London School of Economics and Political Science

The Status and Use of Computer Network Attacks in International Humanitarian Law

Heather Harrison Dinniss

A thesis submitted to the Law Department of the London School of Economics and Political Science for the degree of Doctor of Philosophy

September 2008

ProQuest LLC
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106-1346

Declaration

I certify that the thesis I have presented for examination for the PhD degree of the London School of Economics and Political Science is solely my own work other than where I have clearly indicated that it is the work of others (in which case the extent of any work carried out jointly by me and any other person is clearly identified in it).

I warrant that this authorization does not, to the best of my belief, infringe the rights of any third party.

Abstract

The information revolution has transformed both modern societies and the way in which they conduct warfare. This thesis analyses the status of computer network attacks in international law and examines their treatment under the laws of armed conflict. A computer network attack is any operation designed to disrupt, deny, degrade or destroy information resident in computers and computer networks, or the computers and networks themselves.

The first part of the thesis deals with a States right to resort to force and uses the U.N. Charter system to analyse whether and at what point a computer network attack will amount to a use of force or an armed attack, and examines the permitted responses against such an attack.

The second part of the thesis addresses the applicability of international humanitarian law to computer network attacks by determining under what circumstances these attacks will constitute an armed conflict. It concludes that the *jus in bello* will apply where the perceived intention of the attacking party is to cause deliberate harm and the foreseeable consequence of the acts includes injury, death damage or destruction.

In examining the regulation of these attacks under the *jus in bello* the author addresses the legal issues associated with this method of attack in terms of the current law and examines the underlying debates which are shaping the modern laws applicable in armed conflict. Participants in conflicts are examined as increased civilianisation of the armed forces is moving in lock-step with advances in technology. Computer network attacks also present new issues for the law relating to targeting and precautions in attack which are addressed; objects subject to special protections, and their digital counterparts are also examined. Finally the thesis addresses computer network attacks against the laws relating to means and methods of warfare, including the law of weaponry, perfidy and the particular issues relating to digital property.

Table of Contents

Acknowledgements

An undertaking such as this thesis necessarily requires assistance from many individuals and there are a number of people who have helped me in the formation of my ideas and the writing of this thesis. First and most importantly, I would like to thank my PhD supervisor, Christopher Greenwood for his insightful comments and suggestions, and for keeping me focused on the danger of being too technical at the expense of the law. Special thanks are also due to Christine Chinkin, my supervisor during Chris's sabbatical, who also commented on a draft of the manuscript. Her perceptive insights form the basis of my methodology section, a contribution for which I am profoundly grateful!

Thanks are also due to those specialists in information technology who patiently reviewed my hypothetical examples and advised on the feasibility of certain computer network attacks; in particular Andy Batchelor, Karon James and Michelle Ellis. I am grateful for their assistance, and the fault for any errors remains entirely with the author. Special thanks must also go to Andrew Ladley of Victoria University of Wellington, for his encouragement to continue postgraduate study and for the stories of his adventures that proved so inspirational. I would also like to thank all of my colleagues in the law department of the London School of Economics and Political Science; the drafting of a PhD thesis can be a lonely experience and I am grateful to all my friends for making sure that this was not the case, and for making my time at the LSE so rewarding.

This work was funded in part by the generous Freyberg Scholarship provided by the New Zealand Defence Force and the Research Studentships of the London School of Economics and Political Science.

Finally, and most importantly, I would like to thank my parents for their support and encouragement throughout this thesis; my mother, Ann Dinniss, who has painstakingly proof-read this manuscript, and my father, David Dinniss, who sadly did not live to see it completed. Above all, my thanks go to my husband Marc,

without his support, patience, sense of humour, and steadfast belief, this thesis would not have happened. This thesis is dedicated to him.

Chapter 1 - The World in Which We Live and Fight

On the 16 May 1943, one of the most famous missions of the Second World War, the 'Dambusters' raid, took place. Nineteen Lancaster bombers modified to carry weapons at the cutting edge of technology flew over most of Southern Germany to attack three hydroelectric dams supplying electricity to German industrial installations in the Ruhr valley. Two of the three targeted dams were breached causing significant damage,[1] however eight bomber crews were lost during the mission. Fifty-five years later, a twelve year-old boy hacked into the control system of Arizona's Roosevelt Dam, gaining control of its massive floodgates and the 489 billion gallons of water which it contains.[2] Although the boy was unaware of the fact, federal authorities stated that he could have released the 489 billion gallons of water contained by the dam downstream causing massive amounts of damage. Such an incident demonstrates the power and possibility of computer network attacks if utilised in an armed conflict; it also illustrates the vulnerability of States who are dependent on information infrastructures not adequately protected against this new method of attack.

This thesis examines the law governing the use of force and humanitarian law as it applies to computer network attacks. It represents a systematic analysis of the laws of armed conflict, both *jus ad bellum* and *jus in bello*, as they relate to one of the newest forms of warfare. Computer network attacks (CNA) are "actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and

---

[1] In the Möhne and Ruhr valleys 11 factories were totally destroyed, 114 seriously damaged, 25 road and rail bridges were destroyed and throughout the region power, water and gas supplies were seriously disrupted. Communications by road and canal were severely disrupted and for the remainder of the war the Germans had to divert an additional 10,000 troops to guard the dams. National Archives, *Dambusters: The Legacy* <http://www.nationalarchives.gov.uk/dambusters/legacy.htm> (last accessed 21 August 2008).

[2] Barton Gellman, 'Cyber-Attacks by Al Qaeda Feared', *Washington Post* (Washington D.C.), 27 June 2002, A01. Note that there is debate over the veracity of some of the facts of this case, including the year and severity of the attack and the age of the hacker which are detailed in Appendix 1. However, the example illustrates the point being made here of the change in the method of warfare to achieve the same effect.

networks themselves";[3] computer network attacks form a subset of information operations.[4]

The thesis is divided into two parts. Part one addresses the *jus ad bellum*; it examines computer network attacks as a prohibited act and the permitted responses to such acts under international law. Chapter 2 looks at the qualification of computer network attacks as a use of force contrary to Article 2(4) of the UN Charter and examines the theoretical underpinnings of the prohibition against force in international law in order to address some of the specific characteristics of computer network attacks. Chapter 3 considers when an attack will rise to the level of an armed attack, thus triggering the right of self-defence. The chapter also examines the issue of attribution of attacks which is a particular problem for a method of warfare that generally relies on anonymity. The chapter also addresses other possible responses to computer network attacks, namely counter-measures against an unlawful act and collective measures authorised by the Security Council against a threat to the peace.

Part two of this thesis examines the *jus in bello* and works systematically through those areas of the law of armed conflict for which computer network attacks raise issues. Chapter 4 begins by examining the concept of armed conflict and assessing under what circumstances the law of armed conflict will apply to computer network attacks. The following chapters examine the themes of participants in conflict, targeting and legitimate military objectives, precautions in attack and defence, measures of special protection, the protection of cultural property during armed conflict, and means and methods of warfare (including the law of weaponry).

The thesis is not, however, limited to a point-by-point analysis of the current laws of armed conflict. The rise of computer network attack as a means and method of warfare is born out of, and in turn has influenced, many different societal and military trends; any attempt to analyse how the laws of armed conflict should affect

---

[3] U.S. Department of Defence, *Dictionary of Military and Associated Terms*, Joint Publication 1-02 (2001) <http://www.dtic.mil/doctrine/jel/doddict/index.html> (last accessed 22 April 2008).

[4] The U.S. DoD dictionary defines 'Information Operations' as "The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own". Ibid.

this form of warfare must, therefore, take these trends into account or risk becoming outdated as soon as it is completed. Indeed, with much of the current capacity for computer network attacks remaining classified and the exponential growth of computing and transmission power,[5] any attempt to limit a thesis to present capacity and ignore trends would be foolhardy at best. The thesis also takes account of the ongoing debates between experts taking place in relation to the laws applicable in conventional armed conflicts. These debates, such as the current discourse on direct participation in hostilities, the use of civilian contractors, the applicability of the laws of armed conflict to counter-terrorist operations, and targeting of dual-use facilities, to name just a few, all form the background to the discussion of the law as it applies to computer network attacks.

Raymond Ku has noted that with each controversy involving the Internet, the law is forced to confront cyberspace on two levels.[6] The first is a consideration of what real space rules and legal regimes should apply to cyberspace. At this level we are asked to translate where possible our existing values and legal principles into values and legal principles applicable to cyberspace.[7] On a second level, providing new laws for cyberspace forces us to examine our pre-cyberworld rules as well as our commitment to the values that form the foundation for those laws.[8] Ku's dual analysis can be applied to the interpretation and promulgation of laws to govern armed conflict using computer network attacks. First, it is necessary to examine the current legal regulation of armed conflict and consider how it can be applied to computer network attacks. However in order to do that effectively, it is necessary to return to the underlying principles for those laws and determine whether the values they seek to protect are the same for the societies dependent on information technology who are the victims of such attacks. For example, the laws of armed conflict offer protection to civilian property as a consequence of the principle of distinction. Therefore it is necessary to revisit the reasons *why* we protect civilian property, to determine whether those principles should still apply with respect to digital property, in light of

---

[5] Moore's Law states that computing power will double approximately every two years; Nielson's law states that bandwidth for high-end users will double in the same period.

[6] Raymond Ku, 'Foreword: A Brave New Cyberworld' (2000) 22 *T Jefferson L Rev* 125, 128.

[7] Ibid.

[8] Ibid., 129.

societies' changing conceptions of property as a whole and the importance of digital property to the functioning of information societies.

This need to re-address principles comes at a time when the law of armed conflict, even as it relates to conventional armed conflict, is under greater scrutiny than it ever has been in the past. Increased media attention and the proliferation of non-governmental actors involved in conflict, whether as participants or observers, has resulted in the inherent tensions and ambiguities in the laws of armed conflict being forced into stark relief. Ku argues that before we can consistently apply existing law to the challenges posed by cyberspace, we must resolve conflicting values and clarify the latent ambiguities that justify existing legal rules.[9] However while that may be an ideal solution for application to domestic law issues, the laws relating to the use of force and the conduct of armed conflict owe their existence to a state of perpetual tension between conflicting values; most obviously in the case of the laws of armed conflict, the balance between humanitarian principles and military necessity. Further, it is the very ambiguities that Ku is determined to resolve, that allow public international law to function – in some cases consensus may only be reached by allowing for differing interpretations. Simply put, the application of the law to cyberspace in this case computer network attack technologies, cannot be dependent on the resolution of those conflicts and ambiguities that form an integral part of the functioning of the international system. Some of the tensions that are now becoming apparent are the result of the changing character of warfare, the context in which it is waged, and the societies in which it is conducted. This thesis sets out the competing approaches and examines their validity for the application of the law to computer network attack where these areas of disagreement occur.

The trends affecting modern armed conflict are happening at a societal level as well as at a military and strategic level, thus an understanding of these developments is required in order to understand the legal complexities arising from this new type of warfare. In fact, Alvin and Heidi Toffler point out: "What is known as the [revolution in military affairs] therefore, is extremely important, but it is,

---

[9] Ibid., 127. citing Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books, New York, 1999), 119.

nevertheless, just one facet of the larger civilisational shift, and it needs to be understood in that context".[10] This view is shared by British military historian Jeremy Black:[11]

> "...the material culture of war, which tends to be the focus of attention, is less important than its social, cultural and political contexts and enablers. These contexts explain the purposes of military action, the nature of the relationship between the military and the rest of society, and the internal structures and ethos of the military."

That is to say, that the context of warfare defines it more than the military technology it utilises. That same context will be reflected in the laws that govern warfare through the application of the general principles which underpin it. In particular, the laws of armed conflict represent the point of balance or compromise between two dynamic forces, the requirements of humanity on the one hand, and military necessity on the other. It is the dialectical relation between these two forces, in the light of historical experience, which determines the contents, contours and characteristics of the law of armed conflict at any moment in time.[12] The following sections outline and examine some of the trends that are influencing both society and the military, and hence the legal context in which future armed conflicts will take place. This chapter places the emergence of computer network attacks as a means and method of warfare in its broader context, both in terms of the revolution in military affairs and its wider societal context, in order to understand the drivers of modern armed conflict and the values which the laws of armed conflict seek to protect.

---

[10] Alvin Toffler and Heidi Toffler, 'Foreword: The New Intangibles' in J Arquilla, et al. (eds), *In Athena's Camp: Preparing for Conflict in the Information Age* (RAND, Santa Monica, 1997) xiii-xxiv, xiv.

[11] Jeremy Black, *War in the New Century* (Continuum, London, 2001), 114. cited in Colin S Gray, *Another Bloody Century: Future Warfare* (Weidenfeld & Nicolson, London, 2005), 84.

[12] Georges Abi-Saab, 'The Specificities of Humanitarian Law' in C Swinarski (ed) *Studies and Essays on International Humanitarian Law and Red Cross Principles in Honour of Jean Pictet* (Martinus Nijhoff Publishers, Geneva, The Hague, 1984) 265-280, 265.

1. Societal Trends Generally

1.1. The Information Revolution & Digitisation

The information revolution is one of the defining characteristics of the current age. Advances in information technology are affecting almost every segment of business, society and government in many, if not all, regions of the world.[13] Information has changed the entire structure of society: governmental leadership, national identity, production values, organisational structures and even domestic attributes such as family and religion have all been affected with a speed and global impact on a scale never seen before.[14] In examining the effects of this phenomenon on conflict, four main factors must be taken into account: the ubiquity of information technology, the increasing amount and decreasing cost of information, societies' changing attitudes to, and because of, access to information, and finally, the effects of increased information on organisational structures within both domestic and international society.

1.1.1. Ubiquity

As more and more information becomes digitised and bandwidth expands,[15] societies have become increasingly reliant on networked and electronic information. Information technology is being integrated into everything from appliances and vehicles to business processes and control systems.[16] More importantly, computer systems regulate air traffic control and other transportation networks, oil and gas pipelines, electricity generating systems and networks, sewerage and water treatment facilities, emergency response services, hospital systems and many other systems

---

[13] Richard O Hundley, et al., *The Global Course of the Information Revolution: Recurring Themes and Regional Variations* (National Defense Research Institute, RAND, Santa Monica, 2003) <www.rand.org/publications/MR/MR1680/index.html> (last accessed 16 March 2008).

[14] See generally, Alvin Toffler and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century* (Warner Books, London, 1994).

[15] Digitization refers to the encoding, transformation, and transmission of all information – whether audio, video, graphics or text – into a series of binary numbers i.e. 1s and 0s. See Stephen Saxby, *The Age of Information: The Past Development and Future Significance of Computing and Communications* (Macmillan, London, 1990), 3.

[16] Dorothy E. Denning, 'Cyber-Security as an Emergent Infrastructure' in R Latham (ed) *Bombs & Bandwidth: The Emerging Relationship between Information Technology & Security* (Manas Publications, New Delhi, 2004) 25, 33.

considered part of the critical infrastructure of modern States. Dorothy Denning notes that this trend to ubiquitous computing affects information security in two ways; First there are more targets and more attackers, and secondly attacks can have real world consequences.[17] The first point is fairly self explanatory, the more systems that are networked and run by information technology, the more targets that are vulnerable to attack. The more those systems are networked, the more open they become, and greater numbers of attackers have access to try and crack the system. Denning's second point regarding the real world consequences of such actions is a basic but important one. When computer network attacks were first raised as a possible threat, many were sceptical of their merits, seeing them as purely 'nuisance' attacks of no real consequence for everyday life.[18] This attitude is slowly being revised in the face of increasing domestic incidents of computer network attacks and the beginnings of their introduction for use in armed conflict, both of which illustrate their utility in the real world.[19]

One of the key systems responsible for the cross-over between virtual and real world consequences of information technology are the control systems which regulate most critical infrastructure systems of technologically advanced societies; these systems control power plants, water systems, dams, gas pipelines, chemical plants and reactors to name a few. Supervisory control and data acquisition (or SCADA) systems, distributed control systems (DCS) and other control systems regulate most of the critical infrastructure and have proven particularly vulnerable to attack. In March 2007, researchers from the Idaho National Laboratory launched an experimental cyber attack, hacking into a replica of a power plant's control system and changing the operating cycle of a generator.[20] The attack sent the generator out of control and ultimately caused it to self destruct, alarming the federal government

---

[17] Ibid.

[18] See for example Frontline, *Interview with James Lewis for Frontline: Cyber War! (Interview Conducted on 18 February 2003)* <http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/lewis.html> (last accessed 16 March 2008).

[19] However see Mark Trevelyan, 'Security Experts Split on "Cyberterrorism" Threat', *International Herald Tribune* (Paris), 16 April 2008, <http://www.iht.com/articles/reuters/2008/04/16/europe/OUKWD-UK-SECURITY-CYBERSPACE.php> (last accessed 19 April 2008).

[20] Jeanne Meserve, 'Staged Cyber Attack Reveals Vulnerability in Power Grid', *CNN.com* 26 September 2007, <http://edition.cnn.com/2007/US/09/26/power.at.risk/index.html> (last accessed 20 February 2008).

and electrical industry about what might happen if such an attack were carried out on a larger scale.[21] One of the earliest known incidents of this kind of computer attack, the so-called 'Farewell Dossier' incident, took place in 1982 during the Cold War. Following the theft of technology from Western powers by the Soviet KGB, the CIA of the United States and a Canadian software supplier planted malicious code in the software for a gas pipeline control system which a KGB operative had been sent to steal:[22]

> "[T]he pipeline software that was to run the pumps, turbines and valves was programmed to go haywire, after a decent interval, to reset pump speeds and valve settings to produce pressures far beyond those acceptable to the pipeline joints and welds. The result was the most monumental non-nuclear explosion and fire ever seen from space."

SCADA systems were again compromised in the 1998 Arizona Roosevelt Dam example cited previously. In another example, in 2000 Vitek Boden hacked the control system of the water and sewerage treatment plant in Queensland, Australia. Over a two month period the disgruntled former employee had accessed the system 46 times gaining complete control of the sewerage and drinking water systems for the region and dumping putrid sludge into the area's rivers and parks.[23] Incidents such as these have made States increasingly aware of the amount of critical infrastructure that is controlled by computers and their resultant vulnerability to computer network attacks. Cyber attack has now been listed as one of the major threats to both the U.S. and U.K. critical infrastructure in recent reports.[24] Although they are the most obvious, control systems are not the only link between computers and the physical world which may be affected by computer network attacks. For example, civilian vehicles and air traffic controls are increasingly equipped with navigation systems relying on GPS satellites, the same satellites

---

[21] Ibid. Footage of the generator is available at http://www.youtube.com/watch?v=fJyWngDco3g.

[22] Thomas C. Reed, *At the Abyss: An Insider's History of the Cold War* (Presidio, New York, 2004), 269.

[23] *R v Boden* (2002) QCA 164, Court of Appeal of the Supreme Court of Queensland (Australia); Gellman, 'Cyber-Attacks by Al Qaeda Feared'.

[24] U.S. Department of Homeland Security, *National Infrastructure Protection Plan*, U.S. Department of Homeland Security, (2006) <http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf> (last accessed 28 April 2008); U.K. Cabinet Office, *The National Security Strategy of the United Kingdom: Security in an Interdependent World*, U.K. Cabinet Office, Cm 7291 (2008).

which control U.S. military positions and precision guided missiles. This trend will only continue as the global information environment continues to develop at pace with the development of next generation Internet providing broadband, always-on connection from multiple devices in every aspect of personal, business and public life.

1.1.2. Amount

As information technology pervades more of daily life, the sheer amount of information available is increasing at a phenomenal rate. In 1993, there were about fifty websites in the world; by the end of the decade that figure had surpassed five million.[25] One study has estimated that the total amount of new information produced in 2002 was approximately five exabytes, in print, film magnetic and optical storage media; 92 percent of which was stored on magnetic media, mostly in hard disks, and only 0.01 percent was stored on paper.[26] The amount of new information produced has more than doubled from the estimated two exabytes produced in 1999. The same study estimates that the amount of information available on the surface of the World Wide Web (i.e. fixed web pages) is 170 terabytes, and in depth (i.e. including database driven websites that create web pages on demand) is 91,850 terabytes.[27] Further, the relative cost of transmitting information has dramatically decreased, removing barriers to entry and allowing almost anyone to add information or utilise available information systems.

1.1.3. Societal Change

It is axiomatic to say that the information revolution is fundamentally changing societies. The dramatic change in the linked technologies of computing and communications, sometimes called the third industrial revolution, is changing the

---

[25] Douglas McGray, "The Silicon Archipelago" (1999) Spring *Daedalus* 147-76 cited in Joseph S. Nye, Jr, *The Paradox of American Power: Why the World's Only Superpower Can't Go It Alone* (Oxford University Press, Oxford, 2002), 42.

[26] Five exabytes (5 x10^{18} Bytes) is equivalent to half a million new libraries the size of the US Library of Congress print collections; see Peter Lyman and Hal R. Varian, *How Much Information?*, University of California at Berkley (2003) <http://www.sims.berkeley.edu/research/projects/how-much-info-2003/> (last accessed 9 November 2007).

[27] Ibid. Note that this figure does not include email (440,606 Terabytes) or instant message (274 terabytes) information sources.

nature of governments and sovereignty, increasing the role of non-state actors, and enhancing the importance of soft power in foreign policy.[28] Indeed some academics argue that the change in the mode of communication has a substantial effect on the distribution of power within society, on social evolution as a whole and on the values and beliefs of that society.[29] While all of these societal changes will effect the application and interpretation of the law relating to armed conflict in varying degrees, two in particular deserve further examination here.[30]

First, individuals may turn from traditional sources of national identity to competing social identifications based on ethnic, religious, or other ties which are not dependant on geographical location. This may have a fragmentary effect, amplifying existing divisions in society to the point of armed conflict.

Secondly, increased access to information allows people to see events happening around the world. This may lead to an increased humanitarian consciousness regarding human rights abuses and an increased awareness of actions carried out in the public's name. The result is the so-called 'CNN effect', the influence of media footage on foreign policy. With the advent of live satellite feeds and citizen journalism into the global communications market, the harsh realities of conflict can be beamed into the homes of citizens who see the violence committed in their name. This effect has provided both a powerful tool for governments and a constraint on their behaviour.[31] The events surrounding the shooting down of the U.S. Black Hawk helicopter crew and subsequent television footage of the treatment of the body of one of the crew members in Mogadishu, Somalia in 1993, illustrated the powerful effects

---

[28] Nye, *Paradox*, 43.

[29] For an exposition of 'medium' theory and its effects on the information revolution see Ronald J. Deibert, *Parchment, Printing, and Hypermedia: Communication in World Order Transformation* (Columbia University Press, New York, 1995).

[30] The increasing importance of intangible property will be examined in the section on the knowledge economy in section 1.3 *infra.*

[31] See generally Steven Livingston, *Clarifying the CNN Effect: An Examination of Media Effects According to Type of Military Intervention*, The Joan Shorenstein Center on the Press, Politics and Public Policy, John F. Kennedy School of Government, Harvard University, R-18 (1997) <http://www.hks.harvard.edu/presspol/research_publications/papers/research_papers/R18.pdf> (last accessed 16 April 2008); Margaret H. Belknap, *The CNN Effect: Strategic Enabler or Operational Risk?*, Strategy Research Project, U.S. Army War College (2001) <http://www.iwar.org.uk/psyops/resources/cnn-effect/Belknap_M_H_01.pdf> (last accessed 16 April 2008).

of the new communications environment.[32] The U.S. Government announced a withdrawal from Somalia shortly after the events of October 1993, in large part due to the overwhelming public pressure following the airing of this distressing footage.[33]

1.1.4. Organisational Change

What is certainly clear is that the information revolution is favouring and strengthening networked forms of organisation, often giving them an advantage over hierarchical forms.[34] This enables power to migrate to non-state actors, as they are more easily able to organise themselves into sprawling networks, where every node can communicate with every other node, far more readily than can traditional hierarchical state actors.[35] Brian Nichiporuk and Carl Builder argue that two different processes are at work in weakening the traditional hierarchical structure.[36] First, in businesses engaged in information intensive enterprises, those organisations structured as networks are proving more competitive than traditional hierarchies.[37] The second process weakening hierarchies is the shift from relative poverty to abundance in information, permitting individuals to bypass hierarchies that have – deliberately or inadvertently – controlled or limited information.[38]
Globalisation and the information revolution enjoy a symbiotic relationship, each enhancing the other's effects and capabilities. The advances in technology, particularly information technology, allow cross border integration of communications, taxes, movement of money, goods, services and people, by

---

[32] In October 1993, U.S. Delta Force & Army Rangers launched a mission against Somali warlord General Aideed. Two U.S. Black Hawk helicopters were shot down and the resulting fire-fight and mob action left several U.S. servicemen dead. Following these events, CNN (and other media outlets) aired footage of the body of one of the servicemen being dragged through the streets of Mogadishu to the cheers of the gathered crowd.

[33] The decision to place U.S. troops in Somalia in the first place was also seen by many to be in reaction to footage of starving refuges shown in the media.

[34] John Arquilla and David Ronfeldt, 'The Advent of Netwar (Revisited)' in J Arquilla and D Ronfeldt (eds), *Networks and Netwars* (RAND, Santa Monica, 2001) 1-24, 1.

[35] Ibid.

[36] Brian Nichiporuk and Carl H. Builder, 'Societal Implications' in J Arquilla and D Ronfeldt (eds), *In Athena's Camp* (RAND, Santa Monica, 1997) 295, 297.

[37] Tracy Kidder, *The Soul of a New Machine* (Little, Brown, Boston, 1981), cited in Nichiporuk and Builder, 'Societal Implications', 298.

[38] Nichiporuk and Builder, 'Societal Implications', 297.

reducing or removing the regulatory barriers. Conversely, globalisation is shaping the world in which in the information revolution is playing out.[39] These cultural and societal effects are taking place, for good and ill, across an increasingly networked and interdependent world. Thus the information revolution has spawned the most complex and rapid of interconnectedness and interdependence in history.[40]

1.2. Globalisation, Interdependency and the Changing World Order

If the information revolution is one of the defining characteristics of the modern age, the current era of globalisation must surely be a second. Globalisation takes many forms and effects the economic, political and societal structures in which we live. Much has been written about its effects on the causes of conflict; from a resurgence of nationalist or tribal groupings, rebellion against perceived cultural imperialism, inadequate living and working conditions created by the race-to-the-bottom in the global labour market, to the recent food riots, globalisation has been cited as a causative factor in the resulting unrest. Although far from a fixed definition, globalisation is generally understood as referring to the expansion of networks of interdependence spanning national boundaries that follows the increasingly rapid movement of ideas, money, goods, services and people across these borders.[41]

In the economic sector, globalisation has meant increased transnational production of goods,[42] decreased state control over such bastions of sovereignty as national currency, and the rise of an economy based on knowledge and other intangible assets. To take one example, currency value was once the sole preserve of the nation state. Before the 1970's, national central banks had substantial control over the prices of most major goods through their ability to manipulate interest rates and intervene in foreign currency markets.[43] However the 1997 'Asian Flu' illustrated the

---

[39] Hundley, et al., *Global Course*, 4.

[40] As Colin S. Gray points out, this is not the first era of globalisation in history, the Huns, Alexander the Great and the empires of the Romans and the Byzantines were highly interconnected. See Gray, *Another Bloody Century*, 78-79.

[41] Hundley, et al., *Global Course*, 49.

[42] For an example of transnational, cross-border production of goods, see Thomas Friedman, 'Global Is Good', *The Guardian* (London), 21 April 2005, <http://www.guardian.co.uk/g2/story/0,,1464454,00.html> (last accessed 27 May 2005).

[43] Nichiporuk and Builder, 'Societal Implications', 302.

increased interdependency of the global foreign currency market as economy after economy felt the effects of a currency collapse in Thailand and other parts of South East Asia. Daily turnover on the foreign exchange market now exceeds US$3.2 trillion,[44] leaving state control of currency negligible, and in some cases forcing national governments to adjust their financial and monetary policies to prevent currency devaluation.[45] Commodities and product markets have also gone global and are no longer heavily subject to the policies of national governments or even cartels of national governments.[46] For example in 2001, multi-national corporations accounted for twenty-five percent of world production and sales equated to almost half of the world's GDP.[47] The effects of globalisation are also seen in new business models which have been enabled by the information revolution, such as outsourcing, network production chains and networked internal business models. Outsourcing allows companies to leverage cost savings in countries where the costs of labour are far cheaper than in the parent company's State. While larger companies have bought and maintain their own companies offshore, the concept has allowed smaller players to increase wealth creation by creating networks with other small companies, each concentrating on their niche product to provide customer focused solutions. Internally, the new business models are also changing the architectural organisation of companies, often from vertical integration to horizontal networks.[48] This networked structure, usually based on processes, provides great internal flexibility, an advantage in an environment driven by connectivity and speed, and thus translates into a direct competitive advantage.

If economic globalisation is the principle driving force behind contemporary globalisation, it is its effects on the political landscape, namely the form and context of state power, which is of interest in this instance. Globalisation has empowered

---

[44] Bank for International Settlements, *Trienniel Central Bank Survey: Foreign Exchange and Derivitaves Market Activity in 2007*, Bank for International Settlements (2007) <http://www.bis.org/publ/rpfxf07t.pdf> (last accessed 17 April 2008).

[45] Nichiporuk and Builder, 'Societal Implications', 302.

[46] Ibid., 304. Although as Nichiporuk and Builder point out, this is not the case with extremely rare resources such as diamonds.

[47] UNCTAD, 2001 cited in David Held and Anthony McGrew, 'Introduction' in D Held and A McGrew (eds), *Governing Globalisation: Power, Authority & Global Governance* (Polity Press, Cambridge, 2002) 1-21.

[48] Hundley, et al., *Global Course*, 26.

new actors and placed some traditional forms of governance beyond the reach of national governments.[49] In a world linked by almost instantaneous communication without regard to national borders, political associations have taken on new allegiances, authority and forms. As Held and McGrew point out, "the intimate connection between 'physical setting', 'social situation' and politics, which distinguished political associations from premodern to modern times, has been ruptured; the new communication systems create new experiences, new modes of understanding and new frames of political reference independently of direct contact with particular peoples, issues or events".[50] Thus, disparate groups of individuals or small collectives are now capable of exercising political power across the globe by exploiting the communications networking power of the information revolution. A prime example of the new power of these networks is the recognition of the International Campaign to Ban Landmines (ICBL) in bringing about the implementation of the 1997 Ottawa Convention.[51] The empowerment of these new actors is also happening at multiple levels. Intergovernmental organisations such as the World Trade Organisation, IMF and World Bank wield considerable power through structural adjustment programs; the European Union and other regional alliances now shape policies for their members; international non-governmental groups such as the ICBL, as well as criminal and terrorist organisations such as Al Qaeda increasingly effect the global agenda. Correspondingly, the number of these organisations has increased dramatically. At the beginning of the twentieth century there were just 37 intergovernmental organisations and 176 international non-governmental organisations,[52] by 2006 that number had grown to 970 intergovernmental bodies and 11,859 non-governmental bodies.[53]

---

[49] In addition to the financial and economic governance outline above, States have also lost their power as the major arbiter of information in society, and in many cases much of their control over the movement of goods and people across borders, the EU is an example.

[50] Held and McGrew, 'Introduction', 6.

[51] ICBL was the joint Nobel Peace Prize winner in 1997; another NGO, Médecins Sans Frontières, won the Nobel Peace prize in 1999.

[52] UIA *Yearbook of International Organisations* (Brussels: Union of International Associations, 1997) cited in Held and McGrew, 'Introduction', 7.

[53] UIA *Yearbook of International Organisations* 2003, Appendix 3, Table 1, Available at http://www.uia.org/statistics/organizations/types-oldstyle_2003.pdf (last accessed 14 June 2005).

Globalisation and the interdependence of States has also contributed to matters which had traditionally remained in the purview of the State becoming widely accepted as part of the international community's concern (most notably human rights abuses), thus making the maintenance of closed societies almost impossible. The interdependence between States is also highlighted by environmental globalisation. The actions of many States feed into the effects of phenomena such as global warming, the effects of which will decrease arable land and fresh accessible water which is essential to the survival of all States, not just those with agrarian economies. Increasingly, the availability of water will become a significant cause of conflict.[54]

1.3. The Rise of the Knowledge Economy

The third societal trend of note is the rise of knowledge based economies and the resultant change in attitudes towards intangible property. Alvin and Heidi Toffler argue that at the heart of the information revolution lies a shift in the relationship between tangible and intangible methods of production, and as a corollary, methods of destruction.[55] Although knowledge, in its broadest sense has always been a factor in the economy, in recent decades it has moved from the periphery to a central position.[56] So much so, that the 1998 *World Development Report* stated that "For countries in the vanguard of the world economy, the balance between knowledge and resources has shifted so far towards the former that knowledge has become perhaps the most important factor determining the standard of living – more than land, than tools, than labour".[57] Indeed the dilemma of measuring and quantifying the knowledge assets of a nation, and hence its capacity for socio-economic growth, is something that academics, economists and accountants have struggled with, because it is treated as a 'residual', something that does not fit the category of tangibles,

---

[54] Egypt has already threatened military force on a number of occasions when its privileged position on the Nile River has been threatened by upstream riparians. In 1978 Egypt threatened air strikes against a planned scheme for Ethiopia to take water from the Blue Nile, again in 1995 Egyptian President Mubarak threatened a "response beyond anything they can imagine" when Sudan suggested it might seek to amend the 1959 Nile Waters Agreement. Michael T. Klare, *Resource Wars: The New Landscape of Global Conflict* (Metropolitan Books, New York, 2001), 158.

[55] Toffler and Toffler, 'The New Intangibles', xiv.

[56] Ibid.

[57] World Bank, *World Development Report: Knowledge for Development*, World Bank (1998).

either industrial or agricultural.[58] However this residual category accounts for more than 70% of most developed nations' economies.[59] This resultant change in the status of knowledge or information assets has been troubling for the legal community as well. Intellectual property rules, the most likely body of law for managing intangible property, are insufficient to deal with all intangible property dilemmas. For example, New Zealand found it necessary to amend its Crimes Act to allow electronic transfers of money to be 'things capable of being stolen' following a case in which the Court of Appeal considered that a fraudulent electronic transfer of funds was not theft.[60]

Despite these difficulties, one of the defining characteristics of this age is the conception of intangible assets having hard monetary value, both as product itself and as part of the production chain. With this assignment of value our corresponding perceptions of property have also changed. Intangible property, at least for knowledge economies, has become as important as tangible property for the survival of the national economy. The movement of such intangibles to the fore is not restricted to the wealth-making sections of society; the information revolution reflects a 'civilisational shift' which can be seen in all facets of society, not least of which is the military.[61] This shift will also be reflected in our concept of what must be protected during armed conflict.

2. Military Trends

Georges Abi-Saab notes that the requirements of the principle of military necessity are defined by the evolution of military technology and strategic thought, and it is in the balance between these objective forms and the subjective requirements of

---

[58] Yogesh Malhotra, 'Measuring the Knowledge Assets of a Nation: Knowledge Systems for Development' (Paper presented at the United Nations Advisory Meeting of the Department of Economic and Social Affairs, Division for Public Administration and Development Management, Ad hoc Group of Experts Meeting - Knowledge Systems for Development, United Nations Headquarters, New York, 4-5 September 2003).

[59] Ibid.

[60] *R v Wilkinson* (1999) 1 NZLR 403, Court of Appeal (New Zealand).The Court held that the simple electronic transfer of funds from one account to another did not amount to theft. The Court reasoned that electronic funds were not a thing "capable of being stolen" as they were not a tangible thing, being merely an acknowledgement of a debt owed by a bank to the account holder. The problem was corrected by the Crimes Amendment Act 2003.

[61] Toffler and Toffler, 'The New Intangibles', xiv-xv.

humanity that the laws of armed conflict find their form and content.[62] Both technology and strategy have changed dramatically in Western militaries in recent years as the trends affecting society previously outlined have also affected the armed forces. Alvin and Heidi Toffler have long argued that the way in which a society makes war reflects the way it makes wealth; thus as society progresses from agricultural to industrial to knowledge based economies, so too do the technologies and forms of warfare available to the armed forces of that State.[63] Thus, the character of warfare is a reflection of the societal, economic and technological state of the society from which it comes.[64] The current revolution in military affairs, this sea-change in the way the military thinks about carrying out its primary function, and indeed the way it defines its primary function, broadly reflects the transformation that is taking place in society as a whole.

Although it is axiomatic that technology has transformed modern militaries in recent years, it is not so much the advances in weapons technology, impressive as they have been, which have had the most impact. It is the linking of those highly precise weapons to advanced sensor arrays and the joining up of multiple facets of technological advance in command and control systems that have made the modern military so formidable. Precision munitions are made more formidable by the GPS and other sensor systems available to them. Technology has also evolved the ability to wage war to the point where the concept of a line marking the heart of the battle no longer makes sense;[65] battlefields have become multidimensional and entire countries have become the battlespace.[66] Like the civilian sectors of society, the military is downsizing its operational staff and outsourcing non-essential, or in some cases, even core functions to civilian contractors. Organisational structure is becoming more decentralised with the onset of advanced command and control technology and improved infrastructure. The adoption of network centric warfare as

---

[62] Abi-Saab, 'Specificities', 265.

[63] This progression can be seen in the basic weapons of agrarian societies to the industrialised warfare of mass-produced tanks and guns, through to the high-tech weaponry seen on some of the more advanced militaries of the world. See, Toffler and Toffler, *War and Anti-War*, 57-80.

