New Zealand Government and Critical Infrastructure Ready Reaction to Cyber Terrorism

Allan Charles Watt

A thesis submitted in fulfilment of the requirements for the degree of Master of Science in Forensic Science.
The University of Auckland, 2008.

Abstract

The purpose of this research is to obtain input from government agencies, elements of the critical infrastructure and cyber space, to determine what level of knowledge on cyber terrorism exists. Furthermore, are there ready reaction plans in place, and is staff-awareness training conducted on a regular basis? This probably won't prevent or stop an attack of cyber terrorism, and like any other disaster in the IT world, if contingency planning exists, recovery can be quicker and greater mitigation of costs.

Interview questions were distributed to New Zealand government departments and elements that make up the critical infrastructure, to obtain an insight into the current situation. From this and other comparisons, inferences have been drawn to determine that if some of the groups were targeted would the fact that they could be deficient in knowledge on cyber terrorism, make the effect more intense and longer lasting. It has also provided the state of knowledge, the level of planning and the general readiness that currently exists.

In view of these findings recommendations have been made that will ensure there is consistency across the all organisations, both government and non-government. All organisations, including the government, are reliant on the critical infrastructure and the internet for both operational and domestic survival. It is therefore pertinent that agencies give some consideration to these findings.

Acknowledgments

A Masters Thesis is certainly a task that is complex and time consuming, especially with a topic as enlightening as cyber terrorism. What better supervisor could one have had than Dr. Lech Janczewski, who is fast becoming a world renowned author on the subject. His guidance and assistance has been outstanding.

Due to the nature of research and the sensitivity that surrounded the answers sought, many of the participants approached, were not willing to stand up to the plate and participate. It would have been an opportunity for them to provide some valuable input to what is happening in the real world. Cyber terrorism is very real and it is only a matter of time until a catastrophic event occurs that impacts on peoples lives. For those who took the time to participate thank you, for without your response there would have been no research.

To my forensic peers who have reached this level and beyond, thank you for your motivating support.

To my family; I am back. Thank you for your patience and support, it is encouraging and helps build strength and everlasting bridges. To my beautiful wife Carol, thank you.

And now; "*To PhD, or not to PhD, that is the question*".

Table of Contents

Table of Contents cont.

Table of Contents cont.

List of Figures

Chapter 1. Introduction

1.1. Chapter objective

The objective of this chapter is to provide an introduction to the thesis. It will first identify the problem space, in that it will look at identifying the essence of the problem. It will then look at why the research is being conducted, and in doing so will define the research purpose and objective. The chapter will then look at why the research is important and give an outline of the thesis.

1.2. The problem space

Terrorism as it is known has existed for many years in various different forms. Much of it has been religion-based and/or originating from developing country's radical groups, targeting developed free world countries. As a result of the attacks of 11 September 2001, known as the 9/11 attacks which resulted in the destruction of the World Trade Centre buildings in New York, and other attacks on that day, an irreversible change took place.

These attacks did exactly what they were designed to do, and that is to send a message and to create fear and terror. International travel has changed for ever and so has the point of awareness on the entire issue of terrorism. Governments and large corporations around the world have now become security conscious. Many government departments and corporations are now employing Intelligence Analysts to constantly update management and leaders with advice on security, and any concerns that could have an impact on their entity. The ultimate focus though is to seek intelligence on any potential threats of terrorism, conduct threat assessments and then create counter terrorism measures to either prevent an act occurring or eliminate the terrorists before they act.

Though this may be very effective, it is likely this will also be overcome, like a mutating virus. Terrorists will become wiser and will divert their attention to more complex and sophisticated acts. What better way than to remotely, from any part of the world, conduct an act of terrorism, through the use of the many digital pathways that most governments and large corporations are connected to.

In the digital age, society has become permanently reliant on electronic devices to manage this modern world, most being computers that manage everything from water and sewage management to conducting surgery in hospitals. Attacking any of these systems with the agenda to create terror, plus a few other ingredients is an act of terrorism, being cyber terrorism. The fact that it is a computer that has been the primary victim of the attack, has no bearing on the issue, it is still an act of terrorism. The public at large will ultimately still be the victims and this entire issue is something that must be addressed by management and not passed off to the IT department because it is too hard to understand or comprehend.

Cyber terrorism is a new and emerging threat to the stability of the world.

The viability and stability and control of a country are made up of many components. These include central government, local government and the critical infrastructure that the public and the country require the services of to operate on a daily basis.

As mentioned these elements are reliant on computer systems, for management, control, communication and operations. Should some or all of these organisations have their systems incapacitated as a result of a malicious IT attack, the flow on effect could be costly and disadvantage many, if not totally disrupt the normal operations of everyone within the country.

The Government has agencies such as Centre for Critical Infrastructure Protection (CCIP), who purpose is to monitor security threats and formulate advice and policies for government agencies and any other organisation that is interested.

There are numerous government agencies, each with their own security officers, and many of these are partnered with privately owned organisations that form the critical infrastructure in New Zealand.

Communications, management and control of the country and the infrastructure are now absolutely reliant on the Internet and cyber space. To connect to cyberspace a connection is required either through a direct cable link to a Telecommunications Company (Telco) or to an Internet Service Provider, (ISP). The Telcos and ISPs are also privately owned and are therefore profit-driven as opposed to service driven. The prime goal is to provide continued operation to clients where possible, and security is not a prime focus of these organisations. They are also not required by legislation to abide by directions of CCIP.

So this leaves a problem whereby central government that dictates policy may be prepared, but the critical infrastructure that is privately owned, may not be.

Before any of the organisations can be ready reactive to cyber terrorism, it is foreseen that they should first have knowledge and understanding of what cyber terrorism is and what catastrophic fallout could occur in the event of an attack.

> **The first problem then is: Do the organisations have knowledge of what cyber terrorism is?**

There is a well known management term, “If you fail to plan, you plan to fail”. This also goes for counterterrorism and counter cyber terrorism, in that planning is an essential part of surviving an attack.

> **The second problem: Do the organisations have ready reaction plans in the event of a cyber terrorism attack?**

As outlined above it is critical that counter cyber terrorism planning be conducted, but beyond this, staff need to have knowledge and awareness-training to recognise the warning signs that an attack is under way.

The third problem is: Do the organisations conduct staff-awareness training in preparation should an event of cyber terrorism occur?

Continually IT professionals and even the average user attempts to stay ahead of new security threats to their computers, by updating antivirus software. New threats in cyber terrorism could just as easily occur on a regular basis. Intelligence gathering, information sharing and knowledge seeking on new threats, are all seen as important steps in staying ahead of attackers.

The fourth problem is: Do the organisations have knowledge and have intelligence gathering occurring into cyber terrorism?

Much of the critical infrastructure is now privately owned. As a result these organisations have commercial drivers to maximise wealth for the shareholders. Security is something they have to have to do, so to avoid a loss of provision of services and hence loss of. The drivers are therefore different as opposed to governments', in that theirs is for national security. Hence security may be more for look than feel. It is possible then the level of knowledge and planning for an event of cyber terrorism is likely to be far lower than that of government departments.

CCIP is a government agency and most of the critical infrastructure is privately owned. The private entities have no legislative requirement to abide by any direction of the government, unless there is a state of emergency at the time. So, provided an organisation can function and deliver services, it can carry on even if it poses a threat to the safety of persons or property.

The fifth problem is: Are the privately owned critical infrastructure elements being influenced by CCIP to ensure a common level of security is met, and is the level of planning way less than their government counterparts?

It is therefore considered that if these problems do exist at a major level, then New Zealand could be at risk of being severely effected, should an act of cyber terrorism occur.

1.3. Research purpose and objective

The purpose of this research is by way of obtaining input from government agencies, elements of the critical infrastructure and cyber space to determine: do the problems outlined exist.

A collective analysis will provide an insight into the current situation. From this and other comparisons, inferences can be drawn to determine, if some of the groups were targeted, would the fact that they could be deficient in knowledge on cyber terrorism, make the effect more intense and longer lasting.

Therefore from the cross section of data obtained it can be established, what level of knowledge on cyber terrorism exists, are their ready reaction plans in place and is staff-awareness training conducted on a regular basis. This probably won't prevent or stop an attack of cyber terrorism and like any other disaster in the IT world, if contingency planning exists, recovery can be quicker and greater mitigation of losses.

Moreover, one of the purposes is to compare the results between government agencies, the critical infrastructure and ISPs, to determine if there is a consistent level of readiness across the three separate groups, and are the privately owned entities influenced by the agencies such as CCIP.

It is seen that if ready reaction exists, then this should also provide early warning. This should then result in an attack having less impact on the disruptions to services and loss to life or property, should the latter be a consequence of an attack. Not that any significant cities bounder a major dammed river within NZ, however as a scenario, the following could all be a result of an act of cyber terrorism: 'a dam management company is infiltrated, the dam control system accessed, and the flood gates opened, damage to property through flooding, possible loss of life through drowning and loss of power generation though lack of water'.

This scenario would be an extremity, but one of the purposes of planning, (Thomas, T. 2003), is to have contingences for worst case scenarios. Determining this is within the purpose of this research.

So a clear statement on the purpose of this study can be formulated. The research objective is:

- **To determine the state of the New Zealand Government and critical infrastructure ready reaction to cyber terrorism.**

1.4. Why is this research important

The protection of New Zealand’s government secrets, the critical infrastructure resources and communications path-ways are paramount for continued sustainability in the normal operation of people’s lives. Disruptions to any of these and this sustainability can break down.

The collection of the research material will identify if holes exist in the protection of these resources though lack of knowledge, preparation and planning. If they do then the government may be able to take some steps to rectify what could be seen as a major threat to continuous, harmonious operations within New Zealand.

1.5. Outline of Thesis

Overall the thesis will explore and close the gap between conventional terrorism and cyber terrorism.

Initially a literature review is conducted where it is defined what leads to terrorism and what is cyber terrorism. The motivators and the ingredients are further looked into and then a discussion on the types of potential acts that could have an impact. The importance of planning is then discussed and then a description on the NZ Government’s and elements of the critical infrastructures, understanding and readiness for cyber terrorism.

It will then involve a critical analysis of the results. Planning is an important discipline in any activity and the level of planning is seen as a crucial component in the protection of resources. The degree of planning will also be addressed and then contrasted against other international agencies and a comparison of the collected standards against other international research.

This Thesis is divided into 6 chapters as follows:

Chapter 1. Introduction

This chapter provides and introduction of the problem space, the purposes and objectives and why the research is so important. It concludes with a section on an outline of the Thesis.

Chapter 2. Literature review

This chapter commences with a number of definitions, firstly on what crime is and then progresses through an act of war and then to terrorism. This then leads to the information technology sections where further definitions are provided on items such as information, through to cyber terrorism it self. The risks and what could be the potential outcome from an attack is then discussed. What's more, why it is important to have planning and information sharing to assist with combating cyber terrorism?

Chapter 3. Background information

This chapter introduces the sample and provides an introduction to the New Zealand Government structure and the elements that make up the New Zealand critical infrastructure.

Chapter 4. Methodology

This chapter will discuss the approach adopted to deal with the research questions. It will also define how the study will be undertaken and how the data will be obtained. It then describes what data needs to be collected to provide the answers to the research questions and satisfy the research.

Chapter 5. Discussion and analysis

This chapter then discusses the results provided by the respondents and then analyses them to determine if they have provided the answers sought to satisfy the research questions.

As well as assessing the responses to the questions, what is equally important is assessing, what the New Zealand Government is doing with regard to planning for cyber terrorism and the how the results collected compare with other countries. The focus of this then being: is there an international benchmark for planning on cyber terrorism and where New Zealand fits on that benchmark

Chapter 6. Conclusions, limitations and further research

Finally this chapter will provide an overall conclusion of the results to satisfy the research objective of: To determine the state of the New Zealand Government and critical infrastructure ready reaction to cyber terrorism.

1.6. Conclusion

This chapter has provided a general outline of the project. It then went on to identify the problems and the research questions, which lead to the purpose and objective of the research. An outline on the structure the thesis was then provided.

Chapter 2. Chapter Literature Review

2.1. Chapter objective

It is important that prior to discussing the more in-depth aspects of cyber terrorism, some of the other elements that form part of it are defined. This has been primarily done so it contrasts the differences between a “crime”, an “act of war” and “conventional terrorism”, before discussing their counterparts in the information technology arena.

Hence the starting point is a criminal act, this being a crime. This chapter will then progress though an act of war and on to terrorism and then into the various cyber elements ultimately ending with cyber terrorism and its components.

2.2. Terrorism

This section will focus more on conventional terrorism to provide a platform for advancing on to more complex issues.

2.2.1. Crime

A normative definition views crime as deviant behaviour that violates prevailing norms, specifically, cultural standards prescribing how humans ought to behave. (http://en.wikipedia.org/wiki/Crime)

Without going into a massive legal discussion, many of the laws, be it theft, murder or terrorism have resulted from what society saw over the many years as being moral issues. Things above the law were seen as the “Norms” hence acts that were carried out by people that were less than this and raised issues against morality in essence become law. Over time these have become entrenched by governments into statute.

Hence the definitions are legislative and not so much normative. So a crime is a crime because the law says so.

*Crime means an offence for which the offender may be proceeded against by indictment. (*The NZ definition from the Crimes Act 1961)

An indictment being:
"a formal accusation against an accused. An indictment is drawn up by the Crown once it has been determined that an accused will be tried in the indictable jurisdiction, listing the counts against the accused."

2.2.2. War

What then is war?

> "A state of usually open and declared armed hostile conflict between states or nations" (http://www.answers.com/)
>
> "The object of war is not to die for your country but to make the other bastard die for his."
> *General George S. Patton* (http://thinkexist.com)

Or
"Ultimately the object of war is victory".
*MacArthur (*http://en.wikiquote.org/wiki/Douglas_MacArthur)

From history it is understand, and comprehended that war is as in World War 1, World War 2 and Vietnam. Where armies fought armies for control of land or resources and the conflict usually lasted for years. Terrorism in contrast may be one person and last for minute.

2.2.3. Terrorism defined

The prime focus is that of terrorism and to reflect then, what is the difference between this and the former two items of crime and war.

As put by the US Department of State:

> 'The term 'Terrorism' means the premeditated, politically motivated violence perpetrated against non-combatant targets by sub national groups or clandestine agents, usually intended to influence an audience. Non combatant to include, in addition to civilians, military personnel who at the time of the incident are unarmed and/or not on duty.' (Nelson, B., Choi, R., Lacobucci, M., Mitchell, M., & Gagnon, G. 1999).

The FBI is more direct as follows:

> 'The unlawful use of force or violence against persons or property to intimidate or coerce a Government, the civilian population, or any segment thereof, in furtherance of political or social objectives.' (Nelson, et al. 1999).

The US Department of Defence however has a definition that is perceived to the one mostly recognised worldwide and is as follows:

> 'The calculated use of unlawful violence or threat of violence to inculcate fear: intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious or ideological'. (Nelson, et al. 1999).

The principle difference with this definition is the mention that an act's primary function is intended as creating FEAR. This thesis also has construed that this is also one of the key factors of terrorism, in that the acts are usually intended to create fear so to influence the public or government's decision making. This is also one of the principle differences between an act of war and an act of terrorism: there is usually no intention to succeed by ultimately seizing and taking over a country, but as identified, influence the country by violent acts which create the resulting fear.

Many earlier definitions were not as refined and are more of a differentiation between an act of war and something else acts that was politically motivated by someone other than a member of the Armed forces and were hence labelled as acts of terrorism. (Devost, M. G., Houghton, B. K., & Pollard, N. A. 1996). It was also once thought that an act of terrorism had to be undertaken by a foreign body or non-national of the country in which the act was directed toward, however as will be discussed later cyber terrorism has no boundaries, as facilities such as the internet have removed them and again rejoined the world to a single mass of **Gondwanaland**.

A New Zealand definition is covered in the Terrorism Suppression Act 2002. It is essentially a legal definition as it is derived from the legislation.

The definition in essence identifies that:

A terrorist act is an act intended to cause, in any one or more countries, the death of, or other serious bodily injury to, one or more persons (other than a person carrying out the act):

> "a serious risk to the health or safety of a population:
> destruction of, or serious damage to, property of great value or importance, or major economic loss, or major environmental damage, serious interference with, or serious disruption to, an infrastructure facility, if likely to endanger human life:
>
> introduction or release of a disease-bearing organism, if likely to devastate the national economy of a country. or
>
> The act is an act against a specified terrorism convention as defined, or the act is a terrorist act in armed conflict as defined".

From these definitions it can be seen then that the New Zealand's definition is far wider and covers aspects such as those affecting the country's economy.

Terrorism is “Transnational crime”, being, the, Reaching beyond or transcending national boundaries: “the transnational ramifications of terror networks” (http://www.answers.com/topic/transnational).

Transnational crime is the founding component of terrorism. Shelly, L. (2003), identified that, the merger of transnational crime, terrorism and corruption is profound. The concept that these ideas can be discussed separately is problematic. Highly corrupt societies give little opportunity for legitimate social mobility and their high level corruption is a deterrent to economic growth and investment. Under these circumstances, the employment opportunities of transnational crime groups provide a desirable economic alternative to youth without legitimate opportunities. Terrorist groups flourish in environments where youths have limited chance for advancement within their societies.

The phenomena of transnational crime, terrorism and corruption are all too often viewed as separate phenomena. These phenomena have grown in tandem because the economic and political conditions that give rise to these phenomena are quite similar.

Terrorists and transnational criminals use many of the same strategies to promote their operations, chief among these being the use of information technology to plan and realise their activities.

Most transnational crime and terrorist groups are based in transitional and developing countries. This is well known as a result of the war of terror, through the conflicts with Afghanistan and Iraq.

To further categorise an act of terrorism a number of elements are needed, that is to contrast it further from either a simple crime or an act of war.

The Symantec Security Response white paper on cyber terrorism, (Gordon, S., & Ford, R. 2003), identifies the following elements and gives an example from two different and known terrorist groups:

	LTTE	**AUM**
Perpetrator	Group	Group
Place	Sri Lanka	Japan
Action	Threats/Violence	Violence
Tool	Kidnapping/Harassment	Nerve Gas
Target	Government Officials/Recruits	Legislature/Imperial Palace
Affiliation	Actual/Claimed	Actual/Claimed
Motivation	Social/Political/Change	World Domination

Figure 1: The Symantec Security Response Example on Cyber Terrorism, (Gordon, S., & Ford, R. 2003).

These elements are then seen as the key components that determine the ingredients required to qualify the existence of terrorism itself. Should all of these not be satisfied then it could render it being simply just a criminal act.

When the elements are examined in these categories in terms of the definitions provided by the government agencies, it can be see there is congruence between the terrorism event and the definitions used by the various agencies tasked with providing protection.

The United States Department of State (DOS) defines terrorism as “premeditated, politically motivated violence perpetrated against non-combatant targets by sub national groups or clandestine agents”. Thus, the activities of both of these groups fit the DOS criteria for “terrorism”.

So to be a terrorist act, it must be against non-combatant troops, this then eliminates terrorism from being acts of war by this definition.

Beyond the definition of terrorism are the various types of terrorism that can be categorised. It is these categories that are then the motives that drive terrorists to commit their various acts.

Nelson et al, have determined that a number of groups or categories exist within the definitions of terrorism. These are:

Ethno-Nationalist/Separatist (ENS) Terrorism

ENS terrorists principally seek to achieve political autonomy, usually in the form of a separate state, or work towards the "elevation of the status of one communal group over others". Nationalist groups may also work "to oppose foreign influences in their countries". Both the Basque Fatherland and Liberty (ETA) and the Irish Republican Army (IRA), are examples of this type of terrorism.

Revolutionary Terrorism

Revolutionary terrorists, an example of this is the Red Army Faction in Germany, seeking to overthrow established governments as part of a broad program of social transformation. Although the political ideologies of the revolutionary terrorists can range, they are generally leftists. In contrast to nationalist terrorists, revolutionary terrorists do not "seek to preserve the status quo, the aim is to change the rules of the game". They are interested in a wholesale political transformation, not just the redistribution of territory for a particular ethnic group.

Far Right Extremist Terrorism

Within far-right extremist groups, "there is usually the idea that certain groups of people are inferior or superior as an innate principle. This is combined with an acceptance of violence as a legitimate form of action. Hatred of socialism or communism and a tendency towards authoritarianism are common traits among far-right extremist groups. In

South Africa extremist groups such as Afrikaner Weerstandsbeweging (AWB) still constitute a threat to life and social and economic wellbeing, and have shown themselves capable of political assassinations aimed at destabilisation.

New Age Terrorism

"When the stomach is full, one looks for something else to do". Chinese proverb.

New age terrorist (single-issue) groups turn to violence "when they believe that the issues they promote become too urgent for the slow progress of traditional campaigning". New age terrorist groups, such as anti-abortion and animal rights groups, differ from revolutionary terrorists because new age terrorist groups focus on one issue above all else, where as revolutionary terrorists generally have wider aims. An example of this for this group is the Animal Liberation Front, (ALF).

Religious Terrorism

Religious extremism represents the fastest growing type of terrorism. "In 1968, none of the identifiable active terrorist groups were religious. Today, there are about 50 known groups and about a quarter of them are religious in motivation". Al-Qaeda, is just one of the many religious terrorist groups that exist world wide.

2.2.4. Incidents of terrorism

The acts that are foremost in every persons mind are the acts that changed the world these being those that occurred on 9/11. As a result of this air travellers now get a plastic knife during air travel. Though this is not the forum to discuss it, however it seems ironic when all a predator needs to do is smash a bottle of their duty free and possess a weapon far more capable of inflicting injury that a small metal knife.

Many Embassies have also been the victim of such attacks, predominantly however those belonging to the United States. One of the first major acts of terrorism that gained world media attention and ultimate outrage was the attack that occurred on the Israeli Olympic Team at the 1972 Olympic Games in Munich. On this occasion members of the Palestinian group the Black September movement gained entry to the Israeli Olympic Village and after a skirmish took nine Israelis hostages. They ultimately made it to the airport and came under attack and in the battle killed all the hostages.

The Oklahoma bombing by Timothy McVeigh, was another act that caught authorities unaware and created much havoc. On 19 April 1995 McVeigh parked a yellow rental truck outside a central Oklahoma, city building and walked away, a few minutes later a 4000 pound bomb exploded. The perpetrator, twenty-seven-year-old Timothy James McVeigh, by now safely away from the devastation was convinced he acted to defend the Constitution of the United States, for he saw himself as crusader, warrior avenger and hero. (http://www.crimelibrary.com/serial_killers/notorious/mcveigh/dawning_1.html)

In this incident it was first thought this act had been conducted by Islamic Terrorists, however profiling and excellent investigative work proved it to be Timothy McVeigh. Was this then still to be construed as an act of terrorism? Many believe it was, however the US Government says that it wasn't

2.2.5. The terrorist and their motives

The word terrorism in itself has a perceptive meaning, as in to create terror. Therefore it is to some extent a matter of perception.

The war against international terrorism provides fresh challenges. Identifying the location of the 'enemy' is a significant problem and no amount of leaflets dropped on Afghanistan warning Al Qaeda that 'we are watching you' will remove this. Taylor, P. M. (2002)

There will always be those who will refuse to believe that America is a 'force for good in the world' - and the hardest task in any propaganda campaign is to try and convert the unconverted.

The military advisors to President George W. Bush share many of the concerns about who the real enemies of the new international system really are - rogue states, non-democracies, terrorists, international criminals and drug traffickers.

Huhtinen, A., & Rantapelkonen, J. (2002), also agree and quote Vilho Harle: 'Friends and Enemies come and go at short notice and even change their faces within rather short periods. Today's Friend can become tomorrow's Enemy, and vice-versa.' (Harle, V. 2000)

They then address that, in the war against terrorism, the perception of the enemy started to revolve around the persona of a former friend, Osama bin Laden.

> 'This enemy hides in shadows, and has no regard for human life. This is an enemy who preys on innocent and unsuspecting people, then runs for cover. But it won't be able to run for cover forever. This is an enemy that tries to hide. But it won't be able to hide forever. This is an enemy that thinks its harbours are safe. But they won't be safe forever.' (Bush, G. W. 2001)

Furthermore, on 15 September 2001 the President stated:

> 'This is a conflict without battlefields or beachheads, a conflict with opponents who believe they are invisible'. Even though the President maintains that this is a false interpretation, his statement nonetheless reinforces the perception. Besides, on 26 September the President addressed the question of invisibility again: 'You see, the enemy is sometimes hard to find; they like to hide. They think they can hide -- but we know better.' (Bush, G. W. 2001)

On 14 September 2001 BBC News reported on the enemy using the expression 'America's invisible enemy'. Peter Bergen has written the following about bin Laden in his book Holy War, Inc: 'You can't find him, he will find you'. Bergen suggests that when bin Laden is in the media, he is everywhere. (Bergen, P. L. 2001). This alone is one of the principle components not previously discussed about terrorism, in that though the acts are intended to create fear, that fear must be communicated to and then by the media. It is through these actions that the terrorist rely on to portray their messages. The media actions then entice and to some extent promote terrorism by the mere act of reporting on it and adding fuel to the very terrorists' motives.

Huhtinen et al further state, the security measures of the Salt Lake City Olympics were a manifestation of the fact that the propaganda war had turned against the aggressor. In fact, the feat of bin Laden's impact on a wider scale as presented in the Western media has influenced the Western people the most; they are convinced that the world has become more evil than ever before.

This was clearly their objective and enlightens the fact the objective of terrorism is to create fear and terror.

