit transfers and card payments. With credit transfers, the transaction is authenticated and authorised when the payer's financial institution verifies the identity of the payer and the availability of funds in the payer's current account and sends the information to the payee's financial institution.

During the clearing process two main functions may be performed: the exchange of the payment instrument or of relevant payment information between the payer's and the payee's financial institutions, and the calculation of claims for settlement.

The outcome of this process is a completely processed payment transaction from payer to payee as well as a valid claim by the payee's institution on the payer's institution. The procedures for the exchange of payment instruments or payment information within the financial institutions (i.e. payment scheme providers) may consist of a number of more additional steps: matching of the transactions, sorting of the transactions, data collection (including integrity checks), data aggregation, and sending of the relevant data.

Such processes vary considerably according to the operational and legal features of the different payment instruments. Procedures for the calculation of claims for settlement consist of calculation of gross claims and calculation of net or aggregated claims to be settled. Therefore, in principle and in some countries in practice, claims associated with instruments exchanged through different exchange procedures may be aggregated to determine one single balance to be settled per institution participating in settlement (eg. combining, cheques, cards, wholesale, and retails values).

B) SETTLEMENT INFRASTRUCTURE

Beyond the clearing, process is the settlement process where validated claims from the payee's institution are discharged by means of a payment from the payer's institution to the payee's institution. The settlement process has a number of steps including: collection and integrity check of the claims to be settled, ensuring the availability of funds for settlement, settling the claims

between the financial institutions, and logging and communication of settlement to the parties concerned.

Settlement balances resulting from clearing arrangements may be posted to two types of settlement accounts:

- Correspondent accounts - Pairs of financial institutions hold "nostro" and "vostro" accounts with each other. The institution holding the settlement account as an asset refers to it as a "nostro" account while the correspondent bank providing the settlement account as a liability refers to it as a "vostro" account. The accounts are typically used when payments due to or due from the correspondent banks are to be settled bilaterally:
- Third Party Settlement - Accounts held with a third party financial institution acting as a settlement bank. Multilateral clearing organisations typically rely on a settlement bank where participants maintain individual accounts to which settlement obligations are posted.

In large-value systems, settlement generally takes place in central bank money. In retail payment systems, however, settlement is performed by either the central bank or a private correspondent bank, which means that settlement takes place in central bank money or commercial bank money respectively.

The access to settlement accounts at the central bank may be either open to all institutions participating directly in clearing arrangements or limited to financial institutions satisfying specific criteria (eg institutional type, minimum payment volumes). In the latter case, financial institutions that do not have access to a central bank account settle their payments across the books of a direct participant in settlement, which, in turn, settles across the books of the central bank.

The volume (i.e. the number) of payments to be cleared as well as the number of financial institutions involved represent the major factors in determining the relative convenience of the various types of clearing arrangements. In large-value payments, systems in operation there are generally two types of systems. One that is call real time gross settlement, or RTGS, system and the other is a periodic multilateral netting system.

Bilateral arrangements have not typically represented efficient solutions when large volumes of payments need to be processed for a large number of delivery points. Multilateral arrangements, instead, make the processing of payment instructions more efficient by coordinating the exchange of payment instructions, operating communications networks, and providing processing services. Furthermore, multilateral netting allows participants to minimise the liquid balances necessary for settlement.

C) REALTIME GROSS VS NETTING SYSTEMS

A gross settlement system transfers the total (gross) amount of the funds required. The benefit of RTGS systems are that they provide instant settlement with is unconditional and irrevocable transfer as soon as a payment instruction arrives. However if there are insufficient funds (liquidity) in the sending banks account at the central bank the transaction fails. Settlement refers to the actual transfer of funds from a sending bank to a receiving bank. These are considered "real time" because the payment instructions are executed as soon as they reach the systems usually in a continuous stream of messages from the many members of the system.

The alternative to RTGS systems are netting systems where transfers do not occur immediately when payment instructions are sent, messages are only checked that they meet message criteria. The actual settlements are not accomplished until a specified time (usually the end of the day). After this cutoff point the central system calculates settlement obligations for each participant and informs the participants of their obligations (net payments). The funds in the central accounts of the systems are then transferred.

If counterparties do not have sufficient liquidity they may fail to meet their obligations or create the perception that they may fail. Such a situation can then lead to a financial gridlock as dependant payment transactions fail because funds have failed to arrive in time. The costs associated with this gridlock threat can result in trillion of dollar being effected.

The first modern instance of gridlock followed the failure of Herstatt Bank in the early 1970's. Herstatt's failure and the follow on disruption to international payment flows lead to the creation of the Bank for International Settlements (BIS). In an effort to further strengthen RTGS the BIS issues standards and guides.

Central banks of many developed countries have encouraged the use of real-time gross settlement payments systems for securities and foreign exchange transactions because of the virtual agreement that gross settlement systems make wholesale payment systems more immune to widespread financial disruption.

D) ENABLING TECHNOLOGY

Advances in technology that have supported communications, transport, and logistics have allowed those that participate in the various markets (i.e. factor, product or finance) to be widely distributed. The advent of this technology has further reduced the need for producers and consumers to be physically near a market. Using telecommunications and computers has now removed the need for the household sector to go to a physical market to obtain a wide range of goods and services. In conjunction with these advances in markets, payment systems in place today use information technology and communications to

provide enhanced security and increased the speed at which payments (i.e. money) can circulate.

The advent of the Internet has a fundamental impact on the economy, as it not only changes the efficiency of the markets, it also introduces new environment operations, technical risks, and counter measures. The protection of the systems that provides certainty of payment underpins the entire economy and so its operation influences the enormous number of micro-economic transactions between buyers and sellers, and macro-economic flows between the various sectors. Because of the circular flow of money, instability or uncertainly in any of these flows has a fundamental micro and macro economic impact.

The architecture of payment systems is far from standardised in modern economies and varies across payment instruments. However the Financial Infrastructure, like other Information Infrastructure, can generally be described as consisting of hubs, spokes and connections.

- Hubs - Exchanges, clearinghouses, payment systems, central and large banks that aggregate and relay money, transaction or information
- Spokes (nodes)– Individual Banks, large financial institutions, dealers and agents that send and receive money, securities, and information
- Connections - Public Switched Telephone Network (PSTN), internet private networks and messaging systems that connect Hubs and Spokes

Depending on the threat, risk is either concentrated or diffused by the hub and spoke model of payment and/or security transactions. Clearinghouses act as a central counterparty, and have the potential to mitigate many counterparty risks. However when considered from a systemic perspective, clearinghouses tend to concentrate risks and responsibilities for risk management.

Some counties use operational clearing houses to directly provide all the relevant functions of a clearing process and other have clearing associations (such as Australia) that only establish rules and operational procedures. Currently the most common model is represented by clearing houses responsible for both setting the rules governing the clearing processes and providing relevant operational functions. Sometimes the interbank communication network is even provided by the clearinghouse and in some cases (e.g. Germany and the United Kingdom) all variants can be found.

Regardless of architecture, all countries payment instruments and information are increasingly exchanged among financial institutions through automated procedures. This seems due to both the increasing use of automated payment instruments in retail and wholesale banking, and the automation of paper-based (cheques) clearing procedures.

Central banks generally operate the settlement systems with tiering being very common in settlement arrangements for retail payments, This means that

smaller financial institutions do not settle at the central bank. Instead, they have accounts of participants (often called direct participants). The right and eligibility requirements to hold a central bank account for settlement accounts is widening to allow non-financial institutions to hold such accounts. For example in Australia, firms that provide payment services to customers with a resulting need to settle clearing obligations with other providers are eligible for settlement accounts provided they meet certain conditions.

Although, as a rule, settlement services are provided by central banks, there are some cases for specific payment instruments where settlement occurs in commercial bank money. For example, settlement services for debit and credit cards are sometimes provided by a financial institution acting as settlement bank or sometimes arranged on a bilateral basis between banks.

Significant tiering arrangements (whereby settlement occurs indirectly) may take place in credit card networks, which often have thousands of participating financial institutions with a small number of member financial institutions acting as central service providers.

Where payments are settled through RTGS systems or through book entries in the central bank's settlement accounts system, intraday credit facilities are commonly available, usually against collateral. If the settlement of the clearing balances of payment systems takes place in a deferred net settlement system, intra-day credit will typically be provided implicitly by the system.

Retail payments are typically batched, and then netted (usually on a multilateral basis) for settlement at the central banks each day, however increasing use of information technology may result in this occurring more frequently. The system will migrate from clearing and settling batches of payments once a day to several clearing and settlement cycles every day. Future systems could theoretically allow the real-time clearing and settlement of single retail payments.

Core high value clearing systems

There are many high value clearing systems however global finance is dominated by a small number that include the following:

- FEDWIRE - Federal Reserve's Fedwire Funds Transfer Service,
- TARGET - Trans European Automated Real-time Gross Settlement Express Transfer System
- CHAPS - United Kingdom's Clearing House Automated Payment System
- BOJ-Net - Bank of Japan's large value funds transfer service

E) SWIFT

Society for Worldwide Interbank Financial Telecommunication (SWIFT) was founded in 1973 by 239 banks from 15 countries to facilitate operational messaging between international those banks and counterparties with SWIFT facilities.233 SWIFT provides financial data communication and processing services to support the business activities of worldwide financial institutions for payments, Forex and money markets, as well as securities and trade finance. The messages sent by SWIFT include financial transactions such as customer transfers, bank transfers and foreign exchange confirmations. Not all SWIFT messages are value bearing.

SWIFT is based in Brussels under Belgian law, the National Bank of Belgium acts as lead overseer and is supported in this task by the other G10 central banks, including the ECB. The practical co-ordination takes place in the Committee on Payment and Settlement Systems (CPSS), on which all G10 central banks are represented. It is a non-profit co-operative, wholly owned by its member banks (including central banks) and other financial institutions. SWIFT is a. Membership is granted only to bona fide members of the financial community in the countries in which SWIFT operates. The system operates in all principal financial centres and is steadily extending its operations on a worldwide basis. By 2000, it had 7,125 live users in 192 countries sending 1,274,000,000 messages

In 1997 SWIFT announced plans for its "next generation" of products and services running on a secure internet protocol (IP) network The first phase of this project was realised in 1999 when the "next generation" concept, SWIFTNet, went into operation, offering add-on services such as real-time information. SWIFT Net services offer the financial industry a standard platform for financial communication and messaging and a package of interactive capabilities. SWIFT Net complements the FIN service in supporting real-time financial operations. Using the Internet, SWIFT enhancements known as SWIFT Net service will include:

- SWIFT Net InterACT – an interactive messaging capability:
- FileACT – a new method of transmitting bulk messages: and

In 2000, SWIFT announced its TrustACT system to provide assurance over the identity of corporate trading over the Internet. It also announced e-paymentsPlus, which provides corporate users with web-based payment initiation and assurance services. TrustACT provides the ability to secure business-to-business legally binding messages by validating company identities and providing non-repudiation of messages. SWIFT also announces a partnership with Identrus to provide a global model for trust services.

---

233 SWIFT

Apart from being a central component of RITS, Australia's payment system, SWIFT underpins the global financial information infrastructure. In the EU, SWIFT provides the interlinking messaging service for the 15 central banks participating in TARGET.

SWIFT operates from three tier 1 data centres in Belgium, Holland, and United States connected through highly redundant telecommunications network. Unlike many national or regional payment systems, SWIFT connects members with diverse cultural, legal, financial, and technological approaches. SWIFT sheer size and complexity introduce special vulnerabilities, specifically managing the diversity of environments from which it is accessed.

The SWIFT system and network is protected against unauthorised access, environment faults and emergencies. Access to the SWIFT network is protected by login authorisation codes supplied by SWIFT. Each code is directly tied to a specific terminal and changes with each login. The code tables are sent in two parts by different routes but subsequent security is the responsibility of the bank. Transmission between the bank and the regional processor is typically over leased lines.

Authentication of value-bearing messages is mandatory in the SWIFT system but encryption is not. However, for privacy reasons to increase security, many banks now encrypt their link to SWIFT.

Other specific matters that should be considered in a SWIFT environment include:

• Procedures for the correction and resubmission of rejected outbound messages:

• Procedures in the event of emergencies:

• Control over the handling of incoming messages. Any messages, which cannot be authenticated or which are flagged as possible duplicates should be adequately controlled:

• Control over any automatic interface with the bank's accounting systems or with an automated payment system:

• Security over and amendment of authenticator keys.

SWIFT's role in electronic data interchange (EDI) between international banks for the last two decades is evidenced by the fact that SWIFT's message format protocol has become the de facto international standard for financial EDI.

- Euro Banking Association - Euro 1 system of the
- Belgium - ELLIPS
- Denmark - DEBES
- Australia - RITS

- Finland - BOF-RTGS
- France - TBF/PNS
- Greece - HERMES
- Ireland - IRIS
- Luxembourg - LIPS
- Spain - SPI
- Sweden - RIX
- United Kingdom - CHAPS Euro
- Germany - EAF and ELS remote access[234]
- Italy - Access the BIREL system and to offer domestic banks an alternative for TARGET-related transactions.
- Canada - LVTS
- Croatia - HSVP
- Hungary - VIBER
- New Zealand - SCP
- Norway - NICS
- Slovenia - SIPS
- South Africa - SAMOS
- Venezuela - PIBC

Non-banks cannot make payments using SWIFT directly, but a service has been introduced to enable them to interchange certain types of payment confirmations. Where connection to SWIFT is by an approved interface device (SID), the hardware is supplied by an approved vendor and the software is supplied and maintained by SWIFT. Other interfaces such as IBM's DMNL/DSNL are referred to as computer-based terminals (CBT) and users must install and maintain their own software. Increasingly, the SWIFT systems are linked directly to banks' computer systems allowing SWIFT messages to be automatically generated by the banks payment systems.

F) FEDWIRE

In the United States several thousand banks are member of the RTGS systems FEDWIRE, operating under the U.S. Federal Reserve System. Established in 1913) The Federal Reserve System consists of twelve regional Federal Reserve

[234] The Deutsche Bundesbank and CHAPS have also recently signed agreements with SWIFT and the Oesterreichische Nationalbank is in discussions with SWIFT regarding enhanced SWIFT facilities to access their payment system ARTIS.

Banks privately owned by the member banks of each district and the Board of Governors. The US President appoint the President and Governors for a fixed term to controls the US's money supply and regulate the banking system.

FEDWIRE members including, US organisations and government agencies, international organizations, central banks and foreign governments hold reserve accounts at Federal Reserve Banks

FEDWIRE provides the final, and irrevocable mechanism for clearing US domestically issued cheques, conduct transactions for the Federal Reserve and the Treasury Department. FEDWIRE transactions include funds transfers, and billion of dollars worth of securities transfers, mostly for domestic interbank transactions and many of which are related to federal funds transactions or payments for the purchases of government securities. The primary FEDWIRE operations centre is located in East Rutherford, New Jersey with backup sites in Richmond and Dallas.[235].

G) CHAPS

CHAPS (Clearing House Automated Payment System) started operating in 1984 as an, electronic interbank system for sending irrevocable, guaranteed and unconditional sterling credit transfers in the United Kingdom through high-value settlement accounts held at the Bank of England are operated on an RTGS basis. CHAPS Sterling is the electronic transfer system in the UK for sending same-day value payments from bank to bank. It operates in partnership with the Bank of England in providing the payment and settlement service.

In April 1996, CHAPS developed into an RTGS system to process large-value same-day sterling payments between banks, other than those, which are specifically, related to the settlement of purchases of UK government securities or money market instruments. It is now the second largest Real Time Gross Settlement (RTGS) system in the world, after US Fedwire system. Since becoming full RTGS, there has been no minimum or maximum payment limit within CHAPS Sterling. The control of credit risk against the initiating customer is critical. Each CHAPS payment must be settled at the Bank of England before it is notified to the receiving bank. CHAPS offers its members and their participants a risk-free same-day payment mechanism. Every CHAPS payment is unconditional, irrevocable and guaranteed.

In January 1999, a second CHAPS system – for euro-denominated payments – began operations. This system connects to the EU-wide TARGET system and is entirely separate from the original CHAPS sterling system although both are run by the CHAPS Clearing Company Ltd. There are 21 settlement banks who

[235] _, FEDWIRE*: The Federal Reserve Wire Transfer Service*, 36.

are direct members of the Sterling and/or Euro clearings and around 400 financial institution participants who participate through agency agreements with one of these settlement banks.

CHAPS Sterling was developed to allow its members to communicate freely with one another. This has been achieved by installing a distributed system of computers with common software within member institutions. Messages are set between these computers over a telecommunications network. Because

CHAPS Euro was implemented in 1999 to coincide with the advent of EMU. In its first year of operation, CHAPS euro handled a daily average volume of around 5,900 domestic and cross border payments with a value of around €78 billion and in the first year of operation, it processed 2.5 million payments worth €33,600 billion. The average value of a CHAPS Euro payment is much higher than for CHAPS Sterling, reflecting the relatively lower use of the system by retail customers. The largest single use of CHAPS Euro is for the settlement of foreign exchange transactions. However, there are indications that the business community is starting to make use of CHAPS Euro for paying suppliers. CHAPS euro is currently the second largest cross-border component of the TARGET system by both volume and value.

The Bank of England and the CHAPS Company have now embarked on a programme called NewCHAPS that is an enhanced replacement RTGS service for CHAPS sterling and will support infrastructure and member requirements via a SWIFT platform, central scheduling and functionality, together with a workstation based on SWIFTNet. The CHAPS sterling clearing will then operate on the same technical platform as CHAPS euro. NewCHAPS will be open to all banking institutions that opt for the usage of NewCHAPS as a payment settlement system. It will be able to facilitate both wholesale and retail payments. Within NewCHAPS the development of a central scheduler and an enhanced settlement, process provides members and the central operator with:

- The ability to queue and prioritise payments, leaving their execution completely in the control of the members:

- The ability to reserve headroom meaning, for example, that members can reserve funds for timed settlements such as CLS payments:

- The ability to suspend credits to a stricken member to halt a liquidity drain. This can be set by the central operator either on a multilateral basis or by an individual member on a unilateral basis.

CHAPS was designed to handle high-value payments, it operates with the highest level of security and integrity: every message between members is authenticated and encrypted. CHAPSNET (a managed network provided by BT) provides the connectivity and service for CHAPS payment, security and enquiry links. CHAPS software that interacts with the Bank of England to

receive funds confirmation and to send payment instructions to the receiving bank is resident on each member's computer system

H) TARGET

The Trans-European Automated Real-time Gross Settlement Express Transfer system (TARGET) was implemented in January 1999 with the introduction of the Euro. It brought about the development of a cross-border payment system to provide participants across the European Union (EU) with a uniform platform for processing Euro payments.

TARGET consists of 15 national RTGS systems and the ECB payment mechanism (EPM), which are inter-linked to provide a uniform platform for the processing of cross-border payments. The cross-border part (i.e., that involving two inter linked RTGS systems) represents approximately 40 per cent in terms of value and 20 per cent in terms of volume of all TARGET payments (both cross-border and domestic payments).

TARGET is a real-time system: under normal circumstances, payments reach their destination within a couple of minutes of being debited from the sending participant's account. Each payment is handled individually in a gross settlement system. Acknowledgement of the successful execution of each individual payment order is sent to the sending national central bank in real time. TARGET

Provides intra day finality: settlement is final once the funds have been credited. There are more than 5,000 RTGS participants in TARGET and almost all EU credit institutions are accessible via TARGET. By using TARGET for all their large-value payments, especially those related to money market and foreign exchange, market participants make a substantial contribution to reducing the overall systemic risk within the EU banking infrastructure.

Although TARGET is mainly intended for large-value payments, an increasing number of participants are using TARGET for all their cross-border Euro payment business.

TARGET is available for all credit transfers in Euro between EU countries, including those countries that have not adopted the Euro as their currency (i.e., non-Euro area countries). TARGET processes both interbank and customer payments. Cross-border large-value net settlement systems operating in Euro also settle their end-of-day balances via TARGET. TARGET is already one of the largest payment systems in the world. TARGET processed over 4.3 million domestic and cross-border payments in March 2000, representing a value of almost €24 trillion. These figures show that TARGET is already one of the largest payment systems in the world. TARGET has also attracted corporate cross-border payments. Such payments might indeed be time-critical and the amounts involved can be substantial. Since TARGET started operation, the

number of customer payments has grown considerably. In terms of volume, the share of customer payments in cross-border TARGET traffic has doubled in a year, reaching more than 30 per cent in the first quarter of 2000.

I) CHIPS

The Clearing House Interbank Payment System (CHIPS) was established by the New York Clearing House Association (NYCHA) in 1970 to enable US participating banks to simplify their money transfer activity by replacing the existing paper-based clearing system. It is the central clearing system in the United States for international transactions, handling over 95 per cent of all dollar payments moving between countries around the world and has around 60 member banks. CHIPS is a credit transfer system, which multilaterally nets bank payment obligations and settles these net obligations at the end of the day.

It is an on-line, real-time electronic payment system that transfers funds and settles transactions in US dollars. The network is composed of a small number of settling participants (large U.S. chartered banks that settle end-of-day balances between each other) and a larger number of non-settling participants who maintain accounts with one of the settling banks. Settling participants settle for non-settling participants.

All CHIPS participants must be regulated by the New York State Banking Department, or a local regulatory authority (usually the participant's domestic central bank) and have a branch situated in New York City.

On a typical day over several trillion in business payments pass through CHIPS. This amount represents over a quarter of a million international transactions: foreign trade payments, foreign exchange, securities settlement, and Eurodollar transactions, as well as a growing number of domestic payments.

Card Systems

J) TYPES OF CARDS

A plastic card contains a magnetic strip, which contains details that can be read by ATMs (Automated Teller Machines), and Point of Sale (POS) terminals to enable the customer to draw cash or pay for goods at retailers. In the future, new opportunities will come from the introduction of chip technology onto plastic cards, which will allow additional services to be provided, such as electronic purse schemes (inc smart cards).

There have been significant changes in the way in which plastic cards are used over the past few years, most notably the decline of standalone ATM, cheque guarantee and eurocheque cards. These single function cards are steadily being replaced by multi-function cards.

The following lists some of major types of plastic card provided by banks and other financial businesses to users today:

- ATM Card - Also known as cash cards, cash dispenser card or cash machine card. These are used to withdraw cash and get bank statements from ATMs. They are often combined with a cheque guarantee card
- Charge Card - A plastic payment card, which requires the cardholder to settle the account at the end of a specified period
- Cheque Guarantee Card - Also known as cheque cards. These are issued by a bank or building society to guarantee settlement of cheques paid to third parties or to support the encashment of cheques up to a specified amounts. Most debit and some credit cards may also function as cheque guarantee cards and are known as multi-function cards
- Chip or Smart Card - Hold details on a computer chip instead of a traditional magnetic stripe
- Credit Card - A payment card, which enables the holder to make purchases and to draw cash up to a pre-arranged amount. The credit granted can be settled in full by the end of a specified period or in staged payments, with the balance taken as extended credit:
- Debit Card - A payment card that is linked to a bank or building society account and used to pay for goods and services by debiting the holder's account. Debit cards are usually combined with other facilities such as ATM and cheque guarantee functions:
- Electronic Purse - Also known as a pre-payment card. This is a smart card that has a stored cash value, which can be used to purchase goods and services – it is an alternative to cash. The card can be disposable or re-loadable. Mondex and VisaCash are both electronic purse products.

The card issuing bank or institution must be a member of a card scheme enabling them to issue cards and receive details of card transactions. Card schemes are organisations which manage and control the operation and clearing of transactions through their own rules. Examples of schemes are MasterCard/Europay, Visa, Switch, American Express and Diners Club International.

K) AUTOMATED TELLER MACHINES

Cash machines or ATMs are the most popular method of withdrawing cash from personal accounts. Changes that allow non-banks to participate in the ATM networks further boost the use of ATMs worldwide.

The ATM machine has two input devices. One is the card reader which captures the customer information stored on the magnetic stripe on the back of the ATM card and the other is a small keyboard where the customer inputs their Personal Identification Number (PIN) and chooses the services required.

Communications between these cash terminals and the card owning bank is encrypted and authenticated to provide security and integrity over the transactions as they move over the networks and through the computers of other banks. The ATM accepts the card and the PIN of the cardholder authenticates the card user. This information is transmitted to the central computer of the bank that owns the ATM. If the customer is a customer of that bank, then the card details are checked against the PIN and a credit check is performed on the customer's account. If it is a customer of another bank, the transaction is sent through the reciprocal network to that bank where the checking will take place. If the checks are passed, a message is returned to the ATM and the money is dispensed. In Australia, all major Banks and institutions have connected their systems through an interchange network, which connects the country's ATMs. Many cards issued in Australia also can be used worldwide in cash machines carrying the Visa 'Plus' or MasterCard 'Cirrus' logos. One of the checks that may be performed by the customer's bank is a fraud check process. This is performed by a computer program which analyses such things as previous usage of that card, time of day, amount of charge along with other factors, then screens out fraud risks based on a defined model.

If the card user uses the ATM of the card-issuing bank, then the bank will debit the customer's account. Alternatively, if the card user uses the facilities of another bank, then the card user's bank pays the bank that owns the ATM and then charges its customer. These 'not-on-us transactions' are collated to determine the net settlement position for each machine. At the end of each cut-off period, the differences are settled between the consortiums of banks.

Credit and debit cards can be used by bank customers to pay for goods at retailers who possess POS terminals. The processing flows for both card types are very similar and explained in the next section.

L) CREDIT AND DEBIT CARDS

Credit cards have become an integral way in which people make retail payments. The card allows the holder to pay for goods or draw cash against a credit arrangement with their bank. The credit taken by the customer can be settled in full, each month, in which case no interest is due, or settled in instalments, subject to a minimum monthly payment, in which case interest is payable on the outstanding amount and any future transactions until the amount due is settled in full. Credit limits will be provided to customers in line with their bank's opinion of their creditworthiness.

To facilitate the credit card process banks are members of credit card schemes. The largest of these are Visa, MasterCard, Diners Club International and American Express. Visa and MasterCard do not themselves issue credit cards. Banks or financial institutions join the groups and act as credit card providers

and using the Visa and MasterCard name. American Express and Diners Club International maintain their network name and act as a credit card provider.

In Australia the credit card holder normally prove their identify by signing either a manually produced or a EFTPOS produced voucher containing the payment details. The latter is becoming the most prevalent. In these cases the retailer is normally allocated a 'floor limit' by a bank under which all payments are automatically granted bank authorisation. Payments over this limit are transmitted to the appropriate card scheme for authorisation. These may use computerised fraud detection systems

Once the transaction has been authorised by the card scheme the customer can obtain the goods. The customer's and retailer's bank are debited and credited accordingly by the card scheme's clearing process.

The processing and authorisation of debit cards works in a similar manner. The difference with a debit card is that the payment proceeds are debited to the customer's current account at the time the transaction takes place. This debit can take place either instantly if the transaction has been transmitted to the bank for authorisation or in a few days, time once a bank is instructed of it through the clearing process.

Debit card 'cashback', the retailer giving their customer cash at the same time as they settle the bill for their purchases, is another fast-growing method of obtaining cash. Most Australian cards issues are members of the interchange network.

The Credit card networks provide a global platform, systems and processing services needed by members to develop and run card payment businesses. They also contribute to the establishment of standards for global interoperability and security and new technologies in the card payments industry.

The Maestro service is a worldwide debit service developed jointly by Europay and MasterCard for EFT/POS and ATM networks. There are 166 million Maestro debit cards in issue, which can be used at 2.3 million terminals in 41 countries. An agreement with Cirrus a US-based international ATM network owned by MasterCard) allows European banks to add a worldwide cash access utility to Eurocard and proprietary ATM, electronic debit and cheque guarantee cards. In Europe 253,000 ATMs are available for use with Eurocard/MasterCard and 256,000 ATMs are available for use with Maestro and Cirrus.

Visa International is a non-profit-making membership association owned by 21,000 financial institutions worldwide[236]. Membership is largely limited to

[236] There are six regional divisions: Asia-Pacific: Canada: Central & Eastern Europe, Middle East & Africa (CEMEA): Latin America & Caribbean: United States: and European Union. The regional boards have full autonomy in defining commercial policies and promoting Visa products within their geographical areas.

deposit-taking financial institutions and bank-owned organizations operating in the bank card sector. Visa is managed by an international board and by six autonomous regional boards. The international board is responsible for global policy. The Board provides the operating regulations and manages a worldwide electronic system, which handles authorisations and the transmission of clearing and settlement data.

Visa has developed a portfolio of products – from ATM cash cards and electronic purses to debit and credit cards. It includes PLUS, Visa Electron, Visa Classic, Visa Gold, Visa Platinum, Visa Infinite and Visa traveller's cheques. Visa has also created a range of commercial cards like Visa Purchasing for large companies and Visa Business for smaller companies.

VisaNet is the computer and telecommunications network which links member financial institutions worldwide with the two Visa Interchange Centres located in the United Kingdom and the United States. Each of these centres is capable of processing every Visa transaction in order to ensure the regular working of the system should a disaster put one out of action. Two applications are managed through VisaNet: the Base I authorisation service and the Base II clearing and settlement service.

Before a transaction is finalised, a series of security checks is carried out through VisaNet in order to ensure that the card is valid: has not been lost, stolen or forged: the cardholder's spending limit has not been exceeded and the cardholder's personal identification number PIN), if used, is correct. The Visa authorisation service operates 24 hours a day, 7 days a week.

The Visa International Base II system clears transactions and facilitates settlement. It operates six days a week. To complete such calculations, Visa International supports approximately 180 transaction currencies enabling the processing of international transactions. Members can choose to receive their transaction reports in any of these currencies. The necessary foreign exchange operations are executed by Barclays in London and in Citibank in New York. Settlement is not carried out through Base II, Visa merely provides the data to allow settlement to be carried out. For settlement in US dollars, Chase Manhattan Bank, New York, acts as the settlement bank. For multi-currency settlement, Chase Manhattan Bank, London, acts as the settlement bank. All members may hold their own settlement account with any other financial institution, such that all requests for funds or payments are ultimately settled through the correspondent services of domestic clearing and settlement systems.

Appendix D CPSS 16 - Core Principles for Systemically Important Payment Systems

The Committee on Payment and Settlement Systems (CPSS) of the central banks of the Group of Ten countries, Core Principles for Systemically Important Payment Systems, Bank for International Settlements (BIS), January 2001.

I. The system should have a well founded legal basis under all relevant jurisdictions.

II. The system's rules and procedures should enable participants to have a clear understanding of the system's impact on each of the financial risks they incur through participation in it.

III. The system should have clearly defined procedures for the management of credit risks and liquidity risks, which specify the respective responsibilities of the system operator and the participants and which provide appropriate incentives to manage and contain those risks.

IV.* The system should provide prompt final settlement on the day of value, preferably during the day and at a minimum at the end of the day.

V.* A system in which multilateral netting takes place should, at a minimum, be capable of ensuring the timely completion of daily settlements in the event of an inability to settle by the participant with the largest single settlement obligation.

VI. Assets used for settlement should preferably be a claim on the central bank: where other assets are used, they should carry little or no credit risk and little or no liquidity risk.

VII. The system should ensure a high degree of security and operational reliability and should have contingency arrangements for timely completion of daily processing.

VIII. The system should provide a means of making payments which is practical for its users and efficient for the economy.

IX. The system should have objective and publicly disclosed criteria for participation, which permit fair and open access.

X. The system's governance arrangements should be effective, accountable and transparent.

* Systems should seek to exceed the minima included in these two Core Principles.

Responsibilities of the central bank in applying the Core Principles

A. The central bank should define clearly its payment system objectives and should disclose publicly its role and major policies with respect to systemically important payment systems.

B. The central bank should ensure that the systems it operates comply with the Core Principles.

C. The central bank should oversee compliance with the Core Principles by systems it does not operate and it should have the ability to carry out this oversight.

D. The central bank, in promoting payment system safety and efficiency through the Core Principles, should cooperate with other central banks and with any other relevant domestic or foreign authorities.

Appendix E Australia Government Budgets

Protecting Australia's National Information Infrastructure, Report of the Interdepartmental Committee on Protection of the National Information Infrastructure Attorney-General's Department Canberra, December 1998.
Breakdown of Commonwealth Resource Requirements

	1999/2000	2000/2001	Ongoing
Salaries and Admin			
DSD			
EL2	116,000	116,000	116,000
El1 (2)	201,000	201,000	201,000
APS 6 (2)	160,000	160,000	160,000
APS 4	66,000	66,000	66,000
Salaries	543,000	543,000	543,000
Travel	7,000	20,000	20,000
Equipment Maintenance	Nil	7,000	7,000
Sub Total DSD	550,000	570,000	570,000

PSCC

EL1	101,000	101,000	101,000
APS 6 (2)	160,000	160,000	160,000
APS 4	66,000	66,000	66,000
Salaries	327,000	327,000	327,000
Travel	40,000	25,000	25,000
Advertising	60,000	45,000	35,000
Telecommunications	5,000	10,000	10,000
Consultants (AusCERT)	60,000	30,000	25,000
Equipment Maintenance	Nil	6,000	11,000
Sub Total PSCC	492,000	443,000	433,000

ISLD

LO (0.5)	36,000	36,000	36,000
Salaries	36,000	36,000	36,000
Travel	2,000	1,000	1,000
Sub Total ISLD	38,000	37,000	37,000
Sub Total A-G's	530,000	480,000	470,000

ASIO

EL2	110,000	110,000	110,000
EL1		101,000	101,000
APS6 (2)	160,000	160,000	160,000
APS6 (2)		160,000	160,000
Salaries	270,000	531,000	531,000
Sub Total ASIO	270,000	531,000	531,000

AFP			
AFP L4	110,000	110,000	110,000
Salaries	110,000	110,000	110,000
Sub Total AFP	110,000	110,000	110,000
TOTAL SALARIES AND ADMIN	**1,460,000**	**1,691,000**	**1,681,000**
Capital Costs			
PSCC			
Computing Equipment	20,000	20,000	Nil
Telecommunications Equipment	20,000	5,000	Nil
Sub Total PSCC	40,000	25,000	Nil
DSD			
Computing Equipment	30,000	30,000	Nil
Sub Total DSD	30,000	30,000	Nil
TOTAL CAPITAL	**70,000**	**55,000**	**Nil**
TOTAL PROJECT	**1,530,00**	**1,746,000**	**1,681,000**

Appendix F Key Dates in Economic Security

Selected Events in the evolution of the Australian Financial System based on data from the Financial System Inquiry with additional sources.

Year	Events
1937	Report of the Napier Royal Commission into the Australian Monetary and Banking System
1941	Australian Banks became licensed. They came under the influence of the Commonwealth Bank acting in the capacity of central bank. Profits were explicitly restricted to pre war levels.
1942	Interest rates ceilings were imposed in Australia.
1945	The Australian Banking Act 1945 gave legislative backing to pre war banking regulations (except restrictions on profits). The Australian Life Insurance Act 1945 was passed providing for supervision of life companies.
1947	The Australian Commonwealth Government attempted to nationalise banks.
1960	The new Reserve Bank of Australia (RBA) commenced operations under the Reserve Bank Act 1959. The RBA was to aim for currency stability, maintenance of full employment and prosperity for Australians in undertaking its central banking functions. The first Australian futures market opened, trading greasy wool on the Sydney Greasy Wool Futures Exchange.
1961	The '30/20' rule for life companies and superannuation funds was introduced in Australian, requiring minimum investments in government securities.
1963	Australian Savings banks were allowed to offer personal loans.
1965	The RBA lifted qualitative guidelines on bank lending, no longer restricting banks to lend to particular classes of borrower.
1966	Decimal currency was introduced in Australia.
1970	Provisions in the Banks (Shareholdings) Act 1972 applied from this time in Australia, limiting maximum individual shareholdings to less than 10 % of a bank's capital.
1971	The A$ and NZ$ became linked to the US$ instead of £Sterling.
1972	Australian Trading banks were given increased freedom to negotiate interest rates on deposits greater than $50,000, subject to a maximum rate, for terms between 30 days and four years. The first of the State credit acts was introduced in South Australia.
1973	The Insurance Act 1973 was passed providing for the supervision of general

insurance companies in Australia.

1974 The Financial Corporations Act 1974 contained provisions which could have enabled federal control of a range of financial institutions other than banks, including finance companies and general financiers. Provisions for direct regulation of non-bank financial institutions (NBFIs) (Part IV) were not proclaimed however, although the Act still required reporting of NBFI data to the RBA.

Bankcard was launched in Australia.

1975 Sixteen building societies in Queensland were rescued through establishment of Suncorp, a government owned building society.

1976 The Australian options market commenced trading.

1977 The first automated teller machine was installed in Australia.

1979 The Treasury Note (T-Note) tender system was introduced to replace the 'tap' system for the sale of these Australian government securities. Price for these securities was now market determined for each issue.

The Australian Financial System Inquiry (Campbell Committee) was established.

ANZ Banking Group took over the troubled Bank of Adelaide, after problems with Bank of Adelaide's finance company subsidiary.

1980 The first cash management trust was established in Australia.

Interest rate ceilings on trading bank and savings bank deposits were dismantled in Australia: some limits on minimum and maximum terms on fixed deposits remained.

The Australian Law Reform Commission Report, Insurance Agents and Brokers, was published. The report recommended that insurers should be responsible for the conduct of their agents, but not brokers with whom the insurer deals.

1981 The final report of the Campbell Committee was tabled.

The Commonwealth Government agreed to the mergers of the Bank of New South Wales with the Commercial Bank of Australia and the National Bank of Australasia with the Commercial Banking Company of Sydney.

1982 Australian Savings banks were allowed to accept deposits of up to $100, 000 from trading or profit making bodies.

The minimum term on Australian trading bank fixed deposits was reduced from 30 to 14 days for amounts greater than $50,000, and from 3 months to 30 days for amounts less than $50,000.

The Australian Treasury Bond (T-Bond) tender system was approved.

The Trade Practices Commission (TPC) granted interim authorisation for stock exchanges, previously exempt under anti-monopoly provisions of the Trade Practices Act 1974.

The Australian Law Reform Commission Report, Insurance Contracts, was published. The report's recommendations included the adoption of standard cover for some types of policy.

1983 The Australian Commonwealth Government announced that it would allow entry of 10 new banks, including foreign banks.

The A$ was floated and most exchange controls were abolished

The Australian Treasurer announced the formation of the Martin Committee of Review to assess the Campbell Report.

1984 The Martin Committee of Review endorsed the Campbell Report.

The '30/20' rule was abolished for life companies and superannuation funds.

In Australia, all remaining controls on bank deposits were removed. The restrictions

that were lifted included minimum and maximum terms on deposits, savings bank exclusions from offering chequering facilities, and the prohibition of interest on cheque accounts.

New taxation arrangements for lump sum superannuation payments were introduced.

Foreign investment guidelines on ownership of merchant banks were relaxed.

Australian stock exchanges and the securities industry were deregulated.

The Australian Payments System Council (APSC) was established. Credit Union Services Corporation (Australia) Limited established a mechanism for credit unions to issue cheques on an agency basis.

1985 Sixteen foreign banks were invited to establish trading operations in Australia ¾, the first foreign bank began operations in the last quarter.

Electronic funds transfer at point of sale was introduced.

Capital gains tax was introduced.

1986 The first award based superannuation schemes were established in Australia, along with the development of the electronic funds transfer code of conduct was.

The Australian Cheques and Payments Order Act 1983 was amended to allow NBFIs to issue payment orders and to formalise agency arrangements for cheque issuing.

The cessation of double tax on company dividends was announced in Australia.

1987 In Australia, the dividend imputation system took effect from mid-year.

The Australian Stock Exchange (ASX) commenced operations, amalgamating state exchanges. The ASX established the Stock Exchange Automated Trading System to allow electronic trading of securities.

A worldwide stock market crash occurred.

The Australian Insurance and Superannuation Commission (ISC) was established.

The Occupational Superannuation Standards Act 1987 commenced.

1988 The Australian Commonwealth Government announced new arrangements for superannuation, including earlier taxation of end benefits, superannuation fund access to dividend imputation and changes to Reasonable Benefit Limits.

An issues paper Towards a National Retirement Incomes Policy (Cass Report) recommended measures to establish superannuation as an integral component of the retirement income system.

The RBA introduced consolidated risk-weighted capital requirements for banks, consistent with Bank for International Settlements' proposals.

Perth based merchant bank Rothwells collapsed.

1989 The Australian Banking Industry Ombudsman scheme was initiated.

1990 The Japanese Government was very slow to react to the severe financial sector problems, which had been evident since the early 1990s. However, since 1996, the Government has improved significantly the financial supervisory system and addressed major banks' non-performing loan, provisioning and capital adequacy problems.

1990 ANZ and National Mutual announced plans to merge: the Commonwealth Government opposed the merger on competition grounds.

The Commonwealth Government announced the 'six pillars' policy.

The Pyramid Building Society failed.

A Judicial Manager was appointed for the liquidation of the Regal and Occidental life insurance companies.

The National Companies and Securities Commission froze funds of mortgage trust, Estate Mortgage.

1991 The Commonwealth Bank of Australia acquired the State Bank of Victoria.

Commonwealth Bank shares were offered to the public for the first time.

A twelve-month freeze on redemptions in unlisted property trusts was announced.

The Commonwealth Government announced a Superannuation Guarantee Charge effective from 1 July 1992.

The House of Representatives Standing Committee on Finance and Public Administration (Martin Parliamentary Committee) released a report recommending a feasibility study of direct payments system access for NBFIs, establishment of a high-value electronic payments system, a formal Prices Surveillance Authority (PSA) brief to examine the profitability of the credit card business and the establishment of a code of banking practice.

The Australian Securities Commission (ASC) became the regulator for corporations and for securities and futures markets under Corporations Law.

The General Insurance Enquiries and Complaints Scheme and the Life Insurance Complaints Service were established.

1992 Authorised foreign banks were allowed to operate branches in Australia, but were not allowed to accept retail deposits. Limits on the number of new banks that could be established were removed.

The Commonwealth Government One Nation package introduced pooled development fund and offshore banking unit concessionary taxation arrangements.

Mortgage originator 'Aussie Home Loans' was established.

The Australian Financial Institutions Commission (AFIC) was established to administer the new Financial Institutions Scheme.

The Australian Payments Clearing Association was established.

The TPC report on the Life Insurance and Superannuation industry was released. The report criticised, amongst other matters, the quality of financial advice given by agents and the industry's remuneration systems for agents.

1993 The Commonwealth Government Banking Policy Statement was announced, which included changes to the interest withholding tax arrangements and a call for the PSA to monitor credit card interest rates and fees.

The Australian Bankers' Association released the code of banking practice to be monitored by the APSC.

The Australian Superannuation Industry (Supervision) Act 1993 was passed.

1994 The NSW Government sold the State Bank of NSW to the Colonial Mutual Life Association.

The Insurance Council of Australia introduced the general insurance code of practice. The code encouraged the raising of standards of practice and service for personal lines of business in the insurance industry.

The Australian Superannuation Complaints Tribunal commenced operations.

Two Special Services Providers were issued exchange settlement accounts by the RBA.

1995 The TPC allowed the Westpac acquisition of Challenge Bank, and elucidated market definition criteria for the sector.

The South Australian Government sold the State Bank of South Australia to Advance Bank.

The first international stored value card trials were conducted in Australia.

The Commonwealth Government allowed acquisition of a majority interest in the National Mutual Life Association of Australia by AXA SA, contingent on the

demutualisation of National Mutual and formation of a new holding company for the National Mutual group.

The Australian Life Insurance Act 1995 enhanced the ISC's powers to obtain reports and to conduct on-site inspections. The life insurance code of practice was launched.

1996 The Australian Financial System Inquiry was announced.

Australian Banks, building societies, credit unions and life companies were allowed to provide a retirement savings account product from mid-1997.

Commonwealth Bank shares were offered to the public for the second time.

The Queensland Government announced the merger of Metway Bank and the government owned SUNCORP insurance and finance group.

The Australian Uniform Consumer Credit Code applied from November.

1997 SWIFT announced plans for its "next generation" of products and services running on a secure internet protocol (IP) network

In 1997 and 1998, Thailand, Malaysia and the Philippines all experienced similar currency depreciations, stock market falls and interest rate rises because of the Asian crisis. Thailand and Malaysia also suffered serious financial market and economic turmoil: as a result, both are undergoing significant programs to refinance and restructure their financial sectors, and improve prudential controls. The Philippines' stronger prudential system and extensive foreign currency deposits

From late 1997, Indonesia suffered the world's worst banking crisis since the 1970s. Its cost could reach 80 per cent of GDP and quadruple the country's public debt.

By late 1997, Korea's foreign exchange reserves equalled only two weeks of imports and 8 per cent of foreign debt. As Korea faced the prospect of defaulting on its foreign trade and borrowing obligations, the Government made an emergency arrangement with the IMF. In early 1998, to avert a potential collapse of the financial system, the Government guaranteed bank deposits, tightened capital adequacy ratios and established mechanisms for purchasing banks' non-performing loans and recapitalising banks. These policies were implemented effectively and rapidly, although the Daewoo collapse and related difficulties of investment trust companies introduced new uncertainty regarding the total cost. The Korean Government significantly improved financial market prudential regulations, approaching Bank for International Settlements' standards, and strengthened enforcement. It also strengthened corporate and bank transparency, introduced new international accounting standards and strengthened minority shareholder rights.

St. George Bank merged with Advance Bank

1998 Between 1987 and 1998, Australia's financial and insurance service exports to East Asia rose by an average annual rate of 14 per cent to reach A$183 million: this is 12 per cent of Australia's total exports of these services. Furthermore, financial consultancy service exports are not included in this figure. Driven largely by reinsurance business, exports of insurance services grew at 25 per cent per year after 1987, reaching A$69 million in 1998: financial service exports grew 9 per cent per year over this period, reaching $A114 million in 1998.

While China's financial sector has many features that caused financial crises in other East Asian economies, the Asian financial crisis only modestly affected China. Nevertheless, economic growth slowed during 1998 and 1999, due to poor export performance, relatively tight monetary policy and structural problems, including an inefficient financial sector. Throughout the crisis the Government maintained the renminbi's peg to the US dollar: it is unlikely to free capital controls or move to a floating exchange rate until it completes essential financial sector and state

1999 By the end of 1999, the Indonesian Government will own banks holding 85 per cent of

banking system deposits. Moreover, 75 to 85 per cent of bank loans are non-performing, so the task to recapitalise, restructure and eventually re-privatise banks is massive.

2001 September 11 attack on New York and Washington has impact on key financial systems

Bibliography

[1] _, *Counterfeit Currency in the Middle East.* Jane's Intelligence Review. 1 February, 1996.

[2] _, *New Money for Old, With Care* (Editorial). New York Times. 27 March, 1996.

[3] _, *Real-Time Change*. The Economist. 25 November, 1995.

[4] _, *SWIFT Rolls Out Security Package*. Banking World. March 1994.

[5] Allison, T. *Testimony before the House Banking and Financial Services Committee*, 27 February, 1996.

[6] Altgilbers, L. L. *Compact Explosive Driven Radio Frequency Weapons: Beer Can Devices (S)*. U.S. Army Space and Strategic Defence Command: Huntsville, AL, 13 January, 1995.

[7] Anderson, R. J. *Why Cryptosystems Fail.* Communications of the ACM, November 1994.

[8] Anthes, G. H. *Info-Terrorist Threat Growing*. Computerworld, 30 January, 1995.

[9] Anthes, G. H. *Security Upgrade Rattles Banking Industry.* Computerworld, 12 December, 1994.

[10] Arnold, H. D., J. Hukill, J. Kennedy, and A. Cameron. *Targeting Financial Systems as Centers of Gravity*. *Defence Analysis* (Journal), Vol. 10, No. 2, August 1994.

[11] Auer, J. *Cross-Border Networks for Financial EDI.* World of Banking, May/June 1994.

[12] Bachus, S. (Rep) 27 February, 1996. (Quoted in Congressional Hearings Summaries.)

[13] Bass, T A. *The Future of Money*. Wired, Oct. 1996: 140-143, 200-205.

[14] Black, P. *Soft Kill: Fighting Infrastructure Wars in the 21st Century*, Wired, July-August 1993.

[15] Buzan, B. People, States and Fear: An Agenda for International Security Studies in the Post–Cold War Era, 2nd ed, Harvester Wheatsheaf, New York, 1991.

[16] Buzan, O. Waever and J. de Wilde, Security: *A New Framework for Analysis,* Lynne Rienner Publishers, Boulder, CO, 1998.

[17] C. Trammell, Quantifying the Reliability of Software: Statistical Testing Based on a Usage Model, *Proceedings of the Second IEEE International Symposium on Software Engineering Standards*, Montreal, Quebec, Canada, August 21–25, 1995, IEEE Computer Society Press, 1995.

[18] Campen, A. D., (Ed). *The First Information War: The Story of Communications, Computers and Intelligence Systems*, Fairfax, Va.: AFCEA International Press, 1992.

[19] _, Centre for Strategic and International Studies. *Global Organized Crime*. CSIS: Washington, DC, 1994.

[20] Chilton, E. C. *The New Mission of SWIFT*. *World of Banking*, May/June 1994.

[21] Clawson, P. Testimony Before the House Banking and Financial Services Committee, 27 February, 1996. (From Federal News Service.)

[22] -, Clearing House Interbank Payment System--CHIPS. New York Clearing House Association. 17 September 1996. (www.theclearinghouse.org.)

[23] Cobb, S. *Progress Towards Strong Encryption. NCSA News*, March 1996.

[24] Collins, A. *'The Security Dilemma', in Davis M. J. (ed.), Security Issues in the Post–Cold War World*, Edward Elgar, Cheltenham, 1996,

[25] Conard, J. W. (Ed). *Communications Systems Management*. Auerbach Publications: Boston, 1994.

[26] Corr, Frank and John Hunter. *Worldwide Communications and Information Systems*. IEEE Communications Magazine, October 1992, 58-63.

[27] Craig, David. NASDAQ Blackout Rattles Investors. *USA Today*, 18 July, 1994, 2.

[28] Davies, R .*http://www.ex.ac.uk/~RDavies/arian/origins.html*, 25 September 2000.

[29] Davies, G., Davies, R., *A comparative chronology of money, Part 1: From the origins of agriculture to the industrial revolution*, Journal of Management History

[30] *-, Fedwire: The Federal Reserve Wire Transfer Service*. Federal Reserve Bank of New York. March 1995.

[31] Fialka, J. J. *Drug Dealers Export Billions of Dollars to Evade Laws on Currency Reporting.* Wall Street Journal, 7 April, 1994.

[32] Finder, Joseph. *The Zero Hour*. William Morrow and Company, Inc.: New York, 1996.

[33] Fitzgerald, M. C., *Russian Views on Information Warfare*, Army 44, no. 5, May 1994.

[34] Fukuyama, F. *The End of History and the Last Man*, Penguin Books, London, 1992.

[35] Gingrich, N. *Information Warfare: Definition, Doctrine and Direction*, address to the National Defence University, Washington, D.C., 3 May 1994.

[36] Henry, S. K. *Thinking the Unthinkable Public and private sectors ponder new ways to do business*. January 2002 SIGNAL Magazine 2002

[37] Hobbes, T. *Leviathan,* J. M. Dent & Sons, London, 1959

[38] Hoffman, T. *Financial Message Exchange Uses Upgrade to Cut Customer Charges*. Computerworld, 22 August, 1994.

[39] Huntington, S. P. *The Clash of Civilizations and the Remaking of World Order*, Simon and Schuster, New York, 1996,

[40] Hust, G. R. *Taking Down Telecommunications*. Air University Press: Maxwell AFB, 1994.

[41] Jacobsen C. G., *The New World Order's Defining Crises: The Clash of Promise and Essence*, Dartmouth, Aldershot, Hampshire, 1996.

[42] Johnson, N. F., Dr. N. D. E. Custance. *Blast Vulnerability of Building Structures and the Public from Terrorist Attack*. Proceedings from the 1994 International Carnahan Conference on Security Technology, 12-14 October, 1994.

[43] Kahn, H. *On Thermonuclear War*, Princeton University Press, Princeton, NJ, 1961.

[44] Kelley, E. W. Jr. *Statement before the Committee on Banking, Finance and Urban Affairs,* U.S. House of Representatives, 13 July, 1994.

[45] Keohane R. O. (Ed), *Neorealism and Its Critics*, Columbia University Press, New York 1986.

[46] Kissinger H., *Diplomacy*, Simon & Schuster, New York, 1994,

[47] Knudson, S. E., Walton J. K., and Young F. M.. *Business-to-Business Payments and the Role of Financial Electronic Data Interchange.* Federal Reserve Bulletin, April 1994

[48] Krauthammer C., '*The Unipolar Moment'*, Foreign Affairs, vol. 70, no.1, Winter, 1990/91

[49] Kurtzman, J. *The Death of Money*. Little, Brown and Company: Boston, 1993.

[50] Leaver R. & Richardson J. L. (Eds), *The Post–Cold War Order: Diagnoses and Prognoses*, Allen & Unwin, Sydney, 1993

[51] Libicki, M. *What is Information Warfare?* National Defence University: Washington, D.C., 1995.

[52] Aldrich, Mjr R. *The International Legal Implications of Information Warfare*, Airpower Journal Fall 1996 5 Dec. 1996.

[53] Niel, M. *The Pentagon's New Nightmare: An Electronic Pearl Harbor.* The Washington Post 16 Jul. 1995.

[54] O'Heney, S. *Fedwire Goes With the Flow*. Computers in Banking, December, 1988.

[55] Patrikis, E T, *Remarks Before the Symposium on Risk Reduction in Payments*, Clearance, and Settlement Systems, January, 1996

[56] *-, Proceedings of the 1997 Information Survivability Workshop*, San Diego, California, February 12–13, 1997, Software Engineering Institute and IEEE Computer Society, April 1997.

[57] *-, Proceedings of the 1998 Information Survivability Workshop*, Orlando, Florida, October 28–30, 1998, Software Engineering Institute and IEEEComputer Society, 1998.

[58] Linger R. C., *Systematic Generation of Stochastic Diversity as an Intrusion Barrier in Survivable Systems Software, Proceedings of 32nd Annual Hawaii International Conference on System Sciences,* Maui, Hawaii, January 5–8, 1999 (HICSS-32), IEEE Computer Society, 1999.

[59] Anderson, R. H. Hearn, A. C and Hundley, R. O. *RAND Studies of Cyberspace Security Issues and the Concept of a U.S. Minimum Essential Information Infrastructure,* Proceedings of the 1997 Information Survivability Workshop.

[60] DiNardo, R.L., Hughes D. *Some Cautionary Thoughts on Information Warfare*. Airpower Journal Winter 1995. 10 October 1996.

[61] Rousseau, J. J. *The Social Contract,* J. M. Dent and Sons, London, 1966

[62] Ryan, J. J., Woloscheck, and Leven., B. *Complexities in Conducting Information Warfare*. Defence Intelligence Journal, Vol. 5, No. 1, Spring 1996.

[63] Schwartau, W., *Information Warfare: Chaos on the Electronic Superhighway* New York: Thunders Mountain Press, 1994.

[64] -, *SecureX25*, Society for Worldwide Interbank Financial Telecommunication S.C. October 1995.

[65] Steinborn, D. *Bank Encryption Standards: Insecure Future*? ABA Banking Journal, August 1994.

[66] Katz, S,. *Global Finance: Protection in the Age of Electronic Conflict. infoWarcon5: Electronic Civil Defence for the 21st Century. The Convergence of the Commercial and Military Sectors: Vulnerabilities, Capabilities, and Solutions,* Arlington, VA 5-6 Sept. 1996.

[67] Stoll, Clifford. *Silicon Snake Oil*. Anchor Books: New York, 1995.

[68] Sullivan, Gen G. R. & Dubik, Col J. M., *War in the Information Age,* Military Review 74, April 1994

[69] Toffler, A., Toffler, A., *War and Anti-War: Survival at the Dawn of the 21st Century*, Boston, Mass.: Little, Brown and Co., 1993.

[70] _,*Oversight of Critical Banking Systems Should Be Strengthened*. U.S. General Accounting Office GAO/IMTEC-90-14, January 1990.

[71] -, *US Banks and International Telecommunications*. United States. Cong. Office of Technology Assessment. Washington: US Government Printing Office, 1992.

[72] van Creveld M., *The Transformation of War*, The Free Press, Sydney, 1991.

[73] Van Keuran, E., Wilkenfeld, Dr. J., Knighten, Dr. J., *Implications of the High-Power Microwave Weapon Threat in Electronic System Design*. IEEE Conference Proceedings, 12-16 August, 1991.

[74] Van Keuran, E., Wilkenfeld, Dr. J., Knighten, Dr. J.,*Utilization of High-Power Microwave Sources in Electronic Sabotage and Terrorism*, IEEE Conference Proceedings, 1-3 October, 1991.

[75] von Clausewitz, C. *On War*, (Ed/Trans) Howard M., Paret P. Princeton University Press, Princeton, NJ, 1976.

[76] Waitzman, W. *In a World Without Frontiers,* Every Battle Can Hit Home. *Barron's*, 4 March, 1996.

[77] Waltz, K. *Man, the State, and War: A Theoretical Analysis*, Columbia University Press, New York, 1959.

[78] White, P. T. *The Power of Money.* National Geographic, January, 1993

[79] Carley, W., O'Brien,T. *Cyber Caper: How Citicorp System Was Raided and Funds Moved Around World.* The Wall St. Journal. 18 November 1996.

[80] Yavuz, Dr. D., Dr. F. Eken, and Dr. N. Karavassilis. *Highly Survivable Communications: Complementary Media Packet Switched Networks*. SHAPE Technical Centre Conference, 12-14 April 1994. Published by IEEE.

Glossary

This glossary was compiled from various sources including the US Department of Defence Dictionary of Military and Associated Terms (Joint Pub 1-02, 23 March 1994) and Australian Financial Systems Enquiry.

ABA	Australian Bankers' Association
ABIO	Australian Banking Industry Ombudsman
ABS	Australian Bureau of Statistics
ACCC	Australian Competition and Consumer Commission
ACCI	Australian Chamber of Commerce and Industry
ADR	Alternative dispute resolution
AFIC	Australian Financial Institutions Commission
AFIC Code	Australian Financial Institutions Commission Code 1992
AFMA	Australian Financial Markets Association
AGPS	Australian Government Publishing Service
AIDC	Australian Industry Development Corporation
ALRC	Australian Law Reform Commission
ANZ	ANZ Banking Group
APCA	Australian Payments Clearing Association
APEC	Asia-Pacific Economic Cooperation
APRC	Australian Prudential Regulation Commission
APSC	Australian Payments System Council
ASC	Australian Securities Commission

ASX	Australian Stock Exchange
ATM	Automated teller machine
ATO	Australian Taxation Office
Attack assessment	An evaluation of information to determine the potential or actual nature and objectives of an attack for providing information for timely decisions. See also damage estimation.
Banking Act	Banking Act 1959
Banks Act	Banks (Shareholdings) Act 1972
Biological operation	Employment of biological agents to produce casualties in personnel or animals and damage to plants or materiel: or defence against such employment
BIS	Bank for International Settlements
BITS	Bank Interchange and Transfer System
C2 protection	See command and control warfare.
CBA	Commonwealth Bank of Australia
CEDA	Committee for Economic Development of Australia
CEMTEX	Central Magnetic Tape Exchange
CFM	Commonwealth Funds Management
CFR	Council of Financial Regulators
CFS	Council of Financial Supervisors
CFSC	Corporations and Financial Services Commission
CGT	Capital gains tax
Chemical warfare	All aspects of military operations involving the employment of lethal and incapacitating munitions/agents and the warning and protective measures associated with such offensive operations. Since riot control agents and herbicides are not considered to be chemical warfare agents, those two items will be referred to separately or under the broader term chemical, which will be used to include all types of chemical munitions/agents collectively. The term chemical warfare weapons may be used when it is desired to reflect both lethal and incapacitating munitions/agents of either chemical or biological origin. Also called CW. See also chemical operations, herbicide, riot control agent.
CHESS	Clearing House Electronic Sub-register System
CML	Colonial Mutual Life Assurance Society Limited

Combined warfare	Warfare conducted by forces of two or more allied nations in coordinated action toward common objectives.
Command and control warfare	The integrated use of operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW), and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions. Command and control warfare applies across the operational continuum and all levels of conflict. Also called C2W. C2W is both offensive and defensive: a. Counter C2 prevents effective C2 of adversary forces by denying information to, influencing, degrading, or destroying the adversary C2 system. b. C2 To maintain effective command and control of own forces by turning to friendly advantage or negating adversary efforts to deny information to, influence, degrade, or destroy the friendly C2 system. See also command and control: electronic warfare: intelligence: military deception: operations security: psychological operations.
Counter guerrilla warfare	Operations and activities conducted by armed forces, paramilitary forces, or non-military agencies against guerrillas.
CPA	Competition Principles Agreement
Damage estimation	A preliminary appraisal of the potential effects of an attack. See also attack assessment.
Directed energy protective measures	That division of directed energy warfare involving actions taken to protect friendly equipment, facilities, and personnel to ensure friendly effective uses of the electromagnetic spectrum that are threatened by hostile directed energy weapons and devices.
Directed energy warfare	Military action involving the use of directed energy weapons, devices, and countermeasures to either cause direct damage or destruction of enemy equipment, facilities, and personnel, or to determine, exploit, reduce, or prevent hostile use of the electromagnetic spectrum through damage, destruction, and disruption. It also includes actions taken to protect friendly equipment, facilities, and personnel and retain friendly use of the electromagnetic spectrum. Also called DEW. See also directed energy: directed energy device: directed
Directed energy weapon	A system using directed energy primarily as a direct means to damage or destroy enemy equipment, facilities, and personnel. See also directed energy: directed energy device.
DoCA	Department of Communications and the Arts
DTI	Deposit taking institution
Economic warfare	Aggressive use of economic means to achieve national objectives.
EDI	Electronic Data Interchange
EFT	Electronic funds transfer

EFTPOS	Electronic funds transfer at point of sale
Electromagnetic intrusion	The intentional insertion of electromagnetic energy into transmission paths in any manner, with the objective of deceiving operators or of causing confusion. See also electronic warfare.
Electronic attack	That division of electronic warfare involving the use of electromagnetic or directed energy to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability. Also called EA. EA includes: 1) Actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception, and 2) Employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism (lasers, radio frequency weapons, particle beams).
Electronic protection	That division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition.
Electronic warfare	Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Also called EW. The three major subdivisions within electronic warfare are: electronic attack, electronic protection, and electronic warfare support.
Electronic warfare support	Electronic warfare support provides information required for immediate decisions involving electronic warfare operations and other tactical actions such as threat avoidance, targeting, and homing. Also called ES. Electronic warfare support data can be used to produce signals intelligence (SIGINT), both communications intelligence (COMINT), and electronics intelligence (ELINT).
EPAC	Economic Planning and Advisory Commission (formerly Economic Planning and Advisory Council)
ESA	Exchange settlement account
ESOP	Employee Share Ownership Plan
Event time	Time the hostile event occurred. Also called integrated tactical warning. See also attack assessment: strategic warning.
FCA	Financial Corporations Act 1974
FI Code	Financial Institutions Code
FI Scheme	Financial Institutions Scheme
FID	Financial institutions duty
FIF	Foreign investment fund

FSAC	Financial Sector Advisory Council
FSI	Financial System Inquiry
G10	Group of Ten Central Banks
G20	Group of Twenty
GBE	Government business enterprises
GDP	Gross domestic product
GIO	Government Insurance Office
GSM	Group Speciale Mobile
Guerrilla warfare	Military and paramilitary operations conducted in enemy held or hostile territory by irregular, predominantly indigenous forces. See also unconventional warfare.
HLIC	Housing Loans Insurance Corporation
IBSA	International Banks and Securities Association of Australia
IC	Industry Commission
IMF	International Monetary Fund
Indications and warning	Those intelligence activities intended to detect and report time sensitive intelligence information on foreign developments that could involve a threat to the military, political, or economic interests or to citizens abroad. It includes forewarning of enemy actions or intentions: the imminence of hostilities: insurgency: nuclear/non nuclear attack, its overseas forces, or allied nations: hostile reactions reconnaissance activities: terrorists' attacks: and other similar events.
Information warfare	Actions taken to achieve information superiority by affecting adversary information, information based processes, information systems, and computer based networks while defending one's own information, information based processes, information systems, and computer
Integrated warfare	The conduct of military operations in any combat environment wherein opposing forces employ non-conventional weapons in combination with conventional weapons.
ISC	Insurance and Superannuation Commission
IWT	Interest withholding tax
LGS	Liquid Assets and Government Securities
Life Insurance Act	Life Insurance Act 1995
MCCA	Ministerial Council of Consumer Affairs
MER	Management expense ratio

MFI	Main Financial Institution
NAB	National Australia Bank
NASDAQ	National Association of Securities Dealers Automated Quotation system
NBFI	Non-bank financial institution
NCD	Non-callable deposit
Nuclear warfare	Warfare involving the employment of nuclear weapons.
OBU	Offshore Banking Unit
OECD	Organisation for Economic Co-operation and Development
Operations security	A process of identifying critical information and subsequently analysing friendly actions attendant to military operations and other activities to: a. Identify those actions that can be observed by adversary intelligence systems. b. Determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries. c. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. Also called OPSEC. See also command and control warfare: operations security indicators: operations security measures: operations security planning guidance: operations security vulnerability.
OTC	Over-the-counter
PAR	Prime Assets Ratio
PC	Personal computer
Perception management	Actions to convey and/or deny selected information and indicators to foreign audiences to influence their emotions, motives, and objective reasoning: and to intelligence systems and leaders at all levels to influence official estimates, ultimately resulting in foreign behaviours and official actions favourable to the originator's objectives. In various ways, perception management combines truth projection, operations security, cover and deception, and psychological operations. See also psychological operations.
PFE	Public financial enterprise
PIN	Personal identification number
Political warfare	Aggressive use of political means to achieve national objectives.
PSA	Prices Surveillance Authority
PSB	Payments System Board
Psychological operations	Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective

	reasoning, and ultimately the behaviour of foreign governments, Organisations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behaviour favourable to the originator's objectives. Also called PSYOP. See also perception management.
Psychological warfare	The planned use of propaganda and other psychological actions having the primary purpose of influencing the opinions, emotions, attitudes, and behaviour of hostile foreign groups in such a way as to support the achievement of national objectives. Also called PSYWAR.
PUCL	Panel for Uniform Commercial Laws
RBA	Reserve Bank of Australia
RHQ	Regional Headquarters (Companies)
RIC	Regulated investment company
RIM	Retirement Income Modelling
RITS	Reserve Bank Information and Transfer System
RSA	Retirement savings account
RTA	Retail transaction account
RTGS	Real-time gross settlement
SBSA	State Bank of South Australia
SCAG	Standing Committee of Attorneys-General
SCT	Superannuation Complaints Tribunal
SET	Secure Electronic Transaction
SFE	Sydney Futures Exchange
SG	Superannuation guarantee
SGIC	State Government Investment Corporation
SIS	Superannuation Industry (Supervision) Act 1993
SME	Small and medium sized enterprise
SRD	Statutory Reserve Deposits
SRO	Self-regulatory organisation
SSA	State Supervisory Authority
SSP	Special Service Provider
SVC	Stored value card

SWIFT	Society for Worldwide Interbank Financial Telecommunications
SYCOM	Sydney Futures Exchange screen trading system
Tactical warning	1. A warning after initiation of a threatening or hostile act based on an evaluation of information from all available sources. 2. In satellite and missile surveillance, a notification to operational command centres that a specific threat event is occurring. The component elements that describe threat events are: Country of origin - country or countries initiating hostilities. Event type and size determined by observing trajectory of an object and predicting its impact point.
Tactical warning and assessment	A composite term. See separate definitions for tactical warning and for attack assessment.
TFP	Total factor productivity
TGIO	Tasmanian Government Insurance Office
TPA	Trade Practices Act 1974
TPC	Trade Practices Commission
UCCC	Uniform Consumer Credit Code
Unconventional warfare (UW)	A broad spectrum of military and paramilitary operations, normally of long duration, predominantly conducted by indigenous or surrogate forces who are organized, trained, equipped, supported, and directed in varying degrees by an external source. It includes guerrilla warfare and other direct offensive, low visibility, covert, or clandestine operations, as well as the indirect activities of subversion, sabotage, intelligence activities, and evasion and escape.
Westpac	Westpac Banking Corporation