[64] Gray, *Another Bloody Century*.

[65] Michael N. Schmitt, 'Asymmetrical Warfare and International Humanitarian Law' in W Heintschel von Heinegg and V Epping (eds), *International Humanitarian Law Facing New Challenges: Symposium in Honour of Knut Ipsen* (Springer, Berlin; New York, 2007) 11-48, 16.

[66] Michael N. Schmitt, 'Targeting and Humanitarian Law: Current Issues' (2004) 34 *Israel YB Hum Rts* 59, 59.

a framework has enabled militaries to utilise the power of networking to provide better battlespace knowledge and the related doctrine of effects based operations allows the conduct of faster and more effective operations.[67] Increased situational awareness has also led to the 'pushing down' of strategic decision making so that even unit commanders in the battlespace are able and required to make strategic decisions.[68]

2.1. A Change of Purpose

General Sir Rupert Smith contends that the purpose of warfare has changed. In industrialized war, political objectives were attained by achieving strategic military objectives of such significance that the opponent conformed to the attacker's will – the intention being to decide the matter by military force.[69] Thus, Oppenheim states in his treatise on *International Law* "[w]ar is a contention between two or more States through their armed forces, for the purpose of overpowering each other and imposing such conditions of peace as the victor pleases".[70] Smith argues that instead we now engage in armed conflicts:[71]

> "to establish a condition or conceptual space in which the political objective can be attained by other means and in other ways. We seek to create a conceptual space for diplomacy, economic incentives, political pressure and other measures to create a desired political outcome of stability, and if possible democracy."

This move towards compellance or coersive campaigns reflects a more nuanced and complex use of military force in international relations. Michael Schmitt notes that Operation Allied Force serves as a classic example of a coersive or compellance campaign, as the intent was never to defeat President Slobodan Milosovic's army;

---

[67] An example of the 'speeding' effects of knowledge sharing in the battlespace can be seen in: Joshua Davis, 'If We Run out of Batteries, This War Is Screwed' (2003) 11(6) *Wired* June 2003 <http://www.wired.com/wired/archive/11.06/battlefield.html> (last accessed 29 April 2008).

[68] The need for unit commanders to make strategic decisions was raised by Charles C. Krulak, 'The Strategic Corporal: Leadership in the Three Block War' (1999) 28(1) *Marines Magazine* January 1999 28-34.

[69] Rupert Smith, *The Utility of Force: The Art of War in the Modern World* (Penguin, London, 2005), 270.

[70] Hersh Lauterpacht (ed) *Oppenheim's International Law* (7th ed, Longmans, Green & Co., London, 1952), 202.

[71] Smith, *Utility of Force*, 270.

rather it was to compel a return to the bargaining table and end the systematic and widespread mistreatment of the Kosovar Albanian population.[72] This change in the purpose of warfare affects the relevant doctrine to be adopted to best effect its aims.

2.2. Network Centric Warfare & Effects Based Operations

Changes in the military are not restricted to the weaponry available to them. The organisational changes which have occurred in the commercial sector are now being implemented to yield the same benefits to the military. This move towards network centric warfare enables militaries to utilise power from the effective linking or networking of their forces.[73] In traditional platform centric warfare each component, be it a tank formation, battleship or aircraft, has its own mission and directives, albeit sometimes working in coordination. However, network centric warfare uses the network itself to provide a combat advantage through increased situational awareness and collaboration between the components of the network, thus increasing the speed at which the forces can operate and enhancing mission effectiveness.[74] The speed of decision-making required in order to fully utilise network centric warfare has also resulted in decision making capabilities being pushed down the chain of command.[75] The true value of the network centric warfare framework in the new environment however, is in the application of effects based operations.[76]

The operationalisation of both the change in purpose of armed force and the move toward network centric warfare can be seen in the doctrine of effects based operations which has become dominant in Western military thinking. Effects based

---

[72] Schmitt, 'Asymmetrical Warfare', 37.

[73] Network centric warfare principles have been adopted by several militaries under various rubrics: network enabled capability in the U.K.; network based defence in Sweden; ubiquitous command & control in Australia.

[74] See generally David S. Alberts, John Garstka and Frederick P. Stein, *Network Centric Warfare : Developing and Leveraging Information Superiority* (2nd ed, National Defense University Press, Washington, D.C., 1999).

[75] Andrew M. Dorman, *Transforming to Effects-Based Operations: Lessons from the United Kingdom Experience*, Strategic Studies Institute (2008) 18.

[76] Effects-based operations are not a new concept however their application in light of network centric warfare are interesting. Effects-based operations are coordinated sets of actions directed at shaping the behaviour of friends, foes and neutrals in peace, crisis and war. Edward A. Smith, *Effects Based Operations: Applying Network Centric Warfare to Peace, Crisis, and War* (DOD-CCRP, Washington, DC, 2002), 108.

operations are co-ordinated sets of actions directed at shaping the behaviour of friends, foes and neutrals in peace, crisis and war.[77] In traditional attrition warfare, reduced to its basics, the enemy is defeated by progressively weakening its military forces.[78] This fits neatly with the preambular principle set out in the St Petersburg Declaration of 1868 which states that the only legitimate object which States should endeavour to accomplish during war is to weaken the military forces of the enemy.[79] However, effects based operations utilise selective targeting and choice of means and methods of warfare to achive a desired effect.[80] As Michael Schmitt has noted, although effects based operations have the potential to foster international humanitarian law by systemising the search for alternative targets, they may also lead to the temptation to strike at targets which are not military in nature in order to coerce specific behaviours from opponents who may not value their military capability as highly.[81] This is discussed in more detail in Chapter 6 on targeting.

2.3. Outsourcing & Civilianisation

The increasing civilianisation of conflicts is another trend impacting on the application of humanitarian law to modern conflict. It is taking place through a number of processes, including the escalating prominence of internal armed conflicts in which the majority of war fighters are civilians. In addition, modern militaries increasingly outsource support and even core functions to contractors – some of whom, like private military or security firms, are engaged in armed tactical roles. In the three and a half centuries since the Treaty of Westphalia, the Nation State has been the defining actor in international relations, and has held the monopoly on power and military force. The emergence of transnational armed groups, the increasing number of non-international armed conflicts and the expansion of the

---

[77] Ibid., xiv.

[78] Schmitt, 'Targeting', 60.

[79] 29 November/ 11 December 1868, *Declaration Renouncing the Use, in Time of War, of Explosive Projectiles under 400 Grammes Weight (St Petersburg Declaration)*, Preamble.

[80] Ultimately, the process addresses the causality between actions and their effects; concentrates on desired effects, both physical and behavioural; models the enemy as a system of systems; and considers timing because the desirability of specific effects depends on the context in which they are created. Schmitt, 'Asymmetrical Warfare', 36-37.

[81] Ibid., 37-38.

battlespace to encompass entire territories have meant that civilians are involved in conflicts, both as participants and victims, more than ever.

Militaries are also facing growing pressure to downsize and reduce budgets. As part of this trend, civilian contractors and employees are increasingly used to augment the defence forces as an easy and flexible way to maintain military strength according to constantly changing needs. Further, as weapons and equipment become more technologically advanced, civilians are recruited to provide essential maintenance and support functions, sometimes from the "factory to the foxhole".[82] Civilians are an easy and less expensive way of maintaining access to the latest technical expertise;[83] they can be hired when needed and discharged when the need is no longer urgent. Likewise they do not require the ongoing provision of accommodation, catering, healthcare and the myriad of other services which are required to support members of the armed forces. Nowhere has the use of private military firms been more extensive and controversial that in Iraq. In March 2005 there were more than 20,000 foreign (non-Iraqi) private military contractors in Iraq; 6,000 of these in armed tactical roles.[84]

Civilianisation of conflict is also occurring with the growing interconnectedness of systems and the increase of dual-use objects. Cost considerations also make the military more likely to rely on civilian facilities such as airfields, ports, and other communications centers.[85] For example, military communications often utilise civilian networks, particularly where they travel over satellites.[86] Enhanced interconnectedness also means that knock-on effects of attacks are more likely to affect more civilian systems than in previous conflicts.

---

[82] Michael E. Guillory, 'Civilianising the Force: Is the United States Crossing the Rubicon?' (2001) 51 *AFL Rev* 111, 125. citing an example of Apache Helicopter support technicians deployed during Desert Storm.

[83] Outsourcing allows allows militaries to take advantages of the competitive advantages of the contracting process.

[84] P. W. Singer, 'Outsourcing War' (2005) 84(2) *Foreign Affairs* 119.

[85] Michael N. Schmitt, *The Impact of High and Low-Tech Warfare on the Principle of Distinction,* Program on Humanitarian Policy and Conflict Research at Harvard University (2003) 8 <http://www.hpcr.org/publications/papers.php> (last accessed 18 December 2007).

[86] Arkin puts the figure at 95% of military communications travelling over civilian satellites in 1995.

3. Terminology & Definitions

While an effort has been made to avoid computer jargon, of necessity this thesis uses technical terms and computer terminology. The author has endeavoured to provide definitions and explanations in the text, however a glossary of computing and technical terms has been included in the appendices for the reader's convenience. Writers in this area have also used a changing lexicon as the field has evolved. While Russian experts are still pushing for an official declaration of definitions,[87] most writers in the field have gradually adopted the U.S. Department of Defense terms and definitions. In the beginning most legal analysts wrote in terms of 'information warfare', basing their definitions and analysis on the framework provided by Martin Libicki's seminal work.[88] Over time this term came to refer to a specific subset, namely the propaganda and misinformation aspects, of a wider field called information operations (IO), and the most recent U.S. Joint Publication on Information Operations removes the term information warfare entirely from its lexicon.[89] Computer network operations are further divided into computer network attack, the subject of this thesis, computer network defence and related computer network exploitation. This definition has been adopted by the United States joint forces and remains the standard to which most authors now subscribe.

3.1. Computer Network Attacks

The defining feature of the computer network attack is the fact that both the weapon and the target of the attack is the network itself and the information contained on such networks. This feature distinguishes computer network attacks from forms of electronic warfare, which may also seek to destroy a network, but instead use electromagnetic energy, usually in hardwired weapons such as electromagnetic pulse

---

[87] See for example, Anatolij Streltsov, 'Threat Analysis in the Post Cold-War Order' (Paper presented at the International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, Stockholm, 17-19 November 2004) 21-27, 21.

[88] Martin C. Libicki, *What Is Information Warfare?* (Center for Advanced Concepts and Technology, Institute for National Strategic Studies, Washington, DC, 1995). Martin Libicki's original definition of information warfare is generally compatible with the currently accepted definition of Information Operations in that it is an umbrella term which comprises seven subcategories.

[89] U.S. Department of Defence, *Information Operations*, Joint Chiefs of Staff, Joint Publication 3-13 (2006) iii.

(EMP) generators to achieve their aims.[90] A CNA uses computer code to effect its damage and is capable of causing a myriad of effects depending on the target system's function. Although some authors have taken issue with the definition,[91] on the whole it appears that these concerns stem from a narrow interpretation of the concept of 'information' in the context of the definition.[92] Information in terms of computing, is any data that reduces uncertainty in the state of a system. It includes rather more than the traditional definition of facts and knowledge required by human beings to change or form an opinion.[93] Indeed the U.S. military definition of information is "facts, data or instructions in any medium or form".[94] Thus the operating code of a computer, its automated processes and applications, as well as the files and data it contains are all information. Once one grasps this extended definition, the range of possible effects of a computer network attack become greatly expanded.

Computer network attacks may come in isolation, but will more probably be used in conjunction with a conventional attack, either to ease the way for the conventional attack or to amplify its effects. In the battlespace they may be used to disable the advance warning systems of an air defence network allowing an attacker's air force to advance unseen into enemy territory. This happened during Israel's penetration of Syrian air defences on 6 September 2007 in order to bomb a suspected nuclear site at Dayr az-Zawr, without being engaged or even detected.[95] That attack combined

---

[90] Other forms include other uses of the electromagnetic spectrum such as radar, radio, optics (laser and infrared devices), high powered microwaves as well as warning and counter action systems. Techniques include signal interception, passive listening, electronic surveillance, radar and radio traffic deception as well as jamming and electronic interference. Roland Heickerö, 'Electronic Warriors Use Mail Order Equipment' (2005) *Framsyn Magazine* April 2005 <http://www.foi.se/FOI/templates/Page____4554.aspx#> (last accessed 21 September 2007).

[91] See for example, Yoram Dinstein, 'Computer Network Attacks and Self-Defense' in M N Schmitt and B T O'Donnell (eds), *Computer Network Attack and International Law* (Naval War College, Newport, RI, 1999) 99-119, 102.

[92] Multiple conceptions of the term 'information' appear in the literature surrounding the information revolution, see generally: John Arquilla and David Ronfeldt, 'Information, Power and Grand Strategy: In Athena's Camp - Section 1' in J Arquilla and D Ronfeldt (eds), *In Athena's Camp: Preparing for Conflict in the Information Age* (RAND, Santa Monica, 1997) 141-171, 144.

[93] For a full definition see 'Information' *A Dictionary of Computing* (Oxford University Press, Oxford, 2004).

[94] U.S. Department of Defence, *Dictionary of Military and Associated Terms.*

[95] David A. Fulghum, Robert Wall and Amy Butler, 'Israel Shows Electronic Prowess' (2007) *Aviation Week and Space Technology* 25 November 2007 <http://www.aviationweek.com/aw/generic/story_channel.jsp?channel=defense&id=news/aw112607p2.xml&headline=Israel%20Shows%20Electronic%20Prowess> (last accessed 9 May 2008).

electronic attack techniques in the form of brute-force jamming, precision missiles to eliminate the facility itself, and most interestingly for this thesis, computer network attack techniques. The ability of nonstealthy Israeli aircraft to penetrate without interference rests in part on technology, carried on board modified aircraft, that allowed specialists to hack into Syria's networked air defence system.[96] "Network raiders can conduct their invasion from an aircraft into a network and then jump from network to network until they are into the target's communications loop".[97] Israel is not the only State to have developed this technology. The U.S. has developed 'Suter' network-invasion capability which uses the EC-130 electronic attack aircraft to shoot data streams, laced with sophisticated algorithms, into enemy antennas.[98] The U.S. version of the system has at the very least been tested operationally in Iraq and Afghanistan in the last year, most likely against insurgent communication networks.[99]

Alternatively computer network attacks may also be used to switch off or re-divert calls to an emergency response number after a conventional attack causing further damage and destruction as emergency responders are grounded. An attack against a satellite control centre or other mission critical facilities could severely affect a State's war effort, as could intrusion into a system which sends supplies to the frontline. These examples are a few of the more commonly cited, many more are possible.

3.2. New Laws for Old?

The primary assertion of this thesis is that although computer network attacks raise challenging issues for the current laws of armed conflict, for the most part, existing laws are capable of adapting to the new technology. Indeed, the Martens Clause was drafted with exactly this eventuality in mind. Despite some calls for there to be a new convention which addresses the issues raised by computer network attacks and

---

[96] Ibid.

[97] Ibid.

[98] Ibid.

[99] David A. Fulghum and Douglas Barrie, 'Israel Used Electronic Attack in Air Strike against Syrian Mystery Target' (2007) *Aviation Week & Space Technology* 8 October 2007 <http://www.aviationweek.com/aw/generic/story_channel.jsp?channel=defense&id=news/aw100807p2.xml> (last accessed 10 October 2007).

other information operations,[100] the present author feels that this is unnecessary. The general principles of the laws of armed conflict are aimed at ameliorating the essential nature of conflict which remains unchanged. Human life remains the fundamental value to be protected. The St Petersburg Declaration was founded on a common agreement to fix the technical limits at which the necessities of war ought to yield to the requirements of humanity.[101] The Parties were agreed:

> That the progress of civilization should have the effect of alleviating as much as possible the calamities of war;
> That the only legitimate object which States should endeavour to accomplish during war is to weaken the military forces of the enemy;

Those who call for a new convention generally subscribe to the idea that cyberspace represents a fundamentally different conceptual space in which to fight. However, their approach, illustrated by Brown's assertion that "Cyberspace is nowhere" is simply not reflective of state practice in relation to other areas of Internet law. There does not exist some 'matrix-like' realm of cyberspace which bears no connection to the 'real-world'. Actors still act in physical space, hardware and networks (even wireless and virtual ones) still require physical constructs. However, that is not to argue that computer network attacks fit neatly into the humanitarian law paradigm that has developed over the last century. But it is not the advent of cyberspace, *per se*, that is the problem.

As described above, the information revolution has transformed society fundamentally and on multiple levels. Where the cultural and societal ground shifts, the underlying concepts on which our laws are based may also change; for example, the attributes of physical property that have bound predecessors to the tangible world in their formulations and interpretations of law. Laws, like wars, reflect the principles and values of the societies which draft them. Georges Abi-Saab has commented that the 'requirements of humanity' are subjective, depending on the dominant moral ideas and degree of community feeling obtained among the main

---

[100] See for example, Davis Brown, 'A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict' (2006) 47 *Harv Int'l LJ* 179; Duncan B. Hollis, 'Why States Need an International Law for Information Operations' (2007) 11(4) *Lewis & Clark L Rev* 1023.

[101] *St Petersburg Declaration.*

contenders in society.[102] Those principles can be altered by something as momentous as the information revolution, to the point where conceptions of value are fundamentally changed. Thus, when reviewing the general principles of the laws of armed conflict, this shift in values must be taken into account and the reasoning behind the statements of principle explored. In addition, some of the specific laws which relate to particular means and methods of warfare may need reinterpretation as discussed *infra*.

It must also be borne in mind that while the move toward high-tech warfare in developed nations is on the increase, warfare in many States remains for the most part brutal, physical and violently immediate. It can be easy to lose track of the purpose of these laws when one is dealing with the abstract world of bits and bytes and when targeting can be set up from the safety of an office block half a world away from the battle space. It is imperative that any attempt to interpret the laws of armed conflict to apply to computer network attack, must remain applicable to the traditional forms of kinetic violence for which they were first envisaged.

3.3. Methodology

It may be clear from the forgoing that this thesis utilises many of the tools of modern positivism,[103] however as whole, the author has adopted a hybrid approach to international law as it applies to computer network attack. Throughout this thesis the author has attempted to delineate carefully between *lex lata* and *lex ferenda*. However where the technology does not fit easily with existing law, a closer examination of the general principles is required. As Judge Higgins (as she then was) points out in her dissenting opinion in the *Nuclear Weapons* case:[104]

> Humanitarian law is very well developed. The fact that its principles are broadly stated and often raise further questions that require a response can be no ground for a *non liquet*. It is exactly the judicial function to take principles of general application, to elaborate their meaning and to apply them to specific situations".

---

[102] Abi-Saab, 'Specificities', 265.

[103] For an exposition of modern positivism see the American Journal of International Law *Symposium on Method in International Law* article by Bruno Simma and Andreas L. Paulus, 'The Responsibility of Individuals for Human Rights Abuses in Internal Conflicts: A Positivist View' (1999) 93 *AJIL* 302.

[104] *Legality of the Threat and Use of Nuclear Weapons* (1996) ICJ 226, International Court of Justice, (dissenting opinion of Judge Higgins), para 32.

It is this approach that the thesis adopts when discussing the application of the general principles of humanitarian law to computer network attacks - reasoned development of authoritative starting points consistent with the object and purpose of the law of armed conflict. The author subscribes to the view that principles based on values, such as 'the dictates of humanity', are necessarily subjective and will change over time in accordance with the prevailing view of the societies from which they come,[105] but these general principles are already incorporated into the laws of armed conflict either through treaty obligations or as prescriptions of customary international law.

Humanitarian law represents a carefully constructed balance between military necessity on the one hand and humanitarian principles on the other. To introduce a further level of humanitarian or sociological interpretation to principles of which States and more importantly, individuals, may be held in violation, is disingenuous to the carefully negotiated drafting process which will often rely on minimal consensus and may deliberately ignore the underlying interpretive or conceptual debates in order to achieve a measure of protection. Further, as Judge Cassese has commented: "[A] policy-oriented approach in the area of criminal law runs contrary to the fundamental customary principle *nullum crimen sine lege*".[106]

On the other hand, where this thesis finds the law lacking in detail, or references *lex ferenda*, a more policy-oriented approach is called for. However it is the guiding principles of the laws of armed conflict which are to be referenced; that is, those principles which form the basis of, and are incorporated into, humanitarian law instruments, such as those prohibiting unnecessary suffering, distinction between civilian and military targets or requiring proportionality. These general principles of humanitarian law are aimed at the unchanging nature of war itself. While we have specific laws, most obviously certain of the Hague Regulations and subsequent weapons conventions, which are aimed at the specific character of war (the technologies employed and the strategies involved), taken back to first principles and conscious of the reasons for which they were adopted, the general principles of the laws of armed conflict will apply regardless of the technology utilised.

---

[105] Abi-Saab, 'Specificities', 265.

[106] *Prosecutor v Drazen Erdemovic* (1997) IT-96-22-A, International Criminal Tribuanl for the Former Yugoslavia, Appeals Chamber, (separate & dissenting judgement of President Cassesse), para 11.

3.4. A Word About Examples & Hypotheticals

This thesis deals with a method of warfare which is still in its infancy. Further, most computer network attack tools remain classified in order to protect their usefulness. If the details are known by the adversary, they may be guarded against, thus making the tool ineffective.

Throughout this thesis, examples have been taken from domestic and peacetime computer network attacks and incursions to illustrate points. The aim is not to use them for their precedent value in any direct application to international humanitarian law, an approach which would obviously be incorrect, but rather to act as practical, real-world illustrations of the types of attacks and incursions which are currently taking place. Further, they serve as an indicator, where possible, of the current state of legal analysis of the concepts underlying computer network attacks and digital property.

The present author does not have security clearance and all examples used are those gleaned from publicly available sources and domestic instances of computer network attacks which indicate how such an attack could work if carried out by a party during an armed conflict. Although the facts of each example are provided in the text, a timeline and summary of each attack with its significance for the development of the technology is provided in Appendix 1 for the convenience of the reader. Where hypothetical examples are used, they have been checked with computer engineers and network specialists for their general viability. In so far as is possible without compromising security, the details of specific hypothetical attacks have been checked with those with first hand knowledge of the supposed target. The author is grateful for their kind assistance with these matters, and the fault for any errors remains entirely with the author.

It will also be apparent that this thesis is fairly U.S. centric in its use of examples. This is for the simple reason that the United States has the most publicly available English language information and analysis of this field; where possible the author has attempted to include examples from other jurisdictions.

4. Conclusion

There are several main themes running through this thesis which have been set out and explained in this introductory chapter. By way of summary, they are repeated

here. First, despite the advent of new technology, the essential nature of armed conflict remains the same - it is the advancement of political objectives by organised violence.[107] Secondly, the style and character of warfare reflects the society which wages it. And finally, the underlying principles of the laws of armed conflict are aimed at the fundamental nature of war. The exact content and contours of these principles are determined by the prevailing values of the society affected. Thus, computer network attacks are a product of, and are the greatest threat to, those societies which place a high value on information.

When research for this thesis began there was no comprehensive analysis of the laws of armed conflict as they related to computer network attack. Although some attempts had been made at uncovering the law which might apply, the studies were more descriptive than analytical.[108] During the course of writing, computer network attack has become a fashionable topic of debate and numerous articles have been written on how computer network attacks will be governed under discrete areas of the law of armed conflict. Most suffer broadly from one of two faults; those that understand the technology involved have tended to focus on the new aspects of the technology to the detriment of the general principles underlying the law. Secondly, those that are specialists in the law do not necessarily understand the nuances of the technology being utilised. In addition, with the notable exception of a series of articles written by Michael Schmitt, none offer a systematic analysis based on a complete underlying framework. This thesis aims to fill that gap.
Despite adopting a comprehensive approach, a few ommisions have had to be made in the interests of length. This thesis does not examine the laws of neutrality, nor does it look in any detail at the implications of computer network attack for naval warfare or as an internationally wrongful act short of a use of force.

---

[107] Carl von Clausewitz, J. J. Graham and F. N. Maude, *On War* (new and rev. ed, Kegan Paul, Trench, Trubner & Co., London, 1940); Gray, *Another Bloody Century*.

[108] See Walter G. Sharp, *Cyberspace and the Use of Force* (Aegis Research Corp., Falls Church, VA., 1999); Thomas C. Wingfield, *The Law of Information Conflict: National Security Law in Cyberspace* (Aegis Research Corp., Falls Church, VA, 2000).

PART 1

Jus ad Bellum

Chapter 2 - Computer Network Attacks as a Use of Force in International Law

In May 2007, Estonia became the victim of a prolonged series of denial of service attacks which brought the banking system, many government services and much of the media to a halt.[1] Although no critical infrastructure was compromised, for a highly technology dependent State like Estonia that depends on the Internet for everything from parking to banking to voting, the attacks caused serious disruption and caused an estimated tens of millions of euros worth of damage.[2] Despite earlier explicit accusations that Russia was behind the offensive, the Estonian government backed away from directly accusing the Kremlin of launching the attacks,[3] but requested assistance from its NATO allies under the terms of that alliance. Although no official statement regarding the cyber attacks was released by NATO, one of the clearest indications of State views on computer network attacks came from Estonian defence minister Jaak Aaviksoo who raised the matter with NATO:[4]

> "At present, NATO does not define cyber-attacks as a clear military action. This means that the provisions of Article V of the North Atlantic Treaty, or, in other words collective self-defence, will not automatically be extended to the attacked country... Not a single NATO defence minister would define a cyber-attack as a clear military action at present. However this matter needs to be resolved in the near future"

---

[1] A Distributed Denial of Service attack (DDoS) uses many compromised computers to flood a target system with requests for information until it collapses under the strain. The compromised computers are usually ones that have been recruited to a botnet (usually without their owner's knowledge) and are controlled by a master computer.

[2] Ian Traynor, 'Web Attackers Used a Million Computers, Says Estonia', *The Guardian* (London), 18 May 2007, International 30.

[3] Ibid. Russia categorically denies any involvement and no concrete evidence has been found to substantiate those claims. While technical data shows that some of the attacks came from IP addresses allocated to the Russian Government, there is no evidence that these computers were involved in initiating the attacks, or that they had not been compromised or spoofed.

[4] Ian Traynor, 'Russia Accused of Unleashing Cyberwar to Disable Estonia', *The Guardian* (London), 17 May 2007, Home 1 <www.guardian.co.uk/print/0,,329864981-103610,00.html> (last accessed 20 August 2007).

This attitude is perhaps not surprising given the general reluctance of States to consider acts of indirect aggression as armed attacks,[5] however the incident is significant in that it represents the first time one State has accused another of intentionally launching a computer network attack against it. The incident has bought to the fore important issues for the law regulating the use of force in international relations. While controversies surrounding the rule prohibiting the use of force have mainly focused on issues such as the conditions for self defence or the existence of a right to humanitarian intervention,[6] the advent of computer network attacks has renewed a far more fundamental question: what is the meaning of 'force' in the twenty-first century?

The prohibition of the use of force is one of the cornerstones of international law and is expressed in Article 2(4) of the UN Charter. However, the prohibition is not restricted to the Charter; it represents "not only a principle of customary international law but also a fundamental or cardinal principle of such law".[7] In the *Wall* case the International Court of Justice relied on the *Nicaragua (Merits)* case to affirm that "the principles as to the use of force incorporated in the Charter reflect customary international law".[8] It is also important to note that the threat or use of force is abolished in Article 2(4) only in the 'international relations' of Member States; intrastate clashes therefore are out of reach of the Charter's provision.[9]

---

[5] See generally, Chapter 3 *infra.*

[6] Olivier Corten, 'The Controversies over the Customary Prohibition on the Use of Force: A Methodological Debate' (2005) 16 *EJIL* 803.

[7] *Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America) (Merits)* (1986) ICJ 14, International Court of Justice, para 190. The International Court of Justice also recalled that the ILC had considered this provision to have the character of jus cogens.

[8] *Legal Consequences of the Construction of a Wall in Occupied Palestinian Territory* (2004) ICJ 136, International Court of Justice, para 87.

[9] Yoram Dinstein, *War, Aggression, and Self-Defense* (3rd ed, Cambridge University Press, New York, 2001), 85.

1. Force Defined as Armed Force

The prohibition of the use of force is a cornerstone of the United Nations Charter.[10] Article 2(4) states:

> All members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations.

However the Article, and the exact meaning of the word 'force', has been a source of debate since its enactment. The drafters of the Charter did not define the term, nor has the International Court of Justice or the General Assembly done so since. The debate has centred on whether 'force' is limited to armed force, or includes other forms of coercion such as political and economic measures. The issue of inclusion of political and economic coercion as uses of force prohibited by Article 2(4) of the Charter has been raised repeatedly, particularly by developing and former Eastern Bloc countries, since the San Francisco conference.[11] Although no definitive conclusions have been drawn, the prevailing and commonly accepted view put forward by scholars is that the force referred to in Article 2(4) is limited to armed force.[12] As computer network attacks can result in a myriad of outcomes, the contours of the prohibition must be fleshed out in order to ascertain when attacks will be proscribed under Article 2(4) and the corresponding customary law relating to the use of force in international law. The following discussion looks at the arguments from a textual analysis of the Charter wording, *travaux préparatoires*, historical background and academic analysis.[13]

---

[10] *Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)* (2005), International Court of Justice, para 148.

[11] Albrecht Randelzhofer, 'Article 2(4)' in B Simma (ed) *The Charter of the United Nations: A Commentary* (2nd ed, Oxford University Press, Oxford, 2002), 118.

[12] See for example, Dinstein, *War, Aggression, and Self-Defense*, 86; Randelzhofer, 'Article 2(4)', 117.

[13] Art. 31 of the Vienna Convention on the Law of Treaties 1969 sets out the core interpretative principles that a treaty should be interpreted in "good faith" and in accordance with "the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose". Interpreters of a treaty may include in the context: the preamble, any treaty or instrument made in connexion with the treaty, subsequent conduct and practice of the parties and any relevant rules of international law applicable in the relations between the parties. Art. 32 states that recourse may be made to supplementary means of interpretation, including the preparatory work of the treaty and the circumstances of its conclusion. The following sections consider each of these in turn.

1.1. The Charter Wording

The text of the United Nations Charter refers to force as an unqualified term twice in the entirety of the document, in Article 2(4) and Article 44. The use of the term in Article 44 appears in the context of Chapter VII, and supports a restrictive definition of 'force' by placing it in close conjunction with the qualified term 'armed force', clearly suggesting that the force contemplated by the unqualified term is armed. Article 44 states:

> When the Security Council has decided to use force it shall, before calling upon a Member not represented on it to provide armed forces in fulfilment of the obligations assumed under Article 43, invite that Member, if the Member so desires, to participate in the decisions of the Security Council concerning the employment of contingents of that Member's armed forces.

The decision to use force refers to the preceding Articles 41 and 42 of the Charter, which permit the Security Council to authorise actions necessary to maintain or restore international peace and security, including the use of force. Article 41 relates to measures not involving the use of "armed force" which may include "complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations".[14] Article 42 allows the Security Council to "take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security" and is the article under which the Security Council mandates the use of armed force in international law under the phrase 'all necessary means'.[15] Thus the use of the termed 'armed force' in Article 41, suggests that the force referred to in Article 44 and hence in Article 2(4) is also armed force.

Further support for this view can be found in paragraph seven of the preamble of the Charter which states that "armed force shall not be used, save in the common interest". Michael Schmitt points out that the articles of the Charter are designed to

---

[14] Note that this would tend to indicate that none of these measures would be considered breaches of Article 2(4) were they to be taken unilaterally by individual States, whether they were effected by computer network attacks or by more conventional means.

[15] The list of actions includes "demonstrations, blockade, and other operations by air, sea, or land forces".

give effect to its preambular aspirations.[16] Accordingly, if Article 2(4) were intended to extend beyond armed force, then presumably the preamble, for reasons of internal consistency would not have included the term 'armed'. This paragraph accords with the relationship apparent between Article 2(4) and Chapter VII of the Charter, in particular Article 42 relating to Security Council authorisation of armed force, as discussed above.

Albrecht Randelzhofer has also put forward a teleological interpretation of the Article wording. Randelzhofer argues that were Article 2(4) to extend to other forms of force, such as economic and political coercion, States would be left with no legal means of exerting pressure on States that violate international law.[17] Such a consequence would be unacceptable to the international community in an age where the organs of that community are unable to effectively ensure compliance with international law.

1.2. *Travaux Préparatoires* and Historical Background

The preparatory materials of the Charter do not contain any specific discussion regarding the precise meaning of the term force. However, the *travaux préparatoires* of Article 2(4) detail a proposal by the foreign minister of Brazil to specifically extend the prohibition to the threat or use of 'economic measures' which was rejected.[18] Although Randelzhofer has cited this as evidence that military force is the only intended concern of the prohibition, David Harris states that it is unclear from the texts whether the rejection of the Brazilian amendment is proof that the Article was not intended to prohibit economic force, or that the term force in Article 2(4) was thought sufficient to cover it without specific mention.[19] The latter view appears to stem from the Belgian delegate's comments regarding Brazil's proposed amendment and the phrase 'or any other manner'.[20] Despite this, writers have

---

[16] Michael N. Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework' (1999) 37 *Col J Trans L* 885, 904.

[17] Randelzhofer, 'Article 2(4)', 118.

[18] "Summary Report of Eleventh Meeting of Committee I/1" Doc. 215, I/1/10, 6 UNCIO (6 May 1945) 334, 559 (rejected by 2 votes in favour, 26 against).

[19] D. J. Harris, *Cases and Materials on International Law* (6th ed, Sweet & Maxwell, London, 2004), 890.

[20] The Belgian delegate suggested that the delegate of Brazil had underestimated the effect of the modifications made in the original text, calling attention particularly to the phrase "in any other

generally concluded that the better view is that Western States were not prepared to admit anything other than armed force.[21] While third world States have tried to raise the issue of prohibiting use of economic and political coercion on other occasions, each time it has received a negative vote from Western powers.

It also is interesting to note the discussion following from a proposed amendment to Article 2(4) that required members collectively to resist the use of aggression against Member States.[22] One of the main objections to the amendment was the lack of definition of the term aggression, which resulted in the following comment from the United Kingdom representative when discussing the issue:[23]

> "Apart however from the difficulty in defining aggression and therefore of knowing what the nations were pledged to resist, the use as a standard of an inexplicit word, such as aggression, instead of something explicit such as 'force' would give an opportunity to a state to engage in an act of aggression while calling it by another name"

It is apparent from this statement that the term force was considered an explicit term. As Bond has pointed out, such a characterisation of the term at that time was not questionable; it was clear that force meant military or armed force, and in 1945 that meant traditional weapons employed in traditional ways.[24] Further, in the same discussion a representative of the United States pointed out that in the future there would be many kinds of aggression and that these would be covered in the Charter

---

manner"; and also recalled that the subcommittee had given the point about "economic measures" careful consideration and for good reasons decided against: "Summary Report of Eleventh Meeting of Committee I/1"Doc. 784, I/1/27, 5 June 1945, 6 UNCIO (1945) 334.

[21] However the Western States were prepared to admit, as stated by the UK representative that "that was not to say that all forms of economic and political pressure which threatened the territorial integrity and political independence of another state were permissible, they might well constitute illegal intervention".

[22] "Summary Report of Twelveth Meeting of Committee I/1" Doc. 810, I/1/30, 6 UNCIO (6 June 1945) 342. The New Zealand amendment reads as follows: "All members of the Organisation undertake collectively to resist every act of aggression against any member". The amendment was rejected by a vote of 26 in favour and 18 against, for failing to receive a two-thirds majority.

[23] "Addendum to Summary Report of Twelveth Meeting of Committee I/1" Doc. 866, I/1/30(a), 8 June 1945, 6 UNCIO (1945) 356.

[24] James Bond, *Peacetime Foreign Data Manipulation as One Aspect of Offensive Information Warfare: Questions of Legality under the United Nations Charter Article 2(4)*, Naval War College (1996) 57 <http://handle.dtic.mil/100.2/ADA310926> (last accessed 18 September 2007). It should also be noted that these discussions took place prior to the atomic bombing of Hiroshima and Nagasaki.

by the words "threat to the peace".[25] This indicates that at the time the discussions surrounding Article 2(4) and its proposed amendments were taking place, the perception of force was as a specific (armed) threat and all other incidents which would require flexibility of drafting would be covered by the more general phrase 'threat to the peace'.

The historical background to the Charter also illustrates its development against a background of international efforts to eliminate unilateral recourse to armed force, and provides some insight into the intentions of the drafters of Article 2(4).[26] Edward Gordon has argued that the problems of interpretation of Article 2(4) arise because it is a "legal rule located in the text of a multilateral treaty which requires adaptation to changing circumstances".[27] As Gordon points out, the challenge becomes one of remaining faithful to its core meaning without thereby sacrificing the flexibility required in interpreting constitution norms. The historical antecedents of Article 2(4) are the Covenant of the League of Nations and the Kellogg-Briand Pact. The former (as amended), states that 'any war or threat of war' is a matter of concern for the whole League,[28] and that members of the League will preserve the 'territorial integrity and existing political independence' of members of the League against external aggression.[29] The genetic roots of the present Article 2(4) are clearly visible in the wording. In the years between the adoption of the Covenant of the League of Nations and the adoption of the Kellogg-Briand Pact in 1928, the League Assembly passed unanimous resolutions condemning wars of aggression as international

---

[25] "Summary Report of Twelveth Meeting of Committee I/1" Doc. 810, I/1/30, 6 UNCIO (6 June 1945) 344.