But they raise a major issue here in that, why was the perception of the enemy directed exclusively towards bin Laden, and consequently towards Afghanistan. Why not towards Saudi Arabia, for example, when fifteen of the terrorists involved in the attack of 11 September were from Saudi Arabia?

Therefore through the guerrilla action and terrorism, the invisible enemy makes it impossible for others to perceive its physical being. The problem concerning invisible enemies is that they cannot be destroyed regardless of the amount of armed might used against them: they subsist and operate even among the opponent's troops.

According to the theory of Merleau-Ponty, (Low, D. 2003) the object of influence is always culture-specific and dependent on history. When two parties have different fields of perception, and a different history and culture, it may indeed prove impossible to overcome.

Garfield, A. (2002), also address perception in that: Part of the problem is that the public's perception of such activities is still tainted by association with the Propaganda and

Psychological Warfare campaigns of the past. It is a paradox of our time that both the public and politicians are prepared to tolerate the use of bombs and bullets, but shy away from the use of information as a weapon of war.

Though the acts of terrorism create fear and terror in the first instance, in the long run it also creates anger and the want for retribution. This leads the victims of these attacks to become protagonists.

What then is seen as formative within this is? An act of terrorism requires the group who is conducting the act to have terrorist motives, for without them their actions may be for anything else. People are motivated to steal for money or some kind of gain. If someone has something stolen they don't automatically perceive that it was an act of terrorism, they see it as a criminal act. Therefore perception by those affected also has a component within determining what an actual incident is.

This is the defining point at which the act of terrorism is formulated as a result of two main points:

- The motives of the terrorist.
- The perception of the rest.

It is these principle issues that contrast a terrorist act from that of a crime or an act of war.

2.2.6. What has forced the increase in terrorism?

The main school of thought is the asymmetric Arms Race and the David and Goliath control by the super powers.

As Schwartau, W. (2002), put it, the overwhelming conventional and nuclear asymmetrical superiority has forced our potential global nation-state adversaries to escalate the Asymmetrical Arms Race into new models that we would generally view as terrorism or unwarranted attacks on non-combatant civilians.

Asymmetry is what gives terrorists their strength. They operate so far outside the box of accepted international behaviour (with a few notable nation-state exceptions) that most of us cannot fathom the rationale behind their despicable, if not cowardly acts.

Schwartau also states from a USA point that:

> "How we handle such asymmetries underscores the legal and cultural box in which Western nations have put themselves. When the World Trade Centre was blown up, law enforcement launched an investigation and then a trial took place to prove the guilty were guilty. Oklahoma City, same thing. At the end of 1999, we are only now getting to where a negotiated trial will occur for the Lockerbie tragedy a decade ago. Sure, we strafed Tripoli for a bit, but our symmetrical response to asymmetric attack is still considered civil behaviour. But for how much longer will that be an adequate response? How many terrorist acts will it take to alter our typical symmetrical response into an even more asymmetrical response to the original asymmetrical attack?"

This section has outlined the various definitions of terrorism. One of the common factors is to create fear and terror amongst the victims, and to some extent the perception, is that this is the objective of the antagonists. These acts are also often directed at those who are asymmetric within the race for control. There are also strong schools of thought that such for acts to be classified as terrorism, violence must be perpetrated toward non-combatants.

This is often true under conventional terrorism, however as we make it more difficult, through border controls, airline security, international intelligence sharing, the 9/11 wakeup call and public knowledge, terrorists are going to seek alternative methods to protract their vengeance.

Hence one of these methods will be through the use of Information Technology, as a tool to initiate actions, these actions now coined as acts of cyber terrorism.

2.3. Information combat

This section looks at what information is and why it is so important and how the control of it with information operations and information warfare, can provide a strategic advantage.

2.3.1. Information defined

The world is engulfed in the information era and much of the latter part of the last century and the first part of this has been how we can efficiently and effectively manage, store and move information globally, in every aspect of our lives. Many activities these days have an electronic component involved, whether it be using a swipe card to access a building or sending an email or text message to a friend. These actions are electronic, and the basis for management of electronic components is essentially the computer. This is predominantly known as Information Technology (IT).

IT basically runs our lives and our lives now revolve around it. Most of the systems that form part of the critical infrastructure are also heavily reliant on IT, Supervisory Control And Data Acquisition (SCADA) systems, control manual systems, that in turn are connected to networks and so on. Controlling these also involves the movement of information, as does Internet banking, email clients lists, personnel records and so. It is all information. However he who has control over some of this information can also exert power.

Armistead, L. (2002) adds,

> "Information is power, and how a nation uses that power determines how effective a country can be in influencing the world politic. The use of information to affect international relations has a long and varied history through which the government or leadership elite attempted to control it, thereby exercising power over their people. Yet the tremendous advances in technology over the last decade, most notably in the computer, telecommunications and perception management fields, have forever shattered the monopoly of control over information."

However as Armistead also identifies due to privatisation of the free world, in this new era, the government no longer owns the resources. New Zealand is a classic example where over the last 20 years, many elements of NZ's infrastructure that were once government owned are now either state owned enterprises or completely non government owned, Telecom and NZ Post, being just two examples.

Governments no longer have the monopoly on the flow of information, therefore they can only attempt to coordinate its use as best as possible, some of this is through legislation and regulation. The fact that the power of information has been disseminated from the government to the masses, is a huge and radical change that is only now beginning to dawn on politicians, bureaucrats and the military. This is mainly because information has changed the power structure of international relations.

Perception is also based on ideas, and technology changes ideas and reality. In the past the average citizen, activist, group or organisation was dependent on the government for communication and information infrastructure. That is no longer the case today. There is much more interaction and connectivity between people of the different nations than ever before, and this changes the way that a state must conduct its foreign policy initiatives.

> "Information and education are powerful forces in support of peace. Just as war begins in the minds of men, so does peace."
> President Dwight D. Eisenhower

Information then leads to power and this comes in many forms. The elements that figure most prominently in discussions of international relations are often military, diplomatic, economic and information based.

2.3.2. Cyber crime

Computers don't commit crimes, people do and like conventional crime, war and terrorism, the cyber equivalents will cause the same results, however they use IT to commit the acts.

Firstly looking at cyber crime, some of the literature has identified the following:

Cyber crime is a crime committed through the use of information technology and extends to acts committed through the use of the internet.

"With no jurisdictional boundaries, no geo-political boundaries and instant global communication technology the Internet is often described as 'this century's greatest commercial opportunity". (Ghosh, A. 2003).

Criminologists who have studied criminal offending however, believe that a crime can be analysed using the factors of means, motive and opportunity and hence controlling these factors will lead to a reduction of the occurrences.

It will be difficult for Governments to have success in controlling the **means** of the commission i.e. 'hacker' toolkits, as these are readily available on the Internet and attempting to block measures will fail as those applied to pornography, gambling and pirated software. Reducing the **motive** is at odds with the needs, as if offenders are motivated and an opportunity exists they will take advantage. Hence governments and corporations must focus on reducing the **opportunity** and in part by reducing the vulnerability of systems to intrusion, thereby limiting this opportunity.

Users are heavily reliant on the Internet for all kinds of activities, they purchase items, buy airline tickets and do banking. This information is then susceptible to intrusion and abuse. Schwartau, W. (2002) states that: "Over 22,000 lives are stolen every year through electronic identity theft. More than 500,000 acts of fraud against individuals occur each year. Our lives have become an open book to anyone with an Internet connection and a small chequebook. In Cyberspace we are guilty until proven innocent."

IT then provides a platform for criminals to use to commit offences and the Internet is part of that toolkit.

Fraud is just one type of crime that is heavily committed through the Internet. The internet as it is known is a large number of interconnected networks and as Noel, G. E., Gustafson, S. C., & Gunsch, G. H. (2002), put it, network attacks frequently originate from recreational hackers, but occasionally they involve seasoned cyberspace veterans working for terrorist organisations or hostile nations. Attacks utilise a myriad of vulnerabilities that are relatively easy and cost-effective to exploit, yet protecting against these threats can be difficult given the hundreds of potential entry points for hackers.

So now for crimes such as fraud, we have a means though the Internet to commit them and have criminals as in hackers as the offenders.

Furnell, S. M. (2002) determined that, cyber crime is now a major international issue, the effects of which have been felt in some way by the majority of the developed world. As networked computer systems have grown and matured, so too has the nature of crime and abuse within the environment.

Furnell's table categorises many conventional crimes and other specifically related to IT.

Crime/abuse	Description
Fraud	for private gain or benefit; altering input in an unauthorised way; destroying/suppressing/misappropriating computer output; altering computerised data; alteration or misuse of programs (excluding virus infections).
Theft	of data; of software.
Use of unlicensed software	Using illicit copies of software.
Private work	Unauthorised use of the organisation's computing facilities for private gain or benefit.
Misuse of personal data	Unofficial 'browsing' through computer records and breaches of data protection legislation.
Hacking	Deliberately gaining unauthorised access to a computer system, usually through the use of communication facilities.
Sabotage	Interfering with the computer process by causing deliberate damage to the processing cycle or to equipment.
Introducing pornographic material	Introducing pornographic material, for example, by downloading from the Internet.
Virus	Distributing a program with the intention of corrupting a computer process.

Figure 2: Computer crime and abuse categories from UK Audit Commission (1998).

There are thirteen classifications used by the Computer Security Institute (CSI), as the basis for their 2001 Computer Crime and Security Survey, conducted in collaboration with the FBI. These were as follows (CSI 2001):

- Theft of proprietary information
- Sabotage of data or networks
- Telecom eavesdropping
- System penetration by outsider
- Insider abuse of net access
- Financial fraud
- Denial of service
- Spoofing
- Virus
- Unauthorised insider access
- Telecom fraud
- Active wiretapping
- Laptop theft

Some of the offences conducted by employees with regarding to accessing information or removing it without authority, while within such employment is not an offence. Collecting the evidence and proving an effect case is the key.

The computer industry often regards computer crimes as technical problems with technical solutions. However, legal solutions and knowledge are also vital. Often the technical investigation of illegal behaviour will produce 'proof' and evidence that may be inadmissible or flawed in terms of legal proceedings. (Broucek, V., & Turner, P. 2002).

This is why it is not only essential but critical, that every case where it is perceived that actions conducted through the use of a computer that could result in litigation, they be treated correctly. That means the computers or other IT elements involved must be treated like any other conventional items of evidence and be preserved at all costs. This will usually involve forensically acquiring the data from the media used.

Selling the message to the lay non-forensic IT person is the biggest hurdle yet to be overcome in cyber crime investigations.

2.3.3. Information operations

Cyber Crime-fighting and conventional warfare also uses IT in the form of Information Operations (IO)

Nicander, L. (2002), suggests the following:

> Information Operations (IO)
>
> "The threat against the information society has become increasingly important at the same time as systems and functions important to the society are becoming more dependent on information technology.
>
> The first is a matter of perspective. Information Warfare is based on a security policy perspective and embraces more than IT or cyber-security. The contents and effects of the information (intelligence and psychological operations), viewed as a military instrument or from a strategic/economic viewpoint, are essential components of this cross-sector concept."

Curts, R.J., & Campbell, D.E. (2002), detail from the NSA 1999 that "Information Operations (IO) that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities."

Dearth, D.H. (2002), offers the most important aspects linking aspects of conventional warfare and that similar goals are also sought with IO and IW.

When people speak of “targeting” in the context of IO and IW, some tend to make direct analogies to more conventional warfare. As in attacks on critical infrastructure, attacks on command-and-control centres and capabilities, attacks on computers and information systems. Interest in attacking Critical Infrastructures comes easily to mind, as it is generally a consistent with that what is conducted in conventional warfare in that it inhibits productivity and day to day operations.

IO is the operational management of systems, civilian or military in protecting those systems to ensure continued and uninterrupted operation.

2.3.4. Information warfare

Having defined cyber crime and IO, prior to launching into cyber terrorism, the last object in the way is cyber warfare which is akin in many ways to conventional warfare.

As Davey, J., & Armstrong, H. L. (2002) put it,

> “Information Warfare is a broad term that encompasses many types of offensive and defensive activities involving intelligence, tactics and strategies, and manipulation of information and communications systems. Information Warfare is taking action to degrade or manipulate an opponent’s information resources and defending one’s own information resources. The suggestion that Information Warfare consists of offensive and defensive operations against information resources of a win or lose nature (Denning, 1999) presents only a narrow view. Rather than operations to win or lose, Information Warfare can also include surreptitious operations designed to slow down or temporarily immobilise an opponent or ally, or it may be action targeted to disable a given function.”

By this definition alone IW is an attack on others information resources and not using IW to conduct an act of conventional warfare though the use of IT.

Bigelow, B., Lt Col, (2002), more aggressively defines IW in that:

> We should learn from the example of air warfare. The technical and practical difficulties implicit in conducting warfare in the information domain mean that progress will be slow and undramatic at first, and zealotry is counterproductive. Patience and persistence will pay off in the long term. And if Information Warfare truly has the potential to influence conflicts without the destruction and loss of life associated with other forms of warfare, we have a moral responsibility to develop it.

The US Department of Defence put it though as:

> 'Information Warfare is any action to deny, exploit, and corrupt or destroy the enemy's information and its functions; protecting ourselves against those actions and exploiting our own military information functions'. (Kopp, C. 2003).

As was determined with cyber crime there are a number of elements required before IW can exist. Connectivity to the other party being the foremost this connectivity through the Internet is the most likely mode.

From this an inference can be drawn, then, that IW is an aggressive action against another party's Information resources whether it is, crime related, war related, terrorist related or simply commercial or industrial espionage.

Davey, J., & Armstrong, H. L. (2002), specifically address cyber warfare in that it is seen as a subset of Information Warfare, in which conflict between the combatants is conducted in cyberspace. What is still the subject of much debate, however, is the manner in which Cyber Warfare is best conducted by the attacker on one hand, and the defender on the other.

This however contrasts with many of the other schools of thought in this area as previously discussed. What is the determinant then is what is understood by the meaning of the warfare component as is it warfare in its definition as being an act of war, or warfare as in can describe a conflict in which the resources of two belligerents differ in essence and in the struggle, interact and attempt to exploit each other's characteristic weaknesses. (http://en.wikipedia.org/wiki/Asymmetric_warfare)

These weaknesses to be exploited then could clearly be weaknesses or vulnerabilities in information resources. One such example would be, hacker warfare as in the type of IW that seeks to damage computer systems by exploiting vulnerabilities in them. The attackers through a limited number of interfaces can access these systems while the addition of even a single new interface alters the protection mechanisms considerably. (Xenitellis, S. 2003).

The main concern however is that IW and cyber warfare are growing activities in our globally connected world. The need for skills in offensive and defensive cyber warfare operations is evident from international reports of attacks on government and business communications and computer networks. Computer security Institute (CSI) is a good and constant source of information and reports of attacks. (www.csi.org).

In summary, progressing toward the area of cyber terrorism, there is an interlinking of many of the aspects just discussed. This was also found with the conventional elements and it was in essence the perception and the motives for the actions that determined what an act would be classified as. It is foreseen then that this will follow suit within cyber terrorism as it did with conventional terrorism.

A notable author in this discipline (Denning, D. 2000), had the following to offer and further supports this:

"Cyber Terrorism covers unlawful attacks or threats of attack against computers, networks, and the information stored within those systems. As such Cyber Terrorism can be seen as a tool of Cyber Warfare. Cyber Warfare is a subset of Information Warfare and involves offensive and defensive operations carried out in cyberspace. Cyber Warfare can be carried out by a number of different parties, using a variety of tools. Cyber Warfare attacks could emerge from political opponents, commercial opponents, hackers, disgruntled employees and other internal staff, dissident groups and terrorists. Information Warfare is also used by corporations to gain competitive advantage and government bodies to investigate crimes, intelligence and defence concerns.”

2.4. Cyber terrorism

Having determined what terrorism is, it is time to move forward to the main issue this research is to cover: Cyber Terrorism. As put forward in the previous sections, as it is made more difficult for the predators to commit acts of conventional terrorism, terrorists will look for alternative methods to create fear and gain media attention for their actions.

As in the previous sections this section is predominantly a discussion on determining what is cyber terrorism. There has been much debate on this issue and a large quantity of literature on the topic.

2.4.1. Cyber terrorism defined

The underlying principle component of this research is cyber terrorism and it is the intention to determine how ready New Zealand is, should an incident occur. The largest component of literature reviewed then was: what is cyber terrorism? There is much debate on what it actually is. The bulk of this chapter is then focused around determining what cyber terrorism is, or is not.

There are numerous definitions, Kerr, K. (2003) in her research has coined four principle definitions:

(1) According to the US FBI:

> “Cyber terrorism is any premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents.”

(2) "A definition of Cyber terrorism proposed by the US National Infrastructure Protection Centre is:

> A criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty with a given population, with the goal of influencing a government or population to conform to a particular political, social or ideological agenda."

(3) Denning, D. (2000) defines Cyber terrorism as:

> Unlawful attacks and threats of attack against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Furthermore to qualify as cyber terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear.

(4) Lewis, J. A. (2002) Centre for Strategic and International Studies, defined Cyber terrorism as:

> The use of computer network tools to shut down critical national infrastructures (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population.

The notable points about the FBI definition, is that the attacks are politically motivated and result in violence. Where as the National Infrastructure Protection Centre differs considerably in that it also identifies violence, but also includes destruction and/or disruption of services to cause fear. There is quite a bit of diversity between a criminal act of violence and the disrupting of services. The FBI definition is rather narrow in that, in essence, if it is not politically motivated nor violent then it is not Cyber Terrorism. So by this, a terrorist could hack into a system and cause 2 billion dollars worth of damage and it is not cyber terrorism. This appears to be too restrictive.

The second is broader, but again it is violence, destruction and/or disruption. It is assumed then that the 'and/or' would also be relevant in that it is violence and/or destruction and/or disruption, to cover all the scenarios that could exist.

Denning's definition is also reasonably wide and identifies them as unlawful attacks, which is thought to be an accurate manner of determining the actual *actus reus* component, however it again looks at the aspects of violence against people or property - enough to cause harm. This again focuses on the actual acts of violence, and then if the entire Internet was brought down due to an act of terrorism through a denial of service, then it is not an act of terrorism by this definition, though violence to persons or property and a lot of fear could result from it, should it not be repaired and re-available for use.

The definition by Lewis is reasonably narrow, in that if you open a sewage valve and flood streets with raw sewage, the system has in essence shutdown, so that also is not an act of cyber terrorism, though the mention of critical infrastructure as a target is seen as an important issue. The threat of the release of the sewage could coerce the government however and would be construed as an act of Cyber Terrorism.

From these definitions it can be seen there are a number of components.

A **motivation**, this being some sought of terrorist motive to commit the act.

The **act**, in that it is criminal or unlawful, though hacking on its own is, in many countries. So the mere fact of hacking into the network with terrorist motives could be an act of terrorism.

A **target** for the terrorism, as in governments or civilians, and;

The **type** of act, as in violence, damage to property and the creation of fear, though more so it should be a loss or damage to such an extent that is causes fear, as this is the underlying principle of terrorism.

Given a scenario that a terrorist had access to the Internet, caused damage to the world media system, and was able to distribute propaganda to the effect that governments over the world had been taken over, or that an all out nuclear war had started, would create utmost fear, and should therefore at that scale be an act of terrorism.

The next two definitions are almost complete opposites in that the first one uses computers to cause real-world harm or severe disruption, although narrow is actually one of the broadest yet. The second identifies it as violence against digital property, which appears to be the most restrictive definition yet, in that it limits such an act to one committed against digital property and nothing else.

> "Cyber Terrorism is the leveraging of a target's computers and information technology, particularly via the Internet, to cause physical, real-world harm or severe disruption." (http://en.wikipedia.org/wiki/Cyber Terrorism)

> "Cyber Terrorism is the calculated use of unlawful violence against digital property to intimidate or coerce governments or societies in the pursuit of goals that are political, religious or ideological." (Nelson, et al. 1999)

This violence or destruction can be direct or indirect. Direct as in destroying computers or networks as in a DDOS attack, or indirect as in using the computers to access a SCADA system and in turn shut down power or open up a sewage valve and cause damage.

Kerr also defines it further by stating that cyber terrorism is but one form of cyber attack. Cyber terrorism and cyber attack are used interchangeably and may result in a misunderstanding of the cyber threat in general and the threat of cyber terrorism in particular.

This diminishes Cyber Terrorism to that of a subset of cyber attacks, and that cyber terrorism interleaves with that of cyber threat. However if it creates the **FEAR** factor, regardless then is it not an act of cyber terrorism.

Denning, D. (2002) presents three scenarios as follows:

> "Numerous scenarios have been suggested. In one, a Cyber Terrorist attacks the computer systems that control a large regional power grid. Power is lost for a sustained period of time and people die. In another, the Cyber Terrorist breaks into an air traffic control system and tampers with the system. Two large civilian aircraft collide. In a third, the Cyber Terrorist disrupts banks, international financial transactions, and stock exchanges. Economic systems grind to a half, the public loses confidence, and destabilization is achieved. While none of these or similar scenarios has been played out, many believe it is not a question of "if" but "when"."

This is a plug for the 'for' as opposed to the 'against' as will be discussed later, as some believe cyber terrorism is just a hype, a glorified name for computer crime or as the old saying goes, "*A rose by any other name."* William Shakespeare.

When it comes to discussion of cyber terrorism, there are two basic areas in which clarification is needed. Firstly the confusion between cyber terrorism and cyber crime. Such confusion is partly caused by the lack of clear definitions of the two phenomena. A UN manual on IT related crime recognises that, even after several years of debate among experts on just what constitutes cyber crime and what cyber terrorism, there is no internationally recognised definition of those terms. Second, it is useful to distinguish two different facets of terrorist use of IT:

Terrorist use of computers as a facilitator of their activities, and
Terrorism involving computer technology as a weapon or target. (Conway, M. 2003).

Conway et al, also adds that, regarding the distinction between terrorist use of information technology and terrorism involving computer technology as a weapon/target, only the latter may be defined as cyber terrorism. Terrorist 'use' of computers as a facilitator of their activities, whether for propaganda, communication, or other purposes, is simply that - use.

One of the final definitions to be offered is more complex, but yet more comprehensive, in that it not only includes death or destruction but intimidation. The further mention of the inducement of fear is again seen as a crucial factor in any definition.

> ”Cyber terrorism” can be defined, therefore, as the use, or threat to use, attacks by and on computers and related electronic networks and information to intimidate or kill civilians or incur large-scale destruction or disruption for political purposes. This would include the use of computers and related tools to cause “mass disruption” in information or service flows intended to induce fear or undermine public confidence in essential public services. While the term “cyber terrorism” is often used, however, security analysts argue the low degree of its occurrence.” (Bosch, O. 2002)

Rollins. J., & Wilson. C. (2005) put forward that at least two views exist for defining the term Cyber Terrorism:

- **Effects-based**: Cyber terrorism exists when computer attacks result in effects that are disruptive enough to generate fear comparable to a traditional act of terrorism, even if done by criminals.

- **Intent-based:** Cyber terrorism exists when unlawful or politically motivated computer attacks are done to intimidate or coerce a government or people to further a political objective, or to cause grave harm or severe economic damage.

Not as dramatic but certainly another key issue not touched on with many of the prior definitions is that cyber terrorism is not only about damaging systems but also about intelligence gathering. The intense focus on 'shut-down-the-power-grid' scenarios and tight analogies with physically violent techniques ignore other more potentially effective uses of IT in terrorist warfare: intelligence gathering, counter-intelligence and disinformation. (Bosch, O. 2002)

Some of these alone can have the affect of causing fear and certainly should be considered within a wider definition of cyber terrorism.

2.4.2 Could cyber terrorism be a myth or psychological hype

Defence against network attacks is costly. Be it from a hacker or a terrorist the same defence must be put up. So given this, is it not just preventing security breaches on the network that is the issue and the label, "Cyber Terrorism" a psychological hype.

In 1996 it was suggested that international terrorists lacked the resources to conduct a major impact terror attack within the USA. They would certainly have a different view on this post 9/11.

It is to some extent attitudes like "it will never happen" that will cause intelligence strategists that to coin cyber terrorism as a hype.

As the Computer Crime Research Centre (CCRC) put it, is cyber terrorism a real threat or just a distraction from the day-to-day job of maintaining network security?
http://www.crime-research.org/analytics/Cyberterror_Clear_present

The research then went on to say:

> "Our enemies will use our technology against us, the fact that they may be from a Third World country should not in any way suggest to us that they will not understand how to use our technology. Despite no precedence to support the idea

> of an “electronic Pearl Harbour”, governments continue to warn and even legislate around the issue.

Though at this stage the risk maybe seen as low, that could change at anytime, and as seen some countries take the threat seriously. The difficulty will be that unlike conventional terrorism where a stockpile of weapons, ammunition, explosives could be an indicator of preparation for an attack, also with 9/11 the presence of training manuals also being an indicator to cause some concern. But the possession of an anonymous computer on the Internet is all that is required , especially if the terrorist is sitting in an Internet café in some little town in Iceland and commits a major offensive on some major critical infrastructure on a country on the other side of the world.

CCRC is one that has adopted the negative stance, in that whilst they agree there has never actually been an act of cyber terrorism, there have been plenty of instances of politically motivated hacking incidents that sit outside the realm of simple cyber crime, and they fall short of being acts of cyber terrorism, according to security experts. The consensus seems to be that a cyber attack only becomes cyber terrorism when there is serious damage to property, loss of life, or it causes terror or fear in the target community.

In 2007 the Estonia Government become the victim of a prolonged attack of its IT resources. Part of the attack was a DDoS attack in which selected sites were bombarded with traffic in order to force them offline. Nearly all Estonian government ministry networks as well as two major Estonian bank networks were affected. In targeting Estonia's online seats of political and economic power, the perpetrators sent a threatening message to a country where cabinet-level discussions happen online, and documents are signed by digital signatures. This certainly must be considered an act of cyber terrorism given the impact, the fear created and that it was primarily the government targeted.

CCRC, quote Mogull, R. (2003), the director of Gartner Information Security and Risk Research, who defines cyber terrorism as a “terrorism attack using a digital channel”. The

FBI defines terrorism as “unlawful or threatened use of force or violence against persons or property to intimidate or force a government or civilian population to further political or social objectives”. Mogull in contrast further says that although terrorists are using the Internet to communicate among themselves, their use of the Internet as a “delivery vehicle for a significant, digital terrorist attack is a nightmare scenario not grounded in reality and there have been no losses of life or property because of a digital attack.”

Fostering a climate of fear, disrupting the internet and other communications networks would probably just annoy people and Schneier, B. (2005), like Mogull, claims that companies and consumers should concentrate on “real” threats from criminals, viruses, worms and Trojans.

Schneier further says:

> “It’s a myth that has yet to become to a threat to human life. Nobody's getting blown to bits, I don't think that cyber terrorism exists--if you add 'terrorism' to things, you get more budget. If you can't get e-mail for a day, you're not terrorized, you're inconvenienced."

This clearly appears to be a very negative cynical approach to the entire concept.

It is not difficult to see then that how it is possible to end up in a situation like 9/11 when half the community say it is just a hype - it may never happen. Or it hasn’t happened as yet, as far as they know it hasn’t happened or the attempt failed and it was labelled incorrectly.

But Conway's, (2003), point of view is that, “There is undoubtedly a lot of exaggeration in this field. If your system goes down, it is a lot more interesting to say it was the work of a foreign government rather than admit it was due to an American teenage ‘script-kiddy’ tinkering with a badly written CGI script. If the power goes out, people light a candle and wait for it to return, but do not feel terrified. If their mobile phones switch off, society does not instantly feel under attack. If someone cracks a web site and changes the content, terror does not stalk the streets.”

This is the diversity that exists by researchers in this area, basically they are saying so what if the national grid gets taken out by a cyber terrorist, get out a candle. Have the IT team get out the Disaster Recovery plan and fire up the warm backup server and recommence operation. That may certainly be the case in some instances,

Henych, M., Holmes, S., & Mesloh, C. (2003), further highlight this, where they believe cyber terrorism as an issue remains enigmatic, as the literature that describes it is relatively speculative, in that the extent to which it is a threat remains classified at the highest levels. It is the opinion of the researchers that there exists some empirical evidence and research on the topic of cyber terrorism, but it will remain classified, as it is sensitive to the U.S.'s national security. There does however exist in the literature hints and allegations by various government officials that cyber terrorism is a real and ugly threat, and that the U.S. is clearly more vulnerable to attacks than we are led to believe.

This being the more optimistic, or you could say cynical approach, but it is the internet and open public networks that are the link.

As the Internet continues to expand, and computer systems continue to be assigned more responsibility while becoming more and more complex and interdependent, sabotage or terrorism via cyberspace may become a more serious threat.

There again the fear factor, but fear is an emotion, a psychological perception and thus if an attack occurs that causes fear then the terrorists have achieved their goal and no psychological hype need to exist if average individuals are frightened due to these actions.

It is not the fear component that causes the psychological perception but the receipt of the perception by the recipient that determines if someone is fearful. Therefore a researcher is not in a position to determine if fear would or not would be created, as no two people in the world may have the same fearfulness from a given act. We are all different and think and react differently.

As Tyrrell (2002), put it, “Perception is a powerful tool in cyber-war.”

Having to light a candle, due to the power going out is not a major issue in the short term, though society’s reliance and advancement the of the digital age will provide the platform to cause further disruption.

Nelson et al, have advanced thinking on the entire issue. They consider cyber terror is indeed coming. The anonymity afforded by means of attacking via the Internet, the increasing economic damage that can be done by disruption, and the growing dependence of advanced military command on interconnectivity all suggest that the infosphere is a fertile vineyard in which the terrorist may one day toil with good prospects for substantial rewards.

They have considered three levels of structure:

Simple-Unstructured: The capability to conduct basic hacks against individual systems using tools created by someone else. The organisation possesses little target analysis, command and control or learning capability.

Advanced-Structured: The capability to conduct more sophisticated attacks against multiple systems or networks and possibly to modify or create basic hacking tools. The organisation possesses an elementary target analysis, command and control and learning capability.

Complex-Coordinated: The capability for co-ordinated attacks capable of causing mass-disruption against integrated, heterogeneous defences (including cryptography) and the ability to create sophisticated hacking tools. The organisation possesses highly capable target analysis, command and control, and organisational learning capability.

And finally:

> Our foes have extended the fields of battle – from physical to cyberspace.
>
> *President Clinton, 22 May 1998*.

Like the 9/11 attacks, it won't be until something devastating occurs that people will truly grasp what Cyber Terrorism really is.

With conventional terrorism if an attack attempt fails or is foiled, the capture of the predators or their actions would clearly indicate that it was an attempt at an act of terrorism. Conversely if someone attempts to hack a major critical infrastructure element and is blocked by the firewall and rejected, no one may ever know. It would be just another blocked attempt that probably occurs daily for some locations, and other than the source IP address being captured in a security log, no one is going to investigate it. So without some other evidence it would never be labelled as a failed attempt an act of cyber terrorism and this is what should be a concern.

So if it isn't investigated and the attacker isn't caught, then no one would know if it was a terrorist-motivated attack.

2.4.3 The principle difference between cyber crime and cyber terrorism

Again from the pen of Shakespeare, 'A Rose by any other name' as it is all in the name that is the difference.

As in the case in Queensland, Australia where a former council employee released sewage as a result of an IT attack, if he had been a terrorist carrying out the exact same actions it would have been labelled an act of Cyber Terrorism, but as it was a former disgruntled employee it was realistically an act of Cyber Crime. (http://www.computerworld.com/securitytopics/security/story/0,10801,108735,00.html)

So whether it is cyber crime or cyber terrorism the outcome will be exactly the same, and it is the instigator of the attack and his motives that really determine what it is.

The proportion of cyber crime that can be directly or indirectly attributed to terrorists is difficult to determine. For example, organised criminals use information technology for the movement of money internationally. Where criminals and terrorists work together, members of terrorist groups may be given special training in computer software, or in engineering, to facilitate communications through the Internet. In-house financial specialists and experienced advisors may also knowingly, or sometimes unknowingly, help cyber criminals evade the scrutiny of bank regulators and international investigators. These reportedly may include accountants, bank employees in offshore zones and major financial centres, who may or may not also be terrorists or supportive of the political motives of their clients. (Rollins, et al. 2002).

Again because it is difficult to tell from where a cyber attack originates, an attacker may direct suspicion toward an innocent third party. Likewise, the interactions between terrorist and criminals who use computer technology may sometimes blur the distinction between cyber crime and cyber terrorism. So far, it remains difficult to determine the sources responsible for most of the annoying, yet increasingly sophisticated attacks that plague the Internet.

In some countries it is clearly a crime to be in possession of material that can aid terrorism.

Denning, D. (2000), also agrees, in that terrorists have moved into cyberspace to facilitate traditional forms of terrorism such as bombings, but they use the Internet to communicate, co-ordinate events and advance their agenda. While such activity does not constitute cyber terrorism in the strict sense, it does show that terrorists have some competency using the new information technologies.

The Web is especially popular as a medium for reaching a global audience.

Even in democracies, however, there are limits to what terrorists can post on the Net. Many terrorists are using encryption to conceal their communications and stored files, compounding the difficulties of providing effective counter-terrorism. Hamas, for example, reportedly has used encrypted Internet communications to transmit maps, pictures and other details pertaining to terrorist attacks. Ramsey Yousef, a member of the international terrorist group responsible for bombing the World Trade Centre in 1994 and a Manila Air airliner in late 1995, encrypted files on his laptop computer.

This however does appear to be a contentious issue, in that the use of a computer to assist or facilitate an act of conventional terrorism is not an act of cyber terrorism and would be perceived as a crime or just corroborative evidence in support of the conventional act. Then if using a computer to facilitate an act of conventional terrorism is not an act of cyber terrorism, should not the use of the Internet to distribute propaganda that a terrorist attack is going to occur, whether it has or not, creating fear in some readers, be consider to be an act of cyber terrorism?

As Gordon, et al. (2003), add. "We do not use the term "ice-pick terrorism" to define bombings of ice-pick factories, nor would we use it to define terrorism carried out with ice-picks. Thus, we question the use of the term cyber terrorism to describe just any sort of threat or crime carried out with or against computers in general. At the same time, those who do insist on treating only "pure cyber terrorism" as cyber terrorism are completely missing the true threat posed by the addition of acts in the virtual world to the terrorists' playbook."

Stohl, M. (2006), agrees to some extent that, the main argument is that there has been a failure to distinguish between what has been referred to as "hacktivism", or cyber criminal activities, and cyber terrorism. This means there has been a failure to distinguish between the use of digital means for organisational purposes and the use of digital communications to actually commit acts of terrorism. News outlets and scholars continually cry out that an act of cyber terrorism is imminent, keeping fears high and the sense of security low.

2.4.4 The ingredients of a cyber terrorist Act

To assist further in providing the final elements in determining what is cyber terrorism, like a criminal act there are portions as to what makes up that act. In defining the criminal act these portions are determined by the ingredients of the offence. Burglary is an example from the NZ Crimes Act, 1961. "Break and enter with intent to commit a crime there-in". So an offender must firstly open a window, or a door or smash a window or a door, break the plane of the structure to be entered as in put their hand or entire body inside the structure. Then once inside they then must have the intention of committing a crime, this crime could be theft, rape, intentional damage or murder or they commit the offence of burglary. So if they break and enter with the intention of just having a sleep like Goldilocks did, provided she doesn't eat any of the porridge, she hasn't committed an act of burglary, another offence yes, but not burglary.

The purpose of this discussion is not to carve a criminal definition for cyber terrorism, but to provide some academic explanation and in doing so identify some of the elements that will assist in doing so by proving some of these ingredients.

Gordon, et al. (2003) provided some guidance in regard to conventional terrorism and have also with regard to cyber terrorism in that the following are required:

Perpetrator

Interactions between human beings are complex; while the obvious solutions gravitate toward monitoring, we are concerned with virtualization of interactions, which can lead to relative anonymity and desensitization. Topics of interest include methods to measure and diminish the impact of computer-mediated interactions on potential recruits and the ability for defenders to use virtual identities to influence intra- and inter-group dynamics.

Place

Location exists as an element, but is not a "required" element in traditional terrorism in that an event does not have to occur in a particular location. Thus, whether an act is virtual/virtual, virtual/real world or real world/virtual is of interest only as a factor in modelling solutions. In addition, the Internet has introduced globalization of the environments.

Action

In traditional scenarios, terrorist scenarios typically are violent or involve threats of violence. While there have been many studies of violence in the physical world, more research is called for in terms of “violence” as a virtual phenomenon. Violence in virtual environments is a relatively new field, with many unanswered questions. However, despite the prevalence of traditional violence portrayed in virtual environments, “Cyber Violence” is still very much an unknown quantity. For example, destruction of someone’s computer with a hammer constitutes a violent act. Should destruction of the data on that machine by a virus also be considered “violence”?

Tool

There are an almost uncountable number of ways that the terrorist can use the computer as a tool. Facilitating identity theft, computer viruses, hacking, use of malware, destruction or manipulation of data all fall under this category.

These uses of the computer, when combined with “computer as target” form the “traditional” picture of cyber terrorism.

Target

There are a large number of potential targets that involve, either directly or indirectly, computers. Consider, for example, the impact of “Personal Identity Theft”. While the incidence of identity theft is comparatively low, the impact of theft upon the unfortunate soul whose ID is stolen can be large: terrorists could use the stolen identity to mask their work, carrying out certain operations under their target’s name, not their own.

What appears to be foremost in the realm of terrorism is the motivation of the attacker to commit an act of terrorism and this like a crime is the *mens rea* as in the mental intention of the offender - in this case to commit and act of terrorism and with the use of computers and a network to gain access to commit an act of cyber terrorism.

Gordon et al, also see that these people committing these acts must have an affiliation. A motivation for their intentions can be ratified as terrorism.

Affiliation

It is possible for a person to read all about a given cause and chat with proponents of the cause without ever leaving the safety of his or her own home. New recruits can thus become affiliated with a terrorist group, commit to carrying out given actions, all without ever actually coming into contact with another human being. At the same time, these loose affiliations can complicate investigations and confuse media reports. Additionally, the introduction of computing technology facilitates alliances between groups with similar agendas; this type of affiliation can result in strengthening of the individual organisations as they can immediately acquire access to the information resources of their allies.

Motivation

Political, social and economic changes are the motivations present in real-world terrorism. Combining a dependence on Internet-connected systems for banking and ecommerce with the ability of anyone with a desire and readily available tool to disrupt these areas, results in a situation that is all too clear; unless steps are taken to significantly reduce risks, disaster is inevitable.

Kopcheva, M. (2006) further provides that, outside of computer networks, communications networks can also be targeted for destruction, disruption or hijacking and that there needs to be Objectives and Actors.

Objectives of cyber attack

- Loss of Integrity
- Loss of Availability
- Loss of Confidentiality.
- Physical Destruction

Actors

- Hackers
- Hactivists
- Computer Criminals

- Insiders
- Consultants/Contractors

In summary, breaking the ingredients down, for it to be an act of cyber terrorism, there must be the following:

- The terrorist; a person who must have an affiliation with some terrorist organisation and has knowledge to be able to complete the cyber act.

- A motive for committing this act.

- There must be an objective which will result in violence, destruction or simply something that creates fear.

- An action that must be direct or indirect. Direct as in destroying computers or networks as in a DDoS attack would do, or indirect as in using the computers to access a SCADA system and in turn shut down power or open up a sewage valve and cause damage.

- A target as in a computer or a communication network and

- A means to access the target as in direct physical access, or access through a network such as the Internet to reach the target.

2.4.5 Incidents of cyber terrorism

Below are some incidents that potentially could have occurred as a result of cyber terrorism. But though they may have the outcome, without further information it cannot be fully determined if the persons responsible were in fact terrorists, as in line with the definitions in the previous chapter unless they are, then it isn’t Cyber Terrorism.

Janczewski, L. J. (2007), provided this list.

In 1997, a hacker from Sweden jammed the 911 emergency telephone system in west-central Florida.

In 1997, at Worcester, Mass, a hacker disabled the computer system of the airport control tower.

In 1998, attacks were launched against NASA, the Navy and the Department of Defence computer systems.

In 2000, in Russia, a hacker was able to control the computer system that governs the flow of natural gas through the pipelines.

In 2000, someone hacked into the Maroochy Shire, Australia, waste management control system and released millions of gallons of raw sewage on the town.

It is known from other research that the last incident was conducted by a former disgruntled employee. So to label that as an act of Cyber Terrorism would be no more than media hype.

This is further shown in the details below:

> “Boden, who had been a consultant on the water project, conducted the attack in March 2000 after he was refused a full-time job with the Maroochy Shire local government. He had attempted to gain access to the system 45 times, and his last attempt proved successful, allowing him to release raw sewage into the waterways. Marine life died, the creek water turned black and the stench was unbearable for residents, said Janelle Bryant, investigations manager for the Australian Environmental Protection Agency.”

(Computer World)

In 1996, a computer hacker allegedly associated with the White Supremacist movement temporarily disabled a Massachusetts ISP and damaged part of the ISP's record keeping system. The ISP had attempted to stop the hacker from sending out worldwide racist messages under the ISP's name. The hacker signed off with the threat, "you have yet to see true electronic terrorism. This is a promise." The hacker apparently never made good on his promise, but the threat of a cyber terrorist attack has many people worried. (Denning, D. 2000)

Governments worldwide are particularly concerned with terrorist and state-sponsored attacks against the critical infrastructures that constitute their national life support systems. Internationally there have been attacks against these infrastructures. Hackers have invaded the public phone networks, compromising nearly every category of activity, including switching and operations, administration and maintenance. It is the attacks against critical infrastructure that are going to have the greatest impact on society at large.

They have planted "time bomb" programmes designed to shut down major switching hubs, disrupted emergency 911 services throughout the eastern seaboard, and boasted that they have the capability to bring down all switches in Manhattan.

Banks and financial systems are a popular target of cyber criminals. The usual motive is money, and perpetrators have stolen or attempted to steal tens of millions of dollars. As Denning further advises, Government computers, particularly Department of Defence computers, are a regular target of attack. Detected attacks against unclassified DoD computers rose from 780 in 1997 to 5,844 in 1998 and 22,144 in 1999. While the above incidents were motivated by political and social reasons, whether they were sufficiently harmful or frightening to be classified as cyber terrorism is again a matter of definition and categorisation.

As discussed earlier where Estonia was subjected to a mass cyber-attack by hackers inside the Russian Federation, which some evidence suggests was coordinated by the Russian government, though Russian officials deny any knowledge of this.

News Zdnet.com provides a notional scenario below, and also provides other examples that could potentially be cyber terrorism, however many are merely hackers and not cyber terrorists.

> "In 1998, a 12-year-old hacker broke into the computer system that controlled the floodgates of the Theodore Roosevelt Dam in Arizona, according to a June Washington Post report. If the gates had been opened, the article added, walls of water could have flooded the cities of Tempe and Mesa, whose populations total nearly 1 million."

What they also reported though was:

> "A hacker did break into the computers of an Arizona water facility, the Salt River Project in the Phoenix area. But he was 27, not 12, and the incident occurred in 1994, not 1998. And, while clearly trespassing in critical areas, the hacker never could have had control of any dams, leaving investigators to conclude that no lives or property were ever threatened."
>
> It is like the children's game of "telephone", said Gail Thackery, Assistant Attorney General for Arizona and the prosecutor on the Salt River hacking case. "You get the reality at one end and, at the other end, something completely different".

"In 1996, the power along much of the West Coast corridor went out for nine hours after a tree branch fell on some power lines and, in combination with several other problems, caused a cascading failure. In 1990, a similar event with an AT&T switch touched off a chain reaction that shut down long-distance communications across the United States. It is acts like this that cause people to raise an eyebrow and give some consideration. Were those acts of cyber terrorism, was it a hacker, was it lax security, or was it media hype. Or was it really an act of cyber terrorism to which the governments or organisations who were victim will never admit that they had a vulnerability that allowed someone to get into their network, access systems and have such control to be able to cause damage. In some cases we will never know." (ZNET.com)

What makes matters worse, and this will be looked at further in chapter 6, a high percentage of the critical infrastructure is now privately owned, and in many cases the companies have not been sufficiently educated about information security until recently. The research in this thesis intends to determine if this is in fact the case.

Just days after the 9/11 terrorist attacks the FBI began warning the public that the potential for future attacks exists, and among the threats was that of cyber terrorism. (Spencer, V. 2006) When the U.S. government's new cyber terrorism expert, Richard Clarke, suggested the possibility of a "digital Pearl Harbour", he was greeted with scepticism.

From a researcher's point of view, there will be always limits as to how much information can be obtained from government agencies. Even within NZ agencies such as the SIS, GCSB and CCIP will not fully disclose their readiness, their intelligence cell strength or if they have been infiltrated. This information in the public foray would allow others to exploit this information to aid in further attacks. It is understandable given the protection they must provide to the infrastructure and stability of the country. You would hardly go and tell a burglar the type and quantity of Passive Infra Red (PIR) alarm sensors that exist in a house, or worse still what the alarm code is.

In autumn 2004, organised cyber criminals appear to have infiltrated the computer systems of the London offices of Sumitomo, the Japanese bank, in an attempt to steal £220 million. The cyber criminals reportedly planned to transfer the money to other bank accounts around the world. Officials at the London police fraud squad reportedly stated that Sumitomo is the only incident so far in which an attack by external cyber criminals has nearly succeeded against a major bank. (Rollins et al)

Conway, M. (2003), further provides some instances but again the first instance is a matter of cyber crime and there appears to be no terrorist element within it other than the media hype.

> "In June 2001 a headline in the Boston Herald read 'Cyber Terrorist Must Serve Year in Jail'. The story continued: 'Despite a Missouri cyber terrorist's plea for leniency, a Middlesex Superior Court judge yesterday told the wheelchair-bound man 'you must be punished for what you've done' to Massachusetts schoolchildren and ordered him to serve a year in jail.' Christian Harold, 21, pleaded guilty to 'launching a campaign of terror via the Internet' from his Missouri home, including directing Middle School students to child pornography web sites he posted on the Internet, telephoning threats to the school and to the homes of some children, and posting a picture of the school's principal with bullet holes in his head and chest on the Internet.
>
> According to Kennedy, cracking can escalate to terrorism when a person cracks into a government or military maintained web site; he said cyber terrorism has increased across the United States since the events of 9/11 and law enforcement has traced many of the attacks to Pakistan and Egypt."

The case above is getting closer, but again does it make it terrorism, because it just happens to be a government organisation?

It is known from past conventional attacks that terrorist groups can't wait to blow their own trumpet as soon as they have committed an act. It is all part of the entire deal about them gaining support for their plight. It is likely to be no different with an act of cyber terrorism in that as soon as they have committed an act, provided the actions haven't stifled their ability to do so, they will tell the world.

2.4.6 The cyber terrorist and their motives

Know your enemy and keep him close, is a well know quote from military and other doctrine. The same should be said with cyber terrorism. Knowing who potentially is the threat is the first step in conducting counter terrorism. Intelligence gathering on the threat will assist with any threat assessment.

Colin, B. C. (2005), also asks, who are the cyber terrorists? There are a great many poor movies and too many works of fiction about the hacker and cracker communities. In the popular media, there recently was the Kevin Mitnick incident, where one cracker broke into another cracker's systems. This spawned endless press and at least two best selling books. While this incident received much attention, the events amounted to meaningless children's games.

From the American point of view the most dangerous terrorist group is Al Qaeda which is considered the first enemy for the US. A study that covered the second half of the year 2002 showed that the most dangerous nation for originating malicious cyber attacks is the United States with 35.4% of the cases down from 40% for the first half of the same year. South Korea came next with 12.8%, followed by China 6.2%, then Germany 6.7%, then France 4%. The UK came number 9, with 2.2%. According to the same study, Israel was the most active country in terms of the number of cyber attacks related to the number of Internet users. (Elmusharaf, M. (2004).

It is not surprising to note that New Zealand doesn't even feature. Not surprising if we don't even have any tactical military air strike force, would they waste their time, when there are much bigger fish in the sea.

Moutot, M. (2006) has coined them as; Electronic Jihad's Cyber Soldiers:

> They neither carry weapons nor lay ambushes for soldiers in Iraq or in Afghanistan.
>
> But thousands of radical Islamists are waging a different kind of war from behind their computers, called “electronic jihad”.
>
> These radical Islamic sites have sprung up over the past few years, specialising in the organisation and the co-ordination of concerted cyber-attacks against Israeli, American, Catholic and Danish websites.
>
> All you need to join this anonymous cyber world is an address registered in Iraq or in tribal zones in Pakistan, and basic computer savvy to carry out concerted attacks in which Internauts from the four corners of the world take part.

They also indicate that, they are no bigger threat than any other hacker out there.

> “There is no reason why the radical Islamists should be more competent than the professional hackers of Eastern Europe, for example. It’s not because they are jihadists that they are more dangerous: it all comes down to their technical expertise, and there is nothing in their ideology that makes them better at doing this than anyone else.”

This is very true. To conduct conventional terrorism you need weapons, ammunition, explosives, a location to hide and prepare for an attack, knowledge on how to assemble and use what you have and a method to transport them to the target site.

Conversely, any highly skilled computer programmer, and there must be hundreds of thousands of them in the world with knowledge of IT security systems and firewalls, could conduct an attack of cyber terrorism from their home, office or Internet café and no one would need to know. All you need is a computer and a network connection like nearly every house and office has in New Zealand and those - apart from knowledge - are all the tools you need.

Rollins et al (2005), believe the main concern is that experts now believe that terrorists collaborate with organised crime networks in the Middle East for international smuggling of arms and illegal drugs. Criminal drug traffickers can provide terrorists with access to computer specialists with high-level technical skills. What are the pros and cons of linking counter-terrorism efforts more closely to the efforts of agencies that counter drug trafficking?

Furnell, S.M. (2002) listed the flowing as potential terrorists

- **Cyber Terrorists.** Terrorists who employ hacker-type techniques to threaten or attack against systems, networks, and/or data. As with other forms of terrorism, cyber terrorist activities are conducted in the name of a particular political or social agenda. The underlying objective will typically be to intimidate or coerce another party e.g. a government.

- **Cyber warriors.**
- **Hacktivists.**
- **Malware writers.**
- **Phreakers.**
- **Samurai.**
- **Script kiddies.**
- **Warez d00dz.**

A more detailed explanation of these is contained Appendix A.

From the above, it quickly becomes clear that the issue of hacking is as riddled with alternative classifications as the top-level issue of Cyber Crime.

Fennell et al further provides the following matrix of motivations and hackers. But this is exactly what also constitutes an act of Cyber Terrorism.

	Cyber-terrorists	Cyber Warriors	Hactivist	Malware writers	Old School	Phreakers	Samurai	Script Kiddies	Warez D00dz
Challenge				✓	✓	✓	✓		✓
Ego				✓	✓	✓		✓	✓
Espionage		✓		✓					
Ideology	✓	✓	✓		✓				✓
Mischief				✓		✓		✓	
Money		✓		✓		✓	✓		✓
Revenge	✓		✓	✓				✓	

Figure 3: Hackers and their motivations.

The US Army Handbook (2005) also provides a synopsis of the potential motivations and actions of potential predators.

Threat Source	**Motivation**	**Threat Actions**
Hacker, Cracker	Challenge	Hacking
	Ego	Social engineering
	Rebellion	System intrusion, break-ins
		Unauthorised system access
Computer Criminal	Destruction of Information	Computer crime (e.g. cyber stalking
	Illegal information	Fraudulent act (e.g. replay,
	Disclosure	Impersonation, interception)
	Monetary Gain	Information bribery
	Unauthorised data	Spoofing
	Alteration	System intrusion
Terrorist	Blackmail	Bomb/Terrorism
	Destruction	Information Warfare
	Exploitation	System attack e.g. distributed denial of service
	Revenge	System penetration
		System tampering

Industrial Espionage (companies, foreign governments, other interests)	Competitive advantage Economic Espionage	Economic exploitation Information theft Intrusion on personal privacy Social engineering System penetration Unauthorised system access (access to classified, proprietary and/or technology-related information).
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g. data entry, error, programming error)	Assault on an employee Blackmail Browsing of proprietary information Computer abuse Fraud and Theft Information bribery Input of falsified, corrupted data Interception Malicious code (e.g. virus, logic bomb, Trojan horse) Sale of personal information System bugs System intrusion System sabotage Unauthorised system access

Figure 4: Synopsis of the potential motivations and actions of potential predators. (The US Army Handbook)

Given what has been discussed here, anyone with sufficient IT knowledge with their own PC could become a cyber terrorist threat, providing they have the motivational and affiliation to commit an attack. The rest of what is required can be obtained with a bit of probing, social engineering and surfing to gather all that is needed without leaving home.

Though it will likely be the larger conventional terrorists groups that will be the concern.

Whilst terrorists in general have been discussed, it is possible that a lone individual, as in the Timothy McVeigh incident, could conduct an act of terrorism.

Beyond these activists, some time referred to as radical groups, can also be situations not too dissimilar to what happened in Queensland, Australia - an attack by a disgruntled employee or contractor.

Furthermore it is likely that should a terrorist organisation not have the skill set to conduct a cyber attack, it would source the skills from an underpaid developer in a third world country.

Poor developers in third world countries with the skill set could easily get hired by terrorists to infiltrate systems, break code, write code and modify code.

Ellsmore, N. (2002), agrees, and further identifies with in that, cyber terrorism may be carried out by either a group, such as al Qaeda, or hired expertise. This latter scenario is referred to as “hackers for hire”, and is considered to be of growing frequency, particularly using technically proficient hackers from Eastern Europe. Technology links are generated in developing regions by facilitating financing, rapid planning, and all forms of information sharing. Legitimate corporations have exploited the technological revolution to full advantage by using information technology to co-ordinate their international operations in developed and developing countries. This has helped them overcome problems of international communication in a multi-lingual environment.

But more important, why do terrorists use cyber attacks? As covered previously there are entry barriers to commit conventional acts of terrorism. You may require explosives, firearms, ammunition, knowledge, transportation or as in the 9/11 case, the ability to hijack and aeroplane and fly it into a building.

A network based cyber terror attack though requires just three simple things: a computer that could be located anywhere in the world, possibly the other side of the world where the target is, an Internet connection that could be at home, work or an Internet café, or even through an open wireless access point, And finally a bit of hacking knowledge gained from a web site.

The barriers are minimal.

Cyber terrorists prefer using the cyber attack methods as there are many advantages for doing so. As well as the remoteness that it allows, speed is another factor in that an attack can produce instant results.

Just, J. E. (2006) agrees, in that response times for cyber attacks are comparable to or faster than strategic nuclear scenarios. While there are certainly computer network attacks in which only milliseconds are required for major damage, we hope that a large-scale co-ordinated attack is likely to take somewhat longer, on the order of 20 minutes.

This of course may not be the case especially if intrusion systems fail to detect the attack.

Nelson, et al. (1999) also further enhance the fact that the greatest benefit is low cost of entry.

> Relatively small investment provides a force multiplier and a limited capability:
>
> - The cost of computer hardware continues to decrease
> - Advanced hacking tools which require only minimal knowledge are freely available on the Internet

- You get what you pay for – a low-budget capability is likely to produce low-budget results

The cost-effective nature of cyber terror support and the low start-up costs for simple-unstructured cyber terror allow financially constrained terrorist organisations an effective, low cost entry point. Chat rooms link hackers of different skill levels creating a virtual classroom for learning and exchange of success stories. The Internet is itself a source of malicious software - a variety of tools are freely available for downloading.

For terrorists, a simple-unstructured cyber terror attack may require minimal investment, but the results will also be constrained in their effects. As the level of cyber terror attack increases so the costs of intelligence, human capital and in some cases processing power, escalates.

But also the terrorists can also use the Internet to research information on the critical infrastructure of a country to gain information about the very systems they intend to attack. So the user-friendly, information sharing, knowledge-base world we now live in has the potential effect of coming back and biting us in the face. The old saying “too much information”, may have a different tilt to it now. A terrorist with a computer and network connection, gains the knowledge through the Internet how to hack and launch and attack, downloads the tools, communicates with others about the intended attack, surfs the targeted countries, government sites or critical infrastructure sites, gains knowledge on them, tests the security and then launches the attack on them, without leaving the chair.

The other issue is that we are providing the predators with an even bigger feast daily with the continued growth and provision of online services.

These kinds of attacks first predominated within e-commerce, and have become even more of a problem as government and the military begin to offer many more of their services online, or rely more heavily on distributed information systems to provide their operating data. Current information about the War on Terrorism in Afghanistan for example suggest that this war stands apart in its dependency on the Internet and other closed networks as tools for military planning - obviously defence against of cyber terrorism becomes even more important in this kind of war. (Slay, J. 2003)

Global connectivity has sped up the pace of development through information sharing, but this global connectivity also enhances the attractiveness of IT for terrorist support activities. With IT support, terrorist organisations can communicate globally and instantaneously to enhance their command and control while using commercially available encryption methods and services.

The increasing employment of IT enhances the attractiveness of cyber terror by creating more lucrative target sets and expanding the scope of potential damage. (Ellsmore, N. 2002)

Conversely, some believe that cyber terrorism is not the be all and end all of the future, in that though it could become a nuisance it lacks critical impact. So there are disincentives to pursuing cyber terrorism.

Ellsmore (2002), also puts that cyber terrorism is one of several strategic options available to contemporary terrorist organisations:

- Terrorists have multiple strategic options but limited resources
- A large supply of soft targets means that their traditional methods are still viable
- Cyber terror does not have the potential to produce mass casualties
- Achieving a level of cyber terror capable of producing similar spectacular results requires a significant investment

Though losses could occur, the fact that capabilities for wide spread destruction don’t exist as much as the potential for loss of life, cyber terrorism may be just another one of the tools in the box to be used as required.

In summarising the advantages:

- Cyber terrorism has a lower risk of capture, and can allow supporters of a cause throughout the world to work together.
- Cyber terrorism targets financial systems, and as a result can be used to make a powerful political statement.
- A successful cyber terrorist strike would generate large amounts of publicity and would likely incite fear and paranoia in the public; and

  Cyber terrorist attacks can be quick and cheap. These attacks do not require a great deal of planning – but are more likely to succeed if detailed planning does occur

Finally Denning (2000), concludes that, the next generation of terrorists will grow up in a digital world, with ever more powerful and easy-to-use hacking tools at their disposal. They might see greater potential for cyber terrorism than the terrorists of today, and their level of knowledge and skill relating to hacking will be greater.

The real issue though is what will people say after the crash if a global network Armageddon did occur. Probably the same things they said after 9/11.

2.5 Cyber terrorism management

The management of cyber terrorism risk must be considered an important issue for all aspects of society, not just companies and corporations. Should a major attack occur, we would all be affected. However, in view of the way in which the information network has developed, and the almost complete immersion of much of private enterprise in it, a corporation should analyse its vulnerabilities regardless of societal views.

The dangers in failing to recognise the risks of an attack could be serious. The dangers in recognising the risk but not reacting to it could be equally serious.

As Devost, et al. (2002), put it:

> ”terrorists will always seek to remain just ahead of the counter-terrorism technology curve: sufficiently adaptive to thwart or overcome the countermeasures placed in their path but commensurately modest in their goals (i.e. amount of death and destruction inflicted) to ensure an operation’s success.
>
> In this respect, rather than attacking a particularly well-protected target-set or attempting high risk/potentially high payoff operations, terrorists will merely search out and exploit hitherto unidentified vulnerabilities and simply adjust their plan of attack and tactical preferences accordingly”.

In pursuing this *modus operandi*, a terrorist organisation can reap low-risk, highly visible payoffs by attacking information systems.

There is one major advantage of cyber terrorism in contrast to conventional terrorism. Should an attack be thwarted, it is a simple process to simply change the IP address and direct the attack to another system. Conventional terrorism may require moving to an entire different country.

Planning, training, intrusion detection and monitoring, ring fencing and disaster recovery are all critical factors for cyber terrorism.

2.5.1 Public v private issues and information sharing

Knowing who is the threat is also a key. New Zealand may be a low level target, though many may recall:

- The Rainbow Warrior,

- Neil Roberts, who in 1982 (NZ Herald), walked up to the main entrance of the Wanganui Computer Centre and blow himself up, and

- The bomb in the suitcase at the World Trade Centre office in Wellington, 1984, where Ernie Abbott was killed (newzeal.blogspot.com/2006/06/who-killed-ernie-abbott-my-theory.html),

None of these were really acts of terrorism under the true definition. If they were, if intelligence sources had identified a risk and an adversary, then maybe history would have recorded a different result and three more people would still be alive.

Identifying adversaries through intelligence is also a key. Davey, J., & Armstrong, H. L. (2003) put that every organisation needs to identify its adversaries and that the list should be extensive. From a cyber crime point, attacks could be launched against business organisations by competitors, hackers, clients, suppliers, business partners, disgruntled employees, industrial spies or contractors to name but a few. Then when it comes to Defence environments they say these may be attacked by political groups, governments, hackivists, terrorists or cyber-mercenaries. Again, dependant on who the attackers are and their motives, all or none of the above could be an act of cyber terrorism.

Identifying who in a greater environment is responsible for providing policy, providing standards and sharing of information is critical.

Janczewski, J. L. (2007), agrees it is necessary to determine which groups are likely to utilise Cyber Terrorism to accomplish their goals, and it is important to discuss the reasons that would cause these groups would resort to Cyber Terrorism. Most importantly, in any country who or what organisation bears the responsibility of defence against cyber terrorism.

This situation is not unique to New Zealand, but who does bear the responsibility of defending against cyber terrorism? It has been identified in earlier chapters that CCIP are responsible for policy and coordination with in New Zealand.

Globally as again discussed by Janczewski, most US government organisations have formed groups to deal with cyber-terrorists

- CIA: the Information Warfare Centre
- FBI: investigates hackers
- The Secret Service: banking, fraud and wiretapping cases
- The Air Force: Electronic Security Engineering Teams

Many nations have set up centres for studies on this subject, NZ Centre of Critical Infrastructure Protection (part of GCSB) and similar centres exist in Norway, USA and the UK.

Ellsmore, N (2002), offers that:

> “Within the critical infrastructure industries, we do not know how big the threat posed by information security vulnerabilities truly is. The few computer crime and security surveys that are available present a fragmented, incomplete and inconsistent view of the problem”.

As previously discussed many organisations will not disclose that they have been the victim of an attack due to the organisation not wanting to display that they have vulnerabilities, whilst the Police and media aren’t interested in protection a company’s reputation. As a result of this most statistics are inaccurate.

But competition aside, public and private organisations must share information to fight this global problem, The Business Roundtable suggests that Interpol, with its 178 member countries, is doing a great job in fighting against cyber terrorism, however a joint task force is required to ensure privately owned organisations that provide critical infrastructure share information and adhere to security policies, (Collin, B. C. 2005). Many of these organisations may not want to liaise with a government watch-dog and the establishment of an independent critical infrastructure task force may be required. This task force then liaises with government agencies on behalf of the critical infrastructure elements.

This type of situation will always be a problem, and unless legislation exists to compel the private organisations, critical infrastructure or not, they are at their peril to do as they wish from a commercial direction, as opposed to that which adheres to a CCIP direction.

Stakelbeck, E. (2007), further emphasises that in order to stop attacks, the target would likely need to obtain the cooperation of infrastructure operators, also infrastructure operators are often private entities that do not always have the resources or incentive to respond.

Another reason that attacks are difficult to stop is that the trans-border nature of network infrastructures inhibits effective prosecution of cyber criminals; without legal system coordination, jurisdictional issues may protect attackers from prosecution. In the current legal environment, most adversaries fear no reprisal and can and will attack without risk.

Ghosh. A. K ., & Del Rosso. M. J. (1998), provide the best argument in that:

> “It is important to underscore the fact that private industry owns the critical infrastructures.
>
> The key to providing critical infrastructure assurance is to provide trusted third parties that can collect and disseminate vulnerability information in a trusted manner. Commercial entities do not readily share their vulnerability data with the government

> and other commercial entities for fear of competitive disadvantage as well as possible legal liability."

A central control point such as CCIP is still an absolute must to coordinate the risks from a national perspective.

While cyber terrorism has not occurred on a noticeable scale, it is important to distinguish it from other types of attacks by or on electronic information technology networks, communications and data. The intent to intimidate or kill people or cause mass disruption or destruction for political purposes applies to terrorism however conducted, Bosch, O. (2002). It is critical then that any instance of this must be communicated to the correct authorities so this information can be shared.

Collin, B. C. (2005), strongly agrees, in that the following elements must be considered when building a counter-cyber-terrorist program and also offers:

- "We must accept that while the theories of terrorism stand true, the way in which we approach counter-terrorism, in this case, counter-cyber terrorism, must change.
- We must co-operate and share intelligence in ways we have never before.
- We must enlist the assistance of those individuals who understand the weapons we are facing and have experienced fighting these wars.
- We must learn the new rules, the new technologies, and the new players."

While information sharing will help to enable proactive efforts at securing networks, system administrators also need reactive measures to assist in ending attacks that have already begun. This need is particularly evidence in denial of service attacks, which can be of extended duration and which can cripple a business when they occur.

The Business Roundtable further suggests that:

> “The private sector and the government should co-operate to create joint public and private programs and institutions.
>
> - Improve the ability to warn globally about Internet attacks.
> - Increase the ability to respond quickly.
> - Create a panel of subject-matter experts.
> - Exercise, train and develop processes from lessons learned.
> - Develop a joint program to shore up market confidence.
> - Provide effective oversight and strategic direction.”

Information-sharing globally, nationally, between government agencies and the private sector is therefore crucial, as is education and advice to the private sector, where they are responsible for the management of critical infrastructure, so a secure and coordinated approach exists.

2.5.2 Training

Third party vendors creating back door access to monitor or manage their applications is a risk and should be closed. Any systems administrator or security manager providing this access has lost virtual control of his system. These type of accounts should be closed and open on request by the vendor on an as required basis. If these doors are then opened a heightened state of security awareness can be adopted during the window and extra monitoring conducted.

For that matter any critical system that is connected directly to the public domain, or connected to a network that is, if that connection is not required for its operation should also be severed and connected only on an as required basis. This arrangement can stifle fault management but here are always workarounds.

Awareness training is absolutely critical, computers don’t hack, computers people do. It is absolutely critical that managers, administrators and general users are aware of the risks by providing disclosure of any system information, and should they have external access such as VPN access, that additional awareness be provided. The threat of cyber terrorism creates even bigger risks.

This is further supported by Sproles et al. (1998),

> “Because cyber terrorism is an increasing problem in our society, everyone needs to be aware of what it is and what dangers it presents. Cyber terrorism is a real danger to be looked into by not only computing professionals, but anyone who uses a computer network of any kind”.

President Clinton, in 1996, created the Commission of Critical Infrastructure Protection. The board found that the combination of electricity, communications and computers are necessary to the survival of the U.S., all of which can be threatened by cyber-warfare. Sproles et al (1998).

Regularly training is therefore essential and where access to critical systems is provided, testing to ensure instruction has been assimilated. It is a sure way to determine the message has got through. This method of training doctrine is carried out by the military, including the NZ Army, who has a method to determine that trainees are in fact getting the message and that training is effective.

Any training from the perspective of cyber terrorism awareness must include: the importance of updating passwords regularly, ensuring systems are logged off when not is use, reporting any suspicious network or other system activity and understanding the threat of an inducement to disclose information about passwords or the system in general, as in social engineering and phishing.

Also, training can not be a one off. Refresher training and testing should be conducted regularly and if a major design change or new threat exists, so should training be expanded.

Sproles et al, also offer pointers that must be attended to and should be conveyed to protect against cyber terrorism:

a. All accounts should have passwords and the passwords should be unusual, difficult to guess.

b. Change the network configuration when defects become known.

c. Check with vendors for upgrades and patches.

d. Audit systems and check logs to help in detecting and tracing an intruder.

e. If you are ever unsure about the safety of a site, or receive suspicious email from an unknown address, do not access it. It could be trouble.

Realistically any critical system that also has a remote access functionality, must have a “Remote Access Authentication Mechanism”. Cryptographic token key onetime password methodologies are seen as a method that provides a best practice, should these systems be required to provide remote access. IT and other staff must understand and have training in this.

2.5.3 Planning

Planning is of course still the most critical aspect for the survival of any organisation albeit for a simple hack or an act of cyber terrorism. Any plan must incorporate a number of critical factors, the Certified Information Systems Security Professional (CISSP) training doctrine identifies ten critical domains as follows:

- Access Control
- Telecommunications and Network Security
- Information Security and Risk Management
- Application Security

- Cryptography
- Security Architecture and Design
- Operations Security
- Business Continuity and Disaster Recovery Planning
- Legal, Regulations Compliance and Investigations
- Physical (Environmental) Security.

As these are perceived as industry standards for the protection of Information resources, this section will use these areas as a point of discussion. Aspects that are relevant to a cyber terrorism attack are highlighted.

Any system must have also catered in the planning for C-I-A, to maintain its integrity.

Confidentiality in that it prevents unauthorised disclosure or use of information. The scenario of someone hacking into the Police network and publishing the names and addresses of serving staff is a classic cyber terrorism breach of confidentiality.

Integrity safeguards the accuracy and completeness of information and includes unauthorised modifications to data. In this case in reference to cyber terrorism would be altering data in a SCADA system that could case the release of water from dam causing wide spread devastation.

Availability in that reliable and timely access to information is maintained such as surviving a Cyber Terrorist DDoS attack.

Curts, et al (2002), extend beyond the C-I-A model and identify that we need to look at more than C-I-A, and accept interoperability is a critical factor, for without all the components it may be difficult to cater to the others. Their points are as follows:

- **Authenticity.** The ability to ensure that the information originates or is endorsed from the source that is attributed to that information.
- **Availability.** The ability to ensure that the information is available when needed by the decision maker and/or the decision process.
- **Integrity.** The ability to ensure that the information is protected from unauthorized modification.
- **Confidentiality.** The ability to ensure that only authorized individuals are able to read specific information.
- **Accuracy.** The ability to ensure freedom from error, as related to programs, operations and machine capabilities.
- **Timeliness.** The ability to ensure the delivery of required information within a defined timeframe.
- **Completeness.** The ability to assemble necessary and sufficient information upon which to base a rapid, active information presentation and mission decision.
- **Security.** This attribute encompasses both the physical and information security (INFOSEC) areas.
- **Flexibility.** This attribute includes the ability to be responsive to change, specifically as it relates to the information needs and changing operational environment of those personnel working with the Information Warfare systems.
- **Affordability.** The extent to which Information Warfare system features are cost-effective on both a recurring and non-recurring basis.
- **Continuity.** The uninterrupted availability of information paths for the effective performance of Command and Control functions.
- **Versatility.** The ability to adapt readily to unforeseen requirements.
- **Simplicity.** The ability of the user to maintain a balance between technological sophistication, and standardization with the ability to maximise full use of the Information Warfare systems.
- **Interoperability.** The capability of all IW, C^2W, and C^4ISR systems to work together as a system-of-systems.

Interoperability is compatibility amongst all combined, and individual component information or data elements and procedures. It reflects a secure, seamless, cohesive architecture that satisfies secure information handling at all levels.

It is then imperative for all critical systems to have interoperability strategies, data classifications and management practices in place to avoid a critical failure if they become the victim of a cyber terror attack.

Business Continuity Planning (BCP) and Disaster Recovery (DR) planning are two items that are too often overlooked or placed on the 'we'll get to later' list. As the old saying goes, if you fail to plan, you plan to fail.

Survivability is an especially appropriate concept in the context of computer/telecommunications infrastructure, because, as most network managers will attest, under normal operating conditions some part of a network is almost always broken during any given time period, Yurcik, W. (1999).

With cyber terrorism being an attack on an element of critical infrastructure, it will surely require a BCP to have services up and running as soon as humanly possible. The elements that have been discussed as being part of our life now control our life and we can not operate on a day to day basis without them. But in many cases the non-computerised manual systems that we relied upon for many administration and operational parts of our lives have now gone. Many people employed in the work force today know of no other way of doing things but through the aid of electronic automation. Many people these days would have difficulty living with out their mobile phones alone.

Any BCP for government or critical infrastructure should assess the opportunity to establish emergency backup systems, that allow operation firstly without electricity and then at a lesser levels including operating with just non network based computer systems to cater to all possible alternatives. We could operate for a day without power or network connectivity and many most likely many have, during a failure or even while moving offices, but beyond this business can become effected. This is where continuity planning is required. Many plans for this just simply don't exist, don't go far enough, or are out of date. When considering plans such as this, think of the worst and have a counter strategy, CPDRG. (http://www.contingency-planning-disaster-recovery-guide.co.uk)

With DR planning for IT systems, there is no shortage of literature in existence to provide guidelines for the establishment of a DR plan. A DR plan again needs to cover every possible situation. Given an attack from cyber terrorism is likely to be serious and catastrophic, a worst case situation needs to be included and be tested, and be effective for all government systems and elements of critical infrastructure.

Any DR plan needs to allow for complete independent system operation, as if an attack occurs, though an Immediate Action Plan may provide for network disconnection and recovery action, reconnection may result in an immediate re-attack as the threat may have not as yet been eliminated.

2.6 Research questions

This literature review has provided an insight into the precursors to cyber terrorism and the elements that blend together to establish its existence. It has also identified that planning and training are necessary to provide readiness should an attack occur. From this knowledge a platform can be established, that will allow a comparison of the results obtained through the research, against this benchmark.

The literature review has also assisted in determining what research questions need to be asked to assist in providing an answer to the research objective.

The research objective is:

> **To determine the state of the New Zealand Government and critical infrastructure ready reaction to cyber terrorism.**

To satisfy this objective and from the information provided in this chapter the, following questions need to be addressed.

1. **Do the organisations have knowledge of what cyber terrorism is?**

2. **Do the organisations have ready-reaction plans in the event of a cyber terrorism attack?**

3. **Do the organisations conduct staff awareness training in preparation should an event of cyber terrorism occur?**

4. **Do the organisations have knowledge and have intelligence gathering concerning cyber terrorism?**

5. **Are the privately owned critical infrastructure elements being influenced by CCIP to ensure a common level of security is met, and is the level of planning way less than their government counterparts?**

2.7 Conclusion

This chapter provided much discussion and background on the aspects of terrorism and the aspects and associated components of cyber terrorism. This has then provided the background to provide in-depth knowledge to further enhance research into this area. Some discussion was then provided on what could potentially happen as a result of an attack of cyber terrorism, who could be the targets and what could be the outfall from an attack.

This research is also assessing what level of knowledge, planning, awareness and training exists on cyber terrorism. The latter part of this chapter then focused on those areas to provide past research to assist in determining a standard, to be used as a benchmark against the research.

Chapter 3. Background Information

3.1 Chapter objective

This chapter introduces the materials that will be used in the research and in this case the materials will be data collected from a sample of human participants, these being employees from a number of organisations.

The first section provides a brief description on the New Zealand Government structure.

The participants in this research are NZ Government departments and elements of the critical infrastructure, which include ISPs. An introduction and explanation of their roles is provided and the elements that make up the critical infrastructure are further identified.

3.2 The Sample

In line with the objective of the research, the sample selected to provide the data in order to gain the responses required has come from security officers of government departments and from the elements that make up the critical infrastructure and some ISPs.

3.2.1 The NZ Government Departments

A full description of all the New Zealand Government departments is located at Appendix 1.

The Critical Infrastructure within New Zealand is owned and or controlled by either central government, state owned enterprises, local government or private enterprise, which are either owned by national or international entities.

Health is predominantly central government owned, water, sewage management and the local roading infrastructure are owned and managed by local government, whereas electricity supply and gas are not.

Telecommunications are predominantly privately owned, yet the national grid and power generation facilities are mainly owned by central government.

Given this diversity of ownership and management of the critical infrastructure, security and risk will need good control, management and communications, to ensure notification of any threats are communicated rapidly to all the entities.

Policing and Security

Some of the central government agencies listed below are responsible for the maintenance of law and order and security:

- NZ Defence Force
- NZ Police
- NZ Customs
- Ministry of Agriculture and Forestry (MAF)
- Government Communications Security Bureau (GCSB)
- Department of Prime Minister and Cabinet (DPMC)
- NZ Security and Intelligence Service (SIS)
- Department of Internal Affairs (DIA)

Security and Intelligence however is managed by a number of agencies that fall within these groups these being:

http://www.security.govt.nz/)

NZSIS

The NZSIS is a government agency, responsible for giving the government advice about matters relating to New Zealand's security. The Service has approximately 200 staff, comprising:

- intelligence officers
- support staff, and
- specialists (including linguists, technicians, legal and accounting staff and information professionals

Role

The NZSIS is a civilian intelligence and security organisation. Its threefold roles are:

- to investigate threats to security and to work with other agencies within government, so that the intelligence it collects is actioned and threats which have been identified are disrupted
- to collect foreign intelligence, and
- to provide a range of protective security advice and services to government.

(http://www.nzsis.govt.nz/about/)

GCSB

The Government Communications Security Bureau (GCSB) in New Zealand has a dual role in this field. Firstly GCSB is a major contributor of foreign intelligence to the New Zealand Government through its foreign signals intelligence collection; secondly the GCSB is responsible for providing advice and expertise to ensure that the government's official information is protected.

Role

As an intelligence and security agency the level of information available about the GCSB's role is, by its very nature, restricted. In order to maintain our level of effectiveness we must also retain a certain level of secrecy, especially about our intelligence targets and the details of our capabilities, sources, and methods. However as the public profile of intelligence and security agencies has risen, the availability of information has increased, as has the level of accountability the organisation has to provide.

(http://www.gcsb.govt.nz/aboutus/index.html)

CCIP

The Centre for Critical Infrastructure Protection (CCIP) is a business unit within the Government Communications Security Bureau (GCSB).

Critical National Infrastructure (CNI) is defined as those systems and assets, whether physical or virtual, so vital to New Zealand that the incapacity or destruction of such systems and assets would have a debilitating impact on the security of the nation, the economy, public health and
safety, or any combination of those matters.

CCIP is focused on protecting New Zealand's CNI from cyber-based threats. The Ministry of Civil Defence and Emergency Management is focused on improving New Zealand's resilience to hazards and disasters, which includes increasing the protection from physical threats to New Zealand's CNI.

Functions:

- To provide 24/7 watch and warning advice to the owners and operators of our CNI and the New Zealand Government;
- To investigate and analyse cyber incidents that occur against our CNI; and
- To work with CNI protection agencies both nationally and internationally to improve the awareness and understanding of cyber security in New Zealand.

(http://www.ccip.govt.nz/about-ccip/what-is-cni.html)

EAB

The External Assessments Bureau (EAB) is New Zealand’s central foreign assessments agency. Its function is to provide objective assessments to the Prime Minister, other ministers, senior officials and New Zealand’s diplomatic missions abroad, of external events and developments that bear on New Zealand’s interests internationally. In carrying out this function, EAB's purpose is to help to inform decision making by the Government on external issues.

EAB is one of the six business units of the Department of the Prime Minister and Cabinet (DPMC), and forms part of New Zealand's intelligence community. It uses the widest possible range of information available from open media sources, such as academic research, commentaries by think-tanks, and internet sites. It also draws on diplomatic reporting and other forms of classified material from intelligence sources. This intelligence is provided by the Government Communications Security Bureau and the New Zealand Security Intelligence Service.

DDIS

The Directorate of Defence Intelligence and Security (DDIS) is a component of the Strategic Commitments and Intelligence (SCI) Branch of Headquarters, New Zealand Defence Force (HQ NZDF). The role of DDIS is to provide a central focus for the intelligence and security staff within the New Zealand Defence Force (NZDF). It achieves this by providing direction and coordination of Defence intelligence and security issues, activities and procedures from HQ NZDF in Wellington to the Headquarters Joint Forces New Zealand and the operational units of the NZDF in times of peace, crisis or conflict.

National information infrastructure protection

On 8 December 2000, the E-government Unit of the State Services Commission reported to the Minister of State Services on 'Protecting New Zealand's Infrastructure from Cyber-Threats' and its recommendations were accepted. One recommendation from that report was:

(That Ministers) through the State Services Commission, direct government agencies to adopt specified appropriate IT security standards. These are located at the site below:

(http://www.e.govt.nz/archive/services/safe/internet-security-standards.html)

In February 2001, the State Services Commissioner invited the Government Communication Security Bureau (GCSB) to establish how the recommendation could be implemented. GCSB consulted with 17 agencies that comprise the Government's Interdepartmental Committee on Computer Security (DCCS), developed and presented the Commission with a draft set of standards.

http://www.e.govt.nz/archive/policy/trust-security/niip-report/chapter6.html

3.2.2 The critical infrastructure

The government agencies listed above are policy makers and administrative management agencies. Critical infrastructure is the key to domestic operations within a country. Elements such as water, sewage, power, transport, and communications are critical to the daily operation of a country, hence they are referred to as critical infrastructure.

The following diagram shows how the various Critical Infrastructures depend on each other. Most systems assume the continuing supply of power and telecommunications. (CCIP. 2001).

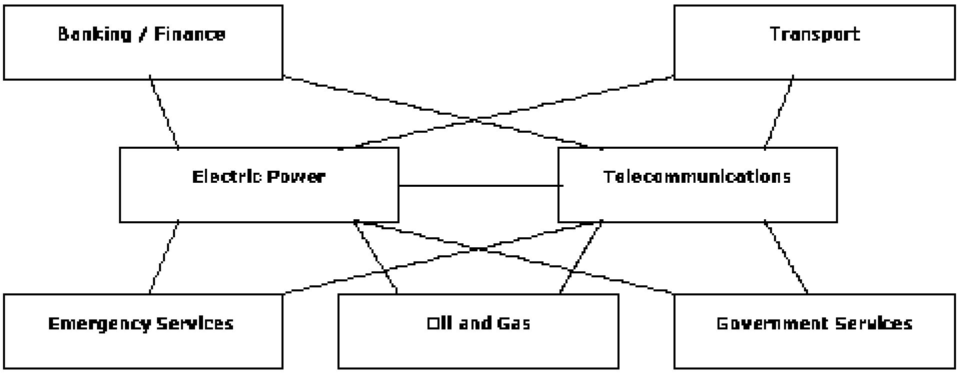

Figure 5: Critical infrastructure dependences

It was not long ago that all of the elements of Critical Infrastructure were owned and controlled by either local or central government. The 80's and 90's saw a change in this paradigm to either that of a state owner-enterprises or complete private ownership. Some deregulation also provided more private ownership of key resources and infrastructural elements.

There are issues with this. Though the government may set some rules and regulations, many of the organisations are free to conduct activities that benefit them from an economical perspective. Though CCIP may dictate policy with regard to the protection of critical infrastructure, unless it is entrenched in law they are not required to abide by it. Private organisations therefore are bound by shareholders demands, competition, marketing situations and developmental growth, in contrast to providing what the public wants. Though the government doesn't own the infrastructure it has a role in ensuring it is adequately protected. Hence this is the principle function of CCIP.

The other issue is that government agencies themselves are also reliant on the use of privately owned critical infrastructure such as the communications networks.

The ownership of critical infrastructure is diverse, (CCIP, 2001):

- Central government departments own items such as the computers running the SWIFTT benefits payment system.
- The Defence and Police forces have computer systems and communications networks.
- Hospitals use computer systems for accounting and administration.
- The Reserve Bank currently operates banking settlements systems.
- State-owned enterprises such as Transpower and Airways own critical networks.
- Much critical infrastructure is in the private sector, including telecommunications and local electricity distribution.

Because of this diversity, there are concerns expressed that commercial incentives are outweigh the needs of infrastructure security. The government must therefore consider how it can assure itself that risk management is adequate.

The following two diagrams also provided by CCIP display threats and vulnerabilities. These models are adapted from Australian and New Zealand Standards.

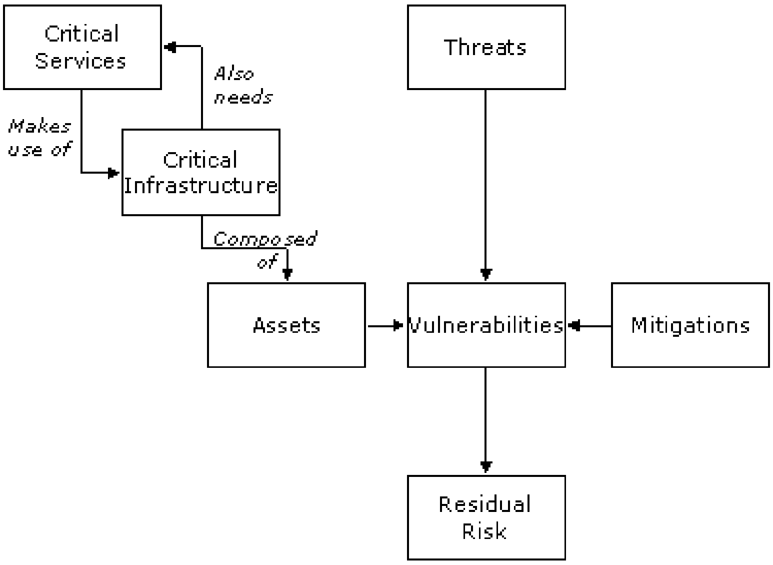

Figure 6: Infrastructure Threats and Vulnerabilities

The diagram at figure 6, shows the critical services depending on infrastructure, some areas of which themselves depend on other services. The components of the infrastructure, referred to as assets, are subject to vulnerabilities. Vulnerabilities may be exploited by threats. The action of a threat on a vulnerability may be mitigated through various strategies.

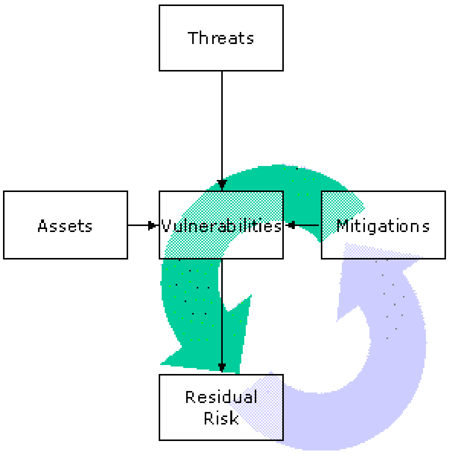

Figure 7: Risk Mitigation Cycle

After risks have been mitigated there is always some residual risk as shown in figure 7, which needs to be assessed. If it is found unacceptable further mitigation measures will need to be applied.

Risk has two components: the consequence, or impact of an event; and the likelihood of the event. Because infrastructure is obviously valuable, physical risks have generally already been considered and some measure of protection applied. The risk of damage to infrastructure from physical threats therefore tends to have a low likelihood, albeit a high consequence.

3.2.3 Critical infrastructure in New Zealand

The following is an overview of the critical infrastructure in New Zealand.

Finance and Banking

The New Zealand finance and banking sector contains retail banks, other financial institutions and purely infrastructural organisations. Retail banks are licensed by the Reserve Bank of New Zealand, which imposes various conditions on their operation. Each bank runs its own retail account processing system. Most maintain accounts with the Reserve Bank from which they pay each other during the course of each day. Interchange and Settlements Limited (ISL) operates payment "switches" which route transactions from one bank to another.

Transport

The most significant section of national transport infrastructure potentially vulnerable to information-related threats is the air traffic control system. This is operated by the Airways Corporation, which is a state-owned enterprise. The major vulnerability is loss of telecommunications systems, which are, in the main, provided via leased bearers. However, most communications links can use multiple routes. Further back-up using satellite capacity is under consideration. Airways Corporation also has a strong service level agreement with its telecommunications provider.

Another section under transport that could have an effect are traffic lights which would be affected from an incident as outlined below. It is possible where some of the traffic lights controlled from a centralised control centre could be targeted if that system was infiltrated.

Electric Power

The electric power industry in New Zealand comprises a number of generators, the national power grid operated by Transpower, local infrastructure ("lines companies") and the various power retailers.

The generators have a number of power stations of different types. While it is quite possible to imagine that these have vulnerabilities, no one generator, or particularly no one power station, is crucial to ensuring continuity of supply. If any one generation company were to fail totally, under most circumstances New Zealand would have enough power. The issue of protection therefore becomes one of commercial prudence for each company, and need not be examined further here.

The retailers, while they market and account for power, do not own the infrastructure - the local lines - which is used to deliver it. Damage to their computer systems and records would harm only their own businesses and they have every commercial incentive to ensure that this does not happen.

Failure of the core networks of Transpower or the lines companies would cause loss of supply. This is not to imply that they are in any way suspect; rather that government has a greater interest in their continued delivery.

Telecommunications

New Zealand has a number of companies offering telecommunications and Internet services. The major telecommunications companies ("telcos") operating in New Zealand offer robust domestic voice and data networks.

New Zealand's international telecommunications pass through one of three submarine cables, or go via satellite. Submarine cables are vulnerable to damage by anchors and fishing gear, and to sabotage. The cables were laid some years apart. Each successive cable has many times the capacity of its predecessor. Failure of the highest capacity cable would thus have a severely detrimental effect on New Zealand's connectivity with the rest of the world.

The Internet

The Internet is increasingly both an important business tool and an infrastructure for commerce. It is central to the whole notion of e-government.

The Internet's importance impels businesses to connect their systems to it. There are, however, significant security risks in interconnecting business systems and the Internet.

It is the nature of the Internet to be open to all, highly decentralised, and to allow (or even encourage) very rapid technical innovation. These attributes, while they have facilitated the explosive growth of the Internet, also lead to significant threats to machines connected to it. The vulnerabilities described below do not just apply to Internet business, but to all businesses with an Internet connection.

Oil and Gas

There are a number of different companies involved in oil distribution in New Zealand. The main retailers are very competitive and are fully aware that any failure on their part would result in loss of market share as consumers switched to alternative suppliers. The Marsden Point oil refinery is shared by several oil companies, but this only provides a proportion of New Zealand's petroleum products, since some are imported. Failure of the refinery for whatever reason would be subject to normal contingency plans for this event. The coastal tanker fleet is also shared, but is not thought to be vulnerable to IT based attack.

Gas is widely used for domestic heating and also supplies at least one power generation station, however it is questionable whether it can be regarded as critical. The commercial incentives on the companies providing gas services are regarded as sufficient to ensure that they protect their infrastructure adequately.

Emergency and Government Services

Defence

The New Zealand Defence Force makes extensive use of telecommunications, both nationally and internationally. For example, NZDF establishments throughout the country are interconnected over leased telecommunications bearers. Communications with deployed forces overseas, and communications with allied nations also generally use leased bearers. Considerable use is also made of the Internet for unclassified communications. But the NZDF also has its own integral communications capabilities with the capacity to provide 'thin red line' communications in the event of disruption of the national or international carriers and has the tested capability to provide emergency communications for Government in the event of civil or other disaster.

Police

The New Zealand Police enterprise communications network and has switch centres in Auckland, Wellington and Christchurch with sufficient redundancy to ensure that operations will be unaffected by the loss of any one centre. The backbone network uses shared sites although some sites are Police owned. The Police Emergency 111 service is operated by a Telecom contractor, who passes calls to police, fire or ambulance as appropriate. Police and fire share the emergency communications network, but ambulance services are disparate organisations so are not integrated. A key police development strategy is the implementation of a common network for all emergency services.

Fire

The New Zealand Fire Service uses communications facilities which it shares with the New Zealand Police, and which are discussed under that heading. There are no significant concerns in this respect.

Revenue and Income Support

Inland Revenue Department and Department of Work and Income handle high volumes of time-critical financial transactions for Government. Disruption to these departments' core infrastructure might have adverse effects for many New Zealanders.

Water

Water is supplied by local authorities and is not part of a national infrastructure as such.

This last issue is where the system can become an issue and breaks down, in that though water distribution is managed by local Government it appears to fall outside of the scope of national infrastructure. To the domestic household, water and power would be seen as the two most critical elements of our critical infrastructure.

The research will hopefully contrast any management concepts in variance of a standard, whereby these remote elements of critical infrastructure may or may not have adequate planning in place against a cyber based attack.

3.2.4 Participants

As listed there are numerous government departments within New Zealand, and furthermore there are a far greater number of private organisations that make up the critical infrastructure, so it is not feasible to canvas every organisation. A representative sample of government departments and private organisations that make up some of the critical infrastructure have therefore been selected. From this it is perceived a representative sample will be provided that will satisfy the research as being sufficient in size.

Due to the conditions imposed, for security reasons the actual names of the private organisations or the staff or actual sections of the government departments cannot be disclosed. The type of services canvassed however can be.

The government departments can be viewed at:
http://newzealand.govt.nz/directory/

The critical infrastructure canvassed were:

Local Government

Electricity Company

Telephone Company

Mobile Phone

Gas

Transport

Water

Sewage

Banking

Ambulance

Hospital

ISP

It is the security officers within these organisations who are the recipient of the questionnaires, as they are considered as the point within these organisations with the knowledge to provide the answers.

3.3 Conclusion

This chapter has provided an introduction to the New Zealand Government departments and the elements together that form the critical infrastructure. As discussed, it is the government and the critical infrastructure that allow the continuous and harmonious operation of a country. Any interruptions to the operation can have an impact that could be disruptive, costly and to some extent cause damage or in some cases loss of life. Should these organisation become a target of cyber terrorism then these problems would be the outcome.

The next chapter will look at how these organisations will assist with the research, the approach, and method of data collection.

Chapter 4. Methodology

4.1 Chapter objective

This chapter will discuss the research methodology that the study will use to answer the questions that were identified at the conclusion of chapter 2. Also to draw attention to the study by providing a definition of the nature of it, and identifying the approach that has been adopted to obtain the answers for the research questions.

It will then address the research problems in that what questions need to be asked of the participants to gain the data required to answer those questions. The interview process will then be discussed.

4.2 Methodology

4.2.1 Approach to research

There are three main research paradigms also referred to as the approaches to research. These being: quantitative, qualitative or mixed research, (Johnson, B. 2007). Quantitative research involves the collection of quantitative data, such as the collection of measurable variables. The types of quantitative research are usually either experimental or non experimental. Qualitative research relies on the collection of qualitative data, often qualitative data will form the basis of a pilot study, where the aim is to get the best possible feel for the situation through broadly defined data, (Markham, S. 2007). Qualitative research types are: Phenomenology, Ethnography, Case Study, Grounded Theory or Historical. A mixed research approach involves mixing of quantitative and qualitative approaches. The types include mixed method and mixed model.

A diagram of the typology of research approaches is as follows:

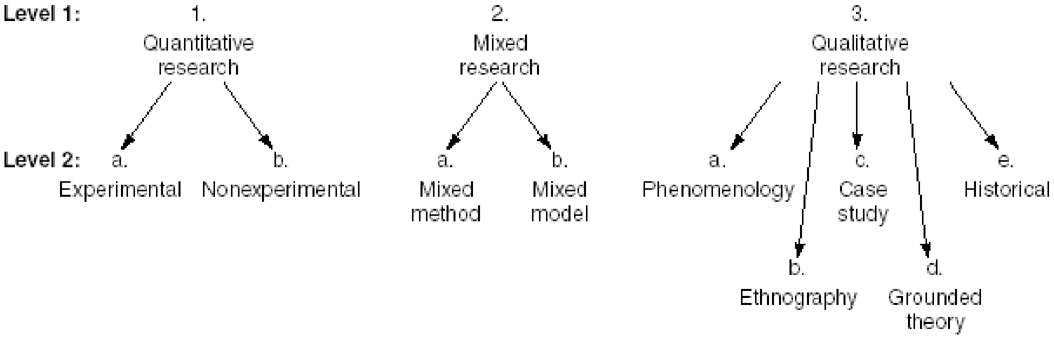

Figure 8: Research topology

The purpose of this research as previously discussed is to determine the state of the New Zealand Government and critical infrastructure ready reaction to cyber terrorism. The focus then is on gaining data from the participants to determine their level of knowledge understanding and readiness on cyber terrorism. A qualitative approach is going to be adopted, using a case study subtype to source the necessary data from the participants.

4.2.2 Method of data collection

Depending on the focus of the research question, the researcher needs to decide whether the study will be exploratory, descriptive, or hypothesis testing. (Tharenou, P., Donohue, R., & Cooper, B. 2006). Exploratory studies are those where the researcher knows little about the situation, or has no information on how similar research problems have been solved. Descriptive studies are those undertaken to describe the characteristics of variables in a situation. Descriptive studies may be conducted in organisations to learn about and describe the characteristics of particular employees. Hypothesis testing studies try to explain the nature of certain relationships, or to establish the differences among groups. Hypothesis testing goes beyond describing the relationships in a situation to understanding the relationships among factors (variables) in a situation.

This study has adopted the descriptive approach as it is intended to focus on the characteristics of an organisation’s understanding of the problem of cyber terrorism.

There are six main data collection methods: (Markham, S. 2007).

- Tests (i.e., includes standardized tests that usually include information on reliability, validity, and norms as well as tests constructed by researchers for specific purposes, skills tests, etc).

- Questionnaires (i.e., self-report instruments).

- Interviews (i.e., situations where the researcher interviews the participants).

- Focus groups (i.e., a small group discussion with a group moderator present to keep the discussion focused).

- Observation (i.e., looking at what people actually do).

- Existing or Secondary data (i.e., using data that are originally collected and then archived or any other kind

Due to the geographical displacement of the participants and their possible reluctance to take time out for an interview, the questionnaire data-collection method has been adopted also.

A cross-sectional study of the results will then be adopted during the analysis.

An interview questionnaire has been prepared for the participants, and this contains 19 questions. Appendix 2. It is intended that the data collected through the interview questionnaires, after analysis, will provide answers to the research questions.

4.3 Research questions

4.3.1 Research question 1

Do the organisations have knowledge of what cyber terrorism is?

To determine what level of knowledge exists in the Government departments, the critical infrastructure organisations and ISPs, the following questions need to be asked to determine the level of knowledge and under standing of cyber terrorism that exists.

- What does your department understand the definition of terrorism to be?
- What does your department understand the definition of cyber terrorism to be?
- Is your department aware of any international incidents of cyber terrorism?
- Is your department aware of any incidents of cyber terrorism in NZ?
- What does your department see as the main threat, should an act of cyber terrorism occur should one be directed at your department?
- Who is considered to be a threat to your department***?***

4.3.2 Research question 2

Do the organisations have ready reaction plans in the event of a cyber terrorism attack?

As identified, planning is critical in any business activity, private or government. This planning also needs to extends to general security, IT security and other incidents such as terrorism and cyber terrorism, It is therefore necessary to obtain data from the participants to determine what level of planning exists for cyber terrorism. The following questions are for that purpose:

- Does your department have a terrorism ready reaction plan?
- Does your department have a cyber terrorism ready reaction plan?
- If so is it current?
- If your department does not have an awareness strategy, training and a ready reaction plan for cyber terrorism does it consider they are necessary? (Please comment on each).
- If they are considered necessary will your department be commencing a ready reaction plan?

4.3.3 Research question 3

Do the organisations conduct staff awareness training in preparation should an event of cyber terrorism occur?

Awareness training is seen as a critical occurrence and though early warning devices and intrusion-detection facilities may exist, it is having staff with the knowledge to recognise and report incidents of abnormality to the appropriate people which is necessary.

Therefore it is important to determine if staff awareness training exists. The following questions address this issue:

- Is there a staff awareness of the risks of an attack of cyber terrorism?
- Is there staff awareness on the likelihood of an attack?
- Is there staff training on the possibility of an attack of cyber terrorism?

4.3.4 Research question 4

Do the organisations have knowledge and have intelligence gathering regarding cyber terrorism?

It was discussed in chapter 1, that IT professionals and the average user continually keep ahead of security threats by continually updating virus software. The same reasoning applies to cyber terror attacks, and it is critical that organisations share information on new threats and that research and intelligence gathering occur to determine what new threats exist. The following questions are designed to draw this information from the participants.

- What does your department foresee the likelihood is, of an act of cyber terrorism occurring?
- What impact would an attack such as a major denial of service have?
- What impact would an attack have such as an incident of trespass on the department's IT resources?

- Is there any knowledge-seeking in cyber terrorism occurring?
- Does your department foresee cyber terrorism being an issue in the future?

4.3.5 Research question 5

Are the privately owned critical infrastructure elements being influenced by CCIP to ensure a common level of security is met, and is the level of planning way less than their government counterparts?

It is envisaged that the government departments will be well prepared and knowledgeable in cyber terrorism. However the level of knowledge and planning in the private sector will be determined from this research. Comparisons can be made between the two groups of interview questions - those from the government source and non-government - to contrast the level of differences that may exist. No specific questions then need to be asked to determine this information.

4.4 The collection process

The type of organisations identified in chapter 3, are the participants in this research. The exact identify of those organisations will remain confidential and will not be advised within this Thesis. Both government and non-government organisations have been approached directly with the questionnaires, a covering letter and other associated documents.

The participants were asked to participate voluntarily in the research and to complete the questionnaire and return it. The returned questionnaires will then be analysed so the answers to the research questions can be obtained. The next chapter will analyse and provide a summary for each of the questions.

4.5 Conclusion

This chapter commenced by identifying that this research will adopt a qualitative approach utilising a case study subtype. The research method was identified as being a descriptive approach. A cross sectional approach will then be utilised to compare results between different participants.

The data collection process was carried out by way of distributing written questionnaires to the participants.

The research questions were further discussed and the questions presented to seek the data required to answer the research questions.

Finally the manner in which the interview questions are to be distributed was discussed.

Chapter 5. Analysis of Results

5.1 Chapter objective

The objective of this chapter is to provide an analysis of each interview question from the results obtained through the questionnaires. A summary of the results are relevant to the specific research question is then provided.

The chapter will be able to identify any differences that occur between organisations, and if any contrast exists in the results between the government agencies and the privately owned organisations. This aspect however will be discussed after the analysis of the other questions.

As well, this chapter will be conducting an assessment from the results to determine if CCIP has influenced the critical infrastructure. It will also assess the comparisons between the organisations - both government and private - and how they compare with international benchmarks.

Even if there is some level of planning and knowledge, if this is below international benchmarks, then in the event of a cyber terror attack a problem still exists that requires attention, to avoid a potential interruption to the provision of critical infrastructure services.

The questionnaires were distributed to 16 government agencies and 15 critical infrastructure, telecommunications companies (Telcos) or Internet Service Providers (ISPs), a total of 30.

A total of 12 completed questionnaires were received, 4 from government, 4 from critical infrastructure and 4 from the Telco/ISP group. This provided an overall return ratio of 40%. Every effort has also been taken to protect the identity of the source of each organisation and the confidentiality of each participant within those organisations. A full list of the responses for each interview question are displayed at Appendix 3.

5.2 Research question 1

Do the organisations have knowledge of what cyber terrorism is?

5.2.1 Interview responses

- **What does your department understand the definition of terrorism to be?**

Summary of responses

- 58% of the responses included the word “fear” as being one of the elements of conventional terrorism.
- 50% of them appear to have been quoted direct from a research source as opposed to having come from current knowledge.
- 66% included an element of harm or violence to civilians.
- One specifically as shown at item 1(c), of Appendix 3, the 4th respondent perceived it as subverting stability of the government but didn’t identify by what means.
- The full list of responses for this question are displayed as item 1, Appendix 3.

From the summary above it can be identified that generally there is a good understanding of what conventional terrorism is. A key factor as seen in chapter 2 is that the object of terrorism is to create fear by threats or damage to persons or property, and is understood to be a part of the general knowledge of the participants. Furthermore as identified in chapter two another key factor is the motivation or affiliation. Though some of the participants identified motivation as in political or religious based, none identified an affiliation with a known terrorist group as a key factor.

From the actions of 9/11 and other attacks, most people have become knowledgeable on conventional terrorism, primarily though media attention. From those attacks many government departments and other organisations have become more risk-averse to the entire terrorism concept and have taken action in preparation for an act of conventional terrorism. It is from these aspects that it is thought to have added to people’s general knowledge and understanding on conventional terrorism.

- **What does your department understand the definition of cyber terrorism to be?**

Summary of responses

- The responses were far more diverse, some of the government agencies were more accurate than the other groups, item 2(a), of Appendix 3.
- 58% concluded it was the same as conventional terrorism but using computers or information technology to do so.
- 25% suggested that it was actions that it inflict harm though the use of technology.
- 25% also suggested the disruption of services was an outcome.
- The full list of responses for this question are displayed as item 2, Appendix 3.

With much less media and general knowledge on cyber terrorism, the understanding by the participants was also much less. Collectively, an accurate definition would be accurate, however individually many were too brief. Conventional terrorism as discussed is about causing harm or fear of harm and in essence creating terror. As identified in Chapter two it is less likely to cause direct harm to victims through an act of cyber terrorism, but more likely to cause damage to property, major disruptions though actual harm to people would be possible fallout from an attack.

Given some of the agencies were responsible for the provision of critical infrastructure services, it is possible from the responses that due to the general lack of knowledge in this area, they may not foresee all the potential vulnerabilities that exist within their organisation. The unauthorised access to a network, followed by negotiating through the systems to the SCADA network and causing a disruption of supply or a release of effluent are actions that are certainly real and must accordingly be seen as a threat.

Though the terrorists and their motives may be the same, the impact of cyber terrorism could be potentially far greater and wider than with conventional terrorism. From these responses, this may not be understood.

- **Is your department aware of any international incidents of cyber terrorism?**

Summary of responses

- This question produced limited responses and where they identified knowledge it was not confirmed or supported by specifics.
- 50% of the government agencies again possessed more knowledge, item 3(a), of Appendix 3.
- The full list of responses for this question are displayed as item 3, Appendix 3.

As covered in chapter two there have not been many major reported incidents worldwide that were confirmed as acts of cyber terrorism. Attacks on information technology resources have occurred worldwide by hackers and other criminals, however these were not terrorist acts. These also gain media attention in the tabloids, but in many cases they have been identified as not being critical systems, and as a result have not gained high media attention. It is only when a major disruption has occurred does the impact gain the attention of the public at large. It is then perceived that people may see an event as terrorism due to the size of the incident, and not that it is an act of terrorism because of the terrorists and their motives.

- **Is your department aware of any incidents of cyber terrorism in NZ?**

Summary of responses

- Though 17% indicated they are regular victims of attack, unless they are investigated it is unknown if they are an attempt at hacking or cyber terrorism.
- Only one (shown at item 4(b), of Appendix 3, the 2nd respondent) said they knew of several instances across NZ, the remainder replied “no”.
- The full list of responses for this question are displayed as item 4, Appendix 3.

Whilst the incidents of hacking gain media attention, there are no known acts of cyber terrorism having occurred directed at a NZ target. It thought then that the one response of having knowledge was most likely a problem with the understanding of the term cyber terrorism. Again this being misconstrued as an act because of its size or attention it has gained and not because the specific ingredients are met.

- **What does your department see as the main threat, should an act of cyber terrorism be directed at your department?**

Summary of responses

- The understanding and responses for this question were more accurate.
- 58% saw a DDoS as being the main threat also loss of access to sensitive information.
- Two provided results that indicated they thought there were no threats.
- The full list of responses for this question are displayed as item 5, Appendix 3.

This question provided some detail that identified there is some understanding of the technical risks present. Some participants who are responsible for critical infrastructure protection did not understand that gaining unauthorised access to their systems held far greater risks. This is again a concern that there is a lack of understanding of all possible risks and should a determined cyber terrorist gain access, remote control of resources could cause absolute havoc.

Many system administrators believe their systems are bullet-proof and probably do not conduct a threat assessment of the risks that could occur. From this response the issue of gaining access to systems that control critical infrastructure and then controlling them is a major concern. Shutting down power, communication networks, releasing water or sewage are all actions that could occur should remote control of the critical infrastructure by a terrorist occur. Some of the participants in this research are responsible for the management of such services.

The response to this question shows there is a lack of understanding of all the potential risks that occur, and though those mentioned are certainly a concern, the others mentioned could have a greater impact and lengthen the recovery period. It appears the participants have looked at this question from an IT perspective, and not have considered the secondary actions, in that the same computer system controls items of physical critical infrastructure. It is the unauthorised interaction with those IT systems that is the cause of concern.

- **Who is considered to be a threat to your department?**

Summary of responses

- Only 25% of the participants provided an accurate response to this question.
- 58% identified the hacking community, competitors or anyone.
- The full list of responses for this question are displayed as item 6, Appendix 3.

For an act to be considered an act of terrorism it must be conducted by a terrorist with terrorist motives. One government agency and one major critical infrastructure organisation addressed the international aspect with specific motives. The remainder did not grasp the aspect of “the terrorist attack”, in that the incidents they have highlighted are merely hackers or disgruntled people.

Again from these responses there appears to be a lack of understanding of cyber terrorism.

5.2.2 Summary

Though there was a reasonable level of understanding on conventional terrorism, the knowledge of cyber terrorism is limited, as is the understanding of the full wider risks of an attack, specifically the secondary actions that could occur once control of a network exists.

This is further confirmed by the responses as to who was considered to be a threat. The response to the suggestion international terrorist organisations were motivated to commit an act of terrorism against NZ was deficient.

5.3 Research question 2

Do the organisations have ready reaction plans in the event of a cyber terrorism attack?

5.3.1 Interview responses

- **Does your department have a terrorism ready reaction plan?**

Summary of responses

- 17% of the organisations have some form of formal planning.
- The other 83% either have nothing or just general contingency plans.
- The full list of responses for this question are displayed as item 7. Appendix 3.

There appears to be a general level of planning for contingencies in case of an incident but nothing terrorism specific. The reaction to an incident of conventional terrorism is likely not to be too dissimilar from any other disaster, however a plan should cover such aspects as terrorism alerts and immediate actions should suspicious actions or a terrorist attack occur. The other types of plans are unlikely to cover this.

- **Does your department have a cyber terrorism ready reaction plan?**

Summary of responses

- No organisations had a specific cyber terrorism plan.
- 58% of the organisations had some form of Disaster Recovery (DR) planning.
- The full list of responses for this question are displayed as item 8, Appendix 3.

None of the organisations have a specific cyber terrorism reaction plan. Most have a DR plan or similar and though a DR plan will assist with network or other system recovery, as previously addressed an act of cyber terrorism can cause non-IT based disasters. Many IT systems are such that they are not unique, that another hard disk drive motherboard or processor can be replaced and data restored to allow the functioning of the system. The issues not addressed in these plans are other contingencies. Some scenarios could be as follows:

- The terrorist gains access/negotiates to the SCADA system causes it to overwork and destruct.
- The terrorist accesses a water supply system and increases the rate of chlorine infusion.
- The terrorist accesses the sewage system and opens sewage valves.
- The terrorist accesses some routers and reconfigures them so voice or digital data is rerouted causing networks to crash or not function correctly.
- A terrorist gains access to a main government system, such as the Police network and publishes the name and home address of every officer on a website.

These are notional scenarios, however each one is also conceivable. Though different plans may cover different contingencies, a specific level of planning is critical and the focus of this research is to assess the level of specific cyber terrorism planning. It would appear from this question alone that it does not exist within the organisation who participated.

- **If so is it current?**

Summary of responses

- The full list of responses for this question are displayed as item 9, Appendix 3.

This question was potentially misunderstood as many answered yes, however none of them had a cyber terrorism specific plan so there were none to be up to date. Yet it is assumed the responses provided reflected their existing plans and in every case, those who had a plan such as a DR plan had it up to date. The inference could then be drawn that, if they kept existing plans up to date, then it is likely they would also keep the cyber terrorism plan up to date should they have had one.

- **If your department does not have an awareness strategy, training and a ready reaction plan for cyber terrorism does it consider they are necessary?**

Summary of responses

- 17% of the organisations suggested that a specific cyber terrorism plan is necessary.
- The others consider their existing plans sufficient.
- Specifically no government organisations as shown at item 18(a), of Appendix 3, considered one necessary.
- The full list of responses for this question are displayed as item 18, Appendix 3.

This further reflects the lack of a full understanding on the issue of cyber terrorism. Conceivably the other plans may cover specific aspects, however cyber terrorism, like conventional terrorism is a complex issue and it is essential that specific planning occurs to address the unique issues presented. The issue such as staff awareness, intelligence gathering, immediate actions and related aspects are not usually components of DR or business continuity plans. Critically the government agencies have a similar attitude to this question as provided by the non-government organisation, which from other research is in contrast to that expressed by CCIP.

It would further appear there is not enough general awareness on cyber terrorism as such, as it is thought should the knowledge exist more attention to specific planning would exist.

- **If they are considered necessary will your department be commencing a ready reaction plan?**

Summary of responses

- 42% of the organisations said that they would action one in the future.
- 25% reiterated their existing plans were adequate and therefore one was not necessary.
- The remainder responded as per the previous question in that they didn’t consider one necessary and therefore would not have one in the future.
- The full list of responses for this question are displayed as item 19, Appendix 3.

This question follows on from the previous one in that if they didn't consider one necessary, then they would not therefore consider it necessary to create one in the future. Some ambiguity appeared to exist in the responses, as some responded conversely to this question against their answer to the previous question, in that they didn't consider it currently necessary to have a cyber terrorism plan yet to this question they responded that they already had one, or would get one in the future. However nearly half of the responses did indicate that either a specific plan or elements relative to cyber terrorism would be added to existing plans.

5.3.2 Summary

Generally there appears to be limited planning for terrorism and more, none whatsoever for cyber terrorism. The attitude is such that it appears many do not see it has a critical issue and it is thought that this is as a result of a general lack of understanding on the issue of cyber terrorism. Some of this misunderstanding is because it is not limited alone to an attack against an organisation's IT resources as previously discussed.

5.4 Research question 3

Do the organisations conduct staff awareness training in preparation for an event of cyber terrorism?

5.4.1 Interview responses

- **Is there a staff awareness of the risks of an attack of cyber terrorism?**

Summary of responses

- 50% of the responses indicated there was no specific training.
- The other 50% provided that there was other training or training to those individuals that were likely to come into contact with the resource that would be affected.
- The full list of responses for this question are displayed as item 10, Appendix 3.

The responses to this question returned more positive results for the ISP/Telco respondents than the critical infrastructure and government agencies. The general reflection on security awareness by the technology-based agencies may be due to the technical IT knowledge present, therefore a greater awareness to the risks and the fall-out that could occur should an attack be successful.

The critical infrastructure and government agencies are just as much, if not a greater target, yet do not conduct training on the risks of an attack. Again, as suggested above, it may be due to a lack of technical knowledge and understanding such that they do not fully comprehend that access to an organisation's outer network that has internal connectivity to deeper more critical systems are only key strokes apart. That once bridged, the same control was possible as a user sitting in front of a major control centre.

- **Is there staff awareness on the likelihood of an attack?**

Summary of responses

- 92% responded that there was no awareness training conducted.
- The full list of responses for this question are displayed as item 11, Appendix 3.

This question was intended to elicit the level of awareness training or knowledge that is passed down to lower level staff. Threat assessments should be conducted by all of these organisations for all situations - terrorism, cyber terrorism, criminal attack, natural disasters and so on.

Where an organisation perceives they are a target for any form of attack, some of this awareness must be passed down to lower level staff, as it is more likely a lower level staff member may encounter something strange, and then raise an alarm accordingly. The knowledge that terrorists and other criminals may attempt to seek knowledge through social engineering that would assist in gaining entry to a bundling or remotely to a network is something that must be passed on to staff through awareness training.

Other lower level staff are sometimes the people who are less knowledgeable and may inadvertently present as a security risk due to them not being fully trained on all the risks that the organisation could encounter.

- **Is there staff training on the possibility of an attack of cyber terrorism?**

Summary of responses

- 17% responded that it is included in other general training however, by far the majority responded that no such training exists.
- The full list of responses for this question are displayed as item 12, Appendix 3.

The dialogue for this question is essentially the same as the previous one, as the passing on of the knowledge of this would be carried out if it existed.

5.4.2 Summary

Generally from this section it would appear that no training on the risks, the likelihood and possibility of an attack occurring exists. As addressed in this section, the key issue is that it may not be IT staff or other technicians who encounter some difficulty with a system. Not having the knowledge to understand that it could potentially be due to a cyber terrorism attack could be a flaw having fatal consequences.

5.5 Research question 4

Do the organisations have knowledge and have intelligence gathering concerning cyber terrorism?

5.5.1 Interview responses

- **What does your department foresee the likelihood of an act of cyber terrorism occurring?**

Summary of responses

- This question produced a mixed selection of answers.
- 75% within the government and ISP/Telco respondents suggested it was “not likely”, as shown at item 13(a), of Appendix3.
- All the critical infrastructure, (item 13(b)), suggested it was, “Just a matter of time”.
- The full list of responses for this question are displayed as item 13, Appendix 3.

These results were interesting, in that nearly all of the participants from each category provided the same result. Three each of the government and ISP/Telco respondents suggested that an attack was not likely, whereas all the critical infrastructure organisations suggested it was “just a matter of time”. From the questions answered so far this was the first situation whereby it was seriously that an attack of cyber terrorism could eventually occur in the future.

The response that was surprising, was from the Telco/ISPs as it is known that two of the participants had been the victim of a successful hacking attack. Had it been a terrorist with terrorist motives it would have constituted an act of cyber terrorism. This again is a cause for concern that the perception exists that it is not likely. This could be two-pronged in that either a terrorist is not likely to target them, or they believe their systems are such that no one could infiltrate them. If it is the latter - two of the participants have previously been a victim of an attack - it is the mindset of being bullet-proof that can be a costly flaw by not being conscious that anything could happen at anytime. The lessons of the 9/11 attacks have taught many this lesson and these should be transposed to planning against an act of cyber terrorism.

- **What impact would an attack such as a major denial of service have?**

Summary of responses

- 50% of the participants suggested a DoS would be critical.
- Only respondent number 3, item 14(b), of Appendix 3, suggested it could be life threatening.
- 75% from the Telco/ISP group suggested it was not critical.
- The full list of responses for this question are displayed as item 14, Appendix 3.

A DoS can mean different things to different organisations. Targeting air traffic control systems and emergency control systems would certainly be life-threatening. Some DoS attacks can be rectified very quickly, whilst others, where some damage has occurred, could take hours while systems are repaired and data is restored from backup.

The surprise was more from the Telco/ISP group in that the loss of provision of digital or voice communication services for more than a few of minutes would be critical. Again, all the critical infrastructure participants have responded on the high side of caution, suggesting the disruption of the supply of their services is a major concern.

- **What impact would an attack have such as an incident of trespass on the department's IT resources?**

Summary of responses

- 50% of the participants suggested a trespass would be critical.
- All the Telco/ISPs suggested it was not critical.
- The entire critical infrastructure suggested it would be critical.
- The full list of responses for this question are displayed as item 15, Appendix 3.

This question is organisation dependent, in that government organisations are more likely to possess information that is sensitive, and in the wrong hands could be the cause of loss of life or other harm to resources. The critical infrastructure elements again have exercised caution as it is through electronic trespass that control of their resources could occur and result in physical damage that could ultimately result in the loss of life.

Again the surprise answer was from the Telco/ISPs, in that should someone gain access and trespass their systems, once they are in they could learn additional aspects of resources or remotely control networks, routers and other communications pathways. Merely observing once trespass is gained is still a major cause for concern, as it is this critical knowledge that could provide detail to conduct other associated attacks on these or other resources.

Given the technical knowledge these organisations possess, this group's answer would have been predicted to be the opposite to that provided. This proves the value of conducting this research.

- **Is there any knowledge-seeking in cyber terrorism occurring?**

Summary of responses

- Only one government organisation as shown at, item 16(a), Appendix 3, respondent 2, answered "yes".
- 50% of the critical infrastructure respondents said there was.
- 75% of the Telco/ISP group also indicated there was.
- The full list of responses for this question are displayed as item 16, Appendix 3.

This was a surprising result in that only one of the government agencies was actively seeking knowledge on cyber terrorism. This was an unexpected result, as it was anticipated the government organisations would have been seeking the most intelligence on potential risks and new threats. Nearly all the critical infrastructure and Telco/ISP groups were seeking knowledge on threats.

The Telco/ISP group possess the biggest risk by nature from an attack against their resources. The attacks that they experience are most likely not terrorist attacks but hackers and others attempting to infiltrate their systems. With this in mind, the tools and methods likely to be deployed by the terrorists would be no different, so the same defences are necessary for that group whether they be terrorists or not the principle difference being the motives and the intentions. Once access has been gained by a terrorist the consequences more likely to be greater, than if it was just the average hacker.

- **Does your department foresee cyber terrorism being an issue in the future?**

Summary of responses

- 50% of the government organisations responded yes.
- The other two groups evenly provided opposing results.
- The full list of responses for this question are displayed as item 17, Appendix 3.

50% of the government agencies foresee it being a problem in the future as did 50% of each of the critical infrastructure and Telco/ISP groups, though most of those who responded negatively did not give an outright ‘no’, but more of a ‘not currently’ response.

If the conscious thought is that the threats to IT resources are likely to increase and get more intense, then this certainly should also be similar for those with terrorist motives. As identified earlier, as conventional terrorism become more difficult to achieve due to increased security, it is only a matter of time until the terrorists turn to cyber terrorism as a principle method for conducting attacks. The same risks then apply coming from this group that from any other.

5.5.2 Summary

The responses to the interview questions for this research question provided results that were lower than what was expected. There appears to be little risk adversity, often half or more of the response did not consider there would be a threat, and appear not to understand the concept of electronic trespass, in that once someone has gained access to the IT resources they can then same control of those resources as if they were sitting in from of the main server terminal.

This shows that more awareness on the threats and actions on cyber terrorism are needed across all domains.

In hindsight an additional interview question should have been included to determine how many users have remote access to their systems from their homes, as many home systems are not secure posing even greater threats to these organisation’s IT resources.

5.6 Research question 5

> **Are the privately owned critical infrastructure elements being influenced by CCIP to ensure a common level of security is met, and is the level of planning way less than their government counterparts?**

Assessing the first part of this question;

> **Are the privately owned critical infrastructure elements being influenced by CCIP to ensure a common level of security is met?**

This was determined from the overall results of the other questions and no direct data was obtained from a specific interview question.

5.6.1 CCIP summary

It would appear the answer to this is clearly "no", they are not influenced by them in anyway. More so it appears neither are some of the government organisations as well. This clearly shows that there is a major security flaw with government and critical infrastructure resources within New Zealand. There is deficiency in knowledge, understanding, training, planning and of the potential risks that could occur through an attack. The non-government agencies are not required to adhere to any direction and education on the entire issue of cyber terrorism initiated by government appears to be deficient.

As addressed in chapter 3, CCIP and other agencies have a number of functions, such as:

- “To provide 24/7 watch and warning advice to the owners and operators of our CNI and the New Zealand Government;

- To investigate and analyse cyber incidents that occur against our CNI; and
- To work with CNI protection agencies both nationally and internationally to improve the awareness and understanding of cyber security in New Zealand."

The level of awareness and cyber security referred to in the CNI within New Zealand is low as shown through this research.

Additionally it would appear the overall results, it is clear that CCIP and the government in general have not influenced the non-government agencies in anyway towards planning for an act of cyber terrorism.

A question not addressed by this research was. How much information if any is received from CCIP? It was considered from the outset that this would have been a very sensitive question and the participants would have been reluctant to answer it. It would have however assisted in determining if a communication problem does exist, is it internal within the agencies or external in communications with CCIP.

5.6.2 Summary of international government's preparation and planning

The second component of this research question is:

Is the level of planning way less than their government counterparts?

A brief summary of international government's preparation and planning is provided at Appendix 4. The following is a discussion on the comparisons of the results.

It is important with most research to have a benchmark and sometimes in scientific research, known as the dependant variable, to compare the results of data collected to determine collectively where the data is placed on a comparative scale.

In this case the benchmark is international governments and therefore it is important for the results collected in this research to be compared, to determine collectively how New Zealand rates amongst these other countries.

However the protection of infrastructure from cyber terrorism point must be to an international level, as it is more likely an attack will be made from an international source and the difference between an attack being local and international is likely to be a difference of milliseconds. It is therefore critical that international standards are met.

As identified in chapter 3, CCIP has a duty to provide policy on the protection of the critical infrastructure. At that level it is in a position to discuss with other security agencies what the standards are.

From this it can be determined that the protection of critical national infrastructure is being taken seriously by other western nations. The important issue is how does New Zealand rate in comparison?

As Ghosh, (1998), put it, "the government must be a partner with commercial industry in developing more robust infrastructures; however, the solution is not for the government to dictate, monitor, regulate or dictate to the infrastructures".

5.6.3 Comparison of research results to other governments worldwide

As was shown in chapter 3, the elements within central government, responsible for security and intelligence appear to be well organised. GCSB, CCIP, Department of Prime Minister and Cabinet and NZSIS have a specific function to maintain security and intelligence and further disseminate information where appropriate.

From the research conducted it appears that most organisations are knowledgeable on terrorism and many have specific terrorism plans outside of other existing plans. Those that do not, have business continuity plans or similar to cater to the requirement of addressing a terrorism plan.

General knowledge of cyber terrorism on aspects on any trends, threats or management of cyber terrorism do not appear to be filtering down to the security officers. This applies not only to government departments that are not in security and management roles, but also to the critical infrastructure and the Telco/ISPs, some of which could provide government security agencies with the same communications pathways as the general public. The literature review in chapter 2 identified that many government agencies world wide are reliant on the privately owned Telcos for the supply of communications services. This is often an issue that is not addressed. Though these Telcos may protect themselves purely for business reasons, the level of security and the impact of failure to supply has far reaching consequences, far more than strictly business-related issues.

In comparison to other governments, specifically those listed in this chapter, it appears the central government structure of New Zealand is not too dissimilar, and the various agencies discussed in chapter 3 cover the aspects of intelligence and security well. The researcher has personal knowledge from prior experience with some of these agencies. They interact and share information and intelligence which certainly enhances each other’s functionality and capabilities. The governments listed have initiatives and directives that address the issue of, knowledge, awareness, training and planning on cyber terrorism for the critical infrastructure within their countries. They specifically take steps to ensure that the aspects listed are filtered down to the critical infrastructure. What cannot be determined, in comparison with this research, is what state of awareness and planning exists within their respective critical infrastructures, other than that discussed in chapter 2.

However, as discussed, the information from central government is not filtering down to the same agencies within New Zealand.

5.6.4 Summary

The New Zealand central government agencies responsible for intelligence, security and planning on cyber terrorism are structured in a manner similar to other governments in the western world. These Governments conduct awareness on the need for preparation for cyber terrorism and attempt to filter this to the critical infrastructure within their countries. Its effectiveness cannot be determined accurately from this research, however what can be determined is that it is not filtering down with in New Zealand.

5.7 Conclusion

This chapter has presented and discussed the results obtained from the interview questions that were returned by the participants.

It has answered the five research questions:

1. **Do the organisations have knowledge of what cyber terrorism is?**
2. **Do the organisations have ready reaction plans in the event of a cyber terrorism attack?**
3. **Do the organisations conduct staff awareness training in preparation should an event of cyber terrorism occur?**
4. **Do the organisations have knowledge and have intelligence gathering concerning cyber terrorism?**
5. **Are the privately owned critical infrastructure elements being influenced by CCIP to ensure a common level of security is met, and is the level of planning way less than their government counterparts?**

In order to answer these research questions, 19 interview questions were submitted to participants from three groups, being government, critical infrastructure and Telco/ISPs.

For question one the answers were rather general and many focused purely on the IT aspect and did not see beyond the fact that once access to systems has been obtained, that a terrorist could remotely control physical infrastructure or have access to highly sensitive data.

Question two indicated that there is limited planning for terrorism, but no specific planning on cyber terrorism at all.

Question three indicated that beyond some general security training no specific awareness training or education on cyber terrorism exists.

Question four showed that some of the organisations conducted some intelligence or knowledge-seeking on current and future risks, and these were primarily by the Telco/ISPs and some of the critical infrastructure. Overall though there appears to be general apathy on the entire issue.

This chapter also addressed the fifth and final research question, this detail being drawn collectively from the answers from the interview questionnaires. It is this detail that also assisted in providing the final answer to the research objective.

Overall it has addressed the matter that knowledge possessed by CCIP and the other agencies is not filtered down to the security officers within some government agencies, critical infrastructure and Telco/ISPs. It also identified that the New Zealand central government agencies responsible for intelligence and security are structured and function the same as their international counterparts. It is unknown if the dissemination of information to critical infrastructure in other countries is effective, however it is not within New Zealand, despite the similar central government structure.

Chapter 6. Conclusions

6.1 Chapter objective

This chapter covers the conclusion of the study, summarises the findings and provides a response to the research objective identified in chapter 1. It also addresses the contributions and limitations of this research and the opportunities for further study in this area of research.

6.2 Research objectives

As identified in chapter 1, the objective of the research is:

- **To determine the state of the New Zealand government and critical infrastructure ready reaction to cyber terrorism.**

To satisfy the objective, five research questions were identified as below and to obtain the data to assist with answering these research questions, 19 interview questions were submitted to the participants of three groups being; government, critical infrastructure and Telco/ISPs:

1. **Do the organisations have knowledge of what cyber terrorism is?**

The answers were rather general and many focused purely on the IT aspect and did not see beyond the fact that once access to systems has been obtained, that a terrorist could remotely control physical infrastructure or have access to highly sensitive data.

The conclusion being: The organisations do not have a good knowledge of what Cyber Terrorism is.

2. **Do the organisations have ready reaction plans in the event of a cyber terrorism attack?**

The answer to this question revealed that there is limited planning for terrorism, but no specific planning on cyber terrorism at all.

The conclusion being: The organisations do not have ready reaction plans for cyber terrorism.

3. **Do the organisations conduct staff awareness training in preparation should an event of cyber terrorism occur?**

This question revealed that beyond some general security training no specific awareness training or education on Cyber Terrorism exists.

The conclusion being: The organisations do not conduct specific staff awareness training on cyber terrorism.

4. **Do the organisations have knowledge and have intelligence gathering concerning cyber terrorism?**

With question four some of the organisations conducted some intelligence or knowledge seeking on current and future risks and these were primarily by the Telco/ISPs and some of the critical infrastructure. Overall though there appears to be general apathy on the entire issue.

The conclusion being: That some general security intelligence gathering is undertaken, however overall it was noted that a major cyber terrorism attack could occur and the impact on their organisation was not considered a major issue at this time.

5. **Are the privately owned critical infrastructure elements being influenced by CCIP to ensure a common level of security is met, and is the level of planning way less than their government counterparts?**

This answer was derived from the overall results of the other questions and no direct data was obtained from a specific interview question. Given the overall results, it is clear that CCIP and the government in general have not influenced the non-government agencies in anyway toward planning for an act of cyber terrorism. If they are, then the influence is not being disseminated to the security officers within these organisations, hence the response that have been received.

Assessing the state of preparedness by other governments, it appears that New Zealand's management of cyber terrorism is primarily central-government policy based. Also no formal structure exists to ensure that the elements that form the critical infrastructure within New Zealand and the Telecommunications and Internet Service Providers are involved, as it appears they are in other developed countries.

The conclusion being: The privately owned critical infrastructure are not influenced by CCIP to ensure a common level of security is met, and the level of planning is way less than their government counterparts?

The overall conclusion in reply to the objective of the research being:

- **To determine the state of the New Zealand Government and critical infrastructure ready reaction to cyber terrorism.**

Is:

The New Zealand Government and critical infrastructure are not in a state of ready reaction to cyber terrorism.

6.3 Recommendations

Based on the findings from this research, the following recommendations are made:

- That an information booklet on cyber terrorism be created for distribution to government departments, critical infrastructure and Telco/ISP's (The recipients). This booklet should identify what cyber terrorism is, the threats, the fallout and who would be affected.

- That the recipients be provided with a sample cyber terrorism reaction plan and that they be encouraged to develop their own

- That the recipient be encouraged to conduct awareness training on the risks and likelihood of a cyber terrorism attack.

- That information sharing and cyber terrorism intelligence bulletins be disseminated to the recipients regularly.

- That a government sponsored annual symposium be established for the recipients to attend, so to assist with the development of a collective cyber terrorism, security and intelligence network.

6.4 Contributions

One of important components of any research is to provide a contribution to new knowledge, (Chinneck, J. 2007). It is from this new knowledge it is possible to learn and then develop new ideas, theories or contingences to prevent the occurrence of a phenomenon.

This study has made the following contributions:

- It has provided an understanding that most of the organisations have a good understanding of what terrorism is, however the knowledge on cyber terrorism is more limited. It is a key factor in that awareness by persons in security positions will cause their agency to have an awareness to a potential attack. This research has also provided and understanding that most of the non-government agencies consider that an attack is unlikely. This then is a concern, in that more awareness and knowledge of potential threats and their outcome is needed.

- Though the security officers have knowledge and awareness of cyber terrorism, very few organisations had specific staff awareness training on cyber terrorism for other staff. This is foreseen as a major issue as it is often non security staff who are the first people to come in contact with an abnormality. This highlights a need for more awareness to limit damage should an attack occur.

- Though many organisations had disaster recovery plans, not many agencies had a specific cyber terrorism plan or a specific mention of cyber terrorism reactions. Specific planning for cyber terrorism is seen has a critical issue. As cyber terrorism advances it could be quite unique in its own right and diverse from other forms of risk, and hence specific plans that can stay abreast with the threats is important.

6.5 Limitations

Two main limitations were encountered:

1. There was a general reluctance to complete the questionnaires by the participants. It is thought some of this was due to the sensitive nature of the questions. In other cases it is likely that there was concern over exposure of the results in that it could show there vulnerabilities and could attract media interest in especially government departments that had inadequacies. It is also thought that had the central government agencies a good handle on the cyber terrorism paradigm, then there should have been no issue in disclosing that they were well prepared. So given the absolute reluctance to participate by many of the central government departments, it could suggest they have no ready reaction for cyber terrorism at all.

2. Collecting the research data by way of questions has its limitations. In many cases the first few questions on assessing the participants knowledge of cyber terrorism had been staged, in that the answers provided were straight from an official resource, most likely from a Google search. Had oral questions been

utilised then participants would have had to provide answers on the fly, and provide a more open response without having the opportunity to research.

6.6 Opportunities for further research

Two further avenues of research could be explored.

1. Verbally interview the IT managers of the critical infrastructure organisations and determine what the level of knowledge, awareness and planning exists and technically assess the architecture of their systems to see how vulnerable they are.

2. For those critical infrastructure organisations that have that Infrastructure controlled by IT systems such as SCADA systems, carryout a physical check to determine how many of the systems that are connected to networks, are also connected to the public domain.

3. Assess the viability of the cyber terrorism plans within these organisations to determine if they are sufficient.

6.7 Conclusion

This chapter highlighted the overall results of the research and recommendations, together with suggestions to cover the anomalies that were identified. The contributions, limitations and opportunities for further research were then provided.

Appendix 1

The structure of the New Zealand Government is as follows:
(http://webdirectory.natlib.govt.nz/dir/en/nz/government-law-and-politics/central-government/departments-and-ministries/)

- Archives New Zealand = Te Rua Mahara o te Kāwanatanga
  Describes the functions and services of the National Archives, the agency responsible for collecting, preserving and providing access to the records of the New Zealand government.

- Child, Youth and Family
  Official name is Department of Child, Youth and Family Services. Has legal powers to intervene to protect and help children who are being abused or neglected or who have problem behaviour, also administers adoption services.

- Crown Law Office
  The Crown Law Office provides legal advice and representation to the New Zealand Government, its departments, ministries and agencies in matters affecting the Crown.

- Department of Building and Housing = Te Tari Kaupapa Whare
  The Department is responsible for administering the Building Act and the Residential Tenancies Act as well as a range of other building and housing related regulations

- Department of Civil Aviation : Ministry of Transport & Civil Aviation
  Official website of the Fiji Department of Civil Aviation.

- Department of Conservation = Te Papa Atawhai
  Information both about and for conservation related topics. Includes information on permits, legislation, publications of the Dept. and current issues.

- Department of Corrections = Ara Poutama Aotearoa
  Information about the Dept. Other roles explained are supporting the Parole Board and District Prisons Boards, and providing information to the courts. Includes, facts and figures and publications.

- Department of Internal Affairs = Te Tari Taiwhenua
  Information about the Department and its services, including information about passports, civil unions, births, deaths and marriages, citizenship applications, gambling regulations, censorship law, internet safety, charitable grants, dog control, local councils, and services for government ministers.

- Department of Labour = Te Tari Mahi
  Brief outline of the structure, mission and goals of the Department, including organisational chart. Includes information about health and safety; employment relations; immigration and the labour market; publications, contacts and latest news.

- Department of the Prime Minister and Cabinet
  DPMC serves the Executive (the Prime Minister, the Governor-General, and the Cabinet) through the provision of high quality impartial advice and support services which facilitate government decision-making at both strategic and operational levels.

- Directory of official information = Te rārangi whakaatu whakaere kāwanatanga
  Directory of central Government departments and organisations, with information on the criteria for requesting official information.

- Education Review Office = Te Tari Arotake Matauranga
  The Education Review Office is the government department which reports publicly on the quality of education in all New Zealand schools and early childhood centres, including private schools, kura kaupapa Māori (Māori language immersion schools), special schools and kohanga reo (Māori language early childhood groups).

- Government Communications Security Bureau
  Basic information about the GCSB, an intelligence and security agency which provides foreign intelligence information and protects government classified or sensitive information.

- Inland Revenue = Te Tari Taake
  Government site, with forms, tax information bulletins and other information for businesses and individuals.

- Land Information New Zealand = Taitu te Whenua
  LINZ holds authoritative information about land surveys and ownership, topographic maps and nautical charts.

- Ministry for Culture & Heritage = Te Manatū Taonga
  The Ministry for Culture and Heritage site includes information on New Zealand arts and history. It also includes online publications.

- Ministry for the Environment New Zealand
  Includes information about the ministry; environmental issues and laws; environmental management and monitoring the state of the environment.

- Ministry of Agriculture and Forestry = Te Manatū Ahuwhenua, Ngāherehere
  MAF is the ministry responsible for agriculture, horticulture, forestry, safe food, a

protected environment, the wise use of the land, the creation of clean, green product and the economic success of those who produce it.

- Ministry of Civil Defence & Emergency Management = Te Rākau Whakamarumaru
  Information about CDEM planning, programmes and the Ministry itself.

- Ministry of Consumer Affairs = Manatū Kaihokohoko
  Provides advice and information for both consumers and traders, including a scamwatch.

- Ministry of Economic Development = Manatū Ōhanga
  The Ministry of Economic Development (formerly Ministry of Commerce) has a policy advice role, with implementation and operational roles as well. The areas of government supported by these roles include business and economic, regulations, consumer issues, energy and telecommunication markets, information technology and the Companies Office.

- Ministry of Education = Te Tāhuhu o te Mātauranga
  Overview of the Ministry, goals, mission, aims, statistics, etc., including official documents such as the strategic plan and many other publications, most in PDF format. Information categorised by level of education, Māori, Pacific and Special.

- Ministry of Fisheries = Te Tautiaki i nga tini a Tangaroa
  MFish ensures that fisheries are sustainably used within a healthy aquatic ecosystem.

- Ministry of Health = Manatū Hauora
  The Ministry of Health is responsible for raising the level of health in New Zealand.

- Ministry of Justice = Tāhū o te Ture
  Provides an overview of the Ministry and New Zealand Courts and their services.

- Ministry of Pacific Island Affairs : social and economic prosperity for Pacific people
  The MPIA, online publications, resources to increase understanding of Pacific peoples, regional news, legal information and information on sources of funding.

- Ministry of Research, Science & Technology
  Overview of the Ministry; information about research and innovation in New Zealand; global innovation; public funding available for research, science and technology in New Zealand; and career options. Online publications.

- Ministry of Social Development = Te Manatū Whakahiato Ora
  The Ministry of Social Development provides strategic social policy advice to the New Zealand Government and provides social services to more than one million New Zealanders.

- Ministry of Tourism = Te Manatū Tāpoi
  Profiles the ministry and the New Zealand tourism industry. Includes online reports and statistics.

- Ministry of Transport = Te Manatū Waka
  The Ministry, its various transport agencies, current issues and publications. Includes information for drivers and road users and for passengers on land, sea, rail and air transportation.

- Ministry of Women's Affairs = Minitatanga mō ngā Wāhine
  The Ministry is a small policy advice agency which focuses on areas where it can make the most difference to improve women's lives.

- Ministry of Youth Development = Te Manatū Whakahiato Taiohi
  Covers the policies, programmes, legislation and services that concern young people in New Zealand.

- National Library of New Zealand = Te Puna Mātauranga o Aotearoa
  The National Library of New Zealand collections and databases, including the Alexander Turnbull Library, the New Zealand National Bibliography, Index NZ, Services for libraries, and Services for schools. Information on exhibitions and events.

- New Zealand Customs Service = Te Mana Arai o Aotearoa
  Information about the Customs Service and information for travellers, visiting craft, importers, exporters and manufacturers.

- New Zealand Defence Force
  About the NZDF. Includes documents, information about operations and medals, links to Navy, Army and Air Force sites and news.

- New Zealand Ministry of Defence = Manatū Kaupapa Waonga
  The Ministry's task is to identify possible risks to New Zealand's security, its overseas trade and investment and the forces and equipment the nation will need to protect these vital interests.

- New Zealand Ministry of Foreign Affairs & Trade = Manatū Aorere
  The site provides covers trade agreements, legal issues, bilateral and regional/multilateral relationships.

- New Zealand Police = Ngā Pirihimana o Aotearoa
  Includes safety tips and information on contacting the Police. The site also contains online publications and news reports, which include a calendar and some video footage.

- New Zealand Security Intelligence Service
  NZSIS provides the Government with timely and accurate intelligence and advice on national security issues.

- New Zealand Serious Fraud Office = Te Tari Hara Tāware
  The Serious Fraud Office as well as how to make a claim, fraud alerts and SFO court cases.

- Parliamentary Counsel Office = Te Tari Tohutohu Pāremata
  PCO is New Zealand's law drafting office responsible for drafting and publishing most New Zealand legislation.

- State Services Commission = Te Komihana o Ngā Tari Kāwanatanga
  Profiles the Commission and provides information on its role in the state sector; public service chief executives; public management; public service values and standards; human resources and EEO; and the mainstream supported employment programme.

- Statistics New Zealand = Tatauranga Aotearoa
  Official information from Statistics New Zealand, including a summary of New Zealand statistics, also products and services and related links. Includes activities and information for school teachers.

- Te Puni Kōkiri
  The Government's principal adviser on the Crown's relationship with iwi, hapū and Māori, and on key Government policies as they affect Māori.

- Treasury = Kaitohutou Kāupapa Rāwa
  Details the organisation of the Treasury the Government's lead advisor on economic and financial policy. Includes online publications, including the latest Budget.

Interview Questions

Cyber Terrorism Research **REF. 2007/259**

Appendix 2.

Questions for the Departmental Security Officer.

1. What does your department understand the definition of terrorism to be?
2. What does your department understand the definition of cyber terrorism to be?
3. Is your department aware of any international incidents of cyber terrorism?
4. Is your department aware of any incidents of cyber terrorism in NZ?
5. What does your department see as the main threat, should an act of cyber terrorism occur should one be directed at your department?
6. Who is considered to be a threat to your department?
7. Does your department have a terrorism ready reaction plan?
8. Does your department have a cyber terrorism ready reaction plan?
9. If so is it current?
10. Is there a staff awareness of the risks of an attack of cyber terrorism?
11. Is there staff awareness on the likelihood of an attack?
12. Is there staff training on the possibility of an attack of cyber terrorism?
13. What does your department foresee the likelihood is of an act of cyber terrorism occurring?

Never *Not likely* *likely* *just a matter of time*

14. What impact would an attack such as a major denial of service have?

Not critical *Critical* *Life threatening*

15. What impact would an attack have such as an incident of trespass on the departments IT resources?

Not critical *Critical* *Life threatening*

16. Is there any knowledge seeking in cyber terrorism occurring?

17. Does your department foresee cyber terrorism being an issue in the future?

18. If your department does not have an awareness strategy, training and a ready reaction plan for cyber terrorism does it consider they are necessary? (Please comment on each).

19. If they are considered necessary will your department be commencing a ready reaction plan?

Appendix 3

Collective Responses for Each Interview Question

1. What does your department understand the definition of terrorism to be?

a. Government

Guided by the Terrorism Act 2002 where Terrorist Act is defined as carrying out such an act internationally it is best to say definitions are often contradictory and confusing.
The Ministry does not have a definition. I would define Terrorism to be any act which would cause major impact on the sovereignty, economy, people of NZ by any person, group or country. It excludes such natural events as share market crashes.
We do not have a formal definition. However we understand the definition to be: the use of violence to inflict terror for political or religious agendas.
A criminal act of violence or sabotage designed to cause significant damage and fear.

b. Critical Infrastructure

Terrorism to us is the unlawful actions, or threat of actions, resulting in harm against law abiding citizens.
Terrorism is the threat or use of violence against civilians to achieve political or ideological objectives by creating fear.
An act that causes harm and fear to civilians.
Using violence (or threats of violence) against people to attain goals they are usually political or religious. This is done via intimidation or coercion.

c. Telco/ISP

The calculated use of violence (or threat) against civilians in order to attain goals, political, religious or ideological, done through intimidation/ or instilling fear
The use or threat or violence that generates fear to bring about political change.
It is a form of violence towards civilians in order to achieve political, economical or ideological goals.
Any action that seeks to subvert the stability or government of a country or countries.

Appendix 3

Collective Responses for Each Interview Question

2. What does your department understand the definition of cyber terrorism to be?

a. Government

Not specifically defined however it would be an act of terrorism facilitated or assisted through computer networks such as internet.
Cyber Terrorism is a subnet of question 1. above and includes all computer based attacks including destruction of individual PC's right through to whole networks including process controller equipment. It also includes theft of information and identity as well as significant denial of service.
We do not have a formal definition. However we understand the definition to be: the unauthorised use of computers and other IT equipment via the internet to inflict terror for political or religious agendas. However it seems that the definition of terror as far as cyber terrorism is concerned is a little blurred.
An act as described above using an electronic medium as the method of attack. Usually using the internet or electronic mail.

b. Critical Infrastructure

Cyber terrorism is the use of technology to inflict unlawful actions, or threats of actions, that may result in harm to law abiding citizens.
Cyber terrorism is the leveraging of a targets computer and IT to cause or threat to cause physical harm or disruption of services.
To causing an attack against civilians through the use of computer technology and networks.
Cyber-terrorism is the use of computing resources to intimidate or coerce others.

c. Telco/ISP

Cause physical, real world harm or severe disruption of a target's computers and information technology particularly via the internet.
The use of computer systems to create the fear identified above.
Similar to the first question only focusing on usage of electronic media like internet, television and radio etc.
As above but using electronic or other technical means to affect the same outcome.

Collective Responses for Each Interview Question

3. Is your department aware of any international incidents of cyber terrorism?

a. Government

Many groups internationally (hamas hizhollah algeria's ahmad Islamic group alqaeda
Yes, however this comes down to definition. I remember during Bill Clinton's rein as President that he requested that all American's to attack the assets of certain Yugoslav Nations on the internet during that war. Is that a valid instrument or war or cyber terrorism? We have detected a Chinese Trojan on one of our PC's attempting to send information to a site in China.
Yes, through media and security bulletins.
No.

b. Critical Infrastructure

There are numerous cases of harm being caused through the infliction of deliberate and malicious use of technology, and deliberate breaches of cyber security. However these events are normally classified as hacking or spamming.
Yes.
No.
Yes

c. Telco/ISP

Those reported in media only eg. Attack on Estonia
Yes.
Yes, but only regarding to major ones.
Indirectly through news media or news groups eg. Chinese Hacker allegations.

Collective Responses for Each Interview Question

4. Is your department aware of any incidents of cyber terrorism in NZ?

a. Government

Not known
Based on the definition in 1. above then no unless we include the theft of information Trojans
No.
No.

b. Critical Infrastructure

As per question 3, there are continual attempts to cause harm through the unlawful use of technology. While most of these threats are deflected, there are also a large number of times when these attacks have resulted in harm within NZ.
Yes. Several instances across NZ.
No.
No

c. Telco/ISP

No
No
Not that I am aware of.
No.

Appendix 3

Collective Responses for Each Interview Question

5. What does your department see as the main threat, should an act of cyber terrorism occur should one be directed at your department?

a. Government

Exploitation of current data, falsifying revenue, money laundering through revenue, false identity, unlawful access to information are all possible.
A. Theft of information which may impact on international negotiations. B. Destruction of Department websites and internal computing infrastructure.
We have not identified any threats.
Loss of sensitive business data and therefore the ability to operate business as usual.

b. Critical Infrastructure

The most serious threat to our company is a malicious attack on our technology assets resulting in a denial of service. Eco-terrorism is potentially the most significant single threat to our company.
Reduction/Loss of service of IT systems.
Causing an attack that would render the computer unusable.
The possible control or shutdown of the Power Stations or defacing the internet causing reputational damage.

c. Telco/ISP

DNS Attack
The threat to central services such as phone and specifically the 111 service to the population.
We can’t see any major threats.
Effective communication and damage control (brand, integrity etc)

Collective Responses for Each Interview Question

6. Who is considered to be a threat to your department?

a. Government

None specific, however threats through system access security.
There are two tiers to this response: 1. Theft of information. Any country or organisation who are signatories or intended signatories to international agreements. 2. Certain developing countries.
We have not identified any threats.
Internal staff, disgruntled ratepayers.

b. Critical Infrastructure

The profile our company has as a critical infrastructure provider within NZ exposes us to the global domain for malicious attacks.
All parties both internal and external.
Anyone who considers us to be a target.
Activist within the environmental/global warming sector.

c. Telco/ISP

Perhaps a competitor in cyber safety information – unlikely
Anybody who would seek to disrupt the essential services identified above.
Can't point to particular people.
Anyone, subversive groups, external parties (Hacking Cracking community).

Appendix 3

Collective Responses for Each Interview Question

7. Does your department have a terrorism ready reaction plan?

a. Government

No we have business continuity planning to recover and respond from potential incidents. No matter what they are about, not terrorism specific.
No.
Yes.
No only a DR plan and a BCP plan.

b. Critical Infrastructure

We do not have a specific terrorism ready reaction plan. We have a series of reaction ready plans available in the event of a number of company attacks. While these plans are not noted as Terrorism plans, the actions contained within the plans would be used in the even of terrorist activity.
As part of a large DR plan.
Yes for immediate action to assist in providing help after an incidence but not for us as victims.
Yes

c. Telco/ISP

No
Continuity, Disaster Recovery, Crisis Management Plans, but no specific Terrorism Plans.
Nothing more specific than general reaction plan.
Not specifically but considered as part of business continuity planning and notification of key business risks.

Appendix 3

Collective Responses for Each Interview Question

8. Does your department have a cyber terrorism ready reaction plan?

a. Government

Same as question 7.
No. Although there are processes and procedures for handling internet based intrusions when detected.
We have an incidence response plan.
As above.

b. Critical Infrastructure

Once again we do not have plans specifically associated with Cyber Terrorism. We have action plans in the event of cyber attacks, viral penetration, and other forms of technology attack.
As part of a DR plan.
No.
No

c. Telco/ISP

No
As above in question 7.
We have plans regarding attacks on our network, but nothing terrorism specific.
Not specifically as above.

Appendix 3

Collective Responses for Each Interview Question

9. If so is it current?

a. Government

N/A - The continuity plan is current.
Yes.
Yes.
No response.

b. Critical Infrastructure

The action plans are reviewed annually and tested on a regular basis.
Yes.
N/A
N/A

c. Telco/ISP

N/A
Existing plans are current.
These plans are current.
No Response.

Collective Responses for Each Interview Question

10. Is there a staff awareness of the risks of an attack of cyber terrorism?

a. Government

In same organisation parts that manage detection and operational attacks.
No. But 8. applies and IT staff are aware of the risks (Technical). Staff are advised on antivirus and the security policy.
No.
Limited.

b. Critical Infrastructure

Staff are aware of the need to be mindful of company security measures associated with potential threats. However this is not specific to Cyber Terrorism.
There is some awareness by those who need to know.
No.
Very limited

c. Telco/ISP

Yes because our staff are very aware of security there is a high understanding of risks.
Within security operation centre only.
Yes we are aware of it.
Not specifically.

Appendix 3

Collective Responses for Each Interview Question

11. Is there staff awareness on the likelihood of an attack?

a. Government

As per 10.
No.
Probably Not.
No.

b. Critical Infrastructure

Staff are aware of the potential and possible impacts if an attack was successful. They are also aware of their role for ensuring that counter measures are maintained.
No.
No.
There is more awareness within the Power Stations

c. Telco/ISP

Yes – as we are not an essential service a govt dept the likelihood is low.
Unlikely.
Yes.
No.

12. Is there staff training on the possibility of an attack of cyber terrorism?

a. Government

Not specifically to cyber terrorism but severity related yes.
No – refer to question 10.
No.
No.

b. Critical Infrastructure

Training on the types of malicious cyber attacks that may be attempted and counter measures is an ongoing process within the company.
No.
No.
No

c. Telco/ISP

No
No
It is included in general staff training.
Not specifically.

Appendix 3

Collective Responses for Each Interview Question

13. What does your department foresee the likelihood is of an act of cyber terrorism occurring?

a. Government

Never	*Not likely*	*Likely*	*Just a matter of time*
		X	
	X		
	X		
	X		

b. Critical Infrastructure

Never	*Not likely*	*Likely*	*Just a matter of time*
			X
			X
			X
		X	

c. Telco/ISP

Never	*Not likely*	*Likely*	*Just a matter of time*
	X		
			X
	X		
	X		

Appendix 3

Collective Responses for Each Interview Question

14. What impact would an attack such as a major denial of service have?

a. Government

Not critical	*Critical*	*Life threatening*
	X	
X	X	
X		
	X	

b. Critical Infrastructure

Not critical	*Critical*	*Life threatening*
	X	
	X	
		X
	X	

c. Telco/ISP

Not critical	*Critical*	*Life threatening*
X		
	X	
X		
X		

15. What impact would an attack have such as an incident of trespass on the departments IT resources?

a. Government

Not critical	*Critical*	*Life threatening*
	X	
	X	
X		
X		

b. Critical Infrastructure

Not critical	*Critical*	*Life threatening*
	X	
	X	
	X	
	X	

c. Telco/ISP

Not critical	*Critical*	*Life threatening*	
X			
X	X		*
X			
X			

* Two boxes were marked by the participant for this question.

Collective Responses for Each Interview Question

16. Is there any knowledge seeking in cyber terrorism occurring?

a. Government

Not sure.
Yes.
No.
No.

b. Critical Infrastructure

Knowledge pertaining to malicious technology threats is being maintained
Yes. Daily checks are made against all key systems and industry services.
No.
No

c. Telco/ISP

Reading is thorough within the organisation so knowledge is picked up about these sorts of risks and incidents.
Yes
No more than is required.
Incorporated within other continual evaluation, consideration and monitoring of security risks in the Telecommunications environment eg. Hacking, Cracking, DoS attacks, Botnets etc.

17. Does your department foresee cyber terrorism being an issue in the future?

a. Government

Yes
Yes. As an escalation of normal internet based instructions.
Not currently but our business attack vectors, motives, can all change.
No.

b. Critical Infrastructure

The issue of harm being inflicted upon the company via technology is an issue both now and into the future.
Yes.
Not immediately but it is a matter for discussion.
Yes

c. Telco/ISP

Yes – not necessarily for our organisation certainly in critical depts.
Yes
Not really.
No response.

Appendix 3

Collective Responses for Each Interview Question

18. If your department does not have an awareness strategy, training and a ready reaction plan for cyber terrorism does it consider they are necessary? (Please comment on each).

a. Government

As detailed in question 7 and 8.
No. In so far as a specialised plan. However Yes if we talk about the increasing threats from the internet.
Not currently.
No. We out source our IT infrastructure to a third party who is a specialist in IT Service Delivery. We expect through our SLA that they would have appropriate solutions in place.

b. Critical Infrastructure

We consider our company has appropriate strategy, policy, training, and ready reaction plans to address the potential threats and risks to the company and its stakeholders.
Yes for all.
Yes. Given the rise of terrorism it is only a matter of time and preparatory action should be taken for planning and training.
Yes on all

c. Telco/ISP

Awareness strategy – would be necessary Training – not necessary Ready reaction Plan – Not necessary.
Strategy – Yes, Training – Yes, Plan – Yes. These could all be incorporated into existing initiatives with a greater level of detail and involvement for the operational security teams.
We have general strategies, training and reaction plans we see as sufficient in terms of cyber terrorism.
No response.

19. If they are considered necessary will your department be commencing a ready reaction plan?

a. Government

N/A
Yes. However it would be something that would need to be mandated by Cabinet or SSC.
We already have one.
N/A

b. Critical Infrastructure

As per question 8 the company maintains plans in the event an act of a malicious attack or cyber terrorism event occurs.
Yes we have already actioned part of plan in relation to DR plan.
Yes some time in the future.
Yes as part of the security review.

c. Telco/ISP

N/A
There will be input from the security department into existing initiatives as and when appropriate.
Yes.
No response.

Appendix 4

Summary of Other National Governments Preparation and Planning

United States of America

There is considerable infrastructure protection activity underway in the United States, both at the federal and state levels. There is significant effort undertaken at federal level to complete vulnerability assessments of critical infrastructure elements with these assessments including 'red teaming' or penetration testing. At state level Hawaii is particularly active and recently hosted a three day seminar on the protection of the electric power infrastructure.

Arguably the most effective protective measure implemented by the US has been the establishment of the National Infrastructure Protection Center (NIPC). The NIPC, which is hosted by the FBI, has widely representative staffing from other national agencies. It serves as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity. It provides timely warnings of international threats, comprehensive analysis and law enforcement investigation and response. The main mission of the NIPC is to detect, deter, assess, warn, respond, and investigate unlawful acts involving computer and information technologies and unlawful acts, both physical and cyber, that threaten or target US critical infrastructures.

United Kingdom

Extensive activity on Information Age Government (IAG) is ongoing in the United Kingdom. Protection of the UK Critical Information Infrastructure (CII) is within the portfolio of the Home Secretary. An advisory committee, the IAG Champions, has drafted a policy for the protection of critical infrastructure and this is currently with the Home Secretary for consideration. BS7799 (equivalent to AS/NZS 4444) [Information Security Management in two Parts: Part 1 is the code of practice for information security management, Part 2 is the specification for information security management systems.] is being advocated as the standard for CII owners, and it is understood that the Cabinet Secretary has invited all departments to advise by 31 December 2000 their plans for adopting/satisfying this standard.

Summary of Other National Governments Preparation and Planning

A close relationship has been developed with the private sector - both business and academic. For example, the Information Assurance Advisory Council established at Kings College London has a diverse membership and is an effective forum. Engagement of infrastructure owners is central to the CII programme with the approach being one of persuasion rather than regulation. The UK government views the establishment of Computer Emergency Response Teams (CERTs) as central to CII and would encourage the development of a CERT for each community of interest within the CII.

Australia

The Commonwealth government has recognised the need for infrastructure protection for several years. An inter-departmental committee was formed and led by the Attorney-General's Department. In December 1998 this produced a report recommending an ongoing effort to protect the National Information Infrastructure.

This figure was intended for coordination and central funds; actual protection activities are to be undertaken by the agencies and companies owning the infrastructure. The interdepartmental committee has continued and has been raising awareness among infrastructure owners, partly through a consultative industry forum involving the private sector. Recently the Attorney-General's department has recommended to the commonwealth government that general IT security promotion (i.e. non-critical infrastructure protection) be passed to the National Office for the Information Economy, an agency concerned with e-commerce and e-government.

Canada

A Critical Infrastructure Protection Task Force (CIPTF) was established in 1 April 2000 within the Department of National Defence, but reporting operationally to the Privy Council Office. Its mandate is to review critical infrastructures in Canada and develop a framework for future action in terms of protecting them. The CIPTF expects to present its report to Cabinet in early-2001.

Appendix 4

Summary of Other National Governments Preparation and Planning

A five-part strategy is being proposed based around strong interaction both with the private sector and with other international critical infrastructure programmes. It is likely that a new organisation for CIP will be established to lead and coordinate the national response. As an interim measure a pilot Government of Canada Information Protection Coordination Centre (GIPCC) has been set up to provide better coordination and management of cyber incidents affecting government departments and agencies.

Bibliography

Armistead, L. (2002). Fall from Glory: The Demise of the US Information Agency during the Clinton Administration. Journal of Information Warfare, Vol 1, issue 3.

Armstrong, H. L. (2002). Denial of Service and Protection of Critical. Journal of Information Warfare, Vol 1, issue 2.

Bergen, P. L. (2001). Holy War, Inc: Inside the Secret World of Osama bin Laden. Free Press.

Bigelow, B., LT Col, US Forces. (2003). Targets, and Effects: Militarising Information Warfare. Journal of Information Warfare, Vol 2, issue 1.

Bosch, O. (2002). Cyber Terrorism and Private Sector Efforts for information Infrastructure Protection. Seoul. ITU.

Broucek, V., & Turner, P. (2002). Forensic Computing. Journal of Information Warfare, Vol 1, issue 3.

Business Roundtable. (2006). Essential Steps to Strengthen America's Cyber Terrorism Preparedness. USA: BR.

Bush, G. W. (2001). Speeches 2001. www.whitehouse.gov

CCIP. (2001). Towards a Centre for Critical Infrastructure Protection. Wgtn: NZ Govt..

Chinneck J, (1999). How to Organise your Thesis Canada. Ottawa: Carleton.

Collin, B. C. (2005). The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge. 11th Annual International Symposium on Criminal Justice Issues.

Conway, M. (2003). Cyberterrorism: The Story So Far. Journal of Information Warfare, Vol 2, issue 2.

Curts, R.J., & Campbell, D. E. (2002). The Impact of Architecture and Interoperability on Information Warfare Systems. Journal of Information Warfare, Vol 1, issue 1.

Davey, J., & Armstrong, H. L. (2003). Dominating the Attacker: Use of Intelligence and Counterintelligence in Cyberwarfare. Journal of Information Warfare, Vol 2, issue 1.

Davey, J., & Armstrong, H. L. (2002). An Approach to Teaching Cyber Warfare Tools and Techniques. Journal of Information Warfare, Vol 1, issue 2.

Bibliography

Dearth, D. H. (2002). Critical Infrastructures and the Human Target in Information Operations. Journal of Information Warfare, Vol 1, issue 2.

Denning, D. (2000). Cyberterrorism. USA: Global Dialogue (Autumn 2000).

Devost, M. G. & Pollard, N. A. (2002). Taking Cyber Terrorism Seriously: Failing to Adapt to Emerging Threats Could Have Dire Consequences. USA: The Terrorism Research Centre.

Devost, M. G., Houghton, B. K., & Pollard, N. A. (1996). Information Terrorism: Can you Trust your Toaster?. USA: The Terrorism Research Centre.

Ellsmore, N. (2002). Cyber-Terrorism in Australia: The Risk to Business and a Plan to Prepare. Aust: SIFT.

Elmusharaf, M. M. (2004). Cyber Terrorism: The new kind of Terrorism. USA: CCRC.

Furnell, S. M. (2002). Categorising cybercrime and cybercriminals The problem and potential approaches. Journal of Information Warfare, Vol 1, issue 2.

Garfield, A. (2002). The Offence of Strategic Influence: Making the Case for Perception Management. Journal of Information Warfare, Vol 1, issue 3.

Ghosh, A. (2003). Sizing the Opportunity for Opportunistic Cybercriminals: Journal of Information Warfare, Vol 2, issue 1.

Ghosh. A. K ., & Del Rosso. M. J. (1998). The Role of Private and Government in Critical Infrastructure Assurance.

Gordon, S., & Ford, R. (2003). The Symantec Security Response white paper on Cyberterrorism. USA.

Harle, V. (2000). The Enemy with a thousand faces. The Tradition of the order in Western Political Thought and History., Westport. Connecticut: Praeger.

Henych, M., Holmes, S., & Mesloh, C. (2003). Cyber Terrorism: An Examination of the Critical Issues. Journal of Information Warfare, Vol 2, issue 2.

Huhtinen, A., & Rantapelkonen, J. (2002). Perception Management in the Art of War. A Review of Finnish War Propaganda and Present-Day Information Warfare. Journal of Information Warfare, Vol 2, issue 1.

Janczewski, L. J. Kuala Lumpur Presentation Slides 13-16 Aug 07.

Johnson, B. (2002). Research Methods. USA: University of South Alabama.

Just, J. E. (2006). Some Useful Capabilities in Countering Cyber Terrorism. USA: University of South California.

Kerr, K. (2003). Putting cyberterrorism into context. www.auscert.org.au

Bibliography

Kopcheva, M. (2006). Cyber Terrorism As A New Security Threat. USA: CCRC.

Kopp, C. (2003). Shannon, Hypergames and Information Warfare. Journal of Information Warfare, Vol 2, issue 1.

Lewis, J. A. (2002). Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. Washington: CSIS

Low, D. (2003).The Relevancy of Merleau-Ponty's Political Theory. USA: University of West Florida.

Markham, S. (2007). The Research Manifesto. QLD: Monash.

Mogull, R. (2005), Cyber Terror is Not Real. Aust: Znet.

Moutot, M. (2006). Electronic Jihad's Cyber Soldiers. Paris: Main and Guardian.

Nelson, B., Choi, R., Lacobucci, M., Mitchell, M., & Gagnon, G. (1999). Cyberterror: Prospects an Implications. CA, USA: US Navy.

Nicander, L. (2002). Information Operations - A Swedish View. Journal of Information Warfare, Vol 1, issue 1.

Noel, G. E., Gustafson, S. C., & Gunsch, G. H. (2002). Network - Based Anomaly Detection Using Discriminant Analysis. Journal of Information Warfare, Vol 1, issue 2.

Rollins. J., & Wilson. C. (2005). Terrorist Capabilities for Cyberattack: Overview and Policy Issues. USA: State Department.

Schneier, B. (2005), Stop Crying Wold Over Cyber Terrorism. UK: Guardian.

Schwartau, W. (2002). Asymmetrical Adversarialism in National Defense Policy, The Marketplace and Personal Privacy. Journal of Information Warfare, Vol 1, issue 2.

Shelly, S. I. (2003). Organised Crime, Terrorism and Cybercrime. Geneve: Baden-Baden.

Slay, J. (2003). A Cultural Framework for the Interoperability of systems. Journal of Information Warfare, Vol 2, issue 1.

Spencer, V. (2002) Cyber Terrorism: Mass Destruction or Mass Disruption. USA. CCRC

Sproles, J., & Byars, W. (1998). Cyber-terrorism. USA; East Tennessee University.

Sproles, J., & Byars, W. (1998). Statistics on Cyber-terrorism. USA: East Tennessee University.

Bibliography

Stakelbeck, E. (2007). Cyber Terror: Defusing the Timebomb. USA: CBN.

Stohl, M. (2006). Cyber Terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games? UK: Andrews.

Taylor, P. M. (2002). Perception Management and the 'War' Against Terrorism. Journal of Information Warfare, Vol 1, issue 3.

Tharenou, P., Donohue, R., & Cooper, B. (2007). Management Research Methods. Melbourne: Cambridge University Press.

Thomas, T. (2003). Contingency Planning And Business Recovery. UK: CPDRG.

Trachtman, J. P. (2004). Global Cyberterrorism, Jurisdiction, and International Organization. USA: Tufts University.

Tyrrell, P.J. (RN). (2002). Protecting the National Critical Infrastructure: Human Dimension From a Government Perspective. Journal of Information Warfare, Vol 1, issue 2.

US Army: 2005: Cyber Operations and Cyber Terrorism: DCSINT Handbook No.1.02.

Xenitellis, S. (2003). A New Avenue of Attack: Event-driven System Vulnerabilities. Journal of Information Warfare, Vol 2, issue 1.

Yurcik, W. (1999). Adaptive Multi-Layer Network Survivability: A Unified Framework for Countering Cyber-Terrorism. USA: University of Pittsburgh.

Websites

www.answers.com

www.thinkexist.com

www.wikiquote.com

www.crimelibrary.com

www.csi.org

www.computerworld.com

http://news.zdnet.com/2100-1009_22-955293.html

http://en.wikipedia.org/wiki/Cyber-terrorism

Bibliography

http://www.crime-research.org/analytics/Cyberterror_Clear_present

NZ Statutes

Crimes Act 1961

Terrorism Suppression Act 2002

Glossary

ActiveX Controls

These controls link to any object--traditionally dynamic content such as tables and buttons that react to mouse clicks--embedded within a Web page. Although ActiveX controls help Web pages spring to life, malicious programmers can easily use them as vehicles for downloading spyware. Install a sturdy browser and firewall that screens your ActiveX Controls, and download them with care, accepting ActiveX only from trusted Web sites.

Adware

Typically, adware components install alongside a shareware or freeware application. These advertisements create revenue for the software developer and are provided with initial consent from the user. Adware displays Web-based advertisements through pop-up windows or through an advertising banner that appears within a program's interface.

Antispyware software

This is a broad term for programs designed to protect a computer from adware and spyware. Almost all antispyware applications feature a scanning engine, which detects suspicious items and removes them from the infected machine. Some antispyware applications also include a real-time-protection module, a shield that alerts users when suspicious programs attempt to install themselves and allows users to deny them.

Backdoor programs

This refers to any software program that allows other users to control machines remotely while hiding any evidence of the fact. Software developers are the most common authors and users of backdoor programs, adding them to make testing easier. Backdoor Trojan horses are spyware programs that sabotage your PC. These specific Trojan horses force a backdoor program onto your machine and infiltrate your system to collect information or install spyware.

Bot

An Internet robot, shortened to "bot," is an automated program that performs a specific timesaving function in lieu of a human operator, such as a spider that trolls Web sites collecting data for market research. Spyware bots secretly install through worms, Trojan horses, and drive-by downloads. They are mostly used to carry out remote attacks, such as denial-of-service (DoS) attacks.

Botnet

A botnet is a network of bots installed on multiple computers, each running identical malware. A botnet can be controlled remotely via an IRC (Internet Relay Chat) server or a peer-to-peer application.

Browser-helper object (BHO)

BHOs are files--most frequently DLLs--that add additional functionality to Internet Explorer. Although many useful programs such as Adobe Acrobat employ BHOs, these files also can be used for unsavory purposes. BHOs associated with adware or spyware can monitor your browsing activities, hijack your home page, or replace certain advertisements with others.

Cracker

Cracker is a shortened name for a criminal hacker. Read more at **hacker**.

Denial-of-service (DoS) attack

Denial of service is an attack designed to block user access to a Web site or network by flooding it with bogus information (such as a surplus of requests). The information overload maxes out the Web site or network's processing capabilities, resulting in the user's inability to access Internet services and making it appear inaccessible. These DoS attacks damage productivity and can be highly frustrating, though the hacker's primary purpose of such attacks is generally disruption and not identity theft.

Distributed denial-of-service (DDoS) attack

This variety of DoS attack enlists multiple compromised computers to flood a single target with bogus information. A criminal hacker can hijack your computer and force it and others to perform a DoS attack against other computers, users, or networks.

Dialer

Traditional modems use a program called a dialer to connect a computer to the Internet, but dialers are perhaps most well-known for their illegitimate purposes. Bad dialers cause your PC to call long-distance or for-pay numbers, rather than your ISP. This most often results in a large telephone bill for the user and a tidy profit for the dialer's creator.

Drive-by

This term is loosely used for a stealth software installation the user does not initiate. In some cases, simply visiting a Web page can download malicious programs to a PC without a user's knowledge or consent. In other cases, a pop-up ad might be used to initiate a drive-by installation.

Evil twin

A spoofed doppelganger of a legitimate wireless access point is known as an evil twin. Often home constructed, the evil twin hotspot offers wireless access for the purpose of collecting the user's data, which can then be exploited or sold.

False positive

False positives can fall into several categories. In an effort to sell software, unscrupulous antispyware programs often will mislead a user into believing his or her machine is infected with spyware when no problems actually exist. The term false positive also can be used when legitimate antispyware applications mistakenly label a benign program as a threat.

Firewall

A firewall is a crucial component in a computer's line of defense, as firewalls prevent unauthorized services or programs from accessing a computer or network resources. Although virtually every corporate network has its own firewall, every personal computer should have one as well. Personal firewalls can come as standalone products or as components built-in to a larger security suite.

Hacker

"Hacker" is a term that often requires more qualification than is given, as hackers can act with intentions and outcomes ranging from beneficial to malicious. To hack a file or a program is simply to deconstruct it or tweak its performance. Therefore the term *hacker* has neutral connotations, encompassing those who tinker with computer programs with no malicious intent, such as computer programmers or security researchers, as well as criminal hackers (also called *crackers*) who seek to damage your system, gain from stored data, or control your PC remotely. Hacking taxonomy is associated by color--*black hat hackers* are malicious, *white hat hackers* are benign, and *gray hat hackers* are characterized by varying motivations.

Glossary

Hijackers

Often installing as a helpful browser toolbar, hijackers may alter browser settings or change the default home page to point to some other site.

Keylogger

Keyloggers are just what they sound like--programs that record every keystroke made on a PC. Though some parental-control applications include keyloggers for monitoring purposes, the ones that come bundled with spyware are far more insidious. These types of keyloggers send sensitive information to a remote computer, where thieves can access data such as credit-card and bank-account numbers, as well as passwords and social-security numbers.

Malware

Malware is generally used to describe a piece of software that exploits or inconveniences the user. It usually refers to the most malicious forms of adware and spyware.

Man-in-the-middle attack

In this particular type of attack, a third party piggybacks on valid user privileges to gain unapproved access to a computer or network. The man-in-the-middle (MITM) attack exploits the authentication process of a one-way authentication (user approved by the network) wireless access point (WAP). MITM attacks are orchestrated by intercepting a valid authentication granted by a network with a one-way authentication setup to any valid Media Access Connection (MAC). With the user's legitimate access as a shield, the MITM has full access to the data flowing in and out of a user's computer.

Pharming

Like phishing, pharming preys on socially conditioned patterns of human behavior to coax sensitive information from victims. Whereas phishers masquerade as legitimate organizations, pharmers hijack sites' domain names to redirect traffic elsewhere. In this way, visitors to an online banking site can be channeled to a mirror site and prompted to provide personal data that crackers can collect and use.

Phishing

Spoofing legitimate organizations to lure users into giving up sensitive data is a favorite technique among security fraudsters. In a common phishing scam, users receive a look-alike e-mail message purportedly from a trusted institution like their bank, alerting them to an urgent need. Users follow the embedded link to a convincing site that requires them to sign in using account information.

Among the subsets of phishing scams, spear phishing targets a specific user demographic, such as gamers. In VoIP phishing, users are directed to verify their account information over the phone rather than on a Web site.

Phreaking

Combining the words "phone" and "freak," phreaking refers to a wide subculture of hacking that involves manipulating and exploiting telephone systems.

Rogue antispyware software

Posing as legitimate antispyware applications, these malicious programs scan a computer and induce false positives to scare users into buying a product. Rogues often attempt to distribute themselves via ominous pop-up ads and can be very difficult to manually uninstall.

Rootkit

Although an exact definition of what constitutes a rootkit is still under debate, it is generally regarded as a piece of software that allows intruders to conceal malicious files and programs from users or system administrators. Rootkits can be extremely hard to uninstall and allow troublemakers to go about their dirty work undetected.

Spam

Originally, the unsolicited bulk messages that inundate a user's account took the form of e-mail messages (mostly advertisements) in which the sender attempted to engage the user in a purchase. Spam has evolved, and unsolicited bulk messages crop up in instant messages (spim), blog comments (splogs), mobile texts (SMS spam), forums, and so on. More than merely annoying, spam attachments can contain viruses and malware or link to dangerous Web sites. Spam is the principle vehicle for phishing scams.

Spoof

Spoofs are misleading Web addresses, spam e-mails, and IP addresses forged by a malicious hacker to look identical to the legitimate organization's materials. They are used to trick users into responding to alerts that appear to be issued by trusted organizations such as banks. Users who respond to the visual fakery and urgency of the requests are prompted to give up private data, which is then often used in identity theft. Spoofs are instrumental in carrying out phishing, pharming, and phreaking scams.

In a pharming exploit, a spoofed IP address of a legitimate company might be scripted to float over the culprit's actual, nonlegitimate IP address in order to make the user believe the site is valid.

Spyware

Spyware refers to programs that gather and transmit the user's personal details or behavior to a third party, often without the user's knowledge or consent. Like adware, it often installs as a third-party component bundled with freeware or shareware, creating a fuzzy distinction between the two.

Tracking cookies

Internet browsers write and read cookies, files with small amounts of data (such as site passwords and settings) based on instructions from Web sites. In many cases, cookies provide a benefit to users. However, in some instances cookies are used to consolidate and track user behavior across different sites, which provides marketers with private information about an individual.

Trojan horses

Trojan horses slip into an individual's system and run without the user's knowledge. They can have many functions. For example, some use a computer's modem to dial long-distance, generating huge phone bills for the computer owner. Unlike viruses and worms, Trojan horses do not make copies of themselves.

Virus

Like human viruses, the computer varieties contain harmful code and spread easily to infect multiple hosts. Viruses are notorious for corrupting hardware, software, and personal files. Viruses cannot spread on their own, requiring users to share infected files through e-mail attachments, flash drives, disks, P2P, Web sites, or any other file-transferring mechanisms.

Worm

Often conflated with viruses, worms also are self-replicating programs; however, they propagate independently of user interaction, often through a shared or direct network connection. Worms may destroy data on individual machines, but mostly inflict their damage by siphoning users' bandwidth or shutting down their computers.

Zombie

Using viruses, Trojan horses, and worms, criminal hackers can remotely operate a compromised machine without the knowledge of its owner. Zombie computers often host programs that allow them to be conscripted by a remote controller into bot armies, called botnets, to launch DDoS attacks.

Zero-day exploit

Malicious hackers have discovered they can increase their level of destruction by cracking the defenses of a product on the same day that news of a vulnerability breaks and/or an ensuing patch is released. Disclosure practices compel software and security vendors to publicly announce flaws, which informs fast-acting exploiters. The resulting zero-day attacks affect users who haven't applied a patch to fix the vulnerability.