CYBERTERRORISM AND PRIVATE CORPORATIONS:

NEW THREAT MODELS AND RISK MANAGEMENT IMPLICATIONS

Toby Blyth

Solicitor, Supreme Court of New South Wales

Disclaimer: The opinions and conclusions contained herein are solely those of the author, and do not reflect policy, institutional opinion, or proprietary information of his employer.

INTRODUCTION

The very late twentieth century has seen an astonishing development in the technical specifications of computers and associated technology. In addition, this developing technology has led to the increasing importance of the Internet in relation to many facets of the organisation of society, especially in the developed, democratic countries.

In these countries, the level of computing power in society, and the technological sophistication of its consumers and corporate entities, enables and requires that a great (and growing) number of transactions and informational activities be carried out or enabled electronically. In many cases, electronic means of information transfer are being used to the exclusion of traditional, hard forms of enablement. Perhaps as a result of this, there is a growing appreciation of the effect that holding information can have upon a given entity's ability to respond - to opportunities and to threats.

Due to the very nature of the Internet and associated means of information storage and transfer, there has been a marked convergence of the public and private sectors in the one network, to the extent that in some cases there is no relevant distinction between matters that would traditionally have been regarded as public and those which would traditionally have been regarded as private.

This gradual convergence has also led to the convergence of identity issues - in that there is an increasingly blurred demarcation between private corporations, individuals and governments. A logical result of this social movement has been the gradual decline of the importance and relevance of the nation-state, in any of its traditional forms.

At the same time as this attitudinal shift in the treatment of information, military analysts have been reconsidering the threat spectrum and the sorts of threats that now face developed societies. In the light of the end of the Cold War, and the "disintegration" of the cohesion of groups that adopted poses inimical to the Western democracies and their allies, the threat spectrum itself has fractured and disintegrated.

Aggression, now disaggregated into new shapes and forms, is now directed at an increasing and new set of targets. As well as the traditional Cold War groupings, developed nations face threats from undeveloped ones due to their status as "developed" per se. Additionally, now that the United States dominates the world geopolitically, other states may resort to the use of force by means of non-state identified actors.

Ominously for private corporations, their growing involvement with the Internet presents threats in several ways. They are increasingly being seen as non-state or meta-state entities, and therefore targets of aggression in their own right, and they are also converging with the military and industrial complexes of their respective home-states, therefore presenting an attractive target to the use of force directed towards the nation state itself.

As information is transferred more and more to electronic networks, populations are increasingly at risk of interruption to those networks - from petty, invisible harassment or thieving, to the doomsday scenario envisaged in the film *James Bond - Goldeneye*.

As pressure to compete grows stronger, there is also the possibility than corporations themselves may employ aggression against their competitors.

The growth of the Internet and the increasing dependence on it in the developed nations leaves them vulnerable to many forms of attacks directed at computer networks and the information stored on them. These attacks can range from physical destruction, to electronic thievery, to the crashing of vital information systems on a grand scale.

The new aggressors in this sort of "warfare" can range form political activists to commercial competitors, to criminals and terrorists.

Traditional corporate command and control structures may not be adequate to deal with new forms of aggression, which may be invisible or may come from new and unanticipated sources and directions. There is some tension between the demands made by consumers and citizens in the developed world for corporate and governmental information transparency and the possibility of means of attack this presents to aggressors.

This paper first discusses in some detail the theoretical underpinnings of the new threat spectrum, and identifies the actors who are or may be important.

In the second section, it deals with some technical aspects of the threat, and its treatment, and discusses the need for a new way of thinking about and approaching corporate command and control and the protection of corporations from electronic attack.

PART I

DEVELOPMENTS IN THE THEORY OF CONFLICT – EXPANSION OF THE THREAT SPECTRUM

"You attack unexpectedly, causing opponents to become exhausted just running for their lives. You burn their supplies and raze their fields, cutting off their supply routes. You appear at critical places and strike when they least expect it, making them have to go to the rescue."[1]

At the start of any consideration of the expansion of the threat spectrum must be a consideration of theoretical developments in the wider area of conflict study – this is, necessarily, the space in which the specific risks facing corporations are situated. central to the discussion of the threat spectrum is a discussion of the Revolution in Military Affairs and the concept of information warfare (and its variants). at the same time, the space in which the corporation exists must also be considered from a fresh perspective.

THE REVOLUTION IN MILITARY AFFAIRS (RMA)

Epistemology and taxonomy

The concept of RMA developed from the work of Soviet military theorists in the early 1970's.[2]

They noted 2 fundamental changes in military approach that occurred in the 20th century:

- The emergence of aircraft, motor vehicles and chemical warfare in World War I.[3]
- The development of nuclear weapons, missiles and computers in World War II.[4]

The *substance* of a revolution in military affairs is by no means new - various "revolutionary" or innovative stages of the development of military procedures have occurred[5]

[1] Sun Tzu, *The Art of War*, 1998, Shambhala, Boston, page 102.

[2] Galdi, T, *CRS Report for Congress - Revolution in Military Affairs? Competing Concepts, Organisational Models, Outstanding Issues*, 11 December 1995, pages 1 and 4; and Thomas, Lt Cnl K, *A Revolution In Military Affairs*, (1996) 5 Research and Analysis, page 1.

[3] Arquilla, J and Ronfeldt, D, *Cyber War Is Coming*, (1993) 12 Comparative Strategy 141-165, also in Arquilla and Ronfeldt, *In Athena's Camp*, RAND, 1997 available at www.rand.org/publications.

[4] Galdi, pages 4 and 9.

[5] Galdi, pages 4 and 5; Thomas, page 1; .

Galdi identifies various developments that arose from these revolutions, including the development of the Blitzkrieg which was used so effectively during the early years of World War II by the German army, the use of aircraft carriers by Japan and the United States and the development of strategic bombing by Great Britain and the United States in the latter part of World War II.[6]

Of course, an immediately obvious turnaround which jumps to mind is the use of nuclear weapons - although they have only been used on 2 occasions in actual conflict, it is beyond argument that the threat of the use of nuclear weapons has significantly altered strategic thinking since 1945.

The terminology of RMA is not standard[7] - some commentators use it to refer to the use of technology itself, others to adaptations by military organisations necessary to deal with changes in technology[8], others to the revolutionary impact of geopolitical or technological change on the outcome of military conflicts[9] - regardless of the epistemological approach adopted, it is unarguable that the RMA concept has been and continues to be a significant factor in military and strategic thinking.

Disaggregation and the decline of the nation-state

Galdi[10] quotes the work of Builder, who discusses the various factors that have emerged which are likely to lead to the necessity for changes in approaches to the use of force in the future. He considers that we may be approaching the era of the "end of the nation-state"[11] - the relative importance of the nation-state will decline, in proportion to the growing importance of the supra-national and sub-national and non-national forces.

[6] .

[7] O'Hanlon, page 8; Rathmell, A, *Informaiton Warfare: Implications for Arms Control*, (1998) 29 Bulletin of Arms Control, pages 8-14, page 1.

[8] RAND Organisation Research Review, *Information Warfare: A Two-Edged Sword*, available at www.rand.org.publications, (*A Two-Edged Sword*)page 1.

[9] Galdi, page 5

[10] Page 6.

[11] Compare Gaddis, J, *Muddling Through? A Strategic Checklist for the United States in the Post-Cold War World*, 3rd International Security Forum and 1st Conference of the PfP Consortium of Defense Academies and Security Studies Institutes, 19-21 October 1998, available at www.isn.ethz.ch, page 9

As the importance of the nation-state declines, the importance of[12]:

- supra-national organisations such as the United Nations or NATO,
- sub-national groups, such as private enterprise, criminal and ethnic groups[13], and
- non-national groups, for example non-state aligned terrorist groups and multi-national businesses[14]

both appear in greater relief and grow in actual significance.[15]

The position of the "stateless" multi-national corporation (whose domicile is often very difficult to ascertain) presents some problems - at one level, it should be placed in the list of supra-national entities. Its activities and presence increasingly stretch over more than one nation-state boundary, and it may be subject of more than one (or sometimes, conceivably, *no*) jurisdiction.

However, some corporations are mere emanations of government, and could possibly be matched to the level of the nation state. Corporations traditionally would be classed as sub-national entities, brought into existence by the operations of the laws of nation-states, yet they are also identified by Builder as "non-national" entities.[16]

The corporation can possibly, therefore, present a unique case - it simultaneously exists and is present in four planes of existence. These planes are by no means always (or possibly ever) complementary. This overlapping (and underlapping in cases of power gaps where corporations may have an existence) presents unique problems for those seeking to deal with the corporation in the epistemological framework set up by RMA.

[12] Rathmell, A, *Cyber-terrorism: The Shape of Future Conflict?*, (1997) Royal United Service Institute Journal 40-46, pages 1 and 5.

[13] Metz, S, *To Insure Domestic Tranquillity: Terrorism and the Price of Global Engagement*, page 65, in Pelletiere, S (ed), *Terrorism: National Security Policy and the Home Front*, 15 May 1995, Strategic Studies Institute, US Army War College, PA.

[14] Steele, R, *Information Peacekeeping: The Purest Form of War,* in, Matthews, J (ed), *Challenging the United States Symmetrically and Assymetrically: Can America be Defeated?*, July 1998, US Army War College, Strategic studies Institute, PA, page 144.

[15] Galdi, pages 6 and 13.

[16] Galdi, page 6.

The growing definitional "amorphosity" and "porosity" of the corporation may lead to the identification of the corporation with any number of entities with which it would traditionally not be linked - for example, McDonalds may be seen to be linked with US government (or even NATO) policy in a way which, in the past, was less likely - both because corporations did not operate on a multi-national level, but also due to a perceived enmeshing of McDonalds' aims[17] with those of (an increasingly difficult to identify[18]) Western-corporate-industrial structure[19]. This issue will be dealt with again later in this paper.

Builder notes that "the ability of nations to control the flow of information, commodities and people is declining, while people are becoming more responsive to global events and opportunities[20]. In addition, military weaponry is diffusing beyond the control of governments. The world created will be one in which conflict will be more frequent and more disaggregated".[21]

In a sense, the growing responsiveness of the elite in Western societies to global, stateless, phenomena mirrors the movement of corporations[22] - while it is less likely that people will fall into an existential lacuna, they may exist on more than one level (traditionally, a person would be viewed as the very foundation of the nation-state - before that as a sub-national level).

The disaggregation noted by Builder is, it is submitted, a necessary corollary to the decline of the nation state, and the effects of the disaggregation of conflict will presumably be felt by government, corporations and individuals.[23]

[17] Sloan, page 57.

[18] Steele, page 145.

[19] Compare Rathmell, *Information Warfare*, page 4.

[20] Devost, M, *National Security in the Information Age*, Thesis presented to University of Vermont, May 1995, available at www.terrorism.com/documents, page 5.

[21] Galdi, page 6; Rathmell, *Information Warfare*, page 1.

[22] Thomas, page 1.

[23] Gaddis pages 1 and 4.

Hierarchies and networks[24]

Thomas[25] notes that traditional US military approaches to RMA emphasise a hierarchical approach. According to the traditional approach RMA means that third wave information age armed forces would only engage other third wave information age armed forces.[26]

This ignores the percolation of power and the means of power downwards to primary and secondary stage groups, as well as the possibility that a group may bypass the traditional hierarchical approach altogether.[27]

These non-military groups are not necessarily organised on a hierarchical basis on two fronts:

- Their organisation may be more fluid, and be closer to a network (for example Hizbollah[28], a militant anti-fur group[29] or a group of anarcho-terrorists[30]) and therefore their response to hostility and aggression may not be along hierarchical lines.
- Their employment of aggression may also not be along hierarchical lines.

Although many corporations may be organised within a hierarchical paradigm[31], the growing power of computer networks[32] and the chaotic nature of the late twentieth-century information system means that corporations will be forced to re-organise along network lines sooner or later[33]. Hence, corporations would almost certainly fall into the first front identified above - that is, they will not respond to aggression in a hierarchical way.

[24] Arquilla and Ronfeldt .

[25] Note X - page 3..

[26] Thomas, page 2.

[27] Thomas, page 1; Rathmell, *Information Warfare*, page 3.

[28] Katzman, K, *Hizbollah: Narrowing Options in Lebanon*, and Sloan, S, *Terrorism: How Vulnerable is the United States?*, page 60, in Pelletiere, S (ed), *Terrorism: National Security Policy and the Home Front*, 15 May 1995, Strategic Studies Institute, US Army War College, PA.

[29] Sloan, page 56.

[30] *The Nuclear Black Market*, Centre for Strategic and International Studies, Washington, 1996. page 9.

[31]

[32] *A Two-Edged Sword*, page 1.

[33] Rathmell, *Information Warfare*, pages 1 to 2.

If non-hierarchical groups use aggression in a non-hierarchised way against a hierarchical structure, it is submitted that the damage that can be effected is likely to be greater than if the target of the aggression is able to and does respond in a more fluid way (as would happen to a corporation organised on a network basis, for example).

Similarly, the use of hierarchical force against non-hierarchised targets may not be particularly effective[34].

The nature of conflict between two networked entities may be quite different to what we are used to seeing[35] - perhaps similar to the situation in apartheid South Africa, where state-condoned quasi-terrorist networks battled with other non-state networks.[36]

Whereas hierarchical paradigms are suitable for military command, a network based paradigm is better suited for the dissemination of information.[37] Its is inevitable that with the development of the instantaneous information network, society as a whole and the various entities that make it up will more and more be organised upon non-hierarchised lines.

It is not the task of this paper to discuss in great detail whether corporations are or should be established according to a hierarchical or network paradigm - it will suffice to say that the instant availability of information[38] and the increasing demands upon corporations to compete and offer goods and services on a world market in extremely tight timeframes, a move towards a network paradigm could be seen as inevitable.[39]

The threat implicit in the percolation of technologies downwards and the potential bypassing of hierarchical paradigms should not be missed - it will enable many different groups which

[34] For example, NATO attacks against Serb paramilitary forces and death squads in Bosnia and Kosovo, and US attacks against non-state terrorist forces in the Middle East.

[35] Gaddis, page 1.

[36]

[37] Thomas pages 2 and 3; Rathmell, *Information Warfare*, page 4.

[38] Rathmell, *Cyber-terrorism*, page 1; Devost page 7.

[39] Gompert, D, *Keeping Information Warfare in Perspective*, RAND Research Review Fall 1995, available at www.rand.org/publications, page 1.

previously did not have access to any form of what might be termed warfare to gain access to third wave information age weapons.[40]

These groups might include terrorists, organised crime groups and private enterprises seeking to gain a competitive edge in an increasingly fierce world of competition.[41]

Criticism of RMA

There has been some criticism of RMA[42] O'Hanlon points out that one of the issues pointed to by RMA enthusiasts is the exponential growth of computer technology.[43] Computer technology and the associated weapons it can facilitate may be useful in a world where western nations prefer high technology stand-off warfare with the absence of (or at least extreme aversion to) own-side casualties, but over-dependency upon computers renders armed forces (and presumably society at large) vulnerable to high-altitude nuclear bursts or radio frequency weapons which can destroy unprotected electronics.[44]

Such electronics can govern targeting, communications and weapon systems in an army. They will also govern information transfer in civilian society and such weapons could, presumably, have a devastating effect if used in a non-military context.[45]

It follows from the discussion above of the porosity of corporations and their enmeshing in what might be called the "new" military-industrial-information complex that corporations will be seen both as legitimate civil targets in a total, "old-fashioned" war, and as legitimate targets in a "new-fashioned" information age war[46] - where the distinctions between a civilian target and a military target may become blurred.

[40] Thomas, page 3; Rathmell, *Information Warfare*, page 3; Rathmell, *Cyber-terrorism*, page 2.

[41] Galdi, page 16; Rathmell, *Cyber-terrorism*, pages 4 and 5.

[42] O'Hanlon .

[43] O'Hanlon, page 1.

[44] Galdi, page16; Thomas, page 2; O'Hanlon, pages 2 and 6.

[45]

[46] Molander, R, Wilson, P and Mussington, D, *Strategic Information Warfare Rising*, 1998, RAND Organisation, MR - 964 -OSD, page 3; Rathmell, *Cyber-terrorism*, page 2; compare Valeri, L *On the Dark Side*, 3 Information Strategy 22-23, available at www.kcl.ac.uk, page 1.

Hot war, Cold War and dead war[47]

"Electronic war no longer has any political objective strictly speaking: it functions as a preventative electroshock against any future conflict. Just as in modern communication there is no longer any interlocutor, so in this electronic war there is no longer any enemy, there is only a refractory element which must be neutralised and consensualised."[48]

Baudrillard's discussion of "non-war" is located in the specific factual matrix of the Second Gulf War. Nevertheless, there is some merit in considering the applicability of non-war to other examples, and in particular, to cyberterrorism.

The Cold War, as the period of armed, hostile stand-off between the USA and its clients on the one hand, and the USSR and its clients on the other, is, arguably, over.[49]

Throughout the Cold War, various hot wars were fought between parties in may non-European, non-North American continents- many with the explicit or implicit backing of the USA and/or the USSR.

Baudrillard considers the Second Gulf War to be a " non-war " - specifically this state arises out of the application of high technology to the means of war - and the distancing of the consumers of the developed world from the reality of aggression via the electronic media.[50]

In both cold and hot war, people are exposed in some way - in hot war, those in the areas where war is being fought are in danger of their lives. Others may protest in the USA or other Western countries. All people were under some threat in the Cold War - due to the possibility that aggression, however slight, might lead to nuclear war between the USA and the USSR.[51]

In a non-war, ordinary people may not be exposed in any meaningful way. Attacks, if they are even perceived to be attacks, can come in anonymous, undetected and undetectable forms. It is possible that Western civilisation will see the decline of the traditional war, and the raise in significance of the " non-war".

[47] Baudrillard, J, *The Gulf War did not take place*, 1995, Power Publications, Sydney, page24.

[48] Baudrillard, page84.

[49] Kissinger, H, *Diplomacy* Touchstone, New York, 1994, chapter 30; Gaddis- Page 2.

[50] Compare Rathmell, *Cyber-terrorism*, page 1.

Builder[52] considers that with the emerging international (dis)order[53], different sorts of forces to those required in conventional "big war" situation scenarios will be required. He considers the principal threats that the US military will have to face in the near future will involve dealing with stateless international terrorists and criminal organisations. This would mean that the focus of attention of military thinking and military efforts would change from small, sophisticated, technically advanced forces to larger organisations carrying out operations at a generally lower level of sophistication.

THE ADDITION OF NEW FORMS OF AGGRESSION TO THE THREAT SPECTRUM - INFORMATION WARFARE

Methods of information warfare (IW)

Definitions

Galdi identifies three interrelated definitions of information warfare[54]:

- Attacking, influencing or protecting military reconnaissance, surveillance, dedicated communications, command and control, fire control and intelligence assets.

- Protecting, influencing or attacking the basic communications links of a society - voice, video or data transfer, electric power or telephone system control commands.

- Using television, radio or print media to attack, influence or protect the attitudes of soldiers, civilian populations or leaders.[55]

In addition, the importation of space as a strategic and geopolitical issue should not be ignored - some activities are facilitated or made possible by space vehicles, such as reconnaissance and

[51] O'Hanlon, page 5.

[52] Galdi page 6.

[53] Compare Gaddis, page 8.

[54] Compare Devost page 7, pages 8 to 9.

[55] Galdi page 7.

intelligence gathering, missile defence, navigation, data transmission, communications and force projection[56].

TRADOC's threat spectrum model

In the "Force XXI Operations" paper, the Army Training And Doctrine Command discussed a threat spectrum model which differs significantly from that commonly perceived to have applied during the cold war as follows (from low-end to high-end)[57]:

- Phenomenological threats - these include environmental disasters, health epidemics, famine and illegal immigration.
- Threats posed by "non-nation forces" - which include sub-national threats involving political, racial, religious, cultural and ethnic conflicts challenging the authority of the nation-state.[58]
- National threats such as organised crime, piracy and terrorism operating outside the authority of the host nation-state.
- Meta-national threats such as religious movements and international criminal movements that operate beyond the nation state.[59]
- Recognisable internal security forces, infantry based armies and armour mechanised based armies (what would in lay terms be considered the usual media for war).

[56] Galdi page 8 - General R Myers of the Air Force Space Command notes that growing dependency of the industrialised nations on the use of space creates substantial vulnerability and that the view of space as a peaceful medium is based on a number of assumptions and perceptions that are not necessarily born out. He notes that "it is also just a matter of time before someone attempts to declare space exclusion zones" - just as we have seen seafaring exclusion zones in every century dating back to the Greek and Roman empires. In this case, someone could disrupt spectrum, stand-up electronic blockades through jamming, or any number of other, nefarious measures to ensure their military and commercial advantage in an increasingly competitive environment". There is discussion of Russian efforts to sell a global positioning system jammer and he notes that there have already been disputes over geosynchronous orbit slot allocation and arguments over frequency allocation between companies - "Implementing Our Vision for Space Control" General R Myers, Commander, Airfare Space Command, remarks to US Space Foundation, Colorado Springs, 7 April 1999.

[57] Galdi, pages 11 to 14.

[58] Compare Arquilla and Ronfeldt; *The Nuclear Black Market* page 4.

[59] Rathmell, *Cyber-terrorism*, pages 9 to 10.

- Conflict involving "complex-adaptive armies" - which would be armies that are smaller and extremely expensive to equip, train and maintain. Military operations would involve high technology equipment, multi-dimensional manoeuvre, precision munitions, smart weapons platforms and enhanced situational awareness.[60]

Rathmell's information spectrum model

Rathmell[61] notes that IW has become a strategic catch phrase in the late 1990's. He defines IW as concerning "struggles for control over information activities. Growing human dependence upon information, and the growth of information networks has led to the common view that information networks themselves should be the target of a properly integrated strategic plan.

He distinguishes 3 levels of IW[62]:

- At the highest level, as an ideational struggle for the mind of an opponent, this encompasses the whole range of psychological, media, diplomatic and military technics for influencing the mind of an opponent, whether a military commander or whole population.[63]

- At the second level, is equated with RMA, and advocates of RMA who stress that the aim of RMA armed forces is to dominate the information spectrum.[64]

- At its lowest level, IW consists of attacks on information flows and activities. It can range from electronic attacks, such as hacking, to physical destruction, deception and psychological operations. In this way, it is a modern variant of Command and Control Warfare, which recognises the increasing dependence of armed forces and governments and economies upon the rapid and reliable processing of information.

[60] Galdi, pages 11 to16 - recent US Air Force Doctrinal White Papers, *Global Reach*, *Global Power* and *Global Presence* deal with similar issues from an air force perspective. This offers discussion of space-based systems for navigation, weather information, secure communications and surveillance; Thomas, page 2.

[61] Information Warfare: Implications for Arms Control.

[62]

[63] Rathmell, *Information Warfare*, page 6.

[64] Thomas, page 2.

Rathmell notes that IW weapons are sometimes labelled "weapons of mass corruption"[65] due to the damage that they can cause to a society without causing any physical damage at the first level.[66]

Aquilla and Ronfeldt's aggression spectrum model[67]

IW may be categorised into 3 levels.

Netwar

Aquilla and Ronfeldt define netwar as "information related conflict at a grand level between nations or societies". Netwar may focus upon the disruption or damage of opposition infrastructure[68], or public opinion. To this extent, it will fall into level 1 discussed by Rathmell above.

It should be noted that netwar is not specifically a means to attack Western countries - Western countries and other state groups with sufficiently advanced technological capability can use net war to attack elicit terrorist groups, drug smugglers or to attack proliferation of weapons of mass destruction. On the other hand, it may be waged against state governments by advocacy groups.[69]

Cyberwar

By the term "cyberwar", Aquilla and Ronfeldt refer to "conducting military operations according to information related principles." It involves a move to network structures which would require some decentralisation of command and control, and may provide greater "top site", a central understanding of the big picture that enhances the management of complexity. As an example, they quote the use of hordes of mounted archers by the Mongols in the 13th century as a classic example of network and cyberwar principles. The Mongols were able to very easily defeat hierarchical defenses put up by feudal societies. Another example was the

[65] Rathmell, *Information Warfare*, page 2.

[66] Rathmell, *Cyber-terrorism*, page 6.

[67] Arquilla and Ronfeldt .

[68] Rathmell, *Cyber-terrorism*, page 7.

[69] Rathmell, *Information Warfare*, page 3; Rathmell, *Cyber-terrorism*, page 6.

command forces of North Vietnam and the Viet Cong, which defeated a world super power in the Vietnamese war.

Cyberterrorism

Cyber terrorism is the final level of information warfare. Rathmell[70] notes that "the importance of intrastate and transnational conflict involving sub-state actors will increase markedly" with the increased availability of IW tools and increasing vulnerability[71] of network nodes[72] in industrialised countries[73].

They identify 3 ways in which sub-state groups can use IW:

- Intelligence gathering, communications, money laundering and propaganda.
- Physical violence against the information activities of a target entity.
- Using digital attack techniques against information activities of a target entity.

The following actors can use IW today:

- Hackers, both amateur and professional[74] (the latter nurtured by governments or businesses and may include many former employees of Eastern Bloc intelligence services. Their employers may include business intelligence firms as well as criminal organisations).[75]
- Criminal groups.[76]
- Politically motivated sub-state groups.

[70] Rathmell, *Cyber-terrorism*, pages 2 to 4.

[71] Sloan, page 55.

[72] *A Two-Edged Sword*, page 1.

[73]

[74] Devost pages 12 to 14.

[75] Valeri, page 1.

[76] Rathmell, *Cyber-terrorism*, pages 3 to4.

The use of IW and the network paradigm

The aim of an IW weapon is not mass destruction per se, but the domination of an opponent by corrupting its information. Accordingly, a minimal degree of force would be required for such domination[77].

Much of the force of the potential threat posed by IW weapons is due to the chaotic nature of international information networks.[78] The networks are chaotic in the sense that the networks from what chaos theorists a dynamic and inherently unstable system. Interference with activities may have far reaching and catastrophic results.[79] Governments, commerce and the public would be unable to trust sources of information and paralysis at most levels would ensue.[80]

Obviously, such a scenario would be appealing to those actors that at nation-state level are without access to weapons of mass destruction and/or large armed forces, and in particular to sub-national and non-national groups.[81] In addition to terrorist and organised criminals, other political groups such as human rights campaigners and anti-fur activists can cause disruption in a cheap, undetectable manner to opponents.[82]

Tied in with the issue of IW is the fact that, in a context of reduction in military spending, more and more of the technological information based functions of armed forces are in civilian hands. These technologies are fully integrated into the global economy and are available both for military and non-military uses.[83] Of course, use of the term "military" in such a context may, in view of the discussion above, be somewhat anachronistic but it is used for convenience.

[77] Molander et al, page 16; Rathmell, *Information Warfare*, page 2; Rathmell, *Cyber-terrorism*, page 3.

[78] Rathmell, *Information Warfare*, page 3.

[79] Rathmell, *Information Warfare*, page 4.

[80] Thomas, page 2; Rathmell, *Information Warfare*, page 3.

[81] Devost pages 21 to 22.

[82] Rathmell, *Information Warfare*, page 3; Rathmell, *Cyber-terrorism*, pages 3 to 4.

[83] Molander et al, page 35; Rathmell, *Information Warfare*, page 5.

With the complete integration into the global economy of such technology, export controls are much more difficult to implement than if it were confined to the military community.[84]

The RAND organisation notes that nearly everything the military does depends on computer driven civilian information networks. About 95% of military communications travel over the same networks used by civilians for faxes and telephoning. Each of these information nodes represents a vulnerable point of attack.[85]

The RAND organisation identifies 4 points which make cyberwar different:

- Waging information war is relatively cheap[86] and anonymous.[87]
- Boundaries are blurred in cyberspace - the ordinary distinctions between public and private interests, war and crime, geography are less pronounced in cyberspace.
- Opportunities abound to manipulate perception in cyberspace.[88]
- IW has no front line and potential battlefields are anywhere network systems allow access. Convergences of points of attack, and other nodes[89], represent particularly vulnerable points.

IW and private corporations

Although the military establishment has put in place certain safeguards from IW attacks, the state of preparation of civilian enterprises is way behind that.[90]

Although the military has some responsibility in relation to its own affairs, some responsibility must lie upon the private sector[91] - in addition to the fact that the private sector has its own

[84] Rathmell, *Information Warfare*, pages 4 and 5.

[85] *A Two-Edged Sword*, page 1.

[86] *A Two-Edged Sword*, pages 2 to 3; Devost page 17.

[87] Devost page 18.

[88] Devost page 17.

[89] Rathmell, *Cyber-terrorism*, page 8.

[90] Gompert page 1

[91] Devost page 31; Gompert, page 1.

interests in reducing vulnerability in cyberspace, the integration of military and private sector interests in the information revolution discussed above demand it.[92]

IW of a sort is by no means a new issue for the private sector - as Valeri[93] points out, unscrupulous companies have always been delighted to take advantage of new opportunities to sabotage or steal from a dangerous competitor. The development of information networks and vulnerable points of attack[94] merely emphasises this and increases the opportunities.[95] He notes that economic and industrial espionage is a global industry with a growing work force.

In addition to industrial espionage activities, internal moles or disaffected employees may destroy information networks, and outside groups such as political activists can also cause significant damage.[96]

[92] Rathmell, *Information Warfare*, page 4.

[93] On the Dark Side

[94] *A Two-Edged Sword*, page 1.

[95] Devost page 11.

[96] Valeri page 1.

PART 2

IMPLICATIONS FOR PRIVATE ENTERPRISES

The progressive enmeshing of the private corporation within the hierarchies and networks of the developed world has been discussed in some detail above.

Private corporations are just as dependent upon the infrastructures[97] that form the basis for modern economy, such as telephony, computer networks, electric power, energy and transportation networks, as military organisations.[98]

Hundley and Anderson[99] have discussed the transition from the existence of the corporation in the physical world to a virtual existence in cyberspace.

Various aspects of society are being transferred to cyberspace[100]:

- Informational activities - for example, educational activities, processes and results of research, engineering designs and industrial processes, and mass information and entertainment media, in addition to private and public records. Often the electronic version is held in preference to and in the absence of paper records.[101]

- Transactional activities - any commercial business and financial transaction and Government activities are now being carried on via computer networks and in the absence of paper records.

- Physical and functional infrastructures - are increasing being controlled by electronics and software rather than mechanical or electrical means.

Such information is vulnerable to both intentional and unintentional attacks.

In addition, the distinctions between warfare, crimes and accidents are increasingly blurred - yet all may have the same damaging results.

[97] Devost pages 14 to 16.

[98] Rathmell, *Information Warfare*, pages 2 and 5; Rathmell, *Cyber-terrorism*, page 1.

[99] Hundley, R and Anderson, R, *Security in Cyberspace: An Emerging Challenge for Society* RAND 1994.

[100] Aquilla and Ronfeldt; Gaddis page 3; Rathmell, *Cyber-terrorism*, page 4; Devost page 6.

[101]

Valeri[102] identifies three general categories of attack, especially applicable to a private enterprise:

- Data destruction.
- Penetration of a system to modify its output.
- System penetration with the goal of stealing information or sensitive data.

The means to mount such an attack are by no means difficult to come by - programmes are available free of charge on the Internet to crack passwords or grab key strokes to recognise them, and there is commercially available software to exploit network file system applications that allow file sharing. An increase or the opening of a too large number of sessions in a given time can crash or disable a computer.[103]

A user or a system may be disabled by "bombing" it with identical and repeated messages and attached files. There is also a means of attack known as "spamming" - sending numerous e-mails to a large number of users that can overload a system.

Valeri also notes that due to the nature of the competitive market, various programmes may be released without proper assessment or testing which may leave exploitable gaps.

The growth of international sub- and non-state groups - Russian organised crime (ROC)

The collapse of the former Soviet Union into what could be termed a "trans-national kleptocracy"[104] has led to some fundamental changes in the international security environment:

- Large amounts of unemployed or underemployed or otherwise disaffected security and KGB operators are now available for hire.[105]

[102] *On the Dark Side*.

[103] Valeri page 2.

[104] *Russian Organised Crime*, Center for Strategic and International Studies, Washington, 1997, pages 15 to 17, and 24 to 32.

[105] Rathmell, *Information Warfare*, page 4; Valeri page 2; *Russian Organised Crime*, pages 51 to 56.

- Large amounts of highly trained and professional scientists and computer experts may no longer have jobs.

- Some countries into which the FSU disintegrated have a nuclear capability or reserves of highly enriched uranium.[106]

- Some estimates are that 60% of the Russian economy is under the control of criminal enterprises - these spread beyond the borders of any particular state.[107]

- Estimates have it that 85% of Russian banks are under criminal control.[108]

- Certain Russian power "power ministries" may not now be serving only the interests of the State.[109]

- Russian organised crime has been identified in particular in the following trans-national areas: money laundering, drug trafficking, commercial fraud.[110]

It must be stressed that at this stage ROC is in what could be termed a nascent state - although it holds much sway in Russia, ROC is yet to reach a truly trans-national existence.[111]

IW and terrorist sub- and non-state groups

The inter-play of corporations and private enterprise with avowed terrorist groups should not be underplayed - here a problem arises in that even if a terrorist organisation has an identifiable and compassing ideology (or proto-strategy) such an ideology would be general in nature and as directably establishing broad principles rather than on issues which would provide analysists with a solid foundation.[112]

[106] Russett, B and Stam, A, *Russia, NATO, and the Future of US-Chinese Relations*, available at www.fas.org/man/nato/ceern, page 8; *The Nuclear Black Market* page 8.

[107] *Russian Organised Crime*, pages 24 to 32.

[108] *Russian Organised Crime*, pages 24 to 32.

[109] *Russia and NATO*, paper by Vorontsov, Y and others, February 1997, The George Washington University, Elliott School of International Affairs, Programme on Transitions to Democracy, page 8, available at www.fas.org/man/nato/ceern.

[110] Molander et al, page 40; *Russian Organised Crime*, pages 39 to 40.

[111] Compare Valeri page 3; Russett and Stam, pages 8 to 9; *The Nuclear Black Market* pages 17 to 18.

[112] Sloan, page 51.

Sloan notes that the artificial and superficial equilibrium imposed by the Cold War has been destroyed and that ROC and FSU instability needs to be added to the countries[113] which have always used terrorism as a form as a diplomacy and as an adjunct to their foreign policies.[114]

He notes that in this New World disorder, smaller states can gain access to a much cheaper form of diplomacy in the use of terrorism - either state sponsored or state condoned.

Interestingly, Sloan notes that[115]:

> "New and dangerous players have emerged in the international arena. The level of instability and concomitant violence is further heightened by the rise to international political significance of non-state actors willing to challenge the primacy of the states. *Whether it be the multi-national corporation or a terrorist group that targets it,* both share a common characteristic. They have each rejected the state-centric system that emerged 175 years ago at the Congress of Vienna.
>
> All of these factors have accelerated the erosion of the monopoly of the coercive power of the state as the disintegration of the old order is intensified. And, this process in all probability gain even greater momentum because of the wide ranging and growing activities of criminal enterprises. These include everything from arms traders and drug cartels, which will provide and use existing and new weapons in terrorist campaigns as a part of their pursued profit and political power.
>
> In sum, present and future terrorists and their supporters are acquiring the capabilities and freedom of action to operate in the international jungle. They move in what has been called the "grey areas", those regions where crime control has shifted from legitimate governments to new half political, half criminal powers. In this environment the line between state and rogue state, and rogue state and criminal enterprise will be increasingly blurred. Each will seek out new and profitable targets through terrorism in an international order that is already under assault." [emphasis added]

The multinational (private) corporation as IW aggressor and/or victim

[113] *The Nuclear Black Market* pages 14 to 16; Sloan, page 52; Metz, page 64.

[114] *Russian Organised Crime*, page 61, Sloan, page 52; .

[115] Page 53.

It is interesting to note that in Sloan's comments there is an appreciation that the multi-national corporation shares a common characteristic with terrorists, that is (to a certain extent) a rejection of this state-centric system. This rejection is by no means complete - both corporations and terrorists exists at a sub-state level in some degree - the corporation may seek the protection of the law of a state, and many terrorist organisations will rely on the protection and assistance of states - whether it be overt or semi-overt, or more covert.[116]

Although some might argue that multi-national corporations and terrorists groups stand at either end of a spectrum, the spectrum would still be that of a movement away from "state-centrism" and the concentration of coercive power in the state - with the danger that they each move so far away from one another that they meet up again.[117] Any ambivalence in allegiance or identification on the part of a non-state quasi-criminal or terrorist organisation towards a corporation could easily find its way into violent activity directed at the multi-national corporation. Such an ambivalence (and an appreciation of the vulnerability of a corporation) would be brought to the fore were a corporation to hire the same cyberterrorists to undermine its competitors (as Valeri points out) - a corporation willing to use such agents and to expose its insides to them puts itself at their mercy should the flow of money dry up or should the cyberterrorists then sell their services to another competitor or organisation which bids higher[118].

In addition, the multi-national corporation, through its existence on many planes of definition at one time, can at any time be seen to be on a similar plane with a sub-state or non-state actor, as well as being on a nation-state plane, thus attracting criticism and violence that would have been directed towards the identifiably "official" organs of the nation-state in previous times.

[116] Compare *The Nuclear Black Market* page 4.

[117] Compare Sloan, page 53.

[118] In the same way that governments unable to pay for their mercenaries during the 15th and 16th century Italian wars and the Thirty Years' War were held to ransom and worse by the *condottieri* they had helped to set up in positions of relative power - Rathmell, *Information Warfare,* page 4. Compare Molander et al pages 22 and 23; and Devost, pages 34 to 35, in which it is suggested that IW should be harnessed as at least a national resource.

As potential targets continue to be hardened in urban areas[119], the visible aspects of multi-national corporations are strengthened and more protected, then activities may move to rural and/or less protected areas.[120]

Many multi-national corporations have now "disaggregated their operations" (to borrow a term from another context) and have placed various aspects of that operation in different geographical areas (and even different countries).

A failure to strengthen and protect a particular part of that operation may cause incalculable damage to a multi-national corporation's network should a weak network node be attacked and disabled.[121]

[119] Sloan, page 59.

[120] Sloan, page 59.

[121] *A Two-Edged Sword*, page 1; Rathmell, *Cyber-terrorism*, page 8.

PART 3

CORPORATE RISK MANAGEMENT

This paper does not propose to present a comprehensive risk management survey for a hypothetical corporation. It does propose to deal with some technical issues relating to methods of attacking computer and information networks, and means of stopping or hindering such attacks.

It will deal in passing with some discrete problems that may be encountered in applying traditional forms of risk treatment to what is essentially a new form of risk, and it will then discuss the need for perhaps a new or revised approach to the risk management system of a corporation in respect of the new form of threat represented by computer terrorism.

Steele[122] has written an interesting paper on what he calls "information peace-keeping". He criticises previous approaches to the use of information for concentrating too heavily on IW and failing to consider the other side of the coin, information peacekeeping (IP). He defines the three elements of IP to be:

- Open source intelligence
- Information technology.
- Electronic security and counter intelligence.[123]

Interestingly, he considers that IP must rely almost entirely upon the private sector[124] for sources and services which will require the development of a new national intelligence and secure approach to take into account what has hitherto been an area in which the private sector has not participated.

He comments specifically upon the enmeshing phenomenon:

> "Perhaps the most important aspect of information operations in the 21st Century is that it is not inherently military; instead, civilian practitioners must acquire a military

[122] Steele, pages 143 to 144.

[123] Page 143.

[124] Pages 143 and 157.

> understanding and military discipline in the practice of information operations, if they are to be effective.
>
> Information peacekeeping is the act of exploitation of information and information technology so as to achieve national policy objectives".[125]

Common to all aspects of information operations (IP, IW and all source intelligence) is open source intelligence. This means that the involvement of the private sector will become more clinical in defence terms in the 21st Century. Along with this must go an increasing identification of the private sector with the defence establishment, both in its own perception and in the perception of outsiders.

IP is not:

- Application of information or information technology in support of conventional military peacekeeping operations (contrary to what some may seem to be RMA thinking).
- Traditional psychological operations or deception operations.
- Covert media manipulation.
- Clandestine human intelligence operations or overt research operations.[126]

If Steele is correct, then attempts to avoid the enmeshing phenomenon or to protest that private corporations are essentially that, private, and rely on this as a defence is unwise. It may also be futile.[127] In any event what is also important is the perception of the other entities with which the private corporation may come face to face (such as sub-State and non-State terrorist groups, the military forces of other nation States and also against other corporate competitors).

[125] Pages 145 and 146

[126] Page 154.

[127] Sloan, page 53.

IDENTIFICATION

The principal actors in any cyber terrorist attack upon a corporation, and the levels on which the attack may be made have been discussed above.

This section of this paper deals with the mechanics of attack and defence.

The United States General Accounting Office (GAO) has produced a report on information security and computer attacks at the Department of Defence[128].

It identifies the following means of attack:

- Installation of a malicious code in an electronic mail message sent over a network machine - as the sendmail program scans the message for its address, you will execute the attacker's code. Sendmail operates at the systems root level and therefore has all privileges to alter passwords or grant access privileges to an attacker.

- Password cracking and theft is much easier with powerful computer searching programs that can match numbers or alphanumeric passwords to a program in a limited amount of time. The success depends upon the power of the attacking computer.

- "Packet Sniffing" - an attack inserts a software program at a remote network or host computer which monitors information packets sent through the system and reconstructs the first 125 keystrokes in the connection. The first 125 keystrokes would normally include a password and any logon and user identification. The could enable the attacker to obtain the password of a legitimate user and gain access to the system.

- Attackers who have gained access to a system can damage it from within, steal information and deny service to authorised users.

[128] United States General Accounting Office, *Information Security: Computer Attacks at Department of Defence Pose Increasing Risks*, Chapter Report, 05/22/96, GAO/AIMD-96-84, May 1996, available at www.fas.org/irp/gao. The discussion of identification, treatment and technical treatment draws heavily upon this report.

- "Trojan Horses" - an independent program that when called by an authorised user performs a useful function but also performs unauthorised functions, which may usurp the user's privileges.

- "Logic Bomb" - an unauthorised code that creates havoc when a particular event occurs (for example, the dismissal of an employee or on a certain date).

It is becoming increasingly impossible for "low knowledge" attackers to use relatively cheap, "high sophistication" attack tools to gain access to what was, historically, a relatively impregnable system.[129]

The addition to this ready availability of high technology attack tools of an increasingly networked global economy, and the integration of corporations within that networked global economy, expedientially increases the risk of attack and the ability of any attacker to cause damage.

TREATMENT

In relation to cyberterrorism and IW, it would seem that treatment at the technical level and along the terms of the GAO report would seem to be most effective.

This has the following advantages:

- It may identify risks at the front end.

- It provides a corporation an opportunity to treat the risk in a technical way.

- It forms the foundation for an effective risk management place.

However, technical risk treatment should not be viewed as the final word in risk management of computer related risks. The GAO report shows that a tax on the US Department of Defence's computer systems (presumably one of the best protected systems in the world) shows that many attacks penetrate the system and even go unidentified at the very end after damage may have occurred.[130]

[129] Rathmell, *Information Warfare* page 3.

[130] Rathmell, *Information Warfare*, pages 3 and 6.

Effective technical risk identification and treatment remain the foundations of proper risk management of cyberterrorism and IW risks.

It does not remove the need for further treatment down the line.

AVOIDANCE

Avoidance is theoretically a perfectly acceptable form of risk treatment.

In practical terms, however, suggesting that a corporation avoid the use of computers in the very late 20th century is absurd.

TECHNICAL TREATMENT

Classified information can be:

- Protected on computers isolated from outside networks.
- Encrypted.
- Only transmitted on dedicated, secure circuits.

The US Department of Defence is working on other security measures, including:

- Firewalls (hardware and software components that protect one set of system resources from attack by outside network users) by blocking and checking all incoming network traffic.
- Smartcards - access cards containing encoded information, some kind of microprocessor and a user interface.
- Network monitoring systems.
- Automated biometrics system - these are in an experimental phase and are systems which examine an individual physiological or behavioural traits and use that information to identify an individual. Some systems are available at this stage but are still being refined for security users.

In spite of this, a vulnerability assessment carried out by the Defence Information Systems Agency showed that a large majority of computer attacks succeed in passing through the protection phase, the detection phase and also failed to be reported[131].

Further, attacks have caused considerable damage.

This has led to the development of guidelines for a good information system security program.

Conceptually, this can be set out at four levels:

- Vulnerability assessments.
- Correction of vulnerabilities.
- Reporting attacks.[132]
- Damage assessments.

The GAO Report identified certain steps that are important in the technical treatment of computer attacks:

1. Clear and consistent information security policies and procedures.[133]
2. Vulnerability assessments to identify security weaknesses at individual installations.[134]
3. Mandatory correction of identified network/system security weaknesses.
4. Mandatory reporting of attacks to help better identify and communicate vulnerabilities and necessary corrective actions.
5. Damage assessments to re-establish the integrity of information compromised by an attacker.

[131] Rathmell, *Information Warfare*, pages 3 and 6.

[132] Rathmell, *Information Warfare*, page 6.

[133] Molander et al, pages 19 and 20.

[134] Molander et al, page 20.

6. Awareness training to ensure that computer users understand the security risks associated with networked computers and practice good security.

7. Assurance that network managers and system administrators have sufficient time and training to do their jobs.

8. Prudent use of firewalls, smartcards and other technical solutions.

9. An incident response capability to aggressively detect and react to attacks and track and prosecute attackers.[135]

Although this study was carried out in the context of attacks on Defence facilities, there is no reason why the principles outlined in the study could not be applied to private corporations.

An overturning of current management perceptions may also be necessary.

INSURANCE - WAR, TERRORISM AND NUCLEAR RISKS EXCLUSIONS

IW and cyberterrorism present some problems in relation to insurance.

Most standard policies will have a war exclusion and a nuclear exclusion.

A typical example of a war exclusion is as follows:

> "... this Policy does not cover damage to any Property Insured caused directly or indirectly by or in connection with or arising from or occasioned through:
>
> 6.1.1 war, invasion, act of foreign enemy, hostilities (whether war be declared or not), civil war, rebellion, revolution, insurrection or the use of miliary or usurped power,
>
> 6.1.2 any order or any Government, Public or Local Authority involving the confiscation, nationalisation, requisition or damage or any property,
>
> 6.1.3 ionising, radiations or contamination by radioactivity from any nuclear waste or from the combustion of nuclear fuel. Nuclear fuel means any material which is

[135] Molander et al, page 33.

capable of producing energy by a self-sustaining chain process of nuclear fission,

6.1.4 nuclear weapons materials."[136]

Standard extended perils fire and property policies may include riot and civil commotion.

The war exclusion was introduced after a large amount of claims arising out of widespread damage caused in the Spanish Civil War[137].

At first glance, it would seem that IW and cyberterrorism would fall within the exclusion clauses of a standard policy.

"Civil commotion" in the context of the Gordon riots of 1780, was defined as "an insurrection of the people for general purposes, though it may not amount to a rebellion, where there is usurped power"; Mansfield CJ, *Langdale v Mason* Park, 968.

Something more than a transient general civil disturbance is necessary [*The Village Belle* 30 LT 232; *Bolivia Republic v Indemnity Mutual Marine insurance Co* [1909] 3 KB 411].

The situation in Beirut in 1976 constituted "civil commotion": *Spinney's Centres and Doumet v Royal Insurance Co* [1980] 1 Lloyd's Rep 406.

Presumably, *physical* attacks by disaffected parts of a community upon a computer system would constitute civil commotion and would therefore be covered. Importantly, damage to *data* on computers may not be property damage within the terms of a property damage policy: *Switzerland Insurance Australia Ltd v Dundean Distributors Pty Ltd* (1998) 10 ANZ Ins Cases 61-388.

[136] Industrial Special Risks Policy Mark V, Clause 6. It should be noted that the ISR Policy also has certain exclusions relating to computer related crime - it is not the place to discuss the nature of the cover in detail here - the ISR has a convenient example of a war and nuclear exclusion, similar to those in standard fire and extended perils policies. The nuclear exclusion clause is common to the vast majority of insurance and reinsurance contracts.

[137] Perry. M, *A Model for Efficient Foreign Aid: The Case for the Political risk Insurance Activities of the Overseas Private Investment Corporation*, [1996] 36 Virginia Journal of International Law 510, page 531

An organised conspiracy to commit criminal acts is *not* a "civil commotion": *London & Manchester Plate Glass Insurance Co v Heath* [1913] 3 KB 311; *Levy v Assicuranzi Generali* [1940] AC 791.

"Civil war" occurs when "a party arises in a state which no longer obeys the sovereign, and is sufficiently strong to make head against [the sovereign], or when, in a republic, the nation is divided into two opposite factions and both sides take up arms": *Brown v Hiatt* 1 Dillon 379. In Beirut in 1976, massive civil strife had not progressed to a state of internal strife between opposing sides and a civil war exception in an insurance policy did not apply: *Spinneys* (cited above).

A state of "war" exists "when differences between states reach a point at which both parties resort to force, or one of them does an act of violence, which the other chooses to look upon as a breach of the peace": *Driefontein Consolidated Gold Mines v Janson* [1900] 2 QB 339.

"War" in the context of an insurance policy does not have a technical meaning[138], and civil strife in Dublin in 1916 was held to be "war" within a policy: *Curtis & Sons v Matthews* [1919] 1 KB 425. An act of retaliation on the part of Israeli government forces against aircraft at Beirut airport was held obiter by the House of Lords not to constitute "an unprovoked or accidentally provoked incident arising during the course of the Assured's operations between Israel/Arab countries", nor did it occur "during the normal course of the Assured's operations *over* Arab/Israeli territory" [emphasis added] within the terms of an alleged coverage clause: *American Airlines v Hope* [1974] 2 Lloyd's Rep 301; compare *Pan American World Airways Inc v Aetna Casualty and Surety Co* [1975] 1 Lloyd's Rep 77.

"Terrorism" can be excluded by a clause excluding "any activity of any organisation the objects of which are or include the overthrowing or influencing of any *de jure* or *de facto* government by terrorism or by any violent means" (see *Spinney's*, cited above).

The nuclear exclusion will not be discussed in detail since its terms are clearer.

The nature of IW and cyberterrorism is discussed above.

[138].*Kawasaki Kisen Kaisha v Bantham SS Co* [1939] 2 KB 544; *Kuwait Airways Cpn v Kuwait Ins Co* [1996] 1 Lloyd's Rep 664.

Damage caused by criminal conspiracies to destroy computer networks might not be covered by a fire and extended perils policy since:

- Data may not be "property" within the terms of the policy.
- Damage (even consequential) caused by attacks may not fall within the civil commotion cover.

Terrorism is more difficult:

- If directed at a government, it would be excluded by a clause such as the one above.
- If directed at a private corporation, it would not be excluded since the corporation is not a government.

Similar problems in relation to destruction of data will apply.

Damage caused to private corporations during a war will be excluded, but at what stage will a "war" be considered to have commenced? As discussed above, some countries employ terrorism as a means of foreign policy actualisation. Whether "state-endorsed" or not, damage caused by this sort of terrorism may fall outside the war exclusion, and also outside the terrorism exclusion.

Damage caused by sub-state pressure groups such as anti-fur activists should also be covered on the same logic.

Obviously, damage caused by nuclear weapons or material will be excluded, but damage caused by electro-magnetic pulse attacks[139] may not be.

This very brief survey shows that insurance may only provide very piecemeal and fragmented cover to the sorts of threats posed by IW and cyberterrorism. There is cover available in the insurance market for computer data damage and the sort of perils that might be the result of an IW attack upon a corporation - the clauses are relatively straightforward in what they cover, although they risk being branded as "exotic" and hence not treated by many risk management

[139] O'Hanlon, page 6; Rathmell, *Cyber-terrorism*, page 6;. Devost pages 9 to 10.

strategies(see below). This discussion centres upon the additional problems which may be encountered in relation to any policy in the event of an unwelcome, aggressive intrusion.

In addition, financial damage caused by the crashing of networks after undetected attack on a computer system will generally not be covered in the absence of some financial risk cover.

To some extent, the fragmented insurance picture is a product of the lack of necessity of society, and of the insurance market as a part of society, to deal with the sorts of problems and threats posed by cyberterrorism. A radical rethinking of insurance cover, and indeed, of the efficacy of the mechanism of insurance itself, in dealing with cyberterrorism and computers will be necessary.

Corporations will no longer be able to rely on insurance to provide a relatively complete risk management programme - if they ever really were able to do it on the past.

In view of the discussion above as to the various levels and various mechanism of IW and cyberterrorism, it is conceivable that damage caused to a corporation's property by some forms of cyberterrorism are not "war, act of foreign enemy, hostilities (within the context of the exclusion)" or otherwise.

It follows, therefore, that standard war and nuclear exclusions should perhaps be redrafted to take into account acts of cyberterrorism and IW, provided some adequate definition can be agreed on in the first place.

This is not to say that war itself is not insurable.

There are forms of marine political risks coverage which include war cover and similarly in respect of energy political risks coverage[140], and terrorism risk itself has been the subject of a UK insurance pool arrangement[141].

Nevertheless, such insurance could be considered "exotic" and is not exactly cheap[142]. Although it is good for risk management purposes that insurance might exist, there is perhaps

[140] Brownlees, K, *Credit Where Credit is Due*, Reinsurance, June 1996, page 17; Wagner, D, *The resurgence of political risk insurance*, (1997) 44 Risk Management pages 56 to 58.

[141] Beatty, A, *Bombs Away?*, Reinsurance, August 1998, page 18.

[142] Brownlees, page 17.

a psychological problem with it being branded "exotic" - for risk management purposes, the risk of cyberterrorism itself may be retrospectively identified as exotic and therefore not considered in risk management audits and in the purchase of insurance.

It follows from the discussion in this paper above that cyberterrorism and IW should not be considered exotic any more, and should be placed progressively on the checklists of those who perform risk management audits and should be firmly in the mind of any person involved in risk in an organisation.

Nevertheless, such a risk requires specialised knowledge and it may only be able to be dealt with properly on an international market.

FINANCIAL RISK TREATMENT

Cyberterrorism and IW risk might be better treated by some form of financial risk treatment, such as:

- Hedging.
- Double trigger mechanisms.
- Other forms of alternative risk transfer, such as shock loss capital raising.[143]

This paper is not the place for a detailed discussion of the various forms of all alternative risk transfers that are emerging in the capital markets, but the option should always be considered.

It should be stressed, however, that insurance or financial insurance is not risk minimisation, but rather risk transference.

The importance of attempts to minimise risk at the "front end" should be stressed and insurance and financial risk treatment only perform at their best when part of an integrated risk management plan.

[143] McVeigh, J and Wood, P, *Asia - Where Go the Dragons: Crisis or Correction*?, Corporate Risk, May 1998, pages 42 to 44; see also papers published by Swiss Re New Markets Division, *New perspectives: risk securitisation and contingent capital solutions*, *Corporate risk financing - the emergence of a new market*, and *Integrated Risk Management Solutions - Beyond traditional reinsurance and financial hedging*, all available at www.swissre.com.

COMMUNITY RESPONSE

Arguably, in view of the progress of the integration of the world economy (or at least that of the developed world) into computer networks and onto the internet means that cyberterrorism and information warfare should really be dealt with as a community matter.[144]

The effects of cyberterrorism on IW could be catastrophic to a community at large, and the costs could also be extreme.[145]

There is theoretically no reason by the private sector should alone bear the costs of treatment.

However, the mere fact that a matter *should* be dealt with at a community level does not mean that they *will* be. Although the community is ultimately the reinsurer of such a risk, it would be foolhardy of any corporation to leave management to the community.

The community is often slow to respond and in the absence of any perceived risk (but from some "doomsayers"), there would be no incentive upon the community to attempt to treat the risk.

In any event, increased costs to corporations in treating cyberterrorism and IW risk could theoretically be passed onto the consumer - the problem for a corporation is the unevenness in application - a prudent corporation that spends large amounts on management of such a risk may not be able to pass the cost on to consumers if other competitors fail to treat the risk and are able to provide cheaper services.

[144] Molander et al, page 19.

[145] Molander et al, page 9.

PART 4

A REVOLUTION IN APPROACH?

Management of cyberterrorism risk must be considered an important issue for all aspects of society, not just corporations. However, in view of the way in which the information network has developed, and the almost complete immersion[146] of much of private enterprise in it, a corporation should analyse its vulnerabilities regardless of societal views.[147]

The dangers in failing to recognise the risk could be serious.[148] The dangers in recognising the risk but not treating it could be equally serious.

It is submitted that, traditionally, corporations have been viewed as organised, and in fact have been organised, in a hierarchical way. Much like a Norman *motte and bailey* castle, where a keep on a central raised mound was encircled by a ditch and a picket, corporations are viewed as entities which are, or should be impervious to the outside world, allowing entry only at designated, protected points. Once within the structure, movement up to the pinnacle of command is meant to be within certain set parameters, and deviation from these parameters is not encouraged.

Flat management structures, it is submitted, merely make the internal passage within the corporate entity somewhat less linear. Flat management does not allow for free ingress from the outside as one of its goals - it may allow for more points of contact between points inside the structure and outside, but these are monitored and controlled.

Over the years, layers of protection have accreted around the structure, much like the walls that were thrown up around the keeps of concentric castles. All of these concentric defences repeat the pattern of controlled and protected points of ingress and egress.[149]

The growth of the information network and the increasing porosity of corporate entitles must lead to a rethinking of the reliance on concentricity and control of entrances.

[146] Compare Metz, page 67.

[147] Thomas, page 3.

[148] Thomas, page 2;

[149] Compare Devost pages 30 to 31.

Corporate entities must have new points of ingress (such as telephony and internet access points) - consumers demand it. Added to this intentional accumulation of entry-points must be those that are either unwittingly left open by a corporate entity, because the advances of technology are not understood, and those which are left open through intention or negligence, where the possibility of unwanted or uncontrolled ingress is appreciated, but nothing is done about it.

Of course, attention should also be paid to points of egress -much damage can be done by an information outflow caused by a disgruntled employee.[150]

Mongol armies were able to defeat many countries in a very short amount of time in the 13th century.[151] Among these were many Western countries with relatively strong standing armies and well-developed defence systems based around a system of fixed castles.

This is a classic example of the collision between a hierarchised force and a networked force - the static defensive system of the West was no match for the fluid, amorphous attack of the Mongols.

If 20% of a mediaeval regiment were eliminated, it is submitted that the regiment would have an extremely hard time responding to further threats, and of doing anything other than fleeing. This would be compounded if a commander were killed. The chains on command and information flow could be critically hampered.

In contrast, eliminating 20% of a Mongol horde would not necessarily impair the ability of the network to function, and even content the conflict until victory. Various commanders, and diversified information and command networks would mean that the group could very quickly regroup and continue essential functioning.

The Mongols provide an interesting analogy for the corporation.[152]

[150] Rathmell, *Information Warfare*, page 3; Valeri, page 2.

[151] Aquilla and Ronfeldt, page3.

[152] Compare Molander et al, pages 10 to 13; Steele, page 151.

A hierarchical corporation, based on a fortress structure, may be vulnerable if an information flow is disrupted. This may be so even where a flat management structure exists within the fortress. The entity may be hard put to regroup and function without great delay[153].

A corporate entity based on a network may be much better placed to respond to a potentially disabling attack. Diversified information and command lines[154] could be called into action and utilised should one line be cut. Such a corporation would be able to continue its core operations in a much shorter timeframe than a defensive-fortress structure.[155] This does not mean to say that a corporation should abandon all controls of ingress and egress, and "open its doors" to the world. Defences from cyberterrorism should be put in place. This discussion highlights the first primary step in risk management - identification.

Potential threats should be identified and provided for. A simple treatment of defensive structures may not be wise, since with the chaotic nature of the information network and the development of new technologies will inevitably mean that new forms of attacks and new holes in the armour will always open, often in unexpected places.[156]

A diversified command and control structure, and the duplication of information supplies may go some way in both treating current risk, and coiping with problems when unforeseen or currently non-existent risks appear.

[153] *Old Madness, New Methods: Terrorism Evolves Toward "Netwar"*, RAND Review, Winter 1998/99, RAND Organisation, available at www.rand.org/publications/RRR, cover story.

[154] Devost page 23.

[155] Devost pages 32 to 33.

[156] Rathmell, *Cyber-terrorism*, page 8.

CONCLUSION

It can be seen that the development of the Internet presents serious threats to the security of the corporation, in addition to the much touted opportunities.

It may be that the more extreme scenarios discussed above may never eventuate - the possibility that they may must be appreciated. It is not advisable for any risk management approach to merely disregard the threats discussed on the basis that they are far-fetched and fanciful - in additional to being technically feasible, either now or in the next two decades or so, the ability of intruders to gain entry to computer systems and disguise the very fact of entyrt makes this a peculiarly difficult threat to appreciate - he undetectability of many attacks per se may lead corporations to a false sense of security, and leave the corporation vulnerable to serious disruption of total disablement in the event of an attack.

As competition between corporations for profit increase, and consumer expectations grow, there may soon be a time that, for some corporations, even a limited disablement may be fatal or nearly so to its continued existence, surely one of the most important post-threat outcomes of any risk management plan.

The growth in the number of aggressors must also be appreciated. Added to the traditional aggressors identified by a corporation are the additional ones that may now see the corporation as a visible surrogate of an entity that is either impregnable from attack or that it is inadvisable to attack.

Some corporations have always been the target of aggression, and the identity and number of aggressors may stay the same. It must be appreciated, however, that new, and very powerful, tools of aggression may now be available to those traditional aggressors.

Traditional forms of risk management are, it is argued, not particularly suitable to the dynamic, disaggregated forms of aggression that will now be presented.

It is submitted that there will need to be a revision of the approach to the determination of risk and the treatment, and allied to this will need to be a fundamental rethinking of the way corporations organise themselves, and the way they present themselves to a risk. Traditional forms of risk management represent an approach positioned in a hierarchical paradigm, and may not deal adequately or at all with new forms of threat posed to a dynamic network.

Until these fundamental issues are addressed, no corporation can truly say that it has identified all forms of risk that are or will be relevant to that organisation.

Nor will it be able to say that it has treated them.

These must be imperatives in an environment where any single risk could conceivably threaten the entity's very survival.