[26] See generally, Edward Gordon, 'Article 2(4) in Historical Context' (1985) 10 *Yale J Int'l L* 271.

[27] Ibid., 273.

[28] Art. 11, Covenant of the League of Nations reads as follows:

> Any war or threat of war, whether immediately affecting any of the Members of the League or not, is hereby declared a matter of concern to the whole League, and the League shall take any action that may be deemed wise and effectual to safeguard the peace of nations. In case any such emergency should arise the Secretary General shall on the request of any Member of the League forthwith summon a meeting of the Council.

[29] Art. 10, Covenant of the League of Nations reads as follows:

> The Members of the League undertake to respect and preserve as against external aggression the territorial integrity and existing political independence of all Members of the League. In case of any such aggression or in case of any threat or danger of such aggression the Council shall advise upon the means by which this obligation shall be fulfilled.

crimes. Indeed, the Pan American conference in 1926 considered such wars to be crimes against the human species.[30]

Under the 1928 Kellogg-Briand Pact States parties "condemn the recourse to war for the solution of international controversies, and renounce it as an instrument of national policy in their relations with one another".[31] However the precise scope of the prohibition on war contained in the treaty has never been whether the treaty prohibits armed force short of war as well as war.[32] Professor Ian Brownlie suggests that the best guide to the meaning of the Pact is to be found in the subsequent actions of the contracting parties.[33] He concludes that there leaves little room for doubt that it was understood to prohibit 'any substantial use of armed force'.[34]

1.3. Subsequent Iterations of the Rule

As can be seen from the foregoing, the rules of the Charter relating to force are brief and cannot constitute a complete code,[35] a fact acknowledged by the International Court of Justice in the *Nicaragua (Merits)* case.[36] Almost from the time that the Charter was drafted, States have tried to elaborate the prohibition on the use of force in General Assembly resolutions to provide greater clarity. However, each of the attempts has left the central issue of the essential nature of 'force' unresolved. It appears that the ambiguity of the wording has been the price of international consensus.[37]

Two other international instruments drafted around the time of the United Nations Charter, the Charter of the Organisation of American States (OAS) and the North

---

[30] W Bishop Jr *International Law: Cases and Materials 1010* (3ed) (1971), cited in Gordon, 'Article 2(4) in Historical Context', 274.

[31] Art. 1, General Treaty for the Renunciation of War 1928, UKTS 29 (1929), *Cmnd, 3410; 94 LNTS 57.*

[32] Harris, *Cases & Materials*, 861.

[33] Ian Brownlie, *International Law and the Use of Force by States* (Oxford University Press, Oxford, 1963), 87.

[34] Ibid. *Cf.* D. W. Bowett, *Self-Defence in International Law* (University of Manchester Press, Manchester, 1958), 136.

[35] Christine D. Gray, *International Law and the Use of Force* (2nd ed, Oxford University Press, Oxford, 2004), 6.

[36] The Court stated that the UN Charter by no means covers the whole area of the regulation of force in international relations. *Nicaragua (Merits)*, para 176.

[37] Gray, *Use of Force*, 8.

Atlantic Treaty (forming NATO) also use the term force without qualification. Perhaps unsurprisingly given their status as collective defence organisations, neither provides any support for the inclusion of economic or political coercion as force. The North Atlantic Treaty uses the terminology of the UN Charter and although Article 2 separately addresses economic concerns it does not refer to economic coercion.[38] The Charter of the OAS (as subsequently amended) refers to the prohibition on use of force in other treaties in Article 22, however force is used as an unqualified term and no guidance is given as to its meaning.[39] However, when discussing such measures for the purposes of its own obligations, Articles 19 and 20 of the OAS Charter avoid using the term force without qualification by using 'armed force' and 'coercive measures of an economic or political character' as separate terms. Michael Schmitt notes that this is perhaps unsurprising given Brazil's attempt at amending Article 2(4) of the U.N. Charter and their membership of the OAS.[40] It is clear that the language employed by the OAS Charter is meant to be interpreted far more broadly that the "use of force" language of Article 2(4). However, as a number of commentators have pointed out, the language is so broad as to be legally unenforceable;[41] if read literally, it outlaws diplomacy.[42]

The issue was addressed again 25 years later in the 1970 General Assembly Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations (hereinafter Declaration on Friendly Relations).[43] The section on the principle of the

---

[38] Art. 2 states that the parties "will seek to eliminate conflict in their international economic policies and will encourage economic collaboration between any or all of them" 4 April 1949, *North Atlantic Treaty,* 34 UNTS 243 (entered into force 24 August 1949).

[39] Art. 22 states that "The American States bind themselves in their international relations not to have recourse to the use of force, except in the case of self defense in accordance with existing treaties or in fulfilment thereof" 30 April 1948, *Charter of the Organisation of American States,* 119 UNTS 3 TIAS No 2361.

[40] Schmitt, 'Normative Framework', 906. citing *OAS Charter.*

[41] Richard W Aldrich, 'How Do You Know You Are at War in the Information Age?' (2000) 22 *Hous J Int'l L* 223, 254. Nicaragua attempted unsuccessfully to rely on this broad language in its case against the United States; however the Court found that it had no jurisdiction to consider either the U.N. Charter wording or articles of the OAS Charter.

[42] Tom Farer, 'Political and Economic Aggression in Contemporary International Law' in A Cassese (ed) *The Current Legal Regulation of the Use of Force* (Martinus Nijhoff, Dordrecht, 1986) 121-132, 121. Threats, more or less subtle, have always been an important feature of the intercourse of States.

[43] *Declaration on Principles of International Law Concerning Friendly Relations and Co-Operation among States in Accordance with the Charter of the United Nations, GA Res. 2625 (XXV)* UN GAOR Supp., 25, 18 122, UN Doc. (1970).

use of force does not clarify the matter as it merely refers to 'force'. This was the result of disagreement between the Western States, who argued that the prohibition only related to armed force, and the Soviet Bloc, European and developing States who argued that "all forms of pressure, including those of a political and economic character, which have the effect of threatening the territorial integrity or political independence of any state" were prohibited.[44] However the Western States were prepared to admit, presciently in the light of the Arab oil boycott of 1973 and 1974, that "that was not to say that all forms of economic and political pressure which threatened the territorial integrity and political independence of another state were permissible; they might well constitute illegal intervention".[45] The Declaration deals separately with political and economic coercion under the heading of the 'Principle not to Intervene', thus indicating that as far as the Declaration is concerned, force is restricted to armed coercion, and that forms of political and economic coercion were to be considered intervention.

The International Court of Justice in the *Nicaragua (Merits)* case held that the Declaration was indicative of the *opinio juris* of the international community, and showed the customary nature of the prohibition as stated in Article 2(4) of the Charter.[46] Although the judgement does not directly address the question of the status of economic or political coercion under the use of force doctrine, the Court does not include such measures in citing the acts which may be considered 'less grave' forms of the use of force. The Court quotes from the sections of the Declaration dealing specifically with the principle of the non-use of force, but also from the principle of non-intervention. In citing the latter, the Court leaves out the opening sentence of the paragraph dealing with political and economic coercion, and only quotes the second sentence relating to armed groups.[47] This is despite Nicaragua's submissions that the country had been subjected to economic coercion at the hands of the United States.[48] This omission and the failure of the Court to

---

[44] UN Doc. A/AC.125/SR.114 (1970) cited in Harris, *Cases & Materials*, 863.

[45] UK representative (Mr Sinclair), UN Doc A/AC125/SR25 (1966), cited in Ibid., 863-864.

[46] *Nicaragua (Merits)*, para 188.

[47] Ibid., para 192.

[48] It should be noted however that Nicaragua did not attempt to argue that the economic coercion involved was sufficient to count as the threat or use of force. Although the Court stated later in the judgement that it would not rule on legal arguments not put forward by the parties (in relation to the prohibition against intervention), the fact that the submission was not even mentioned is significant.

consider Nicaragua's submissions in that regard when discussing Article 2(4) and the associated customary law, indicates that the Court does not include such measures in the definition of force as used in customary international law and the U.N. Charter.[49] Since the *Nicaragua (Merits)* case, the international community has once again affirmed the prohibition against force in the 1987 Declaration on the Non-Use of Force.[50] As with previous General Assembly resolutions, the Declaration separates the concepts of armed intervention and economic and political coercion, however it leaves the main controversies between developed and developing States unsettled.[51]

2. Definition of Armed Force

The international jurisprudence indicates that while the definition of force is to be limited to armed force, the definition of armed force itself is to be interpreted widely. In particular, a direct application of armed force by a State is not necessary for the State to fall foul of Article 2(4), nor have States been able to successfully circumvent the prohibition by arguing that an incident does not affect the territorial integrity or political independence of a State.

The latter argument was raised by the United Kingdom in the *Corfu Channel Case*,[52] however the International Court of Justice dismissed such a narrow interpretation of force by holding that the British action of sending warships to clear mines from the Corfu Channel against the express wishes of Albania amounted to a 'policy of force' such as had given rise to "most serious abuses and such as cannot... find a place in international law".[53] The British claimed that their actions were not in breach of Article 2(4) as they were not directed against the territorial integrity or political independence of Albania.[54] Interestingly, despite this argument being dismissed by

---

[49] It should be noted that the definition of force as used in Art. 2(4) of the Charter was not at issue in the case as the United States has a non-binding clause to multi-lateral treaties.

[50] Arts. 7 & 8, *Declaration on the Enhancement of the Effectiveness of the Principle of Refraining from the Threat or Use of Force in International Relations* GAOR 42nd sess, 73rd plen mtg, UN Doc. A/Res/42/22 (1987).

[51] The remaining differences between developed and developing States are summarised at A/40/41: Gray, *Use of Force*, 9.

[52] *Corfu Channel Case (U.K. v Albania) (Merits)* (1949) ICJ Reports 4, International Court of Justice, 13.

[53] Ibid., 35.

[54] The U.K. were attempting to collect the mines as evidence of Albania's mining operation and classified 'Operation Retail' as an act of self-help. Ibid.

the Court in the *Corfu Channel Case*, Belgium raised the same argument in its pleadings on provisional measures following the NATO intervention in Kosovo in 1999.[55]

The International Court of Justice's broad interpretation of the scope of the term force can also be seen in the *Nicaragua (Merits)* case where the Court clarifies that some indirect forms of support *are* included in the prohibition against force. The Court's judgement affirmed that acts which breach the principle of non-intervention "will also, if they directly or indirectly involve the use of force, constitute a breach of the principle of non-use of force in international relations".[56] In that case, the Court accepted that the provision of assistance to rebel fighters "in the form of the provision of weapons or logistical or other support" could constitute a threat or use of force, or amount to intervention in the internal or external affairs of a State.[57] However not all forms of indirect action, or assistance were to be so considered. In particular, the Court found that "the mere supply of funds to the contras, while undoubtedly an act of intervention in the internal affairs of Nicaragua", would not breach the prohibition of force as contemplated by Article 2(4) and the corresponding customary law.[58] In a controversial discussion, the Court distinguishes between the gravest forms of the use of force, those that constitute an armed attack or aggression, and other uses of force, referred to by the Court as "less grave forms".[59] The Court used the Declaration on Friendly Relations to elucidate these lesser forms of force and determine the legal rules that may apply to them.[60] In particular, the Court emphasised the following paragraphs of the Declaration:

---

[55] Belgium's Oral Arguments *Legality of Use of Force (Yugoslavia v. Belgium) (Request for Provisional Measures)*, CR99/15, 12, stating that NATO has never questioned the political independence and territorial integrity of the Federal Republic of Yugoslavia and claiming that Article 2(4) covers only intervention against political independence and the territorial integrity of a State. The Court did not address these arguments and refused provisional measures on the basis that it lacked prima facie jurisdiction on the merits of the case.

[56] *Nicaragua (Merits)*, para 209.

[57] Ibid., para 193.

[58] Ibid., para 228.

[59] Ibid., para 191. Much criticism has been directed at the *Nicaragua (Merits)* decision based on this elucidation of various levels of force, particularly from American authors. See for example the panel discussion reported at American Society of International Law, 'The Jurisprudence of the Court in the Nicaragua Decision' (1987) 81 *ASIL Proc* 258.

[60] *Nicaragua (Merits)*, para 191.

> Every State has the duty to refrain from the threat or use of force to violate the existing international boundaries of another State or as a means of solving international disputes, including territorial disputes and problems concerning frontiers of States.
>
> .....
>
> Every State has the duty to refrain from any forcible action which deprives peoples referred to in the elaboration of the principle of equal rights and self-determination of that right to self-determination and freedom and independence.
>
> Every State has the duty to refrain from organizing or encouraging the organization of irregular forces or armed bands, including mercenaries, for incursion into the territory of another State.
>
> Every State has the duty to refrain from organizing, instigating, assisting or participating in acts of civil strife or terrorist acts in another State or acquiescing in organized activities within its territory directed towards the commission of such acts, when the acts referred to in the present paragraph involve a threat or use of force.
>
> States have a duty to refrain from acts of reprisal involving the use of force.

There are two points that may be taken from this extract.[61] First, the Court considers that the Declaration codifies the international community's *opinio juris* that certain acts of indirect aggression are capable of being a use of force prohibited by international law, albeit a lesser form.[62] This is significant as many of the arguments raised against computer network attacks being considered a use of force relate to the fact that the results of a computer network attack are often indirect.[63]

---

[61] Again the Court's approach in using the Declaration has been controversial. Some authors argue that the Court has used the Declaration as a source of law, a position which the States Parties to the resolution would never have intended. Authors have also criticised the Court for using the text of the Declaration as indicative of *opinio juris* of the international community without also fully examining the actions of States: see generally, American Society of International Law, 'The Jurisprudence of the Court in the Nicaragua Decision'.But *cf.* Lori Fisler Damrosch, 'Politics across Borders: Nonintervention and Nonforcible Influence over Domestic Affairs' (1989) 83 *AJIL* 1, 8.

[62] This is in accord with the drafting history of Article 3g of the Definition of Aggression which rejected a proposal to include several of the broad range of activities listed as indirect aggression in the Declaration on Friendly Relations. See Pierluigi L. Zanardi, 'Indirect Military Aggression' in A Cassese (ed) *The Current Legal Regulation on the Use of Force* (Martinus Nijhoff, Dordrecht, 1986) 111-119, 116.

[63] The indirectness of computer network attacks is addressed in section 3.1.1 *infra.*

Secondly, the Court included intangible assistance such as 'encouragement'. While it is reading too much into the judgement to treat this as evidence of a prohibition against intangible force, the words "armed intervention and all other forms of interference" imply intent to reach at least some kinds of nonforcible activities. The reports of the special committee delegated the task of drafting the Declaration on Friendly Relations indicate that the participating States had little shared notion of what sort of non-forcible conduct would fall under the proscriptions in the Declaration.[64]

Although 'encouragement' may take many forms, some tangible and some not, the inclusion of 'organisation or encouragement' would suggest that an intangible form was envisaged as well. It is interesting in this regard to compare the Court's treatment of the encouraging statements made by the Ayatollah Khomeini in the *Tehran Hostages* case.[65] Although the case did not consider the Declaration on Friendly Relations, the Court considered that such statements were not sufficient to impute state responsibility for the initial actions of student militants in overrunning the U.S. Embassy in Tehran. However, the Court did hold that such statements were sufficient to turn the continued occupation of the embassy and detention of the hostages into acts of the State. The Court did not consider whether the continuing occupation (or the initial attack)[66] constituted a breach of Article 2(4) of the Charter which had been argued by the United States and dealt with the matter solely with respect to the Vienna Convention on Diplomatic Immunity.

While some commentators have argued that the *Nicaragua (Merits)* case extends the definition of force into things that begin to resemble economic and political coercion, the current author considers that the better view is that force is still restricted to military (or paramilitary) action, however such force may be imputed

---

[64] Damrosch, 'Politics across Borders', 10.

[65] *Case Concerning the United States Diplomatic and Consular Staff in Tehran (United States v Iran)* (1980) 74 AJIL 746, International Court of Justice, para 59. In that case the Ayatollah had made several public declarations inveighing against the United States and holding the U.S. responsible for the trouble besetting that country. On 1 November the Ayatollah had made a statement declaring it was "up to the dear pupils, students and theological students to expand with all their might their attacks against the United States and Israel, so that they may force the United States to return the deposed and Criminal Shah, and to condemn this great plot". Further, congratulatory statements from the Ayatollah following the attack and other statements of official approval were also made.

[66] Presumably because of the lack of imputability to a State party.

through indirect means such as agency. The extension provided by the Court remains tied to armed force, whether in person or by proxy.

The Court in the *Nicaragua (Merits)* case regarded the Charter provisions as dynamic rather than fixed, and thus as capable of change over time through state practice.[67] Although the Court accepted the parties' position that the Charter provisions represented customary law, it also accepted the possibility of the development of new law on forcible intervention allowing a new exception to the prohibition on the use of force in Article 2(4). In setting out the area covered by the prohibition against force the Court stated that Article 2(4) of the Charter represented only part of the customary international law relating to the use of force and stated "The U.N. Charter ... by no means covers the whole area of the regulation of the use of force in international relations".[68] The Court pointed out that the right to self defence stood alongside the Charter and that the Charter text did not go on to regulate all of the aspects of that rule. Bearing that in mind we need now to turn to state practice and the theories of force propounded by other academics.

2.1. State Actions

Given the classified and covert nature of most computer network attacks, a survey of state practice in relation to this type of incident is problematic at best. To date there have not been any computer network attacks that are conclusively attributable to a State outside of traditional conflict scenarios, however some States have made statements regarding the use of computer network attacks and other analogous information operations. As has been stated one of the most difficult issues surrounding computer network attacks is positive attribution of an attack to the perpetrator, as a matter of fact, as well as a matter of law. Most of the incidents detailed below and in the Appendix have suffered from this difficulty, thus making statements of limited use. However, although they must be used with care, the statements, actions and reactions of States also form part of the interpretative framework of Article 2(4).

The most recent and clearest indication of state practice with regard to a specific computer network attack is the international response to the attacks against Estonia

---

[67] Gray, *Use of Force*, 7.

[68] *Nicaragua (Merits)*, para 176.

in 2007. As noted previously, the attacks did not affect critical infrastructure, damage physical property or cause human injury and it appears that States were not prepared to make definitive public statements regarding the attacks as a use of force.[69] NATO Member States were not prepared to accept that the attacks amounted to an armed attack which would initiate the collective self-defence provisions of the North Atlantic treaty, however a NATO spokesperson commented that the attacks were a security issue which concerned NATO.[70] Russia denied all accusations of computer network attacks and stated that the Kremlin comes under attack many hundreds of times a day.[71] In the past, Russia has stated that they will view the effects of a computer network attack as similar to that of the use of weapons of mass destruction and that:[72]

> "[f]rom a military point of view, the use of information warfare means against Russia or its armed forces will categorically not be considered a non military phase of a conflict, whether there were casualties or not...Russia retains the right to use nuclear weapons first against the means and forces of information warfare, and then against the aggressor state itself."

However, this statement has not been reflected in Russia's response to computer network attacks in the recent conflict over South Ossetia where reportedly Russian and South Ossetian sites have come under attacks from Georgian hackers.[73] China has often topped the lists of States engaged in or developing computer network attack capabilities.[74] China has been accused of hacking attacks against government computers in the U.S., France, Germany, the U.K., Australia and New

---

[69] For example U.S. called the attacks "unacceptable" and "pressure on a independant country" but stopped short of calling the attacks force: 'Rice Condemns Ongoing Cyber-Attacks as Estonian Embassy Siege Ends', *earthtimesorg* 4 May 2007.

[70] AFP, 'Cyber Attacks on Estonia Are Security Issue: NATO Chief', *The Age* (Melbourne), 26 May 2007.

[71] 'The Cyber Raiders Hitting Estonia', *BBC News* 17 May 2007, <http://news.bbc.co.uk/1/hi/world/europe/6665195.stm> (last accessed 21 September 2008).

[72] V Tsymbal quoted in T Thomas, 'Russia's Information Warfare Structure: Understanding the Roles of the Security Council, Fapsi, the State Technical Commission and the Military' (1998) 7 *European Security* 156, 161.

[73] Kim Hart, 'Longtime Battle Lines Are Recast in Russia and Georgia's Cyberwar', *Washington Post* (Washington D.C.), 14 August 2008, D01 <http://www.washingtonpost.com/wp-dyn/content/article/2008/08/13/AR2008081303623.html> (last accessed 26 August 2008).

[74] See for example, McAfee, *Virtual Criminology Report*, McAfee Inc. (2007); Symantec, *Symantec Global Internet Security Threat Report*, Symantec, Vol XIII (2008).

Zealand.[75] The Chinese government has denied any involvement in such attacks and despite the problems of attribution it is clear that these States have not considered the access and theft of information a use of force and are content to deal with them as cases of espionage. China has also claimed that it has sustained 'massive' and 'shocking' losses of State and military secrets via the Internet.[76] Although they are non-international examples, Tibet and Taiwan have repeatedly come under attack from alleged Chinese hackers, suspected to have the backing of the Chinese government. The Chinese government has denied all such claims stating that "the Chinese government always opposes the activities of hackers".[77] In September 2002 China announced that it had developed five new information warfare institutes to develop information warfare patterns/weapons/ described as "technological aircraft carriers" and the official news agency Xinhua stated that Chinese military leaders hoped to overcome their military weaknesses, largely outdated hardware, by attacking a technologically superior foe with electronic warfare.[78]

The United States has formally stated that it is their policy to respond to cyber attacks by any means appropriate, including military action.[79] Further, in July 2002, President George W. Bush signed a secret directive ordering the government to develop, for the first time, national-level guidance for determining when and how the United States would launch cyber-attacks against enemy computer networks.[80] The

---

[75] See for example Roger Boyes, 'China Accused of Hacking into Heart of Merkel Administration', *The Times* (London), <http://www.timesonline.co.uk/tol/news/world/europe/article2332130.ece> (last accessed 26 August 2008); John Leyden, 'France Blames China for Hack Attacks', *The Register* (London), 12 September 2007, <http://www.theregister.co.uk/2007/09/12/french_cyberattacks/> (last accessed 26 August 2008).

[76] Leyden, 'France Blames China for Hack Attacks'. Edward Cody, 'Chinese Official Accuses Nations of Hacking', *Washington Post* (Washington D.C.), 13 September 2007, A16.

[77] See for example 'China Denies Hacking Dalai Lama Computer', *CNN* 25 September 2002, <http://europe.cnn.com/2002/TECH/internet/09/25/dalailama.hacking.ap/> (last accessed 28 September 2002); George V. Hulme, 'Taiwan Accuses China of Launching Cyberattack' (2004) *Information Week* 16 June 2004 <http://www.informationweek.com/story/showArticle.jhtml?articleID=22100221> (last accessed 15 September 2007).

[78] 'Military Eyes Electronic Warfare', *Associated Press, South China Morning Post* 28 September 2002, <http://china.scmp.com/chimain/ZZZH3UK2F6D.html> (last accessed 30 September 2002).

[79] Dan Verton, 'The Prospect of Iraq Conflict Raises New Cyber Attack Fears' (2002) *Computerworld Hong Kong* 30 September 2002 <http://www.idg.com.hk/cw/readstory.asp?aid=20020930004> (last accessed 30 September 2002).

[80] Bradley Graham, 'Bush Orders Guidelines for Cyber-Warfare', *Washington Post* (Washington D.C.), 7 February 2003, <http://www.washingtonpost.com/wp-dyn/articles/A38110-2003Feb6.html> (last accessed 21 February 2001).

United States have also revealed limited attempts to use computer network attacks offensively within the scope of the Kosovo campaign; according to newspaper reports the U.S. attempted to divert funds from Milosevic aligned businesses in an attempt to bring pressure to bear on the Serbian leader.[81] Such attempts were limited in scope and ended early due to concerns about the legitimacy and legality of such tactics.[82]

Such reactions and policy statements indicate that States are cautious about labelling computer network attacks as a use of force. Although both the United States and Russia have reserved the right to respond with force against computer network attacks they have not made any comments indicating that any computer network attacks reported to date should be viewed in this manner. To date, with the exception of the 'Farewell Dossier' incident, no computer network attack conclusively attributable to another State has caused physical damage or human injury.[83]

2.2. Theories of Force - Scholastic writings

Although they are in agreement over the customary nature of the prohibition on the use of force, commentators remain deeply divided over the content of the rule. Theories of force and discussion of Article 2(4) of the Charter have come mainly from two different schools of legal theory, those adopting a restrictive approach and those adopting a more expansive one.[84] The first, tending to come from the positivist school, provides a definition of 'force' and determines whether a particular incident falls within the accepted definition. The extensive approach tends to focus more on custom and the context of force. However it can be seen that definitions proffered by scholars in the field from all approaches have common themes running through them. All appear to be united in the need for a physical or violent means which produce a physical outcome. Michael Schmitt refers to physical or kinetic force

---

[81] William M. Arkin, 'The Cyber Bomb in Yugoslavia', Ibid. 25 October 1999, <http://www.washingtonpost.com/wp-srv/national/dotmil/arkin.htm> (last accessed 21 September 2008).

[82] See for example,William M Arkin and Robert Windrem, 'The Other Kosovo War', *MSNBC News* 29 August 2001, <http://www.msnbc.com/news/607032.asp?cp1=1> (last accessed 12 April 2005).

[83] Because of their clandestine nature computer network attacks are perfect fodder for rumours and misinformation; for example, Chinese hackers were inaccurately blamed for causing a massive blackout in the northeastern United States in 2003.

[84] For an extensive analysis of the methodological debates over the the prohibition on the use of force see Corten, 'Controversies'.

applied by conventional weaponry.[85] Ian Brownlie uses a two-part definition requiring the use of a weapon which is employed for the destruction of life and property.[86] Bowett refers to the possible resort to a violent weapon which inflicts human injury.[87] Likewise, Randelzhofer requires acts of violence committed by militarily organised groups.[88]

The need for physical means and the requirement of a weapon came to the fore with the advent of chemical and biological weapons. Ian Brownlie addressed this question in his 1963 work *International Law and the Use of Force by States*, considering whether weapons "which do not involve any explosive effect with shock waves and heat involves a use of force" prohibited by Article 2(4) of the Charter.[89] In concluding that these weapons should indeed be considered force, Brownlie gives two reasons. The first, is that the "agencies concerned are commonly referred to as 'weapons' and as forms of 'warfare'".[90] However, as has been seen in the preceding chapter, this may not be helpful in terms of categorising computer network attacks as force. Both the popular press and academics across disciplines have used the terms information warfare, cyber war and even computer network attack to refer to a vast range of information operations, some of which would never be considered to be uses of force under the Charter.[91] Further the terms 'war' and 'weapons' have found an increasingly political meaning in recent years. At the date of writing, the newspapers contain articles on the present conflicts in Afghanistan and Iraq, however they also contain articles on wars on terror, drugs, crime, and poverty; all politicised uses of the lexicon of humanitarian and international law and none of them aimed at invoking its protection. Used in this manner, the term war is merely used to signify resolve,[92] a point that has been noted by legal commentators and

---

[85] Schmitt, 'Normative Framework', 908.

[86] Brownlie, *Use of Force by States*, 362.

[87] Bowett, *Self-Defence*, 184-199.

[88] Randelzhofer, 'Article 2(4)', 120.

[89] Brownlie, *Use of Force by States*, 362.

[90] Ibid.

[91] See Todd A. Morth, 'Considering Our Position: Viewing Information Warfare as a Use of Force Prohibited by Article 2(4) of the U.N. Charter' (1998) 30 *Case W Res J Int'l L* 567, 590.

[92] Frédéric Mégret, "War"? Legal Semantics and the Move to Violence' (2002) *EJIL* 361.

politicians alike.[93] Thus the semantics of war and weaponry are no longer a useful criterion in determining whether something is a use of force.[94] Further, as was seen in the 2001 anthrax scares in the United States and the release of sarin gas on a Tokyo subway train in 1985, the requirement of a weapons-based delivery system is not an essential requirement for a chemical or biological attack. The International Court of Justice in the *Nuclear Weapons* advisory opinion has stated that the provisions relating to the use of force in the Charter do not refer to specific weapons but rather apply to the use of force regardless of the weapons employed.[95] Brownlie's second and more convincing argument is that the use of chemical and biological weapons should be viewed as force because "these weapons are employed for the destruction of life and property".[96] It is also representative of the second requirement of the majority of academics for a physical outcome to a computer network attack. In advancing his analysis, Brownlie moves the test beyond kinetic impact of shockwaves and heat and toward a wider, result-oriented approach. A purely result-driven approach raises problems of its own however, in that it reopens the door for arguments relating to the inclusion of political and economic coercion. As Cassandra LaRae-Perez points out, once a results-based perspective is adopted, the effects of long term, comprehensive economic sanctions of the kind adopted against Iraq and Cuba, which are as severe as the use of force against those States, can be regarded as falling foul of Article 2(4).[97] However state practice shows that the international community is not ready for this to be the case. The rigorous economic embargo that the United States has enforced against Cuba since the early

---

[93] See for example, Christopher Greenwood, 'International Law and the War against Terrorism' (2002) 78 *International Affairs* 301, 306. Also Tony Blair's comment "Whatever the technical or legal issues... the fact is that we are at war with terrorism" See, BBC News "Britain at War with Terrorism" 16 September 2001 (available at http://news.bbc.co.uk/1/hi/uk_politics/1545411.stm); "Powell Very Pleased with the Coalition-Building Results" 13 September 2001 (available at http://www.usinfo.state.gov/topical/pol/terror/01091366.htm)

[94] Although some of the more populist articles refer to information warfare techniques as weapons of mass disruption, obviously a play on the 'mass destruction' terminology applied to nuclear, chemical and biological weapons, such terms have not achieved widespread usage.

[95] *Nuclear Weapons Case*, para 39.

[96] Brownlie, *Use of Force by States*, 362.

[97] Cassandra LaRae-Perez, 'Economic Sanctions as a Use of Force: Re-Evaluating the Legality of Sanctions from an Effects-Based Perspective' (2002) 20 *BU Int'l LJ* 161.

1960's has not been considered to be a use of force; likewise, neither has the Arab embargo of Israel.[98]

Similarly, Yoram Dinstein argues for a results-based approach when discussing computer network attacks in the context of an armed attack, recognised by the ICJ in the *Nicaragua (Merits)* case as a subset of the use of force.[99] He argues that violent consequences are the key to fulfilling the definition of armed attack:[100]

> "From a legal perspective, there is no reason to differentiate between kinetic and electronic means of attack. A premeditated destructive [Computer Network Attack (CNA)] can qualify as an armed attack just as much as a kinetic attack bringing about the same or similar results – the crux of the matter is not the medium at hand (a computer server in lieu of, say an artillery battery), but the violent consequences of the action taken. If there is a cause and effect chain between the CNA and these violent consequences, it is immaterial that they were produced by high and not low technology"

Dinstein's realist argument focuses solely on the consequences of an attack. As shown above, a *purely* consequence-based approach in an area that lacks the tangibility of traditional military/armed force blurs the distinction with the grey area occupied by political and economic coercion. Thus a theory of force which requires only a particular outcome is insufficient to cover the concerns raised by forms of coercion which the international community is agreed (for the most part) are not to be included as uses of force. However it is also equally clear that the requirement and current analysis with regard to weaponry cannot stand as it is and must be revisited if it is to take into account changes in technology.

Michael Schmitt has argued that not only is a purely consequence-based approach extraordinarily difficult to quantify or qualify,[101] it would also constitute a new normative standard altogether and as such would prove a difficult case for adoption by the international community.[102] Schmitt is an adherent of the second school of

---

[98] Bond, *Peacetime Foreign Data Manipulation*, 59. Interestingly, in the latter case the United States was in the position of the weaker state and argued that the economic coercion by the more powerful Arab states should be considered to be a use of force, a reversal of its position in the Cuban embargo.

[99] Dinstein, 'CNA and Self-Defense', 103.

[100] Ibid.

[101] Schmitt, 'Normative Framework', 911.

[102] Ibid., 917.

legal theory writing on the subject of force, the more expansive contextualist approach epitomized by the New Haven school writers such as Michael Reisman and Myers McDougal.

In his work *Law and Minimum World Public Order,* Myers McDougal has argued that force is merely a degree of major coercion and violence on a trans-national scale.[103] McDougal thus places all forms of coercion on this scale and addresses the problem of the characterisation of the particular coercion as permissible or non-permissible from variables based on past actions, extrapolated forward in accordance with those variables' probable consequences upon the goal values of the kind of world order the scholar prefers:[104]

> "From this perspective, the basic intellectual task is one of characterising the variable contextual factors and policies which relate to the distinction between permissible and impermissible coercion for the guidance of differing particular decision makers".

Developing the theory further, Michael Reisman sets out seven categories where the use of force in international law has achieved some form of international legal authority.[105] He argues that in determining whether a particular act of coercion is lawful or not, the question to be answered is whether a particular act (whatever its justification otherwise) enhances or undermines world order.[106] That is, the critical question is not whether coercion has been applied, but whether it has been applied (a) in support of or against community order and basic policies and (b) in ways in which the net consequences include congruence with community goals and minimum order.[107] However, the contextualist position has fundamental difficulties. Olivier Corten points out, there exists no 'objective law' that expresses social

---

[103] Myres Smith McDougal and Florentino P. Feliciano, *Law and Minimum World Public Order: The Legal Regulation of International Coercion* (Yale University Press, New Haven, 1961).

[104] Ibid., 153.

[105] These categories are self defence, self determination and decolonisation, humanitarian intervention, intervention by the military instrument to replace an elite in another state, uses of the military instrument within spheres of influence and critical defence zones, treaty sanctioned interventions within the territory of another state, use of the military instrument for the gathering of evidence in international proceedings, use of the military instrument in enforcing international judgements, and countermeasures such as reprisals and retorsions. W Michael Reisman, 'Criteria for the Use of Force in International Law' (1985) 10 *Yale J Int'l L* 279, 281.

[106] Ibid., 282.

[107] Ibid., 284.

necessities or the solidarity mechanisms that characterise the international community; it is the interpreter and the interpreter alone who gives sense to what is required in a particular case by those necessities or that solidarity.[108] The idea that the fundamental goals of the community must prevail over any particular rule of law, namely the rule prohibiting armed force, would remove all certainty from international relations, leaving the outcome of any diplomatic encounter highly uncertain as to its legality. And ultimately, that uncertainty is a greater threat to communal values and goals. This methodological schism permeates the debates on the legality of computer network attacks as a use of force and divides commentators on the correct approach to take to this emerging form of warfare.

3. Computer Network Attacks as a Use of Force

As noted above, two main theories of force have emerged out of the current writing in relation to the prohibition against force. The first is the more restrictive, positivist approach which looks at the rules formulated by the international community, in this case the prohibition against force, and argues that anything falling outside that prohibition is legal. Authors adhering to this school include Ian Brownlie, Yoram Dinstein, Christine Gray and, in respect of computer network attacks, James Bond. The second is the more expansive contextualist approach which contends that all coercion falls along a continuum and the position along the continuum is the result of several factors which affect the minimum world order. The contextualist approach can be seen in the work of Michael Schmitt and Michael Reisman.

As we have seen above a results-based approach to the question as to whether a particular attack contravenes the prohibition against 'armed force' leads towards an erosion of the economic and political coercion exclusion. Michael Schmitt has suggested that the use of force proscription is based on the desire of the international community to foster and advance the aspirational values set out in the preamble to the Charter. The prohibition on 'armed' force is a kind of instrumental shorthand way of restricting those acts that are most likely to endanger these objectives and aims. Thus, the international community is not concerned so much with the instrumentality of the coercion but rather the consequences of its use.[109] However,

---

[108] Corten, 'Controversies', 814.

[109] Schmitt, 'Normative Framework', 911.

given that the range of possible consequences of any given kind of attack (i.e. denial of service, virus, intrusions etc) range along a continuum, assessing the consequences of an attack can be a Sisyphean task, making the criteria for placement upon that continuum extremely difficult.

> "The difficulty in looking to consequences themselves as criteria for calculating lawfulness led the Charter drafters to use prescriptive shorthand to achieve their goal. Because force represents a consistently serious menace to intermediate and ultimate objectives, the prohibition of resort to it is a relatively reliable instrument-based surrogate for a ban on deleterious consequences. It eases the evaluative process by simply asking whether force has been used rather than requiring a far more difficult assessment of the consequences that have arisen"[110]

However as seen above with reference to economic and political coercion, it cannot be the case that the only criteria to be used are the consequence-based ones. Despite subscribing to this view, in his article setting out a normative framework for the analysis of computer network attacks, Michael Schmitt has proposed several consequence-based factors which are to be taken into account when determining whether an attack will constitute a use of force: severity of the damage, immediacy of the consequences of the attack, directness, invasiveness of the act into the target state, measurability of the damage, and presumptive legitimacy.[111]

A previous paper by Schmitt considers by whom, and against whom, any attack is effected, what form the attack takes and its aims, when any attack, and specifically, any response to an attack occurs and whether the attack occurs within a State's sphere of influence or critical defence zone.[112] Additional factors are the reason for the attack and the consequences of any attack.
The Court in the *Nuclear Weapons* advisory case stated that in order to apply the Charter law on the use of force and the law applicable in armed conflict, it was

---

[110] Ibid.

[111] Ibid., 914.

[112] Michael N. Schmitt, 'The Resort to Force in International Law: Reflections on Positivist and Contextualist Approaches' (1994) 37 *AFL Rev* 105.

essential to take account of the unique characteristics of nuclear weapons.[113] The same approach may adopted in respect of computer network attacks.

3.1. Characteristics of Computer Network Attacks

The problem with defining computer network attacks as a use of force under current international law is an obvious one. The contemporary prohibition on the use of force (both as treaty law and as customary law) has its roots firmly in the text of Article 2(4) of the United Nations Charter. However at the time that the Charter was drafted, the science of computing had not advanced to such a state where it could be considered to be any sort of threat, and indeed in 1945 the breakthrough towards modern computing was just beginning.[114]

The problems that arise from considering a computer network attack as a use of force stem from the fundamental characteristics of such attacks. Despite the wide range of attacks which fall under the heading of computer network attack, it is possible to distil four characteristics of a computer network attack which distinguish it from its conventional counterparts: indirectness, intangibility, *locus*, and result. Some of these characteristics do not raise significant issues in contemporary international law on the use of force and are easily solved within the existing framework, however other characteristics raise more difficult issues. This section examines each of these characteristics and the arguments that have been advanced to militate against such attacks falling within the definition of force. As will be seen, most arguments can be dealt with under existing law.

3.1.1. Indirectness

Although direct computer network attacks are certainly possible, for example the infiltration of a dam's control system to send water downstream, a large number of possible attacks will manipulate one system to achieve a knock-on effect from something else. Examples of such indirect attacks include a manipulation of GPS

---

[113] *Nuclear Weapons Case*, para 36.

[114] Notwithstanding the important role the Colossus machine played in the British/Allied war efforts at Betchley Park in breaking the ciphers used by the highest level Germans for strategic commands. See http://www.turing.org.uk/turing/scrapbook/electronic.html for an account of the claim to invention of the computer by Alan Turing and the Virtual Betchley Park for details of the role of electronic code breakers during World War II http://www.codesandciphers.org.uk/virtualbp/ (last accessed 14 December 2002).

satellite systems to send an opposing force's missiles off target, manipulation of hospital blood type data resulting in the wrong blood type being given to enemy soldiers, or disabling air traffic control systems. These examples all involve an action which requires further action to be taken by a second actor or object to achieve the desired result. Indirectness, *per se* has not been an issue for the international community. As seen above the International Court of Justice in the *Nicaragua (Merits)* case has held that indirect assistance can be a use of force contrary to international law. The Court based its reasoning as follows:

> The element of coercion, which defines, and indeed forms the very essence of, prohibited intervention, is particularly obvious in the case of an intervention which uses force, either in the direct form of military action, or in the indirect form of support for subversive or terrorist armed activities within another State. As noted above (paragraph 191), General Assembly resolution 2625 (XXV) equates assistance of this kind with the use of force by the assisting State when the acts committed in another State 'involve a threat or use of force'.[115]

However it should be noted in these cases that the further action to be taken has involved a traditional use of armed force. Where the subsequent action does not constitute a 'threat or use of force' such as the example of the hospital records, it seems unlikely under present interpretations of the law that the action could be considered a use of force. Further, not all assistance given to the rebels was considered to be contrary to the prohibition against force, mere supply of funds to the contras did not in itself amount to a use of force.[116] Therefore the causal nexus between an act of a State and a violent physical effect on the victim State will be of critical importance.

Another issue arises where the party who is being 'assisted' has no wish or intention to cause damage but is being used as the unwilling agent of the attacking actor. This is the case where computers are 'recruited' to botnets and used to launch distributed denial of service (DDoS) attacks against a target computer. Attackers in Estonia reportedly enlisted botnets in their attack, including one with in excess of 1 million computers.

---

[115] *Nicaragua (Merits)*, para 205.

[116] Ibid., para 228.

An early precursor is the 1998 'Floodnet' denial of service attack launched by the Electronic Disturbance Theatre (EDT), an activist group tied to the Zapatista rebels in Chiapas, Mexico, against a computer network at the Pentagon. The group was responding to alleged U.S. support for the Mexican government. When users logged on to an EDT website, the Zapatista Floodnet software was downloaded to their computer. As with most DDoS attacks, the software is designed to initiate automatic and repeated requests to reload an IP address, in this case the Pentagon's website DefenceLink. As Floodnet performs automatic reloads of the site, it slows or halts access to the targeted server and clogs bandwidth.[117] What makes the example significant for this thesis was the reaction of the Pentagon who responded in kind, sending a java applet back to the initiating computer and disabling the browser of the computer initiating the attack.[118] The action caused a storm of controversy on the Internet as it involved an offensive attack on civilian computers. Following the incident the Pentagon established a legal team to steer the Joint Taskforce on Computer Network Defense through the difficult legal issues. The taskforce is "prohibited from engaging in offensive information warfare operations like the episode of Sept. 9".[119] It appears likely that for the most part the 80,000 plus computers utilized in the attack were used with the consent of the owner.[120] However such software can be downloaded to a computer without the knowledge of the user. Where a state-owned computer is used in this manner, the effect may appear to be a state-sponsored attack of another State's systems.[121] This appears to be the case in

---

[117] The Electronic Disturbance Theatre views this act as performance art, hence the term theatre in their title and classifies the FloodNet action as virtual or electronic civil disobedience.Coco Fusco, 'Performance Art in a Digital Age: A Conversation with Ricardo Dominguez', 25 November 1999.; see also Karl J Shawhan "Vital Interests, Virtual Threats: Reconciling International Law with Information Warfare and United States Security" (2001) School of Advanced Airpower Studies, Air University, Maxwell Air Force Base, Alabama <http://www.maxwell.af.mil/au/aul/aupress/SAAS_Theses/Shawhan/shawhan.pdf> (last accessed 4 April 2003).

[118] Brian Friel, 'DoD Launches Internet Counterattack' (1998) *Government Executive* 18 September 1998 <http://govexec.com/dailyfed/0998/091898b1.htm> (last accessed 7 August 2008). According to the EDT only 2 computers of the 80,000-plus who participated were crashed by the DoD counterattack.

[119] George I. Seffers, 'Legalities Cloud Pentagon's Cyber Defence' (1999) *DefenceNews* 25 January 1999 3, 26., cited in Shawhan "Vital Interests, Virtual Threats", 37

[120] Fusco, 'Performance Art in a Digital Age'. According to EDT, the FloodNet system advises the user that their IP address may be 'harvested' by the government in any action, and that damage may occur to your machine. The code has now been released as shareware on the Internet and it is likely that the warning messages may be altered or dispensed with altogether by future users.

[121] The problem of attribution of attacks is examined in Chapter 3 *infra.*

the attacks against Estonia in 2007. Although computers inside the Kremlin were used in the attacks, those computers could have been compromised. The incident resulted in Estonia accusing Russia of instigating the attacks, the first time a State had been accused of launching an attack against another State.

3.1.2. Intangibility

The second major characteristic of computer network attacks is the intangibility of the attack; both in terms of the method of warfare and the consequences of an attack. While it may be possible to point at a single piece of malicious code that has caused the problem, legally speaking the problem of intangibility exists on three levels. First, the target of the attack may not exist in the physical world other than as information held on a server. Secondly, the 'weapon' itself is intangible, a piece of binary coding which may cause catastrophic effect. Thirdly, the type of damage the attack causes might also be intangible. A computer network attack that does not touch the physical sphere may nevertheless cause mayhem; the oft-cited hypothetical example is an attack on the New York stock exchange that causes mayhem and panic in the United States. This last aspect of intangibility will be examined in section 3.1.4 *infra.*

Target Intangibility

Computer network attacks, by definition, target information and information systems. However, they may be divided into those which target information systems in order to affect hardware and other physical aspects and those which target information as its own end. Where the target of an attack is a physical entity the effects of a computer network attack fit more easily with current experience. The more difficult issue arises where the target of the attack is information itself. Particularly, where the effect of the attack is not to destroy the information, but to degrade the information target to the extent that it cannot be relied upon. An extreme example of such an attack would be a situation where the medical records of serving military sent to a staging ground in preparation for a conflict were tampered with by altering the blood type records held for those soldiers. Note that the attack has occurred before the traditional conflict has started, the rules of *jus in bello* do not yet

apply, and at the time of the attack the soldiers are not yet *hors du combat.*[122] In the hypothetical situation described above, a complicating factor arises as to whether the massing of troops in a staging ground constitutes a threat or use of force contrary to Article 2(4) of the Charter in any event, thus raising the question whether such a computer network attack would be a proportionate response to a threat.[123] However leaving such questions aside for the time being, we must determine whether such an act constitutes a use of force in and of itself.

Under the results-based theory proposed by Dinstein, the fact that the attack results in serious harm and possible loss of life, places it clearly within the purview of a use of force contrary to Article 2(4). There is a clear chain of causation between the attack and the loss of life - change in data leads to wrong blood being given to soldier, which leads to death by incompatible blood transfusion. And yet gut instinct tells us that this cannot be a correct use of Article 2(4), although almost certainly being contrary to Geneva Conventions. Why not? The fact that the action was carried out prior to the physical consequences of the attack is not a useful distinction. International law recognises that the laying of mines in both territorial and international waters may be an act of force, even though the violent consequences of the act may take place a significant period of time later.[124] The test promulgated by Brownlie also talks about damage to property. In this circumstance the property that is damaged is intangible, *vis* a database. In the event that no loss of life occurs, the only damage which has occurred is to the information or data contained in the database. Is this sufficient property damage to satisfy Brownlie's test of a use of force? Note that under New Zealand and UK intellectual property law at least, data in a database is not considered intellectual property. Therefore it cannot be the case that such damage on its own without further evidence of destruction is sufficient to fall foul of Article 2(4).

As seen above, Brownlie's theory of force also requires a weapon and computer network attacks do not conform to our traditional perception of weapons.

---

[122] This latter point may well be moot because the effective timing of the attack may well be the point at which it causes it damage. At which point the soldiers are likely to be hors du combat if they are requiring blood.

[123] State and juridical practice is divided on the matter. The ICJ has held that military manoeuvres carried out by United States troops near the border of Nicaragua were not sufficient to constitute a use of force: *Nicaragua (Merits)*, para 227.

[124] See Ibid and *Corfu Channel Case* respectively.

Weapons Intangibility

The second question that arises is whether a bitstream of malicious code is sufficiently militaristic or weapon-like to meet the required definition of 'armed' force. As noted previously, Schmitt argues that the instrument-based distinction is a 'prescriptive shorthand' for a set of consequences which affect community values. Thus he argues that:[125]

> "Armed coercion is not defined by whether or not kinetic energy is employed or released, but rather by the nature of the direct results caused, specifically physical damage and human injury. Instrumentalities that produce them are weapons. There is little debate about whether the use of chemicals or biological agents falls within the meaning of armed force, even though the means that cause the injury or death differ greatly from those produced by kinetic force."

That is, a weapon is anything that directly causes physical damage and human injury. Jacobson has argued that 'armed' simply means equipped with weapons of war, and that weapons are tools designed to accomplish a specific mission.[126]
Brownlie's approach was to fit the new technology to the definition. Given that a purely results-based approach does not provide the appropriate distinction between armed and other forms of coercion, the means of producing the results are still significant.
If a computer network attack does not meet some form of weapons criterion then it is likely that the use of such attack techniques will fall within the levels of coercion currently occupied by political and economic coercion. Obviously in the event that these attacks take place during an armed conflict, such acts will be seen as part of the ongoing conflict, and will be judged accordingly; however it is worth emphasising that in this instance, these issues are raised in relation to the exercise of such force by an actor of the State before the commencement of traditional military action.
The definition of weapon in the Oxford English Dictionary is a "thing designed, used, or usable for inflicting bodily harm" or secondly, a "means for gaining

---

[125] Schmitt, 'Normative Framework', 913.

[126] Mark Jacobson, 'War in the Information Age: International Law, Self Defence and the Problem of 'Non-Armed' Attacks' (1998) 21(3) *Journal of Strategic Studies* 1.

advantage in a conflict". While the first definition fits with a traditional use of kinetic violence it is the second definition that may provide the answer for information warfare attacks. As seen above however it must be used with some caution as many tactics, which may gain an advantage in a conflict situation, would not be considered weapons. James Bond gives the example of spy satellites which pass over the territory of States and yet are not considered weapons and whose use is not considered a use of force.[127] He reaches this conclusion on the grounds that satellites merely process data rather than having a direct capability of producing death or physical destruction of property. Bond thus extrapolates this to other pieces of equipment which do nothing but process data and concludes that most, if not nearly all, instances of data manipulation would not equate to employing a weapon and would not constitute the use of force.[128]

The question of weapon intangibility may not be of much use in determining whether new methods of warfare are uses of force prohibited under international law. An analogy with the domestic criminal law of murder is useful in this regard. Murder weapons come in all shapes and sizes and what may be a permissible and useful tool in one regard, for example a wrench, can be transformed into an instrument of death in an instant. The key factors that determine its use as a weapon is not the nature of the object itself, but rather how the object was used, against whom and why.[129]

The problem is compounded by a failure to distinguish between a particular piece of malicious code as a weapon and identifying the computer as a weapon. The weapon of choice for a computer network attack is a series of digits (or bitstream) which comprise a set of instructions. A computer network attack is, therefore, perhaps a perfect example of the principles of domestic criminal law indicated above which interpret a weapon as something being used to injure persons or property. Thus in the example above, a wrench in the hands of a mechanic may be merely a tool of the trade or an instrument of destruction depending on his or her intent. The binary coding required for a computer network attack contains the instructions for the attack and hence represents an almost pure expression of the intent of the attacker.

---

[127] Bond, *Peacetime Foreign Data Manipulation*, 83.

[128] Ibid.

[129] See also Ibid., 86.

3.1.3. Locus

Another argument raised against computer network attacks as a use of force concerns the problem of the locus of the attack and the locus of the target. The locus of the attack was raised early on in the literature with some commentators claiming there was no cross-border action involved in the attack.[130] However this argument is ill-founded. While a border violation may be evidence of a use of force, international law does not require cross-border action to occur before a use of force has been found. For example, an act against a visiting foreign minister or head of state of a country has always been considered an act of force by the host State.[131] Further, the actions of the United Kingdom in the *Corfu Channel* case were held to be a policy of force even though the strait concerned was of the "class of international highways through which passage cannot be prohibited".[132]

The main issue with the locus of the attack is that it can be very difficult to establish with any degree of certainty where the attack was actually generated. Current technology allows attackers to conceal their identity and route any attack through a number of servers based around the globe prior to hitting the target system. For example, the 1998 'Solar Sunrise' attacks, in which a number of U.S. DoD networks were compromised, appeared to be coming from multiple servers in the U.S. as well as the United Arab Emirates, Israel, France, Germany and Taiwan. While this attack is purely a matter of transnational criminal law, the possibilities for a state-sponsored version of the same style of attack exist. The 'Titan Rain' series of intrusions routed stolen data through servers in South Korea, Hong Kong or Taiwan before sending them to computers in Guangdong province in mainland China.[133] Although most analysts believe the Chinese government to be behind the espionage attacks, China has denied all involvement and the attribution cannot be proved. From a law enforcement point of view it may be almost impossible to determine where the attack

---

[130] See for example, Sean P Kanuck, 'Information Warfare: New Challenges for Public International Law' (1996) 37 *Harv Int'l LJ* 272, 286.

[131] See for example the 1993 missile attacks launched by the U.S. in response to an assassination attempt against former President H.W. Bush.

[132] Although part of the northern Corfu Channel forms part of the territorial waters of Albania and Greece respectively, however the international character of the waters and the rights of passage in international law through such waters illustrate the point at hand. *Corfu Channel Case*, 29.

[133] See generally, Nathan Thornburgh, et al., 'The Invasion of the Chinese Cyberspies (and the Man Who Tried to Stop Them)' (2005) 166(10) *Time* 34.

originated, and whether the attack was launched as the first blow in a conventional interstate conflict, terrorist attack, domestic crime or accident.[134] Distributed Denial of service attacks maybe even more difficult to trace as attacks come from multiple computers recruited to a botnet – tracing the controlling computer can be a time-consuming and difficult job. The attacks launched against Estonia in 2007 and Georgia in 2008 are a case in point.

Other scholars have taken issue with the fact that the target of any such attack is located in the information realm i.e. cyberspace, and have argued that this area is not regulated by the current laws of armed conflict.[135] There are two answers to this question and which one is applicable is dependant on the mode of attack. The first answer to concerns over the locus of the target is a practical one. As discussed in Chapter 1 *supra*, data does not exist in the ether of cyberspace; it must reside on a server that is actually present in the physical domain. Although the location for a target with military significance is likely to be hosted on a State's own systems it is also possible that important functions could be located elsewhere, possibly even in a foreign State,[136] so while geographical *boundaries* are not important, the target *is* still embedded in a geographic location. This physical location has been the basis for international consensus on jurisdictional laws relating to cyber crime and electronic transactions and it is hard to see any reason why this should hinder international law in the area of force and humanitarian law.[137]

The other answer is closely related to the following section on the results of a computer network attack which does not affect the physical sphere and is dealt with below.

3.1.4. Result

Computer network attacks incorporate many different techniques from simple denial of service to direct data or system manipulation and the possible results span the

---

[134] Emily Haslam, 'Information Warfare: Technological Changes and International Law' (2000) 5(2) *JC&SL* 157, 162.

[135] See for example, Kanuck, 'Information Warfare: New Challenges for Public International Law', 287.

[136] For example following their virtual declaration of independence, the website of East Timor was hosted on Servers in the Republic of Ireland.

[137] See for example the U.N. model laws on electronic commerce and computer crime.

spectrum from mere inconvenience to catastrophic damage to life and property.[138] Indeed, the flexibility and wide range of possibile results is one of the reasons that such weapons are attractive to the armed forces. However the indeterminate result of a computer network attack is also the characteristic that causes the most uncertainty in applying the legal requirements of force and the laws of war.

First, while a computer network attack may result in death or damage to physical property, it need not do so. The purpose of the attack may simply be to shut off a particular service or function; for example, shutting off a particular telecommunications system to force an opponent to use a more insecure method.[139] Alternatively, the main purpose of the computer network attack may be the denial, corruption or exploitation of the information target itself. For example, the Israeli attacks against the Syrian air defence radar system which allowed their fighters to remain undetected during their raid on a suspected nuclear facility in 2007.[140] Given the character of these attacks, should these results be dealt with in a legal manner in the same manner as conventional uses of force, or should they fall into the category of other means of coercion?

As the United States Joint Chiefs of Staff have stated:[141]

> "Information Warfare can make an important contribution to defusing crises; reducing the period of confrontation and enhancing the impact of informational, diplomatic and military efforts, and forestalling or eliminating the need to employ forces in a combat situation."

In terms of the prohibition against force however, the Brownlie and Dinstein models of force require that the result of a use of force is fatality or damage to property, however no analysis has been undertaken to determine whether such damage to property would include damage to intellectual or other intangible property. Of course, it has always been legitimate in warfare to steal or corrupt the opponent's information, supply them with disinformation and sabotage their weaponry as long

---

[138] For example the 'Farewell Dossier' incident resulted in the "most monumental non-nuclear explosion ever seen from space". Reed, *At the Abyss*, 269.

[139] Schmitt, 'Normative Framework', 888.

[140] See Appendix 1 for details of this attack. Fulghum and Barrie, 'Israel Used Electronic Attack in Air Strike against Syrian Mystery Target'; Fulghum, Wall and Butler, 'Israel Shows Electronic Prowess'.

[141] U.S. Joint Chiefs of Staff, *Information Warfare: A Strategy for Peace... The Decisive Edge in War*, (1996) 5 <http://handle.dtic.mil/100.2/ADA318379>, cited in Schmitt, 'Normative Framework', 892.

as such acts do not constitute perfidy. However this presupposes an armed conflict is already under way between the opposing States. Where such acts take place prior to the commencement of a traditional attack, the permissiveness of these acts in wartime may militate against the question of whether these acts cross the threshold of 'force' in peacetime. Needless to say however they may still have the character of internationally wrongful acts imputing state responsibility for reparations.
Secondly, at the present time it is very hard to determine what the effects of any particular attack may be. One of the consequences of the interconnectivity of electronic resources is that military systems are often using civilian networks. In fact one report estimates that in 1995 ninety-five percent of all U.S. military communications traffic flowed over civilian networks.[142] As well as posing a targeting dilemma, the problem becomes one of accurate mapping of the networks in order to determine what the consequences of each type of attack may be. An attack designed to electronically incapacitate a command and control centre and early warning systems may inadvertently disable critical equipment in a hospital connected via a node on a related network. The unpredictable nature of the results is one of the major problems in assessing the legality of this new form of warfare.

4. Conclusion

The present author considers that where a computer network attack, directly or indirectly, results in a physical consequence, namely destruction of physical property, injury or loss of lives, it will constitute a use of force under Article 2(4). This appears to be clear from interpretation of the relevant legal instruments despite the intangibility of the weapon used; as seen from the discussion above, the weapon criteria is losing its relevancy in today's world. However, where the result of a computer network attack does not manifest itself in the physical sphere (that is, it affects information only), or its physical results are too minimal or too removed from the chain of causation (i.e. the results were not a foreseeable consequence of the act), the attack does not fall clearly within the traditional test for Article 2(4) and will not

---

[142] Richard W Aldrich, 'The International Legal Implications of Information Warfare' (1996) *Airpower* 99, 105. Citing Science Applications International Corporation, "Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance," research report for the chief, Information Warfare Division (J6K), Command, Control, Communications and Computer Systems Directorate, Joint Staff, The Pentagon, Washington, D.C., 4 July 1995.

constitute a use of force. However, the fact that a computer network attack does not rise to the level of a use of force does not imply that it is therefore permissible. It is likely that any computer network attack severe enough to raise this question will be considered an unlawful interference in the affairs of a State, and may in all likelihood amount to a threat to the peace.

Chapter 3 - Armed Attack & Self-Defence in the Digital Age

Having looked at computer network attack as a prohibited act in the previous chapter, this chapter will look at the exceptions to the prohibition, the permissible response to the prohibited act. Other than collective measures, the only exception to the prohibition on force set out in the Charter of the United Nations is the inherent right of collective or individual self-defence in international law, which is codified in Article 51 of the Charter.[1] The application of the right of self-defence in the case of computer network attacks is particularly complicated, for a number of reasons. First, it is difficult to see at exactly what point a computer network attack will rise to the level of an armed attack. As seen in the previous chapter, traditional international law focuses on personal injury, fatality and damage to physical property as measures of the seriousness of an attack. This approach is favoured by most commentators writing on the subject to date,[2] however many catastrophically damaging computer network attacks will not cause any of these deleterious consequences. Further, it is likely that any attack using information operations will not come as a single instance of attack, but as a series of events which, taken separately, may not be sufficient to qualify as an armed attack. This raises the question of the right to respond to 'pin-prick' attacks with a single use of force, a concept which has had a chequered history in international law. The likelihood that computer network attacks will be used in conjunction with, or as a precursor to, a conventional attack may also raise a right to respond to such attacks under the auspices of the controversial doctrine of anticipatory self-defence. For example, will mere intrusion into an air defence

---

[1] Article 51 reads "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security."

[2] See Horace B. Robertson, 'Self-Defense against Computer Network Attack under International Law' in M N Schmitt and B T O'Donnell (eds), *Computer Network Attack and International Law* (Naval War College, Newport, RI, 2002) 122-145, 136, for examples of authors adopting the consequence-based approach.

network be sufficient evidence of an imminent attack following the 2007 Israeli raid on the alleged Syrian nuclear site.

The second major difficulty with computer network attacks as opposed to traditional kinetic attacks is the difficulty of attributing an attack to its original perpetrator. The length of time required to trace an attack makes questions of the necessity of force to repel a computer network attack difficult to satisfy. Questions of proportionality also arise in determining whether it would *ever* be proportionate to use armed force in response to a computer network attack.

This chapter examines these questions in light of current international law, the definition of armed attack and considers in what circumstances force may be used in self-defence against a computer network attack.

1. Armed Attack

Self-defence is a customary law right, inherent in the sovereignty of States, which has been codified for the most part by Article 51 of the U.N. Charter. The customary status of the right has been confirmed by the *Nicaragua (Merits)* case.[3] Article 51 of the Charter allows self-defence in response to an "armed attack" (in French "aggression armée"). The *Nicaragua (Merits)* and *Oil Platforms* decisions confirm that nothing short of an armed attack (with the possible exception of an anticipated armed attack) will trigger the right of self-defence under international law.[4] The *Oil Platforms* case also established that the State using force in self-defence must prove that it has been subjected to an armed attack.[5] However, as with the term 'force', the United Nations Charter has not provided a definition of 'armed attack'. Further, the term was not referred to in the Kellogg-Briand Pact or in the Covenant of the League of Nations, both of which conventions used the term aggression as the opposite of self-defence and hence all attempts at definition were focused on that term.[6] The drafting history of the Charter provides evidence that discussions took place on the difference between an attack and an armed attack (based on the fact that the United

---

[3] *Nicaragua (Merits)*, para 176.

[4] Ibid.; *Case Concerning Oil Platforms (Islamic Republic of Iran v United States of America)* (2003), International Court of Justice, para 51.

[5] *Oil Platforms Case*, para 57.

[6] Stanimir A. Alexandrov, *Self-Defense against the Use of Force in International Law* (Kluwer Law International, The Hague; London, 1996), 95.

States draft of May 11 contained both terms) and although no definitive conclusion was reached, the term was replaced by armed attack only.[7] Professor Ian Brownlie has pointed out that it is likely that the records of the San Francisco conference contain no definition of the phrase 'armed attack' because the term was considered "sufficiently clear" and "self evident".[8] That was certainly the case in the drafting of the North Atlantic Treaty as evidenced by the comments of the Foreign Relations Committee of the United States Senate which noted that the phrase "armed attack" in Article 5 "is ordinarily self evident" and "there is rarely, if ever, any doubt as to whether it has occurred or by whom it was launched".[9] However, since the decision of the Court in the *Nicaragua (Merits)* case, it is clear that an armed attack is a subset of the term 'force' in Article 2(4) and therefore those actions which have been discussed in the previous chapter as falling outside the ambit of the definition of armed force, will automatically fail to qualify as an armed attack. Conversely, not every use of force will meet the criteria of an armed attack, thus resulting in a gap between those actions which constitute a use of force, and those which are an armed attack.

The *Nicaragua (Merits)* decision does not provide any clarification of the definition of armed attack, merely stating that "[t]here appears now to be general agreement on the nature of the acts which can be treated as constituting armed attacks".[10] However the Court fails to reiterate what that agreement may be, merely citing an example as follows:[11]

> "In particular, it may be considered to be agreed that an armed attack must be understood as including not merely action by regular armed forces across an international border, but also 'the sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to' (inter alia) an actual armed attack conducted by regular forces, 'or its substantial involvement therein'. This description, contained in Article 3, paragraph (g), of the Definition of Aggression

---

[7] Foreign Relations of the United States 1945 (Washington, 1967) Vol 1, 674, as cited in Ibid., 98.

[8] Brownlie, *Use of Force by States*, 278.

[9] Report of the Senate Committee on Foreign Relations in the North Atlantic Treaty, June 6, 1949, cited in Alexandrov, *Self-Defense*, 96.

[10] *Nicaragua (Merits)*, para 195.

[11] Ibid.

annexed to General Assembly resolution 3314 (XXIX), may be taken to reflect customary international law."

The Court goes on to consider which actions do not constitute an armed attack, but fall within the gap between acts constituting a use of force and the threshold for an act to qualify as an armed attack.

> "But the Court does not believe that the concept of 'armed attack' includes not only acts by armed bands where such acts occur on a significant scale but also assistance to rebels in the form of the provision of weapons or logistical or other support. Such assistance may be regarded as a threat or use of force, or amount to intervention in the internal or external affairs of other States."[12]

> "As stated above, the Court is unable to consider that, in customary international law, the provision of arms to the opposition in another State constitutes an armed attack on that State."[13]

Thus it would appear that under current international law the definition of 'armed attack', as held by the majority of the Court in *Nicaragua (Merits)*, is still dependent on the "scale and effects" of an attack which must be sufficient to elevate such actions beyond "mere frontier incidents".[14] This view that an armed attack must be of "relatively large scale and with substantial effect", is reiterated by several leading scholars,[15] and is in agreement with the *de minimis* rule for small scale attacks set out in Article 2 of the Definition of Aggression adopted by the UN General Assembly, the example given by the Court in the *Nicaragua (Merits)* case.[16]

---

[12] Ibid. This position was strongly criticised by Judges Schwebel and Jennings in their dissenting opinions, Schwebel holding that the term substantial involvement in the *Definition of Aggression* meant that an armed attack could include financial and logistical support.

[13] Ibid., para 231.

[14] Ibid., para 195.

[15] See for example Albrecht Randelzhofer, 'Article 51' in B Simma (ed) *The Charter of the United Nations: A Commentary* (2nd ed, Oxford University Press, Oxford, 2002) 788, 796. (with accompanying citations).

[16] The Security Council may determine whether actions falling under the examples given in Article 3 do not constitute 'acts of aggression' owing to their lack of gravity. *Definition of Aggression*, Article 2, as cited in Ibid.

Yoram Dinstein argues that the existence of the gap conveys that the use of force must be of sufficient gravity before armed attack is in progress, no matter that it be of small magnitude.[17]

As stated above, the Court confirmed that armed attack is a narrower term than force, stating that it is necessary to distinguish "the most grave forms of the use of force (those constituting an armed attack) from other less grave forms".[18] The resultant gap between force and armed attack results in the peculiar situation where an illegal use of force not tantamount to an armed attack may be launched by one State against another, leaving the victim State unable to respond in self-defence. Logically and pragmatically the gap has to be quite narrow, inasmuch as "there is very little effective protection against States violating the prohibition on the use of force, as long as they do not resort to an armed attack".[19] Michael Schmitt has commented that this distinction makes sense in light of the Charter's central purpose to 'maintain international peace and security', and argues that this creates a rebuttable presumption against the resort by States to violence.[20] "Thus it is logical to interpret the prohibition on the use of force expansively, but characterise exceptions that lie outside the community decisional architecture, such as self-defense, narrowly".[21] Other commentators have argued however that it makes no logical sense to prohibit a State from forcibly defending itself or permitting its allies to come to the State's defence where it is the subject of an unlawful use of force.[22] Any fears of an unwarranted escalation of an incident can be dealt with under the existing rules pertaining to proportionality.[23] Despite such debate, following the *Nicaragua (Merits)* and *Oil Platforms* cases it is now established in international law that a gap exists in the laws relating to armed force and armed attack. However, the thresholds

---

[17] Dinstein, 'CNA and Self-Defense', 100.

[18] *Nicaragua (Merits)*, para 191.

[19] Dinstein, 'CNA and Self-Defense', 100. Randelzhofer, 'Article 51', 661, 664.

[20] Michael N. Schmitt, Bellum Americanum Revisited: US Security Strategy and the Jus Ad Bellum (28 February 2003), transcript available in 176 *Mil L Rev* 364-421.

[21] Ibid.

[22] See for example John Hargrove, 'The Nicaragua Judgment and the Future of the Law of Force and Self-Defense' (1987) 81 *AJIL* 135, 141.

[23] See for example Rosalyn Higgins, *Problems and Process: International Law and How We Use It* (Clarendon Press, Oxford, 1993), 242.

of each of these concepts, and the responses which each allows are yet to be established with any certainty.

This uncertainty makes the classification of any computer network attack particularly difficult. As noted previously, the possible effects of computer network attacks "span the spectrum of consequentiality",[24] thus making classification based on the type of computer network attack impossible. It seems certain however that where a computer network attack causes destruction and fatalities on a par with a conventional attack, a State will have a right to respond in self-defence. This is the conclusion reached in a report by the Office of General Counsel of the U.S. Department of Defence which concluded:[25]

> "[I]f a coordinated computer network attack shuts down a nation's air traffic control system along with its banking and financial systems and public utilities, and opens the floodgates of several dams resulting in general flooding that causes widespread civilian deaths and property damage, it may well be that no-one would challenge a victim nation if it concluded that it was the victim of an armed attack, or of an act equivalent to an armed attack."

However the report fails to separate and analyse the attack in its component parts, combining those components which directly cause death and destruction with less severe attacks. Schmitt focuses on the consequences of the attack rather than on the object of the attack or on the intentions of the attacker; the exception being where the intentions of the attacker are specifically to cause physical damage to tangible objects or injury to human beings, in which case Schmitt considers the resort to armed force is permitted.[26] He argues that self-defence should be limited to operations which are de-facto armed attacks, or imminently preparatory thereto; the net result being a limitation on both sides to resort to CNA techniques which might threaten global stability and on individual responses which might themselves prove destabilizing.[27]

---

[24] Schmitt, 'Normative Framework', 912.

[25] Office of General Counsel, *An Assessment on International Legal Issues in Information Operations*, United States Department of Defense (1999) <http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf> (last accessed 30 January 2007).

[26] Schmitt, 'Normative Framework', 928.

[27] Ibid., 886. This is accord with his generally contextualist analysis discussed in Chapter 2, *infra*.

In contrast, Walter Sharp, one of the early authors on the subject, argues that any intrusion into systems containing information which is critical to the national security of the victim State should be considered an armed attack capable of triggering the right to respond with force.[28] However Sharp's view has not been borne out by state practice which to date has recognised such intrusions as simple espionage, an act which is not prohibited under international law.

Another approach to self-defence is Yoram Dinstein's concept of 'interceptive' self-defence.[29] While Dinstein rejects the notion of anticipatory self-defence,[30] he incorporates actions taken in advance of an actual attack by moving the timing of the beginning of the attack. Dinstein argues that the beginning of an armed attack is not linked to the first shot but rather to the moment of irrevocable commitment to the attack. Once the die has been cast, the armed attack can be said to have commenced and the victim state need not "wait impotently for the inescapable blow".[31] This concept has echoes in the 'target locking' arguments of some States in respect of modern precision-guided missiles. For example, the U.S. argues that an armed attack begins when the radar guiding the missile is locked on and ready to fire, and the rules of engagement of their armed forces reflect this approach.[32] While Dinstein's approach may prove a useful halfway house between traditional self-defence analyses and anticipatory self-defence for kinetic attacks, given the immediate nature of computer network attacks and the fact that an attack can be launched in seconds, it does not seem useful in assessing individual computer network attacks as armed attacks in their own right. Where a computer network attack is launched in conjunction with a traditional attack, the concept may prove more useful. For example, had the 2007 Israeli intrusion into the Syrian air defence radar system been detected, would such an intrusion be sufficient to trigger the right of self-defence, or would Syria need to wait until the system was actually being manipulated in preparation for an air strike? As Micheal Schmitt notes, the question is does the

---

[28] Sharp, *Cyberspace and the Use of Force*, 129.

[29] Dinstein, *War, Aggression, and Self-Defense*, 187.

[30] See section 1.1 *infra* on anticipatory self-defence.

[31] Dinstein, 'CNA and Self-Defense', 111.

[32] Gray, *Use of Force*, 108, n148. For example, in 1998 U.S. aircraft in the no-fly zone over Iraq fired at a missile battery when its radar had locked on to the planes patrolling the zone. Although there was controversy over whether the radar had locked on, the idea that the armed attack had started when the radar locked on was apparently accepted by Iraq and other States: Keesings (1998) 42368.

CNA appear merely preparatory, or is it more likely an irreversible step in the final chain of events.[33]

Michael Schmitt has proposed a three-prong test for determining when a State may respond forcefully in self-defence to a computer network attack (CNA) that does not in and of itself constitute an armed attack:[34]

> 1) The CNA is part of an overall operation culminating in armed attack;
>
> 2) The CNA is an irrevocable step in an imminent (near-term) and probably unavoidable attack; and
>
> 3) The defender is reacting in advance of the attack itself during the last possible window of opportunity available to effectively counter the attack.

Schmitt is careful to point out however that the self-defence is not in response to the computer network attack but rather the attack as a whole, including the computer network attack component. The wording used by Schmitt of the 'last possible window of opportunity' is similar to Yoram Dinstein's reinterpretation of the beginning of an attack as the attacker "embarks upon an irreversible course of action, thereby crossing the legal Rubicon".[35]

1.1. Anticipatory Self-Defence

It is likely that computer network attacks will be used in conjunction with, or as an prelude to, a traditional armed attack. Such attacks designed to 'prepare the battle space' can come in a myriad of forms, including the disablement of intelligence gathering sensors such as satellites and radar posts via computer network attack, disruption of military communications networks leaving units isolated and unable to be scrambled, or on the civilian level, disablement of emergency response networks

---

[33] Schmitt, 'Normative Framework', 932.

[34] Ibid., 933. See also, n130 noting that Michael Walzer has suggested a similar line of reasoning: "The line between legitimate and illegitimate first strikes is not going to be drawn at the point of imminent attack but at the point of sufficient threat. That phrase is necessarily vague. I mean it to cover three things: a manifest intent to injure, a degree of active preparation that makes that intent a positive danger, and a general situation in which waiting, or doing anything other than fighting, greatly magnifies the risk." Michael Walzer, *Just and Unjust Wars: A Moral Argument with Historical Illustrations* (2nd ed, Basic Books, New York, 1992), 81.

[35] Dinstein, *War, Aggression, and Self-Defense*, 172. Although as noted, Dinstein does not advocate anticipatory self-defence, he argues for "interceptive" self-defence, distinguished by the requirement that the attacker has committed itself to an attack in an irrevocable way.

may be launched in anticipation of more traditional kinetic action to follow. It is certainly clear that States are considering how a combination of electronic and traditional attacks might be used in the future. For example, the U.S. actively looked for computer network solutions prior to the 2003 invasion of Iraq, and China is openly looking for an 'assassin's mace' to address the perceived asymmetry of the Chinese military against the U.S. in conventional conflicts, widely believed to incorporate computer network attacks.[36] As Robertson points out, in modern warfare the electronic battlefield will play a crucial role, and any steps that a prospective attacker can take to neutralise or destroy its enemy's command and control, intelligence, communications, or weapons-control networks prior to a traditional attack would gain an enormous advantage.[37] This advantage was seen in the 2007 Israeli attack on the suspected Syrian nuclear site where the air defence radar did not detect the attacking planes until they were disappearing back over the border.[38] While such attacks may not be sufficient to amount to an armed attack in and of themselves, as preparatory moves in a conventional attack, they may be sufficient to justify the use of force under the doctrine of anticipatory self-defence.

1.1.1. Doctrinal Debate and Imminent Attacks

Anticipatory self-defence is one of the most contentious legal doctrines regarding the use of force. There is no consensus in international legal doctrine over the point in time from which measures of self-defence against an armed attack may be taken.[39] The debate centres on whether anticipatory self-defence survived the implementation of Article 51 of the UN Charter which states that nothing in the Charter "shall impair the inherent right of individual or collective self-defence if an armed attack occurs". Those arguing for a restrictive interpretation of the clause interpret this to mean that the right of self-defence is now only available to member States who are the object of an actual armed attack. Gray, Kelsen and Brownlie are some of the leading proponents of this view which is based on the premise that the Charter forbids any

---

[36] David A. Fulghum, 'Frustrations and Backlogs' (2003) 158(10) *Aviation Week & Space Technology* 10 March 2003 33. According to reports these attempts were never put into action due to the interconnectedness of the target systems with foreign owned networks.

[37] Robertson, 'Self-Defense against CNA', 139.

[38] See Fulghum, Wall and Butler, 'Israel Shows Electronic Prowess'.

[39] Randelzhofer, 'Article 51', 803.

use of force on the part of individual members except for the right of self-defence against an armed attack.[40]

Those arguing for a more expansive approach point out that Article 51 specifically reserves the 'inherent right' of self-defence, and the customary right includes the right to respond to an imminent armed attack.[41] Although ultimately disagreeing with the position, Bothe points out that many authors acknowledge that a threat may be so direct and overwhelming that it is just not feasible to require the victim to wait to act in self-defence until the act has actually started.[42] The standard to be applied was set out by U.S. Secretary of State Daniel Webster in his letter regarding the *Caroline* case that the right of self-defence only arises where there is "a necessity of self-defence, instant, overwhelming, leaving no choice of means, and no moment for deliberation".[43] As Greenwood notes, the *Caroline* test was applied by the international military tribunals at Nuremburg and Tokyo, suggesting that a right of anticipatory self-defence against imminent attacks was part of the customary law right preserved by Article 51 of the Charter.[44] The preservation of an inherent right of self-defence and the existence of customary rights outside the Charter wording is also recognized by the Court in the *Nicaragua (Merits)* case which noted that the Charter does not contain all the rules pertaining to self-defence, notably a definition of armed attack and the requirement of necessity and proportionality in any response.[45] The Court expressly did not comment on the lawfulness of a response to

---

[40] Bowett, *Self-Defence*, 188. See also Brownlie, *Use of Force by States*, 275; Ian Brownlie, *International Law and the Use of Force by States: Revisited* (Europaeum, Oxford, 2001); Dinstein, *War, Aggression, and Self-Defense*, 183; Randelzhofer, 'Article 51', 803-804; Gray, *Use of Force*, 130.

[41] Authors subscribing to this expansive view include Bowett, *Self-Defence*, 187-192; Robert Y. Jennings and C. Arthur. H. Watts (eds), *Oppenheim's International Law* (9th ed, Longman, Harlow, 1992), 421; Thomas M. Franck, *Recourse to Force: State Action against Threats and Armed Attacks* (Cambridge University Press, Cambridge, 2002), 97; Christopher Greenwood, 'International Law and the Pre-Emptive Use of Force: Afganistan, Al-Qaida, and Iraq' (2003) 4 *San Diego Int'l LJ* 7.

[42] Michael Bothe, 'Terrorism and the Legality of Pre-Emptive Force' (2003) 14(2) *EJIL* 227, 231.

[43] In that incident, U.K. forces captured, fired and sent over the Niagara Falls a merchant vessel called the *Caroline* which was being used by Canadian rebels and their American forces in attacks against passing British Ships. At the time of the U.K. attack the ship was moored in an American port and two U.S. nationals were killed. One of the British officers, Lieutenant McLeod, was later arrested in the United States on charges of murder arising out of the incident. The British government, seeking McLeod's release, maintained that its forces had acted in self-defence, to which U.S. Secretary of State Daniel Webster replied in what has become the accepted statement of self-defence doctrine at the time. *The Caroline Case* (1837) 29 BFSP 1137-1138, 30 BFSP 195-196.

[44] Greenwood, 'Pre-Emptive Use of Force', 13.

[45] *Nicaragua (Merits)*, para 176.

an imminent armed attack as it was not required on the facts of the case.[46] This approach has been followed in the *Wall* and *Armed Activities* cases, with the ICJ avoiding the difficult questions of self-defence and expressly stating no view on anticipatory self-defence.[47] Two recent U.N. reports have not been so reluctant however. The 2004 report of the U.N. Secretary-General's High Level Panel concluded that there was an existing right of anticipatory self-defence against imminent attacks basing their conclusion on customary international law.[48] Likewise the Report of the Secretary-General the following year expresses the view that responses to imminent threats are fully covered by Article 51 of the Charter.[49]

1.1.2. State Practice

The content of any customary right of anticipatory self-defence must be examined in light of state practice since the inception of the Charter. While state practice is far from conclusive on the matter, two instances in particular tend to indicate that the doctrine has survived. The first is the Israeli-Arab war of 1967. Following escalating tensions between Syria and Israel, Egypt requested the removal of the U.N. emergency force from Egyptian territory, reinforced troops in the Sinai and dispatched troops to Jordon. Egyptian President Nasser also closed the Straits of Tiran to Israeli shipping (an act that Israel had previously made clear it would consider as an act of war) amid statements indicating his intention to eliminate Israel. In response to these actions Israel launched strikes against Egypt's airbases, completely destroying the Egyptian air force.[50] Although Israel initially justified its actions by claiming that it had been attacked first, it later stressed both the character of the Egyptian blockade as an act of war and the very dangerous situation that it found itself in immediately prior to the Israeli attack.[51] Gray rejects this incident as

---

[46] Ibid., para 194.

[47] *The Wall Case; Armed Activities Case*, para 143.

[48] United Nations, *A More Secure World: Our Shared Responsibility Report of the Secretary-General's High-Level Panel on Threats Challenges and Change*, United Nations, UN Doc. A/59/565 (2004) 63, para 188.

[49] UN Secretary General, *In Larger Freedom: Towards Development, Security and Human Rights for All*, United Nations, UN Doc. A/59/2005 (2005) para 124.

[50] For a full exposition of the facts of this incident see A. Mark Weisburd, *Use of Force: The Practice of States since World War II* (Pennsylvania State University Press, University Park, Pa., 1997), 135.

[51] Ibid., 137, citing (1967) UN Yearbook, 175, 195-196.

evidence of an acceptance of anticipatory self-defence stating that "whatever position is taken on the facts of the outbreak of the Six Day War, the point of importance here is that Israel did not claim to be acting in anticipatory self-defence".[52] However Franck notes that Israel's "words and actions clearly asserted a right of anticipatory self-defence against an imminent armed attack".[53] Franck comments:[54]

> "Most states, on the basis of the evidence available to them, did however conclude that such an armed attack was imminent, that Israel had reasonably surmised that it stood a better chance of survival if the attack were pre-empted, and that, therefore, in the circumstances, it had not acted unreasonably. This does not amount to an open-ended endorsement of a general right to anticipatory self-defense, but it does recognize that, in demonstrable circumstances of extreme necessity, anticipatory self-defense may be a legitimate exercise of a State's right to ensure its survival".

This accords with the decision of the International Court of Justice in the *Nuclear Weapons* case, which indirectly commented on the situation when the majority of judges were unable to conclude that the first-use of nuclear weapons would invariably be unlawful if the very existence of the State were threatened.[55]
In comparison, when Israel attacked and destroyed the Tuwaitha Research Centre and Osarik nuclear reactor near Baghdad, Iraq in 1981, the action was "strongly condemned" by the Security Council,[56] and in general States' reactions to the bombing were condemnatory of Israel. In most cases the reaction was based on a conclusion that Israel had failed to demonstrate that there was an imminent threat from Iraq and has thus failed to satisfy the *Caroline* requirements for anticipatory self-defence rather than a general dismissal of a right of anticipatory self-defence.[57] As Greenwood points out, the emphasis on this failure to demonstrate the existence of the imminent threat tends, if anything, to confirm the existence of a right of self-

---

[52] Gray, *Use of Force*, 131.

[53] Franck, *Recourse to Force*, 103.

[54] Ibid., 105.

[55] *Legality of the Use by a State of Nuclear Weapons in Armed Conflicts* (1996) ICJ 26, International Court of Justice, 265, para 105(262)E.

[56] SC Res 487, U.N. SCOR, 2288th Mtg, UN Doc. S/Res/487 (1981).

[57] Franck, *Recourse to Force*, 105.

defence in cases where such an imminent threat was shown to exist.[58] He goes on to cite Rosalyn Higgins who notes:[59]

> "[I]n a nuclear age, common sense cannot require one to interpret an ambiguous provision in a text in a way that requires a state passively to accept its fate before it can defend itself. And, even in the face of conventional warfare, this would also seem the only realistic interpretation of the contemporary right of self-defence. It is the potentially devastating consequences of prohibiting self-defence unless an armed attack has already occurred that leads one to prefer this interpretation – although it has to be said that , as a matter of simple construction of the words alone, another conclusion might be reached."

In assessing what will constitute an imminent attack, Greenwood argues that there are two additional factors which must be taken into account which did not exist at the time of the *Caroline* incident:[60]

> The first is the gravity of the threat. The threat posed by a nuclear weapon, or a biological or chemical weapon, if used against a city, is so horrific that it is in a different league from the threats posed (as in the *Caroline*) by cross-border raids conducted by men armed only with rifles. Where the threat is an attack by weapons of mass destruction, the risk imposed upon a State by waiting until that attack actually takes place compounded by the impossibility for that State to afford its population any effective protection once the attack has been launched, mean that such an attack can reasonably be treated as imminent in circumstances where an attack by conventional means would not be so regarded. The second consideration is the method of delivery of the threat. It is far more difficult to determine the time scale within which a threat of attack by terrorist means would materialize than it is with threats posed by, for example, regular armed forces. These would be material considerations in assessing whether, in any particular case, an attack should be treated as imminent.

It is the view of the present author that a right of self-defence against an imminent attack is established in international law. The impact of computer network attacks as imminent threats is discussed in section 1.1.4, *infra*.

---

[58] Greenwood, 'Pre-Emptive Use of Force', 14.

[59] Higgins, *Problems and Process*, 242.

[60] Greenwood, 'Pre-Emptive Use of Force', 16.

1.1.3. The 'Bush Doctrine' of Pre-Emptive Self-Defence

In recent years the United States has released two national security strategy documents containing a highly controversial attempt at enlarging the right to self-defence to include the use of force to pre-empt an attack which is merely threatened but not imminent. The 2002 National Security Strategy is a carefully worded attempt to extend the concept of anticipatory self-defence by redefining the concept of imminence so as to take into account the exigencies of modern terrorism: [61]

> Legal scholars and international jurists often conditioned the legitimacy of preemption on the existence of an imminent threat—most often a visible mobilization of armies, navies, and air forces preparing to attack.
>
> We must adapt the concept of imminent threat to the capabilities and objectives of today's adversaries.... The greater the threat, the greater is the risk of inaction— and the more compelling the case for taking anticipatory action to defend ourselves, even if uncertainty remains as to the time and place of the enemy's attack. To forestall or prevent such hostile acts by our adversaries, the United States will, if necessary, act preemptively.

The sentiments of the 2002 report are repeated in the National Security Strategy 2006.[62] While at first glance, this may appear to extrapolate logically based on the contingencies of modern weaponry, it compromises the basic premise of anticipatory self-defence laid down in the *Caroline* and the evidence of state practice which has evolved the doctrine since. Greenwood has noted, far from removing the requirement of imminence "...practice also shows that the right of anticipatory self-defence is confined to instances where the armed attack is imminent."[63] He goes on to state "In so far as talk of a doctrine of 'pre-emption' is intended to refer to a broader right of self-defence to respond to threats that might materialize at some time in the future,

---

[61] White House, *The National Security Strategy of the United States of America*, White House (2002) 15 <http://www.whitehouse.gov/nsc/nss.pdf> (last accessed 21 February 2004).

[62] White House, *National Security Strategy of the United States of America*, White House, (2006) 2330 August 2008). Although Gray notes the striking absence of any express reference to international law, the 2006 report does state that "the United States will, if necessary, act pre-emptively in exercising our inherent right of self-defense" most likely an implicit reference to Art. 51 of the Charter: Christine D. Gray, 'The Bush Doctrine Revisited: The 2006 National Security Strategy of the USA' (2006) 5(3) *Chinese Journal of International Law* 555, 561.

[63] Greenwood, 'Pre-Emptive Use of Force', 15.

such a doctrine has no basis in law."[64] Certainly state practice to date has not indicated widespread support for the doctrine and both U.N. reports on security have rejected any wider right of pre-emptive self-defence, indicating it is for the Security Council to take pre-emptive action.[65]

1.1.4. Computer Network Attacks and Anticipatory Self-Defence

There are two situations where anticipatory self-defence may be implicated in the information warfare context. First, where a computer network attack serves as an imminent threat of a conventional attack and secondly, where electronic activity indicates a severe computer network attack (which rises to the level of an armed attack) is imminent.

As with any assessment of an imminent attack the context of a computer network attack must be taken into account. Where a computer network attack is launched as a precursor to conventional attack, the target will be important. If an attack targets early warning systems, radar posts or satellite feeds, military communications, or emergency response systems it is more likely that a State will judge a traditional attack to be imminent. The Israeli attack against the Syrian air-defence network is a case in point. Had Syria become aware of the intrusion and manipulation of its air-defence radar prior to the attack, they would have been entitled to use force in response. The disruption of electrical power grids or financial systems on the other hand is unlikely to be sufficiently indicative of a subsequent conventional attack when viewed in isolation. Thus when Estonia was subject to distributed denial of service attacks against its banking, media and governmental sites, there were no realistic fears that this signalled the beginning of a traditional armed attack. The additional variables, such as positive attribution to a particular actor and possible motivation, are too many and too varied. However, when such attacks are viewed in conjunction with other contextual indicators, States may conclude that conventional attack is imminent.

---

[64] Ibid.

[65] United Nations, *A More Secure World*, para 189-192; UN Secretary General, *In Larger Freedom*, 125. See generally Gray, 'The Bush Doctrine Revisited: The 2006 National Security Strategy of the USA'; Christian M. Henderson, 'The 2006 National Security Strategy of the United States: The Pre-Emptive Use of Force and the Persistent Advocate' (2007) 15 *Tulsa J Comp & Int'l L* 1. for a discussion of international reaction to the 'Bush Doctrine.

The second instance where a computer network attack may be evidence of an imminent armed attack is the use of computer network intrusions to prepare an electronic battlespace. Viruses, worms, Trojan horses and other forms of malware routinely infect unprotected computers with malicious code which may corrupt data, cause a malfunction, record keystrokes, disable virus protection and collect other information such as passwords and other access codes, feeding them back to a remote attacker. One of the most common features of these types of malware is some form of backdoor payload which allows the attacker to access and control the computer at a later date. Such malware spreads and 'recruits' unprotected computers to vast networks of compromised computers called botnets,[66] which can be directed to send large amounts of traffic to particular IP addresses bringing them, and in some cases the transmission routes, to a standstill in a distributed denial of service attack. Botnets were utilised in the distributed denial of service attacks against Estonia in 2007.[67]

The inclusion of backdoor payloads in malware raises interesting questions with relation to anticipatory self-defence.[68] It is clear that a backdoor has no other purpose than to allow an intruder control over the infected computer (whether by direct intrusion or remote control) at a later date. A question which must then be addressed is whether a State has the right to respond in anticipatory self-defence against the perpetrators of a computer network attack with a backdoor payload. Although a backdoor can be used for attacks at any point until it is discovered and removed and such attacks may have far more serious consequences, including those which would qualify as an armed attack, in most cases, the later use is to send spam or launch distributed denial of service attacks causing inconvenience and causing only economic damage. Without further information about the purpose or target of any later attack, the mere creation of a backdoor by a State adversary is not indicative of the type or gravity of the attack to follow; indeed the creation of a backdoor may

---

[66] The largest botnet recorded to date is the Storm botnet with the most accurate estimates claiming up to 80,000 infected computers. Botnets are notoriously difficult to estimate and estimates for Storm have been up to 50 million infected computers. Analysts are agreed however that it has shrunk from its peak.

[67] Gadi Evron, 'Battling Botnets and Online Mobs' (2008) 9(1) *GLIA* 121, 124.

[68] A backdoor is a piece of code which opens a hidden or undocumented access point to the compromised computer or system.

merely be evidence of espionage.[69] Further, the existence of a backdoor would not meet the 'imminent' criteria, as the timescale for any subsequent attack is variable; the attack could be launched within days or years.

Other network intrusions may more indicative, but they will be highly dependent on the circumstances. It should be noted however, that the method of delivery of an attack means that there may be little warning of an impending computer network attack, one of Greenwood's additional factors to be considered when determining whether an attack is imminent.[70] However Greenwood's second factor, the gravity of threat, will depend on the individual threat; as pointed out in the previous chapter, one of the difficulties with assessing computer network attacks is that they span the 'spectrum of consequentiality'.[71] While a computer network attack against critical infrastructure such as electricity grids, dams and oil pipelines would be devastating to modern society, and may result in death and property damage, the gravity of the threat is not comparable to that posed by a nuclear, biological or chemical weapon. In this regard, with the very survival of the State not in question, it is unlikely that the threat would be assessed as imminent.

1.2. Pin Prick Attacks or Accumulation of Events Theory

Computer network attacks falling below the armed attack threshold may still trigger a forcible response by States. The likely strategy of computer network attacks is such that a single strike qualifying as an armed attack is less likely to be launched than a swarm of lesser attacks. In a short story written in 1998, John Arquilla has detailed what a sustained cyber attack might look like;[72] power blackouts, followed by weekly virus attacks of the magnitude of the recent Nimda, Slammer or Mydoom viruses, oil pipeline ruptures all launched within a matter of days of one another. While some of these attacks may cross the threshold of use of force, it is unlikely that any taken on their own would be considered an armed attack under current international law. An analogy may be drawn with cases of repeated cross border

---

[69] Backdoors have been found on computers allegedly compromised by Chinese hackers.

[70] Greenwood, 'Pre-Emptive Use of Force', 16.

[71] Schmitt, 'Normative Framework', 912.

[72] John Arquilla, 'The Great Cyberwar of 2002' (1998) *Wired Magazine* February 1998 <http://hotwired.wired.com/collections/future_of_war/6.02_cyberwar_20021.html> (last accessed 9 February 2002).

incursions. States have claimed a right to act in self-defence against the whole series of incursions as collectively amounting to an armed attack. This so-called 'pin-prick' or 'accumulation of events' theory has been unsuccessfully claimed in the past by several States, including the United Kingdom,[73] the United States,[74] South Africa and Israel,[75] to justify actions purportedly taken in self-defence. Although the Security Council has rejected claims by these States, it has done so on the grounds that such actions were disproportionate to the incursions and looked more like unlawful reprisals, rather than commenting on the doctrine of accumulation of events.

Likewise, the International Court of Justice has avoided discussing the question, although it appears willing to contemplate the possibility of an accumulation of events amounting to an armed attack. The Court in the *Nicaragua (Merits)* case commented with regard to the incursions by Nicaragua into the territory of Honduras and Costa Rica:[76]

> "Very little information is available to the Court as to the circumstances of these incursions or to their possible motivations, which renders it difficult to decide whether they may be treated for legal purposes as amounting, singly or collectively, to an 'armed attack' by Nicaragua on either or both States".

This statement would seem to indicate a willingness on the part of the Court to consider that a series of small attacks on a target may amount to an armed attack when viewed collectively. This is a view reiterated in both the *Oil Platforms* and

---

[73] In 1964 the Southern Arab Federation (SAF) which had military links with the United Kingdom, complained of an armed attack by the Yemen which consisted of a "series of aggressions"; invoking collective self defence at the SAF's request, the UK launched an air strike and destroyed a fort. The Security Council did not accept the reasoning and issued a statement condemning reprisals as incompatible with the principles and purposes of the UN". SC Res 188, 9 April 1964, as cited in Jean Combacau, 'The Exception of Self Defence in U.N Practice' in A Cassese (ed) *The Current Legal Regulation of the Use of Force* (Martinus Nijhoff, Dordrecht, 1986) 9-38, 27.

[74] The U.S. claimed it was acting in self defence against alleged attacks by North Vietnamese naval vessels in the Gulf of Tonkin. Letter of 17 Febuary 1979, S/13094 (SCOR, 36th Year) cited in Ibid., 17.

[75] The Security Council has rejected claims of self-defence by Israel made to justify incursions into neighbouring States to attack palestininian bases, when it attacked Jordan in 1966 (SC Res 228, 25 November 1966) & 1969 (SC Res 265, 1 April 1969), and Lebanon in 1969 (SC Res 270, 16 August 1969), 1970 (SC Res 279, 12 May 1970), 1972 (SC Res 313, 28 February 1972), 1973 (SC Res 332, 21 April 1973) & 1974 (SC Res 347, 24 April 1974). See Ibid.

[76] *Nicaragua (Merits)*, para 231. It should be noted that the Court found that there had not been an armed attack by Nicaragua based on additional circumstances.

Cameroon/Nigeria cases.[77] While not deciding on the point, the Court also appears to permit the concept of an armed attack through cumulative attacks. In both cases while the Court appeared to endorse the concept of a cumulative armed attack, it found that neither the United States nor Cameroon respectively had sufficiently proved the facts or imputability to the other party.[78] If this concept does find greater authority for a forcible response to an accumulation of events, this would obviously apply to computer network attacks as well.

However, not all attacks which are launched from multiple computers will necessitate a cumulative approach to qualify as an armed attack. A distributed denial of service attack of sufficient scale and effect to elevate it above a 'mere frontier incident' would be considered a single attack as the attack originates from a single controller using a master and slave configuration.[79] That is, although the attack appears to come from a series of computers, the compromised computers are receiving instructions from a single controlling 'master' which orders the compromised computers to launch attacks on victim sites.[80] This is merely the electronic equivalent of an attack using more than one soldier, or a wave of bombers in an air strike.

2. Attribution

One of the major problems with any computer network attack is the attribution of the attack to a particular actor. While the origin of some attacks becomes immediately evident, either because the attacker identifies themselves,[81] or because they precede traditional attacks that are easily attributed to a particular source,[82] other attacks will

---

[77] *Case Concerning the Land and Maritime Boundary between Cameroon and Nigeria (Cameroon v. Nigeria: Equatorial Guinea Invervening)* (2002) ICJ Reports, International Court of Justice, para 323; *Oil Platforms Case*, para 64.

[78] *Oil Platforms Case*, para 64.

[79] For a detailed description of Distributed Denial of service attacks, see Bennett Todd, *Distributed Denial of Service Attacks*, (2000) <http://www.linuxsecurity.com/resource_files/intrusion_detection/ddos-faq.html> (last accessed 29 January 2004).

[80] In traditional botnets this is generally through an Internet Relay Chat (IRC) Server. In newer peer-to-peer based botnets such as the Storm worm, the controller publishes commands at specific keys in the network to be found by infected machines, however the net result is the same.

[81] For example, the 'I Love You' virus source code contained the 'signature' of the author.

[82] For example, the Israeli attack on the Syrian air-defences in advance of an air strike.

be launched anonymously. Given the common use of botnets and the frequency of IP spoofing that takes place in computer network attacks,[83] it is difficult to state with any certainty that the entity which appears to be the perpetrator of the attack, is in fact the ultimate attacker.

IP spoofing can be used either to simply mask the origin of an attack, or in a deliberate attempt to place the blame for an attack on another party. An early example of the latter problem occured in 1999 when a denial of service attack was launched against the U.S. Department of Transport. The attack appeared to emanate from a server in Maryland run by followers of the Falon Gong movement; in fact the attack was designed to take down both the Maryland server and the Department of Transport network server leaving the Falon Gong bearing the blame. However the attackers had blundered and the attack was traced to a computer located at the address of China's Ministry of Public Security. No information is publicly available regarding the U.S. response to this attack, however in 2002 Richard Clarke, then White House technology advisor, stated before a Senate Judiciary subcommittee hearing on cyber terrorism that the government had never been able to prove to their satisfaction that a particular government was responsible for a specific unauthorized intrusion.[84]

The proliferation of botnets also makes attribution difficult. As the 2007 denial of service attacks against Estonia proved, it can be very difficult to differentiate between attacks which originate from a particular address and those which are merely utilising a compromised computer. Although some attacks against Estonia were traced to official IP addresses of the Russian authorities, Russia claimed that these computers had been compromised and were being manipulated from outside the Kremlin, a claim which most security analysts believe to be the case.[85]

Of course, problems of attribution aren't restricted to cyberspace. Armed attacks following more conventional patterns are often carried out anonymously, or responsibility is claimed by armed groups which appear unlikely to have the

---

[83] IP spoofing essentially forges the data identifying the sending computer in the header of a data packet so that it appears to originate from a different IP address, thus any response is sent to the forged computer.

[84] Jesse J Holland, 'Bush Advisor Warns Cyberterrorists', *Washington Post* (Washington D.C.), 13 February 2002, <http://www.washingtonpost.com/wp-dyn/articles/A6846-2002Feb13.htm> (last accessed 30 September 2002).

[85] See for example Evron, 'Battling Botnets'.

resources required for such an attack. Further, in the case of state-sponsored terrorism, it is unlikely that any State will step forward to take responsibility for kinetic acts let alone electronic ones. Those factors aside, a victim State must still establish a link between the attacking group and the sponsoring State, the same approach must be taken with electronic attacks.[86] This may be particularly difficult to prove where attacks are launched by groups or loose affiliations of individuals in conjunction with traditional State action. For example, when Russia moved troops into South Ossetia following the Georgian offensive in 2008, the air strikes and ground forces were accompanied by a series of computer network attacks against Georgian servers. While these attacks were certainly not serious enough to amount to armed attacks due to Georgia's limited Internet connectivity, they illustrate the capacity for other actors to effectively 'join-in' a conflict with or without State authorisation. Several security analysts reported botnets alledgedly controlled by the Russian Business Network, a group known to be linked to cybercrime, launching denial of service attacks at Georgian servers. However denial of service attack software was also freely available for download to individual computers from Russian language website stopgeorgia.ru along with a list of targets, making joining the cyber offensive as simple as a few mouse clicks.[87] The Russian Government denies any involvement with the attacks,[88] however the issue raises the difficult question of state responsibility for non-state actors and the degree of state involvement or complicity required before force can be used in self-defence against the State. There is not sufficient space in this thesis to address the issue in depth, suffice it to note that there is little agreement in the international community on the issue in relation to conventional attacks,[89] let alone computer network attacks. However, a State must not knowingly allow its territory to be used as a sanctuary for

---

[86] Dinstein, 'CNA and Self-Defense', 112.

[87] John Markoff, 'Before the Gunfire, Cyberattacks', *New York Times* 13 August 2008, <http://www.nytimes.com/2008/08/13/technology/13cyber.html> (last accessed 26 August 2008); Evgeny Morozov, 'An Army of Ones and Zeroes: How I Became a Soldier in the Georgia-Russia Cyberwar' (2008) *Slate* 14 August 2008 <http://www.slate.com/id/2197514/> (last accessed 2 September 2008).

[88] Siobhan Gorman, 'Georgia States Computers Hit by Cyberattack', *Wall Street Journal* (New York), 12 August 2008, A9.

[89] For a discussion of legal attribution and state responsibility for non-state actors' use of force see generally Gray, *Use of Force*.

terrorists or armed bands bent on attacking military targets or civilian objects in another country.[90]

The difficulty of attribution also affects the victim State's ability to engage in forcible counter-measures in self-defence.[91] The Court in the *Oil Platforms* case held that the burden of proof rests on the State invoking the right of self-defence and that the United States had failed to prove that it had been subject to an armed attack by a particular State, *vis* Iran.[92] "[A victim State] must not rush headlong into hasty action predicated on reflexive impulses and unfounded suspicions; it has no choice but to withhold forcible response until hard evidence is collated and the state of affairs is clarified, lest the innocent be endangered".[93] Such hasty reactions could lead to the escalation of hostilities, something the ban on force was intended to prevent. However, the necessity of waiting for hard evidence of responsibility also opens the possibility that any action taken against a perpetrator once responsibility has been confirmed will be classified as an armed reprisal rather than an action taken in self-defence. Armed reprisals are prohibited under international law.[94]

3. Necessity & Proportionality

All responses to attacks, whether their means of delivery are kinetic or electronic, are subject to the underlying principles of proportionality and necessity. The International Court of Justice has repeatedly confirmed that the rule "whereby self-defence would warrant only measures which are proportional to the armed attack and necessary to respond to it" is well established in customary international law.[95] The principle of necessity in international law requires that any measures taken avowedly in self-defence must have been necessary for that purpose; the principle is strict and objective "leaving no room for any measure of discretion".[96] That is, it is

---

[90] Ian Brownlie, 'International Law and the Activities of Armed Bands' (1958) 7 *International and Comparative Law Quarterly* 712, 734. cited in Dinstein, *War, Aggression, and Self-Defense*, 206.

[91] Sharp, *Cyberspace and the Use of Force*, 133. cited in Dinstein, 'CNA and Self-Defense', 111.

[92] *Oil Platforms Case*, paras 57, 61.

[93] Dinstein, 'CNA and Self-Defense', 111.

[94] *Declaration on Principles of International Law Concerning Friendly Relations and Co-Operation among States in Accordance with the Charter of the United Nations, GA Res. 2625 (XXV).*

[95] *Nicaragua (Merits)*, paras 176 & 194; *Nuclear Weapons Case*, para 41; *Oil Platforms Case*, para 74.

[96] *Oil Platforms Case*, para 73.

not sufficient that force is used after an armed attack, it must be necessary to repel that attack,[97] and non-forcible remedies must either prove futile *in limine* or have in fact been exhausted in an unsatisfactory manner.[98] As Roberto Ago notes, "had [the State] been able to achieve the same result by measures not involving the use of armed force, it would have no justification for adopting conduct which contravened the general prohibition against the use of armed force".[99]

The principle of necessity also gives rise to a related principle, namely that actions taken in self-defence must generally be taken without undue delay.[100] Where a computer network attack has occurred for which there is no obvious perpetrator, the time taken to establish hard evidence of the identity of the perpetrator may militate against a finding that any subsequent action by the victim State is in self-defence. These criticisms were levelled at the United States of America after a delay of several weeks between the September 11 attacks on the World Trade Centre and the Pentagon and subsequent action in Afghanistan.[101] Although dismissing a claim of self-defence on other grounds, the decision of the Court in the *Nicaragua (Merits)* case also criticised the United States for commencing activities purportedly in self-defence several months after the major offensive of the opposition against the Government of El Salvador had been completely repulsed.[102] However, Dinstein notes that this requirement must not be construed too strictly; he points to the delay of approximately five months between the invasion of Kuwait and the authorisation of all necessary means by the Security Council.[103]

The principle of proportionality requires the weighing of the response against its permitted purpose of halting and repelling the attack, or in the case of anticipatory self-defence, preventing it from happening. Individual analysis of the principle will be dependant on the facts of the circumstances, however the action must not be retaliatory or punitive, its lawfulness cannot be measured "except by its capacity for

---

[97] Greenwood, 'Pre-Emptive Use of Force', 23.

[98] Dinstein, 'CNA and Self-Defense', 109.

[99] Roberto Ago, 'Addendum to the Eighth Report on State Responsibilty' (1980) II *UNYB Int'l L Comm'n* 13, 69 para 120.

[100] Ibid., 69; Dinstein, *War, Aggression, and Self-Defense*, 210.

[101] For a discussion on the weakness of this argument, see Greenwood, 'Pre-Emptive Use of Force', 23.

[102] *Nicaragua (Merits)*, 237.

[103] Dinstein, *War, Aggression, and Self-Defense*, 210.

achieving the desired result".[104] This raises the question of whether it will ever be proportionate to use traditional armed force against an electronic attack. The answer must surely be yes. Proportionality does not restrict the defending State to the same weapons or the same numbers of armed forces as the attacking State; nor is it necessarily limited to action on its own territory.[105] Therefore it would be open to the victim of an electronic attack to use whatever weapons it has at its disposal to repel an electronic attack, as long as the response is proportionate to the threat posed. As Ago notes:[106]

> In the case of self-defence, it was essential to avoid the error of thinking that there should be some proportionality between the action of the aggressor and the action of the state defending itself. Proportionality could be judged only in terms of the objective of the action, which was to repel an attack and prevent it from succeeding. No limitations that might prejudice the success of a response to attack could be placed on the State suffering the attack. The concept of reasonable action must of course enter into the matter, since self-defence could not justify a genuine act of aggression committed in response to an armed attack of limited proportions.

Thus, where a computer network attack is used to prepare the battlespace for a kinetic attack, the use of military force would be proportionate to the threat posed by the attack as a whole. However it should be noted that while physically bombing the attacking computers and their owners may be legal, it is not necessarily the preferred method of response.[107] Only a few examples of State intrusion have been made public to date, and no large scale attacks as would justify a forcible response have been reported. Further, state practice in response to electronic probes emanating from other States have not resulted in forcible responses.[108]

---

[104] Ago, 'Addendum', 69 para 121.

[105] Gray, *Use of Force*, 121.

[106] Roberto Ago, 'State Responsibility' (1980) Vol 1 *UNYB Int'l L Comm'n* 188, para 25.

[107] Eric Talbot Jensen, 'Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense' (2002) 38 *Stan J Int'l L* 207, 230.

[108] To date the only forcible response to an attack on a communications network is the street fighting in Lebanon as a result of the cutting of an Hezbollah telecommunications network. The response was condemned by States. However given the non-international nature of the dispute it does not provide any useful indication of state practice in this regard. See generally 'Hezbollah Takes over West Beirut', *BBC News* 9 May 2008, <http://news.bbc.co.uk/1/hi/world/middle_east/7391600.stm> (last accessed 10 May 2008).

Eric Jensen has cited technological solutions designed with a "hack back" feature to trace an attack and reflect similar damage to the sender, or causing some other responsive action.[109] Although much of the available technology is classified, one of the major difficulties to overcome with any automated response is the correct attribution of the attack prior to launching any destructive payload. As seen above, the attack on the U.S. Department of Transport that was attributed to the Falon Gong originated elsewhere, and routing attacks through other actors may serve as a political end in itself.

4. Counter-Measures against Unlawful Acts

Where a computer network attack does not rise to the level of an armed attack a State may still respond with proportionate counter-measures. Where forcible counter-measures are taken in response to an ordinary breach of international law, not constituting an armed attack, they are unlawful.[110] However the International Court of Justice's treatment of the hostile acts taken by Nicaragua against El Salvador and the Republics of Honduras and Costa Rica in *Nicaragua (Merits)* case has muddied the waters somewhat for acts which amount to less grave forms of "illegal military intervention".[111] The Court held that that "proportionate counter-measures" were permissible by the victim State (but not by any third State acting collectively in self-defence).[112] The Court did not venture an opinion as to what form these counter-measures might take, or whether they could include the use of force.
John Hargrove has suggested that either the Court was saying "(a) that there are some acts of force that nobody, not even the victim, may resist by proportionate measures of force; or it was saying (b) that the victim may resist with force provided that it does so alone. There is little to be said in explanation of the latter proposition other than it is simply a second arbitrary announcement of the Court."[113] Hargrove argues that allowing forcible counter-measures "would in one remarkable stroke

---

[109] Jensen, 'Computer Attacks', 231.

[110] Dinstein, *War, Aggression, and Self-Defense*, 226.

[111] The Court held that Nicaragua did supply aid to rebels in the territories of El Salvador, but insufficient evidence of the nature, scale and continuance of such aid. The Court further held that Nicaragua was responsible for certain transborder military incursions into Honduras and Costa Rica. *Nicaragua (Merits)*, paras 152, 164.

[112] Ibid., para 249.

[113] Hargrove, 'Nicaragua Judgement', 141.

manage both to impair the right of self-defense, and to weaken fundamentally the prohibition on the use of force by creating an open-ended and wholly new category of exceptions to Article 2(4) of the Charter, of unknown content and limit."[114] However, Judge Simma in his separate opinion in the *Oil Platforms* case has commented that the Court in the *Nicaragua (Merits)* case cannot, in the context of that case, have understood that to mean mere pacific reprisals.[115] He argues that the Court can only have meant "defensive military action 'short of' full-scale self-defence".[116]

> But we may encounter also a lower level of hostile military action, not reaching the threshold of an "armed attack" within the meaning of Article 51 of the United Nations Charter. Against such hostile acts, a State may of course defend itself, but only within a more limited range and quality of responses (the main difference being that the possibility of collective self-defence does not arise, cf. *Nicaragua*) and bound to necessity, proportionality and immediacy in time in a particularly strict way.

In the *Case Concerning the Gabcikovo-Nagymaros Project*, the International Court of Justice set out a three part test justifying proportionate counter-measures. First the action must be taken in response to an internationally wrongful act of another State and be directed against that State. Second the victim state must have called upon the offending state to discontinue its wrongful conduct or to make reparation for it. And finally the effects of the counter-measure must be commensurate with the injury suffered, taking account of the rights in question.[117] In this regard the test for proportionality differs between counter-measures and self-defence, where the response must be proportional to the threat, rather than the actual harm suffered. However the Court also stated that the purpose of the counter-measures must be to induce the wrongdoing State to comply with its obligations under international law, and that the measure must therefore be reversible.[118] In respect of a computer

---

[114] Ibid., 142.

[115] *Oil Platforms Case*, (per Judge Simma), para 12.

[116] Ibid., per Judge Simma, paras 12-13.

[117] *Case Concerning the Gabcikovo-Nagymoros Project* (1997) ICJ Reports 3, International Court of Justice, para 85.

[118] Ibid., para 87.

network attack this would seem to fit with current state practice, most attacks to date have merely resulted in States requesting the alleged perpetrator of the attack to cease their actions.[119] However the nature of computer network attacks, including the type of attacks they make possible, and most importantly their ability to be reversed, makes computer network attacks particularly useful as a counter-measure against a previous wrongful act of a State. For example, a series of blackouts in response to an internationally wrongful act may be a useful coercive measure.

The 1998 Zapatista 'Floodnet' attacks on the Pentagon's website by the Electronic Disturbance Theatre also provide a model for how electronic counter-measures might work against non-state actors. U.S. Department of Defence specialists created a program that would recognise the Floodnet applet installed on computers trying to access the Department of Defence website. Once the applet was identified, a program was sent back to the activist's computer to shut down their web browser, thus ending the attack.[120] Although criticisms were levelled at the Department for not thoroughly considering the legal ramifications of such a response,[121] the United States decision to respond electronically in this instance, against an attack which they had been expecting, must be considered a proportionate counter-measure, particularly against a demonstrably non-violent protest group.

The danger with such an approach against States is the risk of escalation of such counter-measures into forcible responses. A situation which the Security Council would be likely to determine a threat to international peace and security, as seen in the following section.

5. Threats to the Peace

The other exception to the general prohibition on the use of force in international law is the use of collective security measures. Under Chapter VII of the Charter the Security Council may recommend or authorise member States to engage in measures, including the use of force, to restore international peace and security. However, before the Security Council can recommend action, it must first determine

---

[119] Although it should be noted that in all reported cases to date the suspected perpetrator has denied any involvement with the attack.

[120] Friel, 'DoD Launches Internet Counterattack'.

[121] Seffers, 'Legalities Cloud Pentagon's Cyber Defence', 3.

under Article 39 that a threat to the peace, breach of the peace, or act of aggression exists.[122] In practice, the Council has almost exclusively exercised its powers by finding a 'threat to international peace and security', even in situations where a breach of the peace or act of aggression is obvious.[123] Whether or not there are limits on the Security Council's ability to determine a threat to the peace is the subject of debate amongst scholars,[124] however the range of situations where the Security Council has found a breach of the peace is large and includes the danger of violent counter-measures by States to violations of international law, regardless of their admissibility.[125] The Council has found threats to the peace in internal conflicts such as those in Liberia, Rwanda, Sierra Leone and East Timor;[126] violations of human rights and humanitarian law as in Somalia, Rwanda and Eastern Zaire;[127] violations of democratic principles in Haiti and Sierra Leone;[128] terrorism;[129] nuclear proliferation and even failure to co-operate with international prosecutions.[130] These examples illustrate the broad discretion that the Security Council has to determine that a threat to the peace exists; however Frowein has argued that this does not mean that the notion of a threat to the peace has become limitless. He argues that a threat to the peace exists when, in a particular situation, a danger of the use of force on a considerable scale arises.[131] Although the Security Council has not considered any

---

[122] Art. 39 reads "The Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security".

[123] Jochen Frowein, 'Article 39' in B Simma (ed) *The Charter of the United Nations: A Commentary* (2nd ed, Oxford University Press, Oxford, 2002) 717, 722.

[124] See generally Erika De Wet, *The Chapter VII Powers of the United Nations Security Council* (Hart, Oxford, 2004), 133-134.

[125] Frowein, 'Article 39', 722.

[126] See SC Res788, 19 November 1993 on Liberia; SC Res 918, 17 May 1994, SC Res 929, 22 June 1994 on Rwanda; SC Res 1132, 8 Oct 1997, 1289 7 Feb 2000, 1306 5 July 2000 on Sierra Leone; SC Res 1264, 15 September 1999 on East Timor.

[127] SC Res 794, 3 December 1992 on Somalia; SC Res 929, 22 June 1994 on Rwanda; SC Res 1078, 9 November 1996 on Zaire.

[128] For Haiti: SC Res 841, 16 June 1993; SC Res 917, 6 May 1994; SC Res 940, 31 July 1994 and most recently SC Res 1529, 29 February 2004. For Sierra Leone: SC Res 1132, 8 October 1997; SC Res 1270, 22 October 1999; SC Res 1289, 7 February 2000; SC Res 1306, 5 July 2000.

[129] For example, SC Res 1526, 30 January 2004.

[130] On nuclear proliferation: SC Res 1172, 6 June 1998; On Libya's failure to co-operate with prosecution of the Lockerbie bombers SC Res 748, 31 March 1992.

[131] Frowein, 'Article 39', 726.

computer network attacks to date,[132] based on this assessment it would appear that a computer network attack would constitute a threat to the peace where it is of sufficient gravity that a State is likely to respond to it with force regardless of its categorisation as an armed attack or not, or where the attack is of the type of attack which indicates further violence to follow, whether electronically or by kinetic means.

Once the Security Council has determined a threat to the peace, the Council may make recommendations, or require States to take action under Articles 40, 41 and 42 of the Charter, for the restoration or maintenance of international peace and security. Interestingly, once the Security Council has deemed a situation a threat to the peace, it 'is free to take measures against any entity which it considers to be an obstructive factor in the restoration of peace'.[133] Thus, having determined the situation in Angola in 1997 to be a threat to international peace and security, the Council then imposed sanctions on UNITA (Union for the Total Independence of Angola), a non-state entity.[134] This will be of particular significance in respect of computer network attacks which are launched by disaffected groups 'joining in' conflicts, although as outlined *supra*, positive attribution will always be a factor.

Under Article 41, the Security Council will decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures. These may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations.[135] This would also include the disruption of Internet access such as that demonstrated by the United States in response to the 1998 attack by the Electronic Disturbance Theatre and arguably would also encompass denial of service attacks launched against the media, banking and telecommunications infrastructure of a State.

---

[132] Georgia raised the issue of alleged Russian cyber attacks in the context of the 2008 conflict with Russia over South Ossetia, however the point was not taken up by the other members and no resolution was forthcoming. S/PV.5961, 19 August 2008. As noted previously, attribution of the attacks is far from certain.

[133] Dinstein, *War, Aggression, and Self-Defense*, 287.

[134] SC Res 1127, 1997, cited in Ibid.

[135] Art. 41, U.N. Charter.

Where non-forceful measures have been unsuccessful or if the Council determines that such measures would be inadequate, the Council may authorise action under Article 42 by such air, sea, or land forces as may be necessary to maintain or restore international peace and security. Examples include demonstrations, blockade, and other operations by air, sea, or land forces of Members of the United Nations.[136] It appears unlikely that the Security Council would find it necessary to authorise force against a computer network attack. As pointed out earlier, force is not necessarily the preferred means of countering a cyber attack because of the distributed nature of many methods of attack. However, it should be noted that the where an attack or ongoing series of attacks cannot be prevented or stopped by electronic means the Security Council would be able to authorise the use of force

6. Conclusion

As with the previous chapter relating to the use of force, the classification of computer network attacks as armed attacks, sits on top of a deep doctrinal divide between those who would argue for a wide interpretation of the right to self-defence and those who would restrict it. The present author believes that in regard to computer network attacks, a restrictive view of armed attack and the subsequent right to self-defence is preferable. Given that the accurate attribution of attacks is by no means certain and States acting in self-defence are not restricted to responding in kind, the danger of computer network attacks escalating into traditional conflict is apparent. That is not to say that States cannot respond to computer network attacks that do not rise to the level of an armed attack; a State may still respond with proportionate counter-measures or appeal to the Security Council for a finding that the attacks amount to a threat to the peace.

[136] Art. 42, U.N. Charter.

PART 2

Jus in Bello

Chapter 4 – The Applicability of the Laws of Armed Conflict to Computer Network Attacks

The laws of armed conflict apply to all situations of armed conflict, whether or not war is declared, and regardless of whether the parties involved recognise the state of armed conflict or indeed, the opposing force. The determination is deliberately, a factual rather than a legal one. None of the instruments relating to the laws of armed conflict deal with computer network attacks explicitly, therefore the question must be asked whether the laws of armed conflict should apply to computer network attacks at all, and if so, under what circumstances a computer network attack would be sufficient to trigger the application of those laws. As with much of the application of the law to computer network attacks, the advancement of technology into a qualitatively different type of weaponry (rather than merely a difference in scale), requires a re-examination of the terminology. The question of the applicability of the laws of armed conflict to computer network attacks arises in three distinct circumstances: First, where computer network attacks are used with traditional weapons in an ongoing conventional armed conflict; secondly, where computer network attack are launched on their own; and finally, where the use of conventional weapons is insufficient in and of itself to qualify as an armed conflict, but it is accompanied by extensive computer network attacks. In some circumstances, a computer network attack may also represent an opening salvo in a wider conflict, and might therefore indicate the beginning of the application of the laws of armed conflict. The existence or not of an armed conflict is of particular relevance as the outbreak of an armed conflict between two States will lead to many of the rules of the ordinary law of peace being superceded, as between the parties to the conflict, by the rules of humanitarian law.[1] For example the right to seize one another's property, use force against each other and detain nationals will become materially different.

[1] Christopher Greenwood, 'Scope of Application of Humanitarian Law' in D Fleck (ed) *The Handbook of Humanitarian Law in Armed Conflict* (Oxford University Press, Oxford, 1995) 39-63, 40.

1. Armed Conflict

The Geneva Conventions apply in full to "all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognised by one of them" or in "all cases of partial or total occupation of the territory of a High Contracting Party, even if the said occupation meets with no armed resistance".[2] The Conventions also apply to and in respect of any non-contracting party, where that party accepts and applies the provisions of the Conventions itself. Additional Protocol I references Common Article 2 of the Conventions, and states that it also applies to "armed conflicts in which peoples are fighting against colonial domination and alien occupation and against racist régimes in the exercise of their right of self-determination".[3] In relation to conflicts not of an international character, that is, internal armed conflicts, Common Article 3 of the Conventions and Article 1 of Additional Protocol II, both refer to the term 'armed conflict' as the trigger for the application of humanitarian law principles.[4]

The term 'armed conflict' is not defined anywhere in the Conventions. This was a deliberate attempt by the drafters of the Conventions to avoid the political and legal wrangling that had occurred over the legal definition of war, and the ensuing distinctions between a state of war, a police action, or any other form of hostile action.[5] The determination is intended to be factual rather than legal. Pictet's commentary to the Conventions takes a broad view stating that:[6]

> "Any difference arising between two states and leading to the intervention of armed forces is an armed conflict within the meaning of Article 2, even if one of the parties denies the existence of a state of war. It makes no difference how long the conflict lasts, or how much slaughter takes place."

---

[2] Common Art. 2, Geneva Conventions 1949.

[3] Art. 1, Additional Protocol I.

[4] Additional Protocol II contains additional criteria for its application including control of territory by an armed group under a responsible command, capable of sustained and concerted military operations and capable of implementing the protocol. For a full discussion of the application of the laws of armed conflict to internal armed conflicts see Lindsay Moir, *The Law of Internal Armed Conflict* (Cambridge University Press, New York, 2002).

[5] 'Article 2' in Jean S. Pictet, *The Geneva Conventions of 12 August 1949: Commentary* (International Committee of the Red Cross, Geneva, 1952), 32.

[6] Ibid.

Likewise the International Committee of the Red Cross (ICRC) takes an expansive view of armed conflict, maintaining that in the case of cross-border operations, the first shot suffices to trigger an international armed conflict:[7]

> "By using the words 'from the outset' the authors of the Convention wished to show that it became applicable as soon as the first acts of violence were committed, even if the armed struggle did not continue. Nor is it necessary for there to have been many victims. Mere frontier incidents may make the Convention applicable, for they may be the beginning of a more widespread conflict."

Given this apparent denial of a *de minimis* level of intervention, it would appear that computer network attacks could well come within the ambit of armed conflict. However this view is not universally held and the statement regarding the length and intensity of the conflict is not necessarily borne out by state practice. Christopher Greenwood notes that it is by no means clear that most States would regard an isolated incident or exchange of fire as an armed conflict, however serious the consequences, bringing into operation the full panoply of the Geneva Conventions.[8] While there are examples of relatively minor incidents where a State has claimed protection of the laws of armed conflict, there have been a number of border clashes and naval incidents, which have not been treated as armed conflicts.[9] For example, during the *Dogger Bank Incident* of 1904 the Russian Navy's North Sea fleet opened fire on British fishing trawlers believing them to be Japanese warships. The incident was closed by payment of compensation to the British government for the lives of the two men lost, the sinking of one trawler and injury and damage to other trawlers and crew.[10] On 8 June 1967, Israeli fighter jets and torpedo boats attacked the *USS Liberty*, in the eastern Mediterranean, killing thirty-four crew members and wounding 171 more. The officially accepted explanation for the attack has been that it was a tragic mistake, and the U.S. accepted an apology and compensation for the

---

[7] ICRC, 'Article 6', Commentary to Geneva Convention IV, 59.

[8] Christopher Greenwood, 'The Law of War (International Humanitarian Law)' in M D Evans (ed) *International Law* (Oxford University Press, Oxford, 2003) 789-821.

[9] Greenwood, 'Scope of Application of Humanitarian Law', 42.

[10] *Finding of the International Commission of Inquiry Organized under Article 9 of the Convention for the Pacific Settlement of International Disputes, of July 29, 1899 (the Dogger Bank Incident)* (1905) 2 AJIL 931-936, The International Commission of Inquiry between Great Britain and Russia arising out of the North Sea incident.

losses despite the controversy over the official findings.[11] Similarly in 1987 when the *USS Stark* was struck by missiles launched from an Iraqi fighter jet under a misapprehension that it was an Iranian tanker, the United States was prepared to accept an apology and compensation for the 37 lives lost and damage to the frigate.[12] In contrast, when a U.S. Navy pilot was shot down and captured by Syrian forces over Lebanon in 1983, the United States maintained that this incident amounted to an armed conflict and the pilot was thus entitled to prisoner of war status.[13] Reports from Syria also appeared to assume that this was the case.[14] Similarly, when U.S. helicopters fired on the Iranian vessel the *Iran Ajr* during a mine laying operation and forced its crew to abandon ship, the rescued sailors and the bodies of their less fortunate compatriots were swiftly repatriated. Although the status of those particular sailors was never publicly discussed between the United States and Iran, the ICRC delivered a note to the United States stating that "such situations and their consequences fell within the scope of the Geneva Conventions".[15]

A survey of these incidents, some of which led to extremely strained diplomatic relations, tends to suggest that States' willingness to classify events as an armed conflict appears to be based on the perceived intentions of the other party, an assessment which is often largely influenced by *realpolitik.* However, where prisoners have been taken, a willingness to extend the protections of the Conventions to captured personnel appears to be a major driver behind the classification of such incidents as armed conflicts.

---

[11] Several crew members and intelligence officials dispute the findings of the official inquiry stating that the attacks were deliberate. See generally, William D. Gerhard and Henry W. Millington, *Attack on a Sigint Collector, the U.S.S. Liberty*, National Security Agency (1981). For an article concluding the attack was deliberate see Walter L. Jacobsen, 'A Juridical Examination of the Israeli Attack on the USS Liberty' (1986) 36(Winter) *Naval Law Review* 69.

[12] Jim Hoagland, 'U.S., Iraq to Confer on Air War', *Washington Post* (Washington D.C.), 25 May 1987, 1.

[13] Although President Reagan later stated "I don't know how you have a prisoner of war when there is no declared war between nations. I don't think that makes you eligible for the Geneva Accords [sic]", it appears that this was simply an error on the President's part. 'President's News Conference on Foreign and Domestic Issues', *New York Times* 21 December 1983, A 22.

[14] Thomas L Friedman, 'Widened Cabinet Sought in Beirut', Ibid. 8 December 1983, 18; Thomas L Friedman, 'Syria Says Airman Seized in U.S. Raid Will Not Be Freed', *New York Times* 6 December 1983, A 1.

[15] ICRC, 'External Activities: September-October 1987' (1987) 27(261) *IRRC* 650. Note however that the ICRC did not make clear whether this determination was made by reference to the laws relating to neutral shipping or armed conflict.

1.1. Intervention of the Armed Forces

Pictet's commentary requires the intervention of the armed forces of a State as a precondition of armed conflict. This approach raises two problematic issues in respect of contemporary conflicts. First, in modern armed conflict, particularly in an age characterised by the civilianisation of the military and outsourcing of key defence functions, the armed forces of a State may not be the only actors engaged in its armed conflicts. The use of unmanned Predator drones by the United States Central Intelligence Agency in the ongoing war in Afghanistan is a case in point. For example, on 13 January 2006 the CIA ordered an air strike by a Predator drone that fired air-to-ground missiles at the Pakistani village of Damadola, close to the border with Afghanistan.[16] The air strike was targeting a high level Al-Qaeda leader, but failed to eliminate him; eighteen other people were killed in the attack. The United States military denied any involvement in the strike.[17] Although this attack took place in the context of an established and wider armed conflict, an attack such as this launched in peacetime would not fall within Pictet's definition, and illustrates the changing nature of the participants involved in contemporary armed conflicts. However, while it may not always be the armed forces of a State who conduct such activities, it is clear that some nexus with governmental authority will be required to instigate an international armed conflict.

The second issue with Pictet's requirement of the involvement of the armed forces is that military forces are often used against other States and groups for tasks other than an armed conflict – for example, aerial surveillance and reconnaissance.[18] Michael Schmitt thus contends that a dispute resulting in the commitment of armed forces cannot be the sole criterion for establishing an armed conflict. He argues that the reference to the armed forces is more logically understood as a form of prescriptive shorthand for activity of a particular nature and intensity.[19] That is, when a dispute

---

[16] Dafna Linzer and Griff Witte, 'U.S. Airstrike Targets Al Qaeda's Zawahiri', *Washington Post* (Washington D.C.), 14 January 2006, A A09 <http://www.washingtonpost.com/wp-dyn/content/article/2006/01/13/AR2006011302260_pf.html> (last accessed 16 September 2008).

[17] Ibid.

[18] Michael N. Schmitt, 'Wired Warfare: Computer Network Attack and the *Jus in Bello*' in M N Schmitt and B T O'Donnell (eds), *Computer Network Attack & International Law* (U.S. Naval War College, Newport, R.I, 2002) 187-218.

[19] Ibid., 372.

reaches the level that a State deems it necessary to involve the armed forces, it has reached a sufficient level to be considered an armed conflict.

Internal armed conflicts are even more problematic. Involvement of the armed forces of a State are not required for an internal armed conflict, however the identity of the parties involved determine which legal regime will apply. Although nothing in Common Article 3 defines internal armed conflicts in terms of the parties involved, Additional Protocol II is more selective. Internal conflicts between the armed forces of a State and dissident armed forces or organised armed groups may be covered by Additional Protocol II, conflicts between other government agencies and such groups do not qualify.[20] Louise Doswald-Beck comments that any computer network attack launched by a group, however well organised, is likely to be seen solely as criminal behaviour to be dealt with by agencies other than the military, even though the potential for damage could be enormous.[21] However, given the move to recognition of armed attacks by non-state actors the author considers that this position can no longer be supported.

The Appeals Chamber of the International Criminal Tribunal for the Former Yugoslavia in the *Tadic* case, considered the temporal and geographical scope of the term armed conflict, holding that:[22]

> "an armed conflict exists wherever there is resort to armed force between states or protracted armed violence between government authorities and organised armed groups or between such groups with a state. International humanitarian law applies from the initiation of such armed conflicts and extends beyond the cessation of hostilities until a general conclusion of peace is reached; or, in the case of internal conflicts, a peaceful settlement is achieved. Until that moment, international humanitarian law continues to apply in the whole territory of the warring states or,

---

[20] An explanatory note inserted into the Report of Committee I describes 'armed forces' as: "All the armed forces.... According to the views expressed by a number of delegations, the expression would not include other government agencies the members of which may be armed; examples of such agencies are the police, customs and other similar organisations". According to Moir this leaves grey areas in the protocol. For a discussion of armed forces in internal conflict, see Moir, *The Law of Internal Armed Conflict*, 38-40, 104-105.

[21] Louise Doswald-Beck, 'Some Thoughts on Computer Network Attack and the International Law of Armed Conflict' in M N Schmitt and B T O'Donnell (eds), *Computer Network Attack and International Law* (Naval War College, Newport, RI, 2002) 163-186, 165.

[22] *Prosecutor v Dusko Tadic* (1995) Case No. IT-94-1-AR, International Criminal Tribunal for the Former Yugoslavia, Appeals Chamber, para 70.

in the case of internal conflicts, the whole territory under the control of a party, whether or not actual combat takes place".

This definition does not address the nature of the parties involved in an international armed conflict, leaving open the possibility that institutions other than armed forces may be involved. Internal armed conflicts reflect the breadth of parties covered by Common Article 3 of the Conventions.

1.2. The Requirement of Armed Force

Although Pictet's definition of armed conflict refers only to a 'difference' between States, the test in *Tadic* shows that armed force or armed violence is the requirement for armed conflict.[23] The refinement of the test by the Tribunal also separates the level of violence required for international and internal armed conflict by requiring a level of protraction of the violence in conflicts not of an international nature. This is in keeping with the requirements set out in Common Article 3 and Article 1 of Additional Protocol II that the laws of armed conflict are not to apply to internal disturbances and tensions, such as riots, isolated and sporadic acts of violence and other acts of a similar nature. Both internal and international armed conflicts however, require the use of armed force. As with the term armed attack, armed force is not defined in international law (its definition undoubtedly being considered self-evident). However, as discussed in Chapter 2 *supra*, armed force is to be construed somewhat broadly, in particular the term includes indirect forms of support for the application of force. Thus where a computer network attack, directly or indirectly, results in injury or death, or destruction of physical property, it will constitute a use of armed force. Whether a computer network attack can amount to a use of armed force will be a factual determination, likely to be established over time by state practice, however a survey of the current thinking shows that it is likely that a certain level of physical damage will also be required.

[23] It should be noted that there was no question in the *Tadic* case of whether there had been such force or violence used against the people of the former Yugoslavia, the case addressed the question of the international or internal nature of the armed conflict that took place in the Balkans.

2. Application to Computer Network Attacks

A number of authors have discussed the applicability of the laws of armed conflict to computer network attacks. Mark Shulman has no difficulty in finding that "[a]s with other armed conflict, defensive [information warfare] operations are subject to the restraints of LOAC and its principle of proportionality", despite observing that "information warfare is neither 'armed' in the traditional sense, nor does it necessarily involve 'conflict'.[24] Other writers however are less sure of the application of the laws of armed conflict. Richard Aldrich claims that a physical manifestation such as an explosion is required.[25]

> "'Armed conflict', as presently understood, seems far less likely to be applied to the simple manipulation of bits inside a computer, although this may soon change since the nefarious manipulation of bits could, in some cases, already cause significantly more harm than could a bomb".

Emily Haslam has analysed the approaches of Shulman and Aldrich and concludes that while it is welcome that the authors do not treat computer network attacks and other information operations homogenously, they fail to establish a test which either works within the framework of the laws of armed conflict, or sets out the appropriate components of information warfare which should be taken into account (means and results respectively).[26] Other authors have addressed the issue in different ways; for example, after a flawed analysis equating armed conflict to the definition of aggression and using the terms armed force and armed attack synonymously, Hanseman concludes that the laws of armed conflict will apply to computer network attacks where the "consequences of the attack are equivalent to the damage done by traditional weapons".[27] Scott, writing on disruption of telecommunications, argues

---

[24] Mark R Shulman, *Legal Constraints on Information Warfare*, Center for Strategy & Technology, Air War Center, Occasional Paper No.7 (1999). Note that Shulman's use of the term information warfare rather than computer network attack relates, in part, to his broader definition but also the date of the paper. As discussed in Chapter 1, earlier literature tends to use the term information warfare rather than specifying computer network attacks. Shulman's paper concentrates on information attacks that seek to alter "information without visibly changing the physical entity within which it arises."

[25] Aldrich, 'International Legal Implications', 102.

[26] Haslam, 'Information Warfare', 167.

[27] Robert G Hanseman, 'The Realities and Legalities of Information Warfare' (1997) 42 *AFL Rev* 173, 184.

that the laws of armed conflict readily apply to computer network attacks: "In determining the constraints imposed on computer network attack by the law of war the focus of analysis must be the intent and likely results of an attack, not the novel method of attack".[28]

As noted above, the question of the applicability of the laws of armed conflict to computer network attacks arises in three distinct circumstances:

(i) where computer network attacks are utilised as part of a ongoing conventional armed conflict;

(ii) where computer network attack are launched on their own; and

(iii) where the use of conventional weapons is insufficient in and of itself to qualify as an armed conflict, but it is accompanied by extensive computer network attacks.

2.1. Application during Conventional Armed Conflict

The question of whether the laws of armed conflict apply to computer network attacks launched during a conventional conflict can be dealt with fairly briefly. The first possible argument is that the law should not be applied as the Conventions were drafted significantly before the technology to launch such attacks was available.[29] This argument can be dismissed on several grounds. First, the inclusion of the Martens Clause in the Geneva Conventions and the specific inclusion of Article 36 of Additional Protocol I indicate that the drafters of the Conventions anticipated the development and use of new weapons, means and methods of warfare.[30] The fact that the drafters require States to determine the legality of new methods of war by reference to the Protocol in and of itself indicates their acknowledgement of the applicability of the laws to newer technology. Secondly, the

---

[28] Roger D. Scott, 'Legal Aspects of Information Warfare: Military Disruption of Telecommunications' (1998) 45 *Naval Law Review* 57, 59.

[29] Schmitt, 'Wired Warfare'. Schmitt also raises a further possible argument that the LOAC do not apply to computer network attack because they are not specifically mentioned in the Conventions. This is swiftly dealt with – an examination of the Martens Clause shows that new methods and innovations are clearly anticipated by the laws.

[30] Art. 36 of Additional Protocol I states: "In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party".

issue was addressed and dismissed by the International Court of Justice in relation to nuclear weapons in the *Nuclear Weapons* case in 1996.[31] The Court held:[32]

> Indeed, nuclear weapons were invented after most of the principles and rules of humanitarian law applicable in armed conflict had already come into existence; the Conferences of 1949 and 1974-1977 left these weapons aside, and there is a qualitative as well as quantitative difference between nuclear weapons and all conventional arms. However, it cannot be concluded from this that the established principles and rules of humanitarian law applicable in armed conflict did not apply to nuclear weapons. Such a conclusion would be incompatible with the intrinsically humanitarian character of the legal principles in question which permeates the entire law of armed conflict and applies to all forms of warfare and to all kinds of weapons, those of the past, those of the present and those of the future.

Such a clear statement by the Court indicates that the Conventions and other general legal principles of the laws of armed conflict are applicable to computer network attacks, despite the fact that the technology is new, or the fact that such attacks are qualitatively different to weapons systems which have come before. This has led some commentators to state categorically that "there is no doubt that an armed conflict exists and the law of armed conflict applies, once traditional kinetic weapons are used in combination with new methods of computer network attack".[33] However, it should be noted that computer network attacks may be distinguished from both conventional weapons and nuclear weapons in one significant respect that was not at issue in the *Nuclear Weapons* case and therefore not anticipated by the Court. The extent and type of damage inflicted by a computer network attack depends entirely on the objective and design of the attack itself. Conventional weapons and their nuclear counterparts have a single effect when employed against a

---

[31] *Nuclear Weapons Case;* Schmitt, 'Wired Warfare', 189.

[32] *Nuclear Weapons Case*, para 86. The Court also cited with approval, the written statement of New Zealand: "International humanitarian law has evolved to meet contemporary circumstances, and is not limited in its application to weaponry of an earlier time. The fundamental principles of this law endure: to mitigate and circumscribe the cruelty of war for humanitarian reasons. (New Zealand, Written Statement, 15, paras 63-64).

[33] Knut Dörmann, 'Applicability of the Additional Protocols to Computer Network Attacks' (Paper presented at the International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, Stockholm, 17-19 November 2004) 139-154, 141. See Also, Doswald-Beck, 'Some Thoughts on Computer Network Attack and the International Law of Armed Conflict', 165.

target – *vis* physical destruction, injury and loss of life - and thus may be regulated as a category. The difficulty comes when dealing with a form of attack that may or may not cause physical destruction and may only indirectly cause loss of life or injury to individuals.

2.2. Computer Network Attack on its Own

The flexibility of the attack medium and the diversity of possible consequences of computer network attacks have raised a further argument against the application of the laws of armed conflict to such attacks. Although it is clear that one cannot apply a blanket rule against all computer network attacks, the question must be asked, can computer network attacks on their own be capable of being an armed conflict so as to trigger the application of the laws of armed conflict? The criteria established by the ICTY in *Tadic*, the ICRC commentary by Pictet and subsequent state practice indicate that a computer network attack will be considered the start of an armed conflict where the attacker is a state organ or armed group, that launches a computer network attack which is intended to cause, or which actually causes, physical damage to life and/or property. It is the perceived intention and consequences of the attack that must be addressed and this is where Pictet's definition departs from state practice. Further, where the attack is launched by an armed group, the attack must be part of a protracted series of attacks (whether or not such attacks are computer network attacks) in order to establish that they are not isolated or sporadic acts of violence.

2.2.1. Armed Force

This author has argued that computer network attacks can constitute a use of force under Article 2(4) of the U.N. Charter,[34] but a separate question must be asked whether such attacks are to be considered 'armed force' in such a way to initiate the application of the laws of armed conflict. Given the broad scope of possible information operations, it is not clear where on the spectrum the line will be drawn regarding what amounts to an armed attack and what may be a use of armed force, or whether a further demarcation will occur between force generally and armed force.

---

[34] See Chapter 2 *supra*.

Following the discussion regarding armed attack above,[35] it seems clear that any computer network attack launched by the armed forces, or some other organ of a State and causing large scale physical damage or personal injury equivalent to that caused by a conventional attack will be considered both an armed attack and the start of an armed conflict. However an attack designed to merely neutralise the air defence network of a country by switching it off, would not. Although if the attacking State's air force were to take advantage of that window of opportunity to launch a conventional attack, that would then trigger the application of the laws of armed conflict, the start of which may then be backdated to the computer network attack. Admittedly this may only be a matter of minutes or hours. For example, had the 2007 raid by Israel against the alleged Syrian nuclear site escalated further, the laws of armed conflict would have applied from the start of the engagement with the single Syrian radar site at Tall al-Abuad near the Turkish border.[36]

2.2.2. Humanitarian Principles

The motivation underlying the application of the laws of armed conflict is to limit the damage caused by hostilities and provide care for the casualties.[37] As Louise Doswald-Beck points out, this would militate in favour of an expansive interpretation of when the laws of armed conflict should begin to apply.[38] Greenburg et al, while not discussing the definition of armed conflict, addresses the issue of whether information warfare is war, and point out that international law draws "a strong distinction between traditional, kinetic force and the infliction of hardship or suffering on a government or population".[39] Computer network attacks which merely cause discomfort, inconvenience or even a certain level of suffering are not sufficient to equate to an armed conflict. Michael Schmitt has argued that the purposes of

---

[35] See Chapter 3 *supra.*

[36] The radar site was attacked with a combination of electronic attacks, computer network attacks and precision bombing. This would have been the case even without the precison bombing. See generally: Fulghum, Wall and Butler, 'Israel Shows Electronic Prowess'.

[37] Doswald-Beck, 'Some Thoughts on Computer Network Attack and the International Law of Armed Conflict', 164; Dörmann, 'Additional Protocols'.

[38] Doswald-Beck, 'Some Thoughts on Computer Network Attack and the International Law of Armed Conflict', 164.

[39] Lawrence T Greenberg, Seymour E Goodman and Kevin J Soo Hoo, *Information Warfare and International Law* (CCRP, Washington D.C., 1998), 19 <http://www.dodccrp.org/files/Greenberg_Law.pdf> (last accessed 7 September 2008).

humanitarian law are such that it must be reasoned that armed conflict occurs when a group takes measures that injure, kill, damage or destroy.[40] He also considers that the term includes actions "intended to cause such results or which are the foreseeable consequences thereof."[41] He goes on to argue that in the case of computer network attacks:[42]

> "...humanitarian law principles apply whenever computer network attacks can be ascribed to a State are more than merely sporadic and isolated incidents and are either intended to cause injury, death, damage or destruction (and analogous effects), or such consequences are foreseeable. This is so even though classic *armed* force is not being employed. By this standard, a computer network attack on a large airport's air traffic control system by agents of another State would implicate humanitarian law. So too would an attack intended to destroy oil pipelines by surging oil through them after taking control of computers governing flow, causing the meltdown of a nuclear reactor by manipulation of its computerized nerve centre, or using computers to trigger a release of toxic chemicals from production and storage facilities. On the other hand, humanitarian law would not pertain to disrupting a university intranet, downloading financial records, shutting down Internet access temporarily or conducting cyber espionage, because, even if part of a regular campaign of similar acts, the foreseeable consequences would not include injury, death, damage or destruction."

This analysis appears convincing in most respects. However Schmitt's extension of the term to incorporate the foreseeable consequences of an attack (which he uses to cover such actions as the shutting down of air traffic control systems), should be balanced particularly against the perceived intention of the attacking party. Where an attack is launched against a target which is not so obviously linked to the consequences, a blanket prohibition would a) beg the question of what is foreseeable to the attacker and b) preclude any assertions of mistaken identity such as those promulgated in the case of the *Dogger Bank, USS Liberty* and *USS Stark* incidents.

---

[40] Schmitt, 'Wired Warfare', 373.

[41] Ibid.

[42] Ibid. (footnotes omitted).

2.3. Computer Network Attacks in Support of Conventional Attacks

The third situation in which the applicability of the laws of armed conflict is raised occurs where a conventional attack is launched, which would not by itself qualify as an armed conflict, but which is supported by extensive computer network attacks. In that situation the accompanying computer network attacks would serve as an indicator of the intentions of the opposing party. For example, it would prove difficult for a State to claim a case of mistaken identity in the bombing of a ship, if it were later discovered that the radar system had been tampered with so that the ship's commander believed that the attacking aircraft were in fact allied military planes, and incoming missiles were not detected because the onboard defence system had been remotely turned off. There has been much speculation that this combined tactic will be used by armed groups to multiply the impact of any conventional attack. For example, the consequences of a small conventional attack in a metropolitan city would increase several-fold if at the same time the city experienced a power-cut, including power to traffic signals and hospitals, the emergency response telephone number was disconnected or jammed, and the water supply was cut off. It is likely that such a combination of attacks would also be considered sufficient to qualify as an armed conflict under the accumulation of events theory set out in Chapter 3 *supra*.

3. Territory

Internal armed conflicts conducted through the means of computer network attack also raise an additional issue in respect of territory. Common Article 3 of the Geneva Conventions applies to armed conflicts not of an international character "occurring in the territory of one of the High Contracting Parties". Likewise, Article 1 of Additional Protocol II also requires that the armed conflict in question must take place in the 'territory of the high contracting party'. Despite some commentators' arguments that conflicts involving computer network attacks take place in the somewhat ethereal plane of cyberspace, in general such discussion has been replaced by an understanding that it is the effects of these attacks on tangible objects and individuals which creates obligations and responsibilities under the laws of armed conflict. This is so even in the few discrete cases where communications equipment controlling assets in a particular State are located offshore, or even where the State's

entire online presence is hosted in a foreign State.[43] Although not relating to computer network attack, the decision of the Appeals Chamber of the International Tribunal for the Former Yugoslavia in *Kunarac et al* is instructive:[44]

> There is no necessary correlation between the area where the actual fighting is taking place and the geographical reach of the laws of war. The laws of war apply in the whole territory of the warring states or, in the case of internal armed conflicts, the whole territory under the control of a party to the conflict, whether or not actual combat takes place there, and continue to apply until a general conclusion of peace or, in the case of internal armed conflicts, until a peaceful settlement is achieved. A violation of the laws or customs of war may therefore occur at a time when and in a place where no fighting is actually taking place. As indicated by the Trial Chamber, the requirement that the acts of the accused must be closely related to the armed conflict would not be negated if the crimes were temporally and geographically remote from the actual fighting. It would be sufficient, for instance, for the purpose of this requirement, that the alleged crimes were closely related to hostilities occurring in other parts of the territories controlled by the parties to the conflict.

Thus any State or armed group finding itself in an armed conflict involving the use of computer network attack, will be required to apply the laws of armed conflict to the whole of the territory of the State; or alternatively, in the case of the armed group, to any territory under its control. This latter requirement raises the question of in what manner an armed group can control territory.

Article 1 of Additional Protocol II requires armed groups to "exercise such control over a part of its territory as to enable them to carry out sustained and concerted military operations and to implement this Protocol." The Diplomatic Conference considered several proposals to clarify the amount of territory which should be controlled,[45] however they chose not to adopt any of these proposals and instead linked the control of territory to the ability first to launch sustained and concerted

---

[43] See for example, Charles Arthur, 'The Day East Timor Was Deleted', *The Independent* (London), 28 February 1999, Features 8; Chris Nuttall, 'Virtual Country 'Nuked' on Net', *BBC News* 26 January 1999, <http://news.bbc.co.uk/1/hi/sci/tech/263169.stm> (last accessed 4 April 2003).

[44] *Prosecutor v Dragoljub Kunarac et al* (2002) (IT-96-23&23/1), International Criminal Tribunal for the Former Yugoslavia, para 57. (footnotes omitted).

[45] Proposals considered by the committee included a requirement that it should be a 'non-negligible part of the territory' or a 'substantial part of the territory': See Claude Pilloud, et al., *Commentary on the Additional Protocols of 8 June 1977* (Martinus Nijhoff, Geneva, 1987), para 4465.

military operations, and secondly to apply the Protocol. While the restrictiveness of this provision has been roundly criticised by scholars in the context of conventional internal conflicts,[46] the use computer network attacks raises an interesting possibility. In the information age, territory is largely irrelevant. Armed groups can launch sustained and concerted computer network attacks against a State without ever capturing any significant territory. Of course, the desirability of undertaking such a strategy would be dependant on the purposes of the rebellion - although it should be noted that wars of national liberation (in which control of territory would be key) are covered by Additional Protocol I which does not contain any requirement for territorial control. In contrast to their approach to Common Article 3, the Diplomatic Conference decided that some cut-off point was required to show that conflicts must have reached a critical point before Additional Protocol II should apply.[47] The criterion of 'sustained and concerted' military operations was arrived at in an effort to find criteria for the critical point, implying duration and intensity, but on a more objective assessment.[48] This selection of criteria has opened the door for computer network attacks to meet the lower threshold of, and be covered by, Additional Protocol II where their more conventional counterparts remain under the auspices of Common Article 3.

The second criterion for application of the Additional Protocol II is that the armed group's control of territory must be sufficient to enable it to apply the Protocol.[49] Waldemar Solf has argued in respect of the civil conflict in El Salvador:[50]

> "I doubt that a movement that does not control a single town and whose political arm is situated in another country, with only loose links to the movement's organised armed groups, has the capability of implementing the Protocol. I question whether it can implement the judicial standards of article 6, the standards established for the treatment of detained persons under article 5, and the standards established

---

[46] Moir, *The Law of Internal Armed Conflict*, 105-106. The provision has been particularly criticised in respect of those internal conflicts involving guerrilla warfare.

[47] Ibid., 106.

[48] Pilloud, et al., *Commentary*, para 4465; Moir, *The Law of Internal Armed Conflict*, 106.

[49] For a criticism of this rather circular argument see Michael Bothe, et al., *New Rules for Victims of Armed Conflicts* (Martinus Nijhoff Publishers, Leiden, 1982), 625; Moir, *The Law of Internal Armed Conflict*, 108.

[50] Waldemar A Solf, 'Comment: Non-International Armed Conflicts' (1981-1982) 31 *Am U L Rev* 927, 932. These comments were made with respect to the 12 year civil conflict in El Salvador which ended in 1992.

under articles 7-12 for the protection of wounded, sick, shipwrecked, and medical personnel units".

While the same issue is raised in conflicts involving computer network attacks, if the conflict is waged *only* by these means, it may be that the necessity for the above standards set out by the Protocol and highlighted by Solf is negligible. Concerted computer network attacks which obey the principles of distinction and do not result in severe physical damage, may not result in wounded or detained persons. That will be highly dependent on the purpose of the conflict. Of course it may be argued in counterpoint that if there is no need for the protection of wounded etc, there is no need for the application of the Protocol in the first place.

4. Conclusion

As with the previous chapters, application of the laws of armed conflict to computer network attack requires us to revisit first principles in order to interpret humanitarian norms for the information age. It appears likely that the laws of armed conflict will apply to most computer network attacks launched by States (or in the case of internal armed conflicts, organized armed groups) where there is a physical manifestation resulting in damage to property and more importantly, injury or death to individuals. While it may not be necessary for the level of damage or injury caused to rise to the level of an armed attack as discussed in chapter three, any attack will need to be of significant seriousness to raise it above the *de minimis* level indicated by current state practice. The attacks must be more than isolated incidents and in the case of internal armed conflict, the online hostilities must be protracted and of a nature to raise them above the level of riots and other internal disturbances.

Chapter 5 - Participants in Conflict: Combatant Status, Direct Participation and Computer Network Attack

The beginning of the twenty-first century has seen huge changes in the war-fighting capacities of the modern military. Regardless of one's opinion about the existence of a revolution in military affairs, one thing is certain: the people involved, and the technologies available to them have changed significantly. Information operations, and in particular computer network attacks, have raised many challenging questions for the laws of armed conflict. This chapter focuses on the problems that computer network attack raises in regard to the participants in armed conflicts. Indeed, one of the most pressing problems facing the laws of armed conflict may not be how to deal with combatants or civilians who carry rifles on the frontlines, but rather in determining the status of personnel armed with CPUs and keyboards sitting at a desk a continent away.[1] The reason for this is two-fold; first it is not obvious how the requirements for lawful combatancy will translate onto a medium where anonymity is the norm and distance and proximity are largely irrelevant. Secondly, the specialist nature of new technologies and the downsizing of military forces have resulted in increased civilianisation of State armed forces. Care must be taken in deciding what roles can be outsourced to civilian contractors, without jeopardising their legal protections under international conventions.

The law of armed conflict makes a fundamental distinction between combatants and civilians.[2] The former have the right to participate in hostilities and may attack, kill and wound enemy combatants and destroy military objectives. Conversely, civilians are not allowed to directly participate in hostilities. Their status as civilians enables them to enjoy protection from the dangers arising from military operations and they are not allowed to be the object of an attack. Where civilians do take a direct part in hostilities, they lose their status as protected civilians for the period of their involvement and may be liable for punishment either through domestic or international criminal processes for their actions. This chapter will address both the

---

[1] Kenneth Watkin, *Combatants, Unprivileged Belligerents and Conflicts in the 21st Century*, HPCR (2003).

[2] See *Nuclear Weapons Case*, 257.

question of what legal requirements must be met by combatants involved in computer network attacks in order to maintain combatant privileges, and what level of involvement in computer network attacks will constitute direct participation in hostilities by an actor. In particular the question of when civilian employees will be deemed to be directly participating in hostilities, thus losing their civilian privileges, must be addressed. This chapter also examines States' obligations in relation to young would-be cyber-soldiers and whether the increasing numbers of embedded civilian contractors are at risk of falling foul of mercenary provisions.

1. Combatant Status

In international armed conflicts, combatants are further distinguished into two categories. First, those people who are members of the armed forces of a belligerent party (with the exception of medical and religious personnel), even if their specific tasks are not related to active hostilities; and second, any other person who takes an active part in hostilities.[3] This second group are unlawful combatants.[4]
Unlawful or unprivileged combatant status can be achieved in one of two ways. Either, the individual's primary status is that of a combatant and they lose their privileged status through lack of compliance with the requirements of lawful combatancy; or they are civilians who directly participate in hostilities. Unlawful or unprivileged combatants may be targeted in the same manner as a combatant but they do not enjoy any of the privileges of lawful combatancy, nor those of civilian protection. The most important privileges of lawful combatancy are the legal shield that it provides for acts which would otherwise be illegal (for example murder), and the entitlement to prisoner of war status in the event of capture by the enemy.

The concept of combatant status is one which sits more securely in international armed conflicts, indeed some scholars would argue that it has no place in discussions involving internal armed conflicts. However, as discussed in Chapter 1, traditional interstate conflicts account for only a small minority of the world's current

---

[3] Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict* (Cambridge University Press, Cambridge, 2004), 27.

[4] Such people are also known as unprivileged belligerents however for the purposes of this paper they will be referred to as unlawful combatants. See Richard R Baxter, 'So-Called 'Unprivileged Belligerency': Spies, Guerrillas, and Saboteurs' (1951) 28 *BYBIL* 323.

conflicts.[5] The majority of conflicts are fought by non-state actors, whether they are insurgent groups fighting against the State,[6] hybrid conflicts with both internal and international elements,[7] multiple armed groups fighting each other on the territory of a State,[8] or a transnational group fighting internal or State armed forces.[9] The notion of a lawful combatant does not fit any of these groups. While Article 13(2) of Geneva Conventions I and II and Article 4 of Geneva Convention IV provide protection for volunteer groups and militia who are not incorporated into the armed forces, they are generally accepted to apply only to situations of occupied territory or wars of national liberation.[10] The position under Article 43(2) of Additional Protocol I is much clearer – only members of the armed forces of a party to the conflict (with the exception of medical and religious personnel) have the right to directly participate in hostilities. It should be noted however that the use of the term 'armed forces' in Additional Protocol I refers both to regular and irregular troops. It is clear that the States participating in the Geneva Diplomatic Conference which resulted in the Additional Protocols did not intend to go so far as to upgrade rebels to the status of 'lawful combatants', a move which in their view, would have entailed legitimising the rebels' struggle.[11] While States remain the primary focus of international relations and allegiance, they are unwilling to accept the principle that insurgent fighters are anything other than criminals. However as the global conflict paradigm shifts from a model where States maintain the monopoly on politically motivated violence, to a model where sub-state, trans-state and in some cases supra-state actors

---

[5] Of the 118 conflicts recorded by the Uppsala Conflict Database between 1989-2006, only 5.8% were traditional interstate conflicts. However, a further 21.3% constituted internationalised internal conflicts which would include international elements. Lotta Harbom and Peter Wallensteen, 'Armed Conflict, 1989-2006' (2007) 44(5) *Journal of Peace Research* 623, 624.

[6] See for example the conflicts between the Tamil Tigers in Sri Lanka, Maoist rebels in Nepal, Chechen separatists fighting Russia.

[7] The conflict in the territory of the former Yugoslavia is an example of this.

[8] There are currently 5 separate armed groups on the territory of the Democratic Republic of the Congo fighting against each other. Somalia is another example.

[9] For example, Al Qaeda against the Northern Alliance and the United States.

[10] This thesis will not discuss the categorisation of the Chechen conflict as a war of national liberation.

[11] Antonio Cassese, 'The Status of Rebels under the 1977 Geneva Protocol on Non-International Armed Conflicts' (1981) 30 *International and Comparative Law Quarterly* 416, fn2. In the last two weeks of the final session of the conference, any provisions which could imply recognition of insurgent parties were deleted; Adam Roberts and Richard Guelff, *Documents on the Laws of War* (3rd ed, Oxford University Press, Oxford, 1999), 482.

are encroaching on traditionally state controlled areas, this area may need to be revisited in the future.

1.1. Requirements of Combatant Status

Yoram Dinstein has usefully identified seven cumulative conditions for lawful combatancy.[12] The first four are cumulative conditions set out by the Hague Regulations and Geneva Conventions for the applicability of prisoner of war and lawful combatant status: (i) being under the command of a person responsible for his or her subordinates; (ii) having a fixed distinctive sign recognisable at a distance; (iii) carrying arms openly; and (iv) conducting operations in accordance with the laws and customs of war.[13] An additional two may be implied from Article 4(A)(2) of Geneva Convention III, that of (v) organisation and (vi) belonging to a party to the conflict. Finally, a seventh condition may be inferred from case law, which denies prisoner of war status to any person owing a duty of allegiance to a detaining power.[14] Members of the armed forces of a party, militia and volunteer forces must comply with these conditions to be accorded the status of a prisoner of war or lawful combatant.[15] Several of these conditions raise particular issues with respect to computer network attack; others simply require reinterpretation for the digital age.

Responsible Command

The first condition, that of being commanded by a person responsible for his/her subordinates, merely excludes individuals, or groups of individuals, from independently waging war on the enemy. Warnings against this kind of behaviour have been seen in the press by U.S. officials attempting to dissuade U.S. based hackers from 'joining-in' the conflicts against Afghanistan and Iraq.[16] However in

---

[12] Dinstein, *Conduct of Hostilities*, 33-37.

[13] Art. 13(2) Geneva Conventions I & II and Art. 4(2) Geneva Convention IV.

[14] *Public Prosecutor v Koi et al* (1968) AC 829, Privy Council. (per Lord Hodson). The Privy Council considered that the principle was one of customary international law; *cf.* Rogers who argues that this decision has probably not survived the introduction of Additional Protocol I, A. P. V. Rogers, *Law on the Battlefield* (2nd ed, Manchester University Press, Manchester, 2004), 32.

[15] Pictet, *Commentary*, 48. See also *Osman Bin Haji Mohamed Ali and Another v the Public Prosecutor* (1969) 1 AC 430, Privy Council, 449.

[16] David F. Gallagher, 'Hackers; Government Tells Vigilantes Their 'Help' Isn't Necessary', *New York Times* 20 February 2003, G1 5.

2008 the action by Russia against Georgia over South Ossetia, was accompanied by distributed denial of service attacks launched by individuals, and facilitated by non-state groups.[17] Such actions are clearly not permitted, and no individual engaged in such attacks would be entitled to claim combatant immunity for their part.

Distinction

The second and third conditions, that of having a fixed distinctive sign recognisable at a distance and that of carrying arms openly, may be dealt with together as they cause similar problems for computer network attack. The problem stems primarily from the anonymity that is characteristic of the Internet, namely that it is impossible to tell who is sitting at any particular computer. The intention of the two requirements is to eliminate confusion in the distinction between civilians and combatants, and to prevent deception.[18] However the rules were drafted in an era when warfare involved a certain amount of physical proximity between opposing forces. For the most part, combatants could see one another and hence distinguish between combatant and non-combatant, friend and foe. In the instance of a computer network attack, where the adversaries are plainly not in sight of each another (and may be half a world away), the usefulness of these conditions has diminished. The principle of distinction on which they are based however, remains fundamental. Although problematical, the issue is not without precedent. Vehicles, engines of war, aircraft, tanks and boats etc are all required to be marked with the distinctive sign of the belligerent party whenever partisans are on board.[19] Given the impossibility of determining the user of a particular computer at any given moment, the requirement to display a distinctive sign may be applied to the computer from which the attack is launched. One method of achieving such markings would be to require any computer network attack to emanate from a designated military IP address.[20] A form of

---

[17] See for example Morozov, 'An Army of Ones and Zeroes'.

[18] Dinstein, *Conduct of Hostilities*, 37.

[19] This is in line with the long established regulations in international law regarding the flag in the case of war at sea. Pictet, *Commentary*, 60.

[20] Every device (computer, server etc) that communicates over the Internet is assigned a four number numerical address (e.g. 168.212.226.204) that uniquely identifies the device and distinguishes it from other computers on the Internet. Each address is registered with one of three registry bodies to avoid duplicates. Creating a class of military addresses, or another form of military network designator would be a relatively simple matter.

electronic marking is already in use for medical transports appearing on radar or IFF technology, albeit with the opposite intention of marking a protected object.[21] Such an approach would also address the issue of the obligation of an individual to wear uniform while carrying out such an attack. Members of armed forces not wearing uniform aboard properly marked warships or military aircraft and taking part in hostilities are and remain combatants regardless of this circumstance.[22]

Attractive as this suggestion may initially seem, it is not without problems of its own. In the age of computer network attack where range and visibility are no longer requirements for targeting, requiring a computer to be marked as a military computer is tantamount to painting a bulls-eye on any system to which it is connected. At any one time the Internet is being searched or 'crawled' by millions of software bots intent on finding connected computers.[23] A bot searching for military designated IP addresses would be able to find them in a matter of minutes.[24] Once found, there are no lines to retreat behind and no way to move the computer out of range other than to disconnect the computer, a solution which is likely to disrupt the normal running and/or usefulness of the system. Any computer remaining connected to the Internet in anyway would be solely reliant on its electronic defences to prevent intrusion. In addition, it is not only potential enemy forces that will attempt to access military computers. For example, the U.S. Department of Defense is an attractive target for regular hackers, and the number of attacks on its systems has grown steadily. For example, in 1992 U.S. Department of Defense and military computers came under attack from intruders approximately 53 times.[25] By 1997 the annual number of attacks had risen to 780, that number had risen again to almost 40,000 times in 2002,

---

[21] Additional Protocol 1, Annex 1, Art. 8. IFF stands for Identification Friend or Foe, a secondary radar system that transmits an identification code when the transponder is triggered by detection of the target by the primary radar.

[22] Knut Ipsen, 'Combatants & Non-Combatants' in D Fleck (ed) *The Handbook of Humanitarian Law in Armed Conflicts* (Oxford University Press, Oxford, 1999) 65-104, 101.

[23] Bots (also called spiders) are used legitimately to create search engines, mailing lists, indexes etc and less legitimately to trawl for undefended computers that might provide access to systems or recruitment possibilities as a zombie or slave.

[24] In fact a list of military IP addresses has been circulating the Internet for several years, however the IP ranges specified are for fixed installations which may contain multiple dynamic IP addresses within the range. See for example, 'U.S. Gov IP Addresses You Should Not Scan' (2007) *Hellbound Hackers* 21 June 2007 <http://www.hellboundhackers.org/articles/721-US-GOV-IP-ADDRESSES-YOU-SHOULD-NOT-SCAN.html> (last accessed 13 September 2008).

[25] Schmitt, 'Normative Framework', 885 n25.

despite a brief dip in attacks following the 11 September 2001 terrorist attacks when many U.S. military networks were disconnected from the Internet.[26] U.S. governmental and military systems remain high caché targets for independent hackers, not to mention those hackers deliberately attempting to access classified military information.

Additionally, most attacks do not proceed directly from the originating computer to the target. Attacks are likely to be routed through several intermediary servers (each with its own IP address) in various locales before the attack reaches the target computer. Tracing an attack back to its origin takes time and at the present state of technology, it is not always possible to ensure that the apparent source of the attack is in fact the end of the trail. While the legitimacy of this tactic is perhaps more pertinent to discussions of perfidy and camouflage, it illustrates a problem with the solution proposed.

On the other hand, it may be argued that in the high-tech battlespace there is no practical need for such distinguishers. During a computer network attack against military assets, the originator is either a lawful combatant or a civilian directly participating in hostilities; in either case, he or she may be legitimately targeted. While this holds true for targeting judgements made in the heat of battle, a more sophisticated determination of an individual's status is required in the event that the originator is captured to ensure protection of the rights of prisoners of war. Obviously this situation is far more likely to apply to the combatant who is not sitting a continent away but is physically present in the battlespace. What then of the requirement to distinguish the individual combatant from the civilian population? Although the technological revolution in military affairs means that warfare is moving away from a situation where there is a clear set of enemy lines, it is not always the case. A common sense approach to the problem should suffice. Where a combatant engages in a computer network attack in circumstances where they are in physical proximity to opposing forces such that there is a risk that they may be mistaken for a civilian, the requirement to wear a uniform or other distinctive mark would remain. Where there is no danger of deception or of the combatant being

---

[26] James F Dunnigan, *The Next War Zone: Confronting the Global Threat of Cyber Terrorism* (Citadel Press Books, New York, 2003), 85. Note that Dunnigan's figure for attacks in 1999 was 22,144 attacks. Latest figures from the Pentagon show the number of attempted intrusions from all sources in 2005 totalled 79,000.

mistaken for a civilian, the need for an individual to wear a distinguishing emblem is irrelevant.[27]

The problems involved in applying the requirement to wear distinguishing marks and carry arms openly have arisen in other cases of non-traditional conflict, namely the situation of guerrilla fighters in occupied territory. The requirement that combatants wear a fixed distinctive emblem visible from a distance has been relaxed somewhat as a result of Article 44(3) of Additional Protocol I, which recognises that there are some situations in which the nature of hostilities make it impossible (or suicidal) for a combatant to distinguish him or herself at all times.[28] In those cases the requirement is restricted to the engagement and such times as the individual is visible to the adversary in the preceding military deployment. The controversial provision is aimed primarily at guerrilla fighters, whose use of covert tactics are designed to address inequality between the military and logistical means of the parties.[29] However, an argument may be made that computer network attacks are an example of a type of warfare, the nature of which is anticipated by this provision. CNA is by its very nature a covert method of warfare and many authors have cited its possible use as a force multiplier for militarily weaker opponents.[30] If this is the case, it raises the possibility that preparatory moves for a CNA may be attempted from non-military computers (for example electronic probing and reconnaissance, sending a virus with a back-door payload to enable access to vulnerable systems or

---

[27] Mark R Shulman, 'Discrimination in the Laws of Information Warfare' (1999) 37 *Col J Trans L* 939, 956.

[28] The article provides "in order to promote the protection of the civilian population from the effects of hostilities, combatants are obliged to distinguish themselves from the civilian population while they are engaged in an attack or in a military operation preparatory to an attack. Recognising, however, that there are situations in armed conflicts where, owing to the nature of the hostilities an armed combatant cannot so distinguish himself, he shall retain his status as a combatant, provided that, in such situations, he carries his arms openly: (a) during each engagement, and (b) during such time as he is visible to the adversary while he is engaged in a military deployment preceding the launching of an attack in which he is to participate...."

[29] Pilloud, et al., *Commentary*, 527. Some States have argued that this provision is mainly restricted to resistance movements in occupied territories and indeed some countries (e.g. the United Kingdom) have stated in their reservations to the convention that their acceptance of this clause is limited to such territories and wars of self-determination.

[30] See for example Schmitt, 'Normative Framework', 897; Michael J Robbat, 'Resolving the Legal Issues Concerning the Use of Information Warfare in the International Forum: The Reach of the Existing Legal Framework, and the Creation of a New Paradigm' (2000) 6 *BUJ Sci & Tech L* 10.

recruiting zombie computers to a botnet for a distributed denial of service attack),[31] but that once the attack proper starts, it would need to emanate from a designated 'combatant' computer or system.[32]

Compliance, Organisation & Allegiance

The remaining requirements for lawful combatancy do not change markedly with the advent of computer network technology. The obligation to conduct hostilities in accordance with the laws of armed conflict will be the same, regardless of the technology employed by the combatant. The level and type of organisation required to satisfy the fifth requirement is affected by the changing structures of parties to conflicts generally, but the nature of their weaponry does not raise any particular issues.[33] Certain computer network attack techniques, for example distributed denial of service attacks, allow for a more dispersed structure of the armed group, allowing group memebers who are geographically dispersed to play a more active role in co-ordinated actions. However this is a factual issue rather than a legal one. If the group does not have the requisite organisation (whether in network or hierarchical form), maintain discipline and supervision, its members cannot be lawful combatants. Likewise, the sixth condition, namely that a combatant must belong to a party to the conflict, will deny protection to vigilante groups of hackers from 'joining in' the confrontation in much the same way that protection is denied to independent guerrilla groups fighting for a cause without a relationship to a belligerent party.[34] The seventh requirement that the person does not owe a duty of allegiance to the capturing power will apply equally in the case of electronic attackers as it does to traditional combatants.

---

[31] Note that New Zealand has specifically included a declaration interpreting the term 'visible' to include visible any form of surveillance, electronic or otherwise. This would appear to be broad enough to encompass sweeps of all activities against military IP addresses, a situation which may require all preparatory manoeuvres against NZ to emanate from a designated computer.

[32] This may raise further issues about whether a distributed denial of service (DDoS) attack could ever be legal as it may amount to hiding in the demography, one military computer amongst thousands of civilian zombies. However such an attack would tend to be considered a nuisance attack rather than one of the main threats that could cause damage.

[33] See generally, John Arquilla, David F. Ronfeldt and United States. Dept. of Defense. Office of the Secretary of Defense., *Networks and Netwars: The Future of Terror, Crime, and Militancy* (RAND, Santa Monica, 2001) <http://www.rand.org/publications/MR/MR1382/>, for a description of the evolving nature of parties from military style hierarchies to networks.

[34] *Public Prosecutor v Koi et al.*

1.2. Saboteurs and Spies

The laws of armed conflict do not prohibit sabotage or espionage,[35] however capture of a combatant while engaged in either act, will result in loss of privileged status and the perpetrator will not be entitled to treatment as a prisoner of war. Article 24 of the Hague Regulations 1907 states that "Ruses of war and the employment of measures necessary for obtaining information about the enemy are considered permissible".[36] Likewise, Additional Protocol I allows ruses of war and provides that any member of the armed forces taken by the adverse party while engaged in espionage is not entitled to prisoner of war status.[37] Traditionally, both sabotage and espionage require the combatant to be operating behind enemy lines, that is, in territory controlled or occupied by an adverse party. However, advanced technology means that sensitive information can be retrieved from, and damage can be caused in, the territory of the adverse party without ever setting foot in it. No-one would deny that war-time electronic eavesdropping or aerial surveillance are accepted methods of gathering information provided that the operative remains outside the territory of the adverse State (or wears distinctive emblems while engaged in such activities).[38] However the issue that is raised by computer network attack is its proactive and clandestine nature of the intrusion and an actor's ability to manipulate data and information inside the territory, while remaining physically outside.

1.2.1. Sabotage

It is possible to argue that many acts of computer network attack will amount to acts of sabotage where a State engages in acts of disrupting or disabling damage to opposition resources in a clandestine manner, in other than occupied territory. This is precisely the type of attack for which computer network attacks are likely to be used. While sabotage is not in and of itself internationally culpable (unless committed by a person resident in occupied territory, who is not a member of the armed forces), it

---

[35] So long as acts of sabotage are directed at a legitimate military target.

[36] Art. 24, Hague Convention IV Respecting the Laws and Customs of War on Land 1907.

[37] Arts. 37(2) and 46 respectively.

[38] Some questions arise when the espionage takes place in the exclusive economic zone or territorial waters of the target country; see the 1968 case of the *USS Pueblo* in North Korean waters, or the more recent 2001 case of the US EP-3 surveillance plane which crashed after colliding with a Chinese F8 fighter jet. It should be noted that both were peacetime incidents.

will result in the loss of combatant privileges and prisoner of war status on capture. The cases of *Ex Parte Quirin* in which eight German saboteurs were convicted of 'unlawful combatancy' for unsuccessful sabotage missions in the United States,[39] and *Ali* which involved the sabotage of a civilian building in Singapore.[40]
In *Ex Parte Quirin,* eight Germans landed secretly on the shores of the United States in German uniform with explosives for the purposes of sabotage. While they landed in German uniforms, on landing they changed into civilian clothing and proceeded to travel to their destinations. They were captured. The Supreme Court of the United States held:[41]

> "The spy who secretly and without uniform passes the military lines of a belligerent in time of war, seeking to gather military information and communicate it to the enemy, or an enemy combatant who without uniform comes secretly through the lines for the purpose of waging war by destruction of life or property, are familiar examples of belligerents who are generally deemed not to be entitled to the status of prisoners of war, but to be offenders against the law of war subject to trial and punishment by military tribunals."

The Court went on to hold:[42]

> "The law of war cannot rightly treat those agents of enemy armies who enter our territory, armed with explosives intended for the destruction of war industries and supplies, as any the less belligerent enemies than are agent similarly entering for the purpose of destroying fortified places or our Armed Forces. By passing our boundaries for such purposes without uniform or other emblem signifying their belligerent status, or by discarding that means of identification after entry, such enemies become unlawful belligerents subject to trial and punishment."

In a similar case, *Ali v Public Prosecutor*, two members of the Indonesian army entered a bank in Singapore in civilian clothing and deposited a bag containing nitroglycerine in the stairwell. The bag exploded killing three civilians. Three days later the perpetrators were rescued from the sea and arrested, still wearing civilian

---

[39] *Ex Parte Quirin et al* (1942) 317 US 1, Supreme Court of the United States.

[40] *Osman Bin Haji Mohamed Ali and Another v the Public Prosecutor.*

[41] *Ex Parte Quirin*, 31.

[42] Ibid., 37.

clothes and carrying no identity documents. The Privy Council confirmed the Federal Court of Malaysia's decision that:

> "... members of enemy armed forces who are combatants and who come here with the assumption of the semblance of peaceful pursuits divesting themselves of the character or appearance of soldiers and are captured, such persons are not entitled to the privileges of prisoners of war."

In both these cases, the act of sabotage, and the basis of their culpability as unlawful combatants, was committed by entering onto the territory of the victim State in civilian dress and committing (or attempting to commit) acts of destruction. The difficulty that technology now brings is that such acts of sabotage are now capable of being committed without the perpetrator setting foot in the territory of the victim State. It is now possible to commit acts of sabotage by entering into an adversary's computer systems in a clandestine manner (i.e. through a backdoor) and causing significant damage to State interests. Like most issues involving computer network attack, the legal status will depend on the type of attack being envisaged.

The simplest instances of sabotage by computer network attack are those utilised on a daily basis by civilian virus writers around the world. An attacker sends an email to the recipient which incorporates a virus or other malicious code; the code activates upon opening the email or email attachment and damages information resident on the recipient's computer networks.[43] As long as the email does not purport to be from a person or organisation with protected status or claim to offer terms of surrender or some other perfidious simulation, the combatant remains entitled to POW status in the event of capture. This is the electronic equivalent of sending dangerous items though the mail i.e. letter or parcel bombs. The computer system is merely being used as a delivery device.

A direct intrusion into a system or network however may be more akin to sneaking across borders to directly cause damage. Given that the physical act of crossing a border or passing into enemy occupied territory is no longer necessary to cause covert damage, a question may be raised as to whether the actor being physically

---

[43] Damage estimates from computer network attacks such as viruses are notoriously difficult to quantify as there are no agreed standard measures. However, it is estimated that viruses cost businesses billions of dollars every year.

present in the territory is a fundamental element of sabotage. Yoram Dinstein has argued in relation to espionage that the combatant must be physically located in an area controlled by the enemy for the offence to crystallize.[44] An alternative reading would require only that the effects of the act take place in the territory, in much the same way that traditional 'shot across the border' cases and more recent domestic cases of computer intrusion are prosecuted in the State where the damage occurs.[45] This is the fundamental territorial principle set out in the *Lotus Case.*[46] This approach argues that it is the act of deception for the purposes of destruction which negates combatant status. This would also fit with the reasoning set out in the *Hostages Trial* where "guerrillas were actually said, in legal intendment, to resemble spies in that the enemy punished such activities not because of their illegality in an international sense but because of the danger they presented to him".[47] The fact that acts of covert damage can now be performed from outside the territory controlled by the enemy does not eliminate the danger and in fact, makes it more difficult to detect. Under this analysis, a covert intrusion into a system resident in the territory of a victim State, with the intention of causing damage, while disguised as something other than a combatant, is likely to be considered sabotage with the resultant loss of combatant status for any operative thus caught. An intrusion attempt directly from a military computer would remain legitimate, as there is no deception involved.

1.2.2. Espionage

In the case of electronic espionage, multiple peacetime instances of which have been made publicly available,[48] it is doubtful that this will raise any new difficulties.

---

[44] See section 5.2.2 *infra*; Dinstein, *Conduct of Hostilities*, 209.

[45] See generally Antonio Cassese, *International Criminal Law* (Oxford University Press, Oxford, 2003), 278., citing *Rivard v United States* (1967) 375 F 2d 882, U.S Ct. App., 5th Cir.: "[a]ll the nations of the world recognize the principle that a man who outside of a country wilfully puts in motion a force to take effect in it is answerable at the place where evil is done".

[46] *The Lotus* (1927) Series A No.10, Permanent Court of International Justice.

[47] Baxter, 'So-Called 'Unprivileged Belligerency': Spies, Guerrillas, and Saboteurs', 336. Citing *United States v List et al* (1949) Trials of War Criminals, XI (1950), 1245; War Crimes Reports, VIII (1949) 56.

[48] One example, code-named 'Titan Rain', consists of a series of coordinated attacks launched against U.S. computer systems since 2003. The attacks are highly sophisticated intrusions against unclassified networks, in which the attackers have gained access, copied as many files as possible from the computer, transmitted them via way stations to China and made a near clean exit. Systems compromised include NASA, the World Bank, military sites such as Redstone Arsenal military base, and defence contractors such as Lockheed Martin. Unusually for cyber intrusions, the origin of the

Espionage in time of war is not a violation of the laws of armed conflict, as evidenced by Article 24 of the Hague Regulations, or indeed of any other international law. Capture results in the loss of combatant status and the right to prisoner of war treatment and will be prosecuted under the national laws of the State. Under the Hague Regulations, a key factor in the offence of espionage is the attempt to gain information in the zone of operations of a belligerent. Additional Protocol I extends the zone of operations to all territory controlled by the enemy.[49] Yoram Dinstein has stated that this means that the combatant must be physically located in an area controlled by the enemy. "A person stationed on his own State's side of the front line – say, clandestinely monitoring or deciphering enemy radio signals – is not a spy".[50] While this latter statement is undoubtedly correct, it does not follow that combatant must necessarily be physically located in enemy controlled territory. A distinction can be made between the passive collection of radio signals from outside a specified zone of operations, and the active intrusion into a system either controlled by an adverse party, or resident on enemy territory, for the purposes of information collection. Passive collection of information (even when assisted by the strategic placement of a listening post), does not require an act which would allow the opposing State to assert any grievance or jurisdiction over that act. A similar computer-based equivalent would be use of a listening post system such as Echelon to intercept emails, telephone calls and other data traffic off satellite communications, or taking advantage of an unsecured wireless network to intercept traffic travelling across that network.[51] However, using the analysis set out in the section above with relation to sabotage, it can be argued that it is the *act* of collection of the information which must occur in the territory controlled by the enemy. Active

---

attacks was quickly and clearly traced to three routers operating in Guangdong province China, however it is unclear whether the attacks are emanating from military, corporate or individual operators. The Chinese government denies any involvement. Bradley Graham, 'Hackers Attack Via Chinese Web Sites', *Washington Post* (Washington D.C.), 25 August 2005, A 1; Thornburgh, et al., 'The Invasion of the Chinese Cyberspies (and the Man Who Tried to Stop Them)'.

[49] The Commentary to Additional Protocol I states that the additional protocol did not intend to change the substance of the traditional rules of espionage adopted in The Hague, but merely sought to supplement and elaborate them. This conclusion was confirmed by the wording of Art. 39(3) (Emblems of nationality), which refers to the "existing generally recognized rules of international law applicable to espionage".

[50] Dinstein, *Conduct of Hostilities*, 209.

[51] Echelon is the signals intelligence collection system operated between the U.S., U.K., Australia, Canada and New Zealand.

penetration into a network controlled by the enemy in order to collect information (by breaching firewalls and other electronic defences), would be enough to situate the collection of information from that system in the territory of the adverse party. In the same manner that sabotage is distinguished from ordinary military operations in the section above, it is the clandestine character of the activity and the spy's intention to deceive, that distinguishes espionage from the reconnaissance, scouting or surveillance performed by military forces and by individual members of the armed forces.[52] It is this fact that prevents the operators of unmanned aerial vehicles (UAVs), which have been operating in war zones since the 1950s, from being classed as spies. An intrusion attempt launched directly from a military computer would remain legitimate, as there is no deception involved.

There is one additional factor which must be taken into account with computer based forms of espionage. Spies are excused for any liability for their actions under national law once they rejoin the army to which they belong.[53] If the spy in question never leaves his or her lines it seems unlikely that they will ever be at risk of capture before regaining their combatant privileges. However a combatant stationed inside the territory of the opposing forces, or in any other territory, would run the same risks as any other spy.

2. Direct Participation by Civilians

Civilians are entitled to protection from the dangers arising from military operations and may not be targeted until, and for such time as they take an active or direct part in hostilities.[54] Where civilians do take a direct part in the hostilities, they lose their protected status for the period of their involvement and may be liable for punishment either through domestic or international criminal processes for their actions. However the question of what actions will amount to direct participation in hostilities is one which continues to raise difficult issues for the laws of armed

---

[52] Erik Castrén, *The Present Law of War and Neutrality* (Suomalaisen Tiedeakatemian Toimituksia, Helsinki, 1954), 152. cited in Dinstein, *Conduct of Hostilities*, 111.

[53] Art. 31 Hague Regulations; Art. 46(4) Additional Protocol I.

[54] Common Art. 3 Geneva Conventions; Art. 51(3) Additional Protocol I. Common Article 3 of the Geneva Conventions employs the term 'active' rather than 'direct' as used in the Additional Protocols. The distinction between active and direct participation was discussed by the International Criminal Tribunal for Rwanda in the *Akayesu* case which held that the terms are so similar that they should be treated as synonymous: *Prosecutor v Jean-Paul Akayesu* (1998) Case No. ICTR-96-4-T, International Criminal Tribunal for Rwanda, para 629.

conflict. Civilians have played a vital supporting role in warfare throughout history, and modern warfare is no exception. Civilians are widely employed by the armed forces, both as contractors and as full-time employees, or they may accompany the armed forces for a variety of other reasons. The use of contractors in particular, has increased exponentially in recent years as the combined effects of the technological revolution and 'privatisation through outsourcing' have been used to ensure continuing military might, while reducing costs.[55] For example, in 2006 over 38,000 contractors were serving with coalition forces in Iraq in functions from cleaners and cooks, with an additional 30,000 providing security for both the military and other contractors and guarding convoys and military installations.[56]

The use of civilians has arisen particularly with regard to technologically advanced methods of warfare. Civilians maintain complex weapons systems such as the F-117 Nighthawk fighter, B-2 Spirit bomber, M1 Abrams tank, and TOW missile system, and have both maintained and operated the Global Hawk and Predator UAVs.[57] This high level of outsourcing takes place for a number of reasons. First, it is far more cost effective to hire civilian contractors to maintain and operate the systems which run the military than to train military personnel to do so. Despite the (generally) higher salaries of contractors, they do not require the training and infrastructure costs of military personnel. Second, the systems being used are seldom standard inventory; for the most part, they are too specialised and often still in the throes of research and development.[58] It is clear that military personnel are being trained in computer network attack capabilities,[59] however it is also apparent that civilian contractors are

---

[55] Guillory, 'Civilianising the Force: Is the United States Crossing the Rubicon?' 111.

[56] As at 1 May 2006, the number of civilian logistics personnel was reportedly 38,305, Brookings Institution, *Iraq Index*, Brookings Institute (2006) 15 <http://www.brookings.edu/iraqindex> (last accessed 12 September 2008). It is unclear whether this data relates only to the US Central Command Area of Responsibility. Figures on the numbers of security contractors are harder to come by but a recent figure in a Frontline report put this figure at an additional 35,000 both Iraqi and non-Iraqi contractors. http://www.pbs.org/wgbh/pages/frontline/shows/warriors/faqs/.

[57] Michael N. Schmitt, 'Humanitarian Law and Direct Participation by Private Contractors or Civilian Employees' (2004) 5(2) *Chi J Int'l L* 511, 512.

[58] Michael N. Schmitt, 'Direct Participation in Hostilities and 21st Century Armed Conflict' in H Fischer, et al. (eds), *Crisis Management and Humanitarian Protection* (Berliner WissenschaftsVerlag, Berlin, 2004) 505-529, 523.

[59] See for example, C. Todd Lopez, 'Military Students Get Lesson in Cyberwarfare', *Air Force Print News* 3 May 2006,

used by the military to run their information systems. As these information systems become both targets and weapons, such contractors find themselves involved in hostilities on an unprecedented scale. It is therefore essential to carefully delineate which tasks are permissible non-combatant support and which will constitute unlawfully participating in hostilities.

2.1. Requirements of Direct Participation

Although there remains significant debate over the definition and requirements of 'active' or 'direct' participation,[60] the commentary to Article 43 of Additional Protocol I indicates that the phrase includes "acts which are intended by their nature or their purpose to hit specifically the personnel and the *matériel* of the armed forces of the adverse party".[61] The commentary goes on to state that "direct participation in hostilities implies a direct causal relationship between the activity engaged in and the harm done to the enemy at the time and place where the activity takes place".[62] A similar assessment is seen in the commentary to Additional Protocol II relating to Article 13(3) of the Protocol; it requires a 'significant causal relationship' between act and immediate consequence.[63] As a result, any determination of status will need to be done on a case-by-case basis, an approach confirmed by the International Criminal Tribunal for the former Yugoslavia in *Tadic*.[64]

> "It is unnecessary to define exactly the line dividing those taking an active part in hostilities and those who are not so involved. It is sufficient to examine the relevant facts of each victim and to ascertain whether, in each individual's circumstances, that person was actively involved in hostilities at the relevant time".

<http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1186049,00.html> (last accessed 11 May 2006).

[60] See for example the ICRC, *Direct Participation in Hostilities under International Humanitarian Law*, ICRC (2003) <http://www.icrc.org/web/eng/siteeng0.nsf/html/participation-hostilities-ihl-311205> (last accessed 18 August 2008); ICRC, *Second Expert Meeting - Direct Participation in Hostilities under International Humanitarian Law*, ICRC (2004) <http://www.icrc.org/web/eng/siteeng0.nsf/html/participation-hostilities-ihl-311205> (last accessed 18 August 2008).

[61] Pilloud, et al., *Commentary*, para 1679.

[62] Ibid.

[63] Ibid., para 4787.

[64] *Prosecutor v Dusko Tadic* (1997) 36 ILM 908, International Criminal Tribunal for the Former Yugoslavia, para 616.

Hays Parks has defined civilian participation in warfare as a spectrum between total non-participation on one end (what has sometimes been termed the 'pure' civilian) through war effort, military effort and finally direct participation in military operations.[65] Such categories were based on the 1979 ICRC Conference of Government Experts which resulted in the Additional Protocols. It is widely recognised that acts that help the general war effort do not constitute direct participation,[66] however where the line is to be drawn is a subject of intense debate between commentators which has still not been settled.[67] A.P.V. Rogers has argued for a narrow construction of a 'direct part in hostilities', stating that actions such as arms production, military engineering work or military transport (including the oft-cited example of the ammunition truck driver) would not be deemed direct participation.[68] He argues that to hold otherwise places civilian protection severely at risk. However the same argument has been used by both Hays Parks and Michael Schmitt to advocate a wider construction. Parks has stated that civilians working toward the military effort are far more combatant than civilian, and has argued for an expansive approach, which would include intelligence gathering and logistical support for combatant forces as direct participation.[69] Using the traditional example of the status of the civilian driver of an ammunition supply truck, Parks thus finds that the truck driver should be a lawful target of attack.[70] Rogers has dismissed this view as creating a class of quasi-combatants based on job description, a situation that has been expressly rejected by the Commentary to the Protocol.[71]

In an attempt to find a more general rule, Michael Schmitt has argued that the best approach is to assess the criticality of the act to the direct application of violence against the enemy.[72] Although direct cause and effect is unnecessary, there must be

---

[65] See generally, W. Hays Parks' categories of civilian participation as considered by the 1979 ICRC Conference of Government Experts: W. Hays Parks, 'Air War and the Law of War' (1990) 32 *AFL Rev* 1, 132.

[66] Pilloud, et al., *Commentary*, para 1679.

[67] The ICRC and The TM Asser Institute have engaged in a series of expert meetings to debate the question. ICRC, *Direct Participation 2003;* ICRC, *Direct Participation 2004.*

[68] Rogers, *Law on the Battlefield*, 9.

[69] See Parks, 'Air War and the Law of War', 132.

[70] Ibid., 132.

[71] Pilloud, et al., *Commentary*, para 1679; Rogers, *Law on the Battlefield*, 9.

[72] Schmitt, 'Humanitarian Law and Direct Participation', 534; Schmitt, 'Direct Participation', 505.

sufficient causal proximity to a foreseeable consequence of harm or other disadvantage to the enemy.[73]

> "[T]he civilian must have engaged in an action that he or she knew would harm (or otherwise disadvantage) the enemy in a relatively direct and immediate way. The participation must have been part of the process by which a particular use of force was rendered possible, either through preparation or execution. It is not necessary that the individual foresaw the eventual result of the operation, but only that he or she knew their participation was indispensable to a discrete hostile act or series of related acts."

He further argues that any grey areas should be interpreted towards in favour of finding direct participation to protect the law and provide an incentive for civilians to remain as distant from conflict as possible. Thus under Schmitt's analysis, the civilian driver of an ammunition supply truck is not taking a direct part in hostilities when driving from the factory to the ammunitions depot, but would be when driving from the depot to the front.[74] Both Parks and Schmitt maintain that to grant immunity to civilians who are intimately involved in the conflict is to risk engendering disrespect for the law by combatants who are put at risk by their actions.[75] In others words, the actions of the relatively small number of civilians supporting the military should not endanger the lives of civilians who have no part in the conflict.

Some scholars have argued that direct participation includes not only activities involving the delivery of violence, but also acts aimed at protecting personnel, infrastructure or material.[76] These problems have arisen in Iraq in relation to private security contractors engaged to defend military installations.[77] U.S. military doctrine

---

[73] Schmitt, 'Humanitarian Law and Direct Participation', 533.

[74] Schmitt, 'Direct Participation', 504.

[75] Parks, 'Air War and the Law of War', 132; Schmitt, 'Direct Participation', 505.

[76] U.S. Air Force, Pam.110-34, Judge Advocate General: Commander's Handbook on the Law of Armed Conflict (1980, §2-8) commenting that the rescue of downed airmen would constitute taking direct part in hostilities, cited in Jean-François Quéguiner, *Direct Participation in Hostilities under International Humanitarian Law*, Program on Humanitarian Policy and Conflict Research at Harvard University (2003) <http://www.ihlresearch.org/ihl/pdfs/briefing3297.pdf> (last accessed 13 September 2008). See also, U.K. Ministry of Defence, *The Manual of the Law of Armed Conflict* (Oxford University Press, Oxford; New York, 2004), §12.69.

[77] See PBS Frontline, *Interview with Stephen Schooner - Private Warriors* <http://www.pbs.org/wgbh/pages/frontline/shows/warriors/interviews/schooner.html> (last accessed

(and international law) states that contractors are allowed to carry arms for the purposes of defence only,[78] however Peter Singer has noted that despite this, contractors are in fact being used for roles which clash with that doctrine, and that the very function for which they are being hired mandates their use in combat roles.[79] For example, if States are hiring a private military company to guard a key installation in a combat zone, or to escort a convoy through insurgent territory which is renowned for attacks on convoys, it is then disingenuous to argue that the contractors are armed solely for self-defence.[80] Michael Schmitt has stated that a civilian government employee or private contractor defending military personnel or military objectives from enemy attacks directly participates in hostilities.[81] These arguments accord with Article 49 of Additional Protocol I, which states that the term 'attacks' incorporates acts of violence against the adversary, whether in offence or defence. This definition would appear to extend to those technicians who engaged in *active* defence of military computer networks such that harm is caused to the attacking adversary or their equipment.

One further point deserves brief comment. Traditionally geographic proximity to the battle lines has also been used as a rough guide to ascertaining the status of the civilian concerned, however this measure is no longer decisive in twenty-first century combat. Not only have traditional battle lines been replaced by amorphous battlespaces, but physical proximity to that space is no longer required. Even before computer networks are considered, missiles and other weapons may now be loaded onto aircraft or otherwise launched from continents away and strike any point on the globe.

---

13 September 2008). Also, for example the use of the private military firm Blackwater to defend the Coalition Government Headquaters in Najaf, Iraq which subsequently came under attack. Dana Priest, 'Private Guards Repel Attack on US Headquarters', *Washington Post* 6 April 2004, A01 <http://www.washingtonpost.com/ac2/wp-dyn/A53059-2004Apr5?language=printer> (last accessed 13 May 2006). See section 2.4 *infra.*

[78] Rumsfield letter cited in Schmitt, 'Humanitarian Law and Direct Participation', n11. http://www.house.gov/skelton/5-4-04_Rumsfeld_letter_on_contractors.pdf

[79] PBS Frontline, *Interview with Peter Singer - Private Warriors* <http://www.pbs.org/wgbh/pages/frontline/shows/warriors/interviews/singer.html> (last accessed 13 September 2008).

[80] Ibid.

[81] Schmitt, 'Humanitarian Law and Direct Participation', 538.

2.2. Offensive Computer Network Attack

Despite the need to examine the context of particular actions, it is clear that any civilian engaged in a proactive, offensive computer network attack against an adversary's networks or personnel would be taking a direct part in hostilities in much the same way that a civilian taking up conventional arms would be. This is the case regardless of whether the attack was designed to cause damage in and of itself, or whether it was designed to support a conventional attack, for example, disabling an enemy's air defence network prior to the launch of conventional air strikes. The fact that damage is caused by reason of computer manipulation rather than conventional arms is irrelevant.

2.3. Computer Network Attack System Support

The issue becomes more complex when applied to civilians engaged in activities less immediately linked to hostilities. While IT support is a concept that seems ripe for civilian outsourcing, maintenance of systems and networks which are used to launch computer network attacks may be viewed as maintenance of a weapons system, placing the technicians who maintain these networks at risk of direct participation in hostilities. Knut Ipsen has argued that direct participation includes 'use of a weapons system in an indispensable function', although he gives no guidance as to which functions should be considered indispensable.[82] Two questions come out of this statement; first, whether a system used for launching computer network attacks is a weapons system and second, whether maintenance and support of that network constitutes an indispensable function such that it would amount to direct participation in hostilities.

The U.S. Department of Defense dictionary of military terms defines a weapons system as "[a] combination of one or more weapons with all related equipment, materials, services, personnel, and means of delivery and deployment (if applicable) required for self-sufficiency."[83] Depending on the type of computer network attack envisaged, the weapons involved may be malicious coding (in the case of Trojans,

---

[82] Ipsen, 'Combatants & Non-Combatants', 67.

[83] U.S. Department of Defense, *Dictionary of Military and Associated Terms (as Amended through 20 March 2006)* (Washington D.C., 2001) <http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf> (last accessed 13 September 2008).

viruses and other kinds of backdoor attacks) or the network itself in the case of intrusion and sabotage. In either case it is quite clear from this definition that networks used to launch computer network attacks would fall within this definition, either as the weapon itself or as the means of delivery and deployment.[84] Maintenance of a weapons system would seem to be an act which has a direct causal relationship with the harm done to the enemy,[85] and yet the maintenance of more and more military systems is being outsourced as part of the drive for cheaper, smaller, more streamlined armed forces. The U.S. Air Force Congress now requires that maintenance and repair for all new critical weapons systems be under contractor support for at least four years and for life for non-critical systems.[86] This so-called 'factory to foxhole' support includes weapons systems such as the Patriot missile system, JSTARS,[87] data processing systems and the Fox nuclear chemical biological reconnaissance system, combat aircraft and the Abrams M1A1 tank.[88] Further, civilian contractors staff the entire information operations cell supporting the U.S. Southern Command, which is responsible for defence operations in 32 countries in Central and South America and the Caribbean.[89] Despite this evidence of state practice to the contrary, maintenance of these systems, particularly maintenance that takes place once a system has come under attack and are aimed against a direct intrusion, would amount to direct participation in hostilities. How then to reconcile state practice with the inescapable conclusion that maintenance is an indispensable

---

[84] For a contrasting view see Gregory F. Intoccia and Joe Wesley Moore, 'Communications Technology, Warfare, and the Law: Is the Network a Weapons System?' (2006) 28 *Hous J Int'l L* 467, 479. While arguing that the network should not be considered a weapons system, Intoccia & Moore base their opinion on an overly broad definition of the network which encompasses practically the entire range of communications equipment available both at national and international level.

[85] Note that this is not a universal view. Although disagreeing with the merits of it, Parks does not consider that the maintenance of the Swiss Air Force by civilian engineers would constitute direct participation under the terms of Additional Protocol I: Parks, 'Air War and the Law of War', n397.; but *cf* Schmitt, 'Direct Participation', 508.

[86] "Outsourcing and Privatization" 1988 Air Force Congressional Issue Papers Extract cited in Steven J. Zamparelli, 'What Have We Signed up For?: Competitive Sourcing and Privatization - Contractors on the Battlefield' (1999) XXIII(3) *AFJ Log* 9.

[87] JSTARS (Joint Surveillance Target Attack Radar System) offer an airborne, standoff range, surveillance, and target acquisition radar and a command and control centre to those managing a conflict. It possesses secure data links with air operations centre, army mobile ground stations and other military command, control & intelligence assets: Schmitt, 'Direct Participation', 512.

[88] Zamparelli, 'What Have We Signed up For?' 13; Schmitt, 'Humanitarian Law and Direct Participation', 518.

[89] Dan Verton, 'Navy Opens Some It Ops to Vendors' (2000) *Federal Computer Week* <www.fcw.com/fcw/articles/2000/0821/pol-navy-08-21-00.asp> (last accessed 15 April 2004).

function in the delivery of violence. Schmitt argues that immediate maintenance and support, that is, support not of a routine nature, may be seen as direct participation – parallels may be drawn with civilian aircraft engineers in charge of maintaining, loading and launching aircraft hundreds of miles away from a conflict zone.[90] Whereas other routine maintenance falls into a different category and should not be so considered.

2.4. Generic IT Support

Another question arises in the case of the civilian technician employed to maintain military networks, not directly involved in offensive information operations, but which may subsequently come under attack by computer network attacks. In highly technologically advanced militaries, particularly those who rely heavily on their networking capabilities for an advantage, disruption of the networks which link the various components of the military together will create a significant advantage for an opposing force. Thus for example, any U.S. military network, including those which utilise civilian assets either wholly or in part, becomes a useful and legitimate target (subject always to the principle of proportionality). In 2000 the U.S. Navy opened up all defensive information operations, including information assurance and other defensive security operations, as "non-inherently governmental" job functions and thus open to outsourcing.[91] It seems clear that routine systems maintenance, security updates and other generic IT functions which are not related to hostilities (CNA or otherwise) would not be considered direct participation. Merely, setting up security protocols on a network would be akin to civilians helping with the war effort to lay down barbed wire on the beaches in advance of a suspected landing. However as seen above, guarding a military objective against enemy action and defence of a military installation does comprise direct participation in hostilities. At what point does the technician, cease to become a protected civilian merely supporting and maintaining a network (including network security measures), and become an active participant defending a military objective? A conservative view would dictate that at the very moment the system comes under computer network attack, civilians must step away from their posts. However, in contrast to defence of a 'real world' military

---

[90] Schmitt, 'Direct Participation', 512.

[91] Verton, 'Navy Opens Some It Ops to Vendors'.

objective, defence of a system or network may not require the use of force by the defenders. For instance, when private contractors came under fire defending the Coalition Headquarters in Najaf, Iraq in 2004, a three and a half hour firefight ensued that used thousands of rounds of ammunition and hundreds of grenades, and resulted in the wounding of three coalition personnel and an unspecified number of Iraqi casualties.[92] In contrast, defence of a computer network seldom results in casualties and solely defensive measures may not even comprise a use of force.[93] Although the application of force is not a criterion for direct participation, it may be that this disjuncture from damage removes network defence sufficiently from the chain of causation to disqualify it from direct participation. Although in this respect it is useful to note Michael Schmitt's comment that civilians performing defensive functions frees up soldiers for other combat missions, thereby further contributing to hostile action.[94] As with each of these scenarios, the specific circumstances of the civilian's actions will need to be assessed.

Computer network operations pose an additional issue in relation to the difficulty in attributing attacks to a specific actor.[95] Civilians are entitled to defend property from criminals and looters without such actions constituting direct participation in hostilities; thus civilian technicians are entitled to defend military networks from regular hackers. Not only are military networks a prime target for enemy forces, they come under increasing attack from civilians during time of war as well.[96] Given the anonymous nature of the Internet and the current lag in tracing the source of attacks, civilian technicians are unlikely to be able to determine whether or not they are directly participating in hostilities. They will be unable to ascertain immediately who is perpetrating the attack, and in many cases even where it is determined that a

---

[92] Priest, 'Private Guards Repel Attack on US Headquarters'. Coalition wounded comprised two contractors and one marine.

[93] See Chapter 2 *supra.*

[94] Schmitt, 'Humanitarian Law and Direct Participation', 538.

[95] See Chapter 3 *supra.*

[96] The 2008 computer network attacks launched against Georgian government and other websites are a prime example of this. Computer network attacks have also accompanied the Arab-Israeli conflict and Zapatista uprisings in Mexico among other incidents. Interestingly, despite predictions of this behaviour in Iraq, the number of intrusions remained stable, although a large number of website defacements did occur: Peter Rojas, 'The Paranoia That Paid Off', *The Guardian* (London), 24 April 2003, 27.

civilian is behind the attack, it will not be possible to determine if there is a sufficient nexus between the attack and any ongoing hostilities.[97]

2.5. Mercenaries

The increased numbers of civilian employees and contractors working for the military also raises issues regarding their possible classification as mercenaries. As set out in the section above, civilians accompanying the forces without being part of it are granted prisoner of war status under Article 4(4) Geneva Convention III, however those directly participating in hostilities, for example where contractors are engaged to conduct proactive offensive computer network attacks, run the risk of being categorised as mercenaries. It is clear that both individual hackers and private military companies (PMCs) specialising in computer network operations have attempted to, or are in fact, acting with States to provide computer network attack possibilities.[98] Although the use of mercenaries in warfare is an ancient practice, in post-colonial times mercenaries have fallen from favour and have become *personae non grata* in international relations.

Under the Geneva Conventions, mercenaries (along with "other militias") qualify as lawful combatants as long as they meet the conditions set out in Article 13(2).[99] However that position had changed by the implementation of the Additional Protocols. Adopted in the wake of nearly two decades of post-colonial struggles for self-determination in Africa, Additional Protocol I provides that mercenaries do not have the right to be combatants and deprives them of their right to be treated as

---

[97] Obviously in cases where attacks are accompanied by website defacement, such as have occurred in the above cases, the link with ongoing hostilities will be easier to ascertain. See for example,Izhar Lev, 'E-Intifada: Political Disputes Cast Shadows in Cyberspace' (2000) 12(12) *Janes Intelligence Review* 16; Steve Mertl, 'Cyberspace Experts Await Full-Scale Attack', *Globe & Mail* (Canada), 27 December 2002, A11; Reuters, 'Cyber-War Rages over Iraq', *ZDNet News* 31 March 2003, <Http://www.zdnet.com/newstech/security/stoty/0,2000024985,20273268,00.htm> (last accessed 31 March 2003).

[98] See for example PBS Frontline 'Interview with Hacker' *Cyberwar!* (PBS Airdate 24 April 2003) Available at http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/hacker.html (last accessed 29 May 2004); Ruth Alvey, 'Russian Hackers for Hire: The Rise of the E-Mercenary' (2001) 13(7) *Jane's Intelligence Review* 52.

[99] The conditions are set out in section 1 above, i.e. responsible command, having a fixed distinctive sign, carrying arms openly and conduct in accordance wit the laws and customs of war. See Dino Kritsiotis, 'Mercenaries and the Privatisation of Warfare' (1998) 22 *Fletcher Forum of World Affairs* 11, 16.

prisoners of war if captured.[100] Significantly, given the historical context of the outlawing of mercenarism, Additional Protocol II relating to non-international armed conflicts does not contain any provisions relating to mercenaries.[101]

The definition of a mercenary is set out in Article 47(2) of Additional Protocol I:[102]

> A mercenary is any person who:
>
> (a) is specially recruited locally or abroad in order to fight in an armed conflict;
>
> (b) does, in fact, take a direct part in the hostilities;
>
> (c) is motivated to take part in the hostilities essentially by the desire for private gain and, in fact, is promised, by or on behalf of a Party to the conflict, material compensation substantially in excess of that promised or paid to combatants of similar ranks and functions in the armed forces of that Party;
>
> (d) is neither a national of a Party to the conflict nor a resident of territory controlled by a Party to the conflict;
>
> (e) is not a member of the armed forces of a Party to the conflict; and
>
> (f) has not been sent by a State which is not a Party to the conflict on official duty as a member of its armed forces.

The conditions of the article are cumulative and it is widely considered that taken together the conditions are unworkable against contemporary 'soldiers for hire'.[103] It is particularly difficult to apply the definition to modern-day private military companies for a number of reasons. First, the definition of mercenaries applies only

---

[100] Art. 47(1), Additional Protocol I. Mercenaries are also banned under the 1977 OAU Convention for the Elimination of Mercenaries in Africa and the 1989 International Convention against the Recruitment, Use Financing and Training of Mercenaries.

[101] For an in-depth analysis of the history and evolution of the prohibition against mercenaries see Leslie C. Green, 'The Status of Mercenaries in International Law' in L C Green (ed) *Essays on the Modern Law of War* (Transnational Publishers, Dobbs Ferry, NY, 2000), 529; Todd S Milliard, 'Overcoming Post-Colonial Myopia: A Call to Recognise and Regulate Private Military Companies' (2003) 176 *Mil L Rev* 1.

[102] The same definition can be found in the *International Convention against the Recruitment, Use, Financing and Training of Mercenaries* UN GAOR 44th Sess., Supp No.43, UN Doc. A/RES/44/34 (1989).

[103] See for example Milliard, 'Post-Colonial Myopia', 42; Peter W. Singer, 'War, Profits, and the Vacuum of Law: Privatized Military Firms and International Law' (2004) 42 *Col J Trans L* 521, 524.

to natural persons, so the PMC itself cannot be held accountable. Secondly, because of their corporate structure, individuals are hired and paid as contractors by the company, not by a party to the conflict, which enables them to hide behind its corporate veil. In addition, both contractors and PMC's are often hired for multiple purposes, not for a specific conflict. In some cases nationality may be extended to contractors for the express purpose of avoiding the provisions.[104] Finally, individual contractors may be incorporated into the armed forces of the State or given special status such as detectives, regardless of their nationality.[105] All of these difficulties can be addressed as conditions of the contract of hire, to the extent that that one commentator has been caused to remark that "any mercenary who cannot exclude himself from this definition deserves to be shot – and his lawyer with him!".[106] However, in modern conflicts the increasing use of private contractors and the disjuncture between States' *policy* on the use of contractors in particular roles and their *actual* use, means that despite the ability to manage the risk of mercenary status through contractual terms, some contractors may find themselves exposed.[107] As seen above, in an age of high-tech militaries, where the cost of training soldiers to operate increasingly complex and specialised systems in prohibitive, contractors are being used to deliver, support and in some cases even operate systems. This clearly brings them within the direct participation requirement and the recruitment specifically for the purposes of armed conflict. Individual contractors who are foreign civilians, and are recruited for their specific computer network attack capabilities in respect of a particular conflict are at risk of falling into this category. Private contractors are routinely paid salaries in excess of that paid to their military counterparts, a fact that has caused resentment amongst serving military personnel, and despite the concern over determining the motivation of an individual, many

---

[104] Samia Kazi Aoul, et al., *Towards a Spiral of Violence?*, (2000) <http://www.miningwatch.ca/updir/Memorandum-final-en.pdf> (last accessed 18 August 2008).

[105] For example, a 1997 contract between Sandline International (a PMC) and the government of Papua New Guinea, for provision of military assistance to deal with a secessionist rebel movement on Bougainville Island, provides that Sandline personnel are to be enrolled as "special constables". http://coombs.anu.edu.au/SpecialProj/PNG/htmls/Sandline.html (last accessed 1 May 2006).

[106] P. W. Singer, *Corporate Warriors: The Rise of the Privatized Military Industry* (Cornell University Press, Ithaca, 2003).

[107] See PBS Frontline 'Interview with Peter Singer' *Private Warriors* (PBS interview conducted on 22 March 2005) Available at http://www.pbs.org/wgbh/pages/frontline/shows/warriors/interviews/singer.html. (last accessed 13 September 2008).

contractors operating in Iraq are open about the fact that they are there for financial gain.[108]

It should be noted that Additional Protocol I merely removes combatant privilege and rights to prisoner of war status from a mercenary (thus rendering them an unlawful combatant); it does not criminalize the status of mercenaries, nor does it make criminal the recruiting, training or financing of mercenaries.[109] Such acts are made criminal by both the OAU Mercenary Convention and the U.N. Mercenary Convention, and any contractors found to be in breach of those provisions and their hiring states may be punished.[110] However as Dinstein points out, the U.N. Convention has not been widely ratified.[111]

3. Child Soldiers

It should also be noted that the Optional Protocol to the Convention on the Rights of the Child specifically bars persons under the age of eighteen from taking a direct part in hostilities.[112] Under both Additional Protocols, the age is fifteen.[113] The obligation on States under both Protocols is to 'take all feasible measures' to ensure that children under the specified age do not take a direct part in hostilities.[114] The Appeals Chamber of the Special Court for Sierra Leone held that the prohibition against child recruitment had crystalised as customary international law entailing

---

[108] In 2005 in Iraq, guards working for private military firms could typically make US$400-600 per day, approximately twice the salary of a U.S. soldier. Guards employed by Blackwater (an American PMC, charged with guarding U.S. Ambassador Paul Bremer, the former head of the Coalition Provisional Authority) are paid up to US$1000 a day: Frontline *Private Warriors*, 2005. (PBS: USA, 21 June 2005).

[109] Milliard, 'Post-Colonial Myopia', 41.

[110] Ibid., 19.; *OAU Convention for the Elimination of Mercenaries in Africa,* OAU Doc. CM/433/Rev.L Annex 1; *International Convention against the Recruitment, Use, Financing and Training of Mercenaries*, UN Doc.

[111] Dinstein, *Conduct of Hostilities*, 52.

[112] Arts. 1-4, Optional Protocol to the Convention on the Rights of the Child on the involvement of children in armed conflict UN Doc. A/RES/54/263 (25 May 2000) entered into force on 12 February 2002.

[113] Art. 77(2), Additional Protocol I; Art. 4(3) Additional Protocol II, note however that Additional Protocol II does not make a distinction between direct and indirect participation.

[114] Ibid. A compromise was reached was reached in the drafting of the Optional Protocol to allow more flexibility for those States allowing the recruitment of persons under the age of eighteen into the armed forces. See U.N. Economic and Social Council, *Report of the Working Group on a Draft Optional Protocol to the Convention on the Rights of the Child on Involvement of Children in Armed Conflicts in Its Sixth Session*, UN Doc. E/CN.4/2000/74 (2000) para 57-59.

individual criminal responsibility by 1996.[115] The Commentary to Additional Protocol I states that the parties resolved to use the word 'feasible' as it was used elsewhere in the Protocols and thus it should be understood as meaning 'capable of being done, accomplished or carried out, possible or practicable'.[116] While it is certain that this will prohibit armed forces from actively recruiting minors, there is scope for young volunteers to be utilised. Given the ease with which young hackers (many of which are aged between 12 and 16) can now launch attacks, either through their own skill or by utilising another's coding, consideration must be given to what measures States may be required to put in place to ensure that minors do not participate by launching their own attacks on enemy forces. As Happold has pointed out, whether something is practicable is a question referring to whether in the particular circumstances of the moment, the efforts required to do it are not disproportionate to the results obtained on having done so.[117] It seems likely that any effort to track down and prevent underage hackers would be vastly disproportionate to the result, particularly in circumstances where they are operating outside the battlespace. Armed groups distinct from the national armed forces are not permitted to use, recruit or accept volunteers under the age of eighteen under any circumstances.[118] Certainly statements such as the general admonition issued by the U.S. in respect of patriotic hackers 'joining-in' the conflict in Iraq would be an easy practical measure for States to implement.[119]

---

[115] *Prosecutor v Norman (Decision on Preliminary Motion Based on Lack of Jurisdiction (Child Recruitment))* (2004) SCSL-04-14-AR72(E)-131, Special Court for Sierra Leone, para 53. (with Judge Robertson dissenting).

[116] Pilloud, et al., *Commentary*, 692,900. Note that the commentary on the Optional Protocol argues that a comparison of the French texts implies that the term feasible in the optional protocol should be interpreted more widely than in the Additional Protocols, however admits that its exact interpretation is uncertain and in any event will be controversial given the context of any particular case.Tiny Vandewiele, *Commentary on the United Nations Convention on the Rights of the Child, 46 Optional Protocol : The Involvement of Children in Armed Conflicts* (Martinus Nijhoff Publishers, Leiden; Boston, 2005), 27.

[117] Matthew Happold, 'Child Soldiers in International Law: The Legal Regulation of Children's Participation in Hostilities' (2000) 47 *NIL Rev* 27, 34.

[118] Art. 4, Optional Protocol on the Rights of the Child. States must also take legal measures to prohibit and criminalise such practices.

[119] Gallagher, 'Hackers; Government Tells Vigilantes Their 'Help' Isn't Necessary'.

4. Conclusion

The combination of increased civilianisation and high-tech methods of warfare have raised some interesting challenges for the laws of armed conflict and in particular the determination of combatant status. The decreased relevance of time and proximity to the battlespace, and the nature of the online environment have created problems for the relevance and interpretation of the law requiring distinction between civilian and combatant. While technical solutions are available, they are not without problems of their own. Other requirements of lawful combatancy merely require reinterpretation for the digital age.

One of the main classes of unlawful combatants, civilians engaged directly in hostilities, has also increased in numbers with the changes in the armed forces. While it seems clear that those engaged in proactive offensive computer network attacks will be considered to be taking a direct part in hostilities, the situation is more confused for those taking a less immediate role. Regardless of the difficulties and the need for case-by-case analysis, it is clear that a view must be reached in broad terms as to the line between legitimate support and direct participation so that civilians are not unknowingly conceding their right to protection.

Chapter 6 – Targeting & Precautions in Attack

Computer network operations allow for both the precise targeting of particular systems vital to an adversary's war effort and the ability to cause wide-spread disruption to everyday life. Like any other military operation, when computer network attacks are employed in an armed conflict, targets selected for attack must conform to the principles of distinction, proportionality and necessity; however computer network attacks also raise a number of specific issues with regard to targeting and precautions in attack. In addition to the pressures currently being exerted on the principle of distinction by modern conflict (of which technological advance is a major factor), the question is raised as to when a computer network attack becomes an attack for the purposes of international humanitarian law. Most, although not all, targeting restrictions are based on attacks, and as Michael Schmitt has pointed out, not all computer network attacks will rise to this level. Further, the very nature of the network design means that knock-on effects of attacks can be far reaching. This raises the required level of understanding of the connectivity of the attacked network far above what might be required for a conventional attack in order to exercise the appropriate precautions in attack.

Computer network attacks also increase the opportunities for attacks by allowing the targeting of objectives which would otherwise be prohibited by the principle of proportionality. By minimising collateral damage and incidental injury, targets which would have been off-limits for neutralisation by traditional kinetic means are made permissible by the simple expedient of turning them off.

1. The Principle of Distinction

Article 48 of Additional Protocol I codifies the basic rule that parties must distinguish between civilian objects and military objectives:

> In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives.

This is a modern restatement of the principle of distinction which has been held by the International Court of Justice to constitute one of the "cardinal principles" of the laws of armed conflict and one of the "intransgressible principles of international customary law".[1] It is further enshrined in the Statute of the International Criminal Court which dictates that "intentionally directing attacks against civilian objects, that is, objects which are not military objectives" constitutes a war crime in international armed conflicts.[2] Although neither Common Article 3 nor Additional Protocol II contain any requirements for precautions in attacks,[3] the Appeals Tribunal in the *Tadic* case extended the application of the principle to conflicts not of an international nature. Citing with approval General Assembly resolutions, the Court recognised the principle of distinction as a principle of customary international law applicable "in conflicts of any kind".[4] The Hague Regulations of 1899 and 1907 also lay down certain protections for civilian property and undefended places;[5] specific protections are also provided for cultural property which are discussed in Chapter 8 *infra*.[6] However it should be noted that the Hague Regulations clearly imply that there is no conventional legal prohibition on the bombardment of civilians in defended places.[7] The emphasis on differentiating between defended and undefended targets in the Hague Regulations was made obsolete by developing methods of warfare and was replaced by the development of a definition of 'military objective', consideration of the concept of indiscriminate attacks and the introduction of proportionality in the 1923 Hague Rules of Air Warfare.[8]

---

[1] *Nuclear Weapons Case*, para 79.

[2] Art. 8(2)(b)(ii), Statute of the International Criminal Court .

[3] Art. 13(1), Additional Protocol II contains a general principle that "the civilian population and individual civilians shall enjoy general protection against the dangers arising from military oprations". The commentary notes that this codifies a principle of customary international law, and notes that the implementation of such a protection requires that precautions are taken in both attack and defence: Pilloud, et al., *Commentary*, 1448, para 4772.

[4] *Tadic (Interlocutory Appeal)*, 112, 127.

[5] Art. 23(g) forbids the destruction and seizure of enemy property unless that action is imperatively demanded by the necessities of war. Art. 25 provides the attack or bombardment, by whatever means, of towns, villages, dwellings, or buildings which are undefended is prohibited.

[6] Art. 27, Hague Regulations.

[7] Richard R Baxter, 'The Duties of Combatants and the Conduct of Hostilities (the Law of the Hague)' in UNESCO (ed) *International Dimensions of Humanitarian Law* (Martinus Nijhoff, Dordrecht, 1988) 93-134, 115.

[8] Judith G. Gardam, 'Proportionality and Force in International Law' (1993) 87(3) *AJIL* 391, 400.

The increased targeting opportunities offered by computer network attack capabilities come at a time when changes in the types of armed conflicts and the emerging dominant theory of warfare, namely effects-based operations, are causing an underlying tension in the laws of armed conflict regarding the continued pre-eminence of the principle of distinction in modern warfare. Two schools of thought advocate the expansion of permissible targets to include previously prohibited civilian objects, but for fundamentally different reasons. The first approach is partially expounded in the United States expanded definition of 'military objective' which includes war-sustaining objects, which is discussed in section 2.2 *infra*, and finds its most extreme expression in the work of Charles Dunlap.[9] Dunlap argues:[10]

> We need a new paradigm when using force against societies with malevolent propensities. We must hold at risk the very way of life that sustains their depredations, and we must threaten to destroy their world as they know it if they persist. This means the air weapon should be unleashed against entire new categories of property that current conceptions of LOAC put off-limits.

There is not sufficient room in this thesis for a full discussion of the arguments of Dunlap's paper, and this has been addressed extensively in other places.[11] There are also those who attack the principle of distinction from the opposite side, arguing that the principle relies on an outdated world view in which large-scale interstate wars were the norm.[12] One such author, Gabriel Swiney argues that strict adherence to the principle in an age of non-international armed conflicts violates the equal protection of laws, precluding the rule of law and endangering the lives of those whom it was designed to protect.[13] He argues that asymmetry handicaps insurgent parties in the conduct of non-international armed conflicts, thus forcing insurgent parties to reject

---

[9] Charles J Dunlap, 'The End of Innocence: Rethinking Non-Combatancy in the Post-Kosovo Era' (2000) Summer *Strategic Review* 9.

[10] Ibid., 14.

[11] See for example contributions by Schmitt, Oeter, Parks in Wolff Heintschel von Heinegg and Volker Epping, *International Humanitarian Law Facing New Challenges: Symposium in Honour of Knut Ipsen* (Springer, Berlin; New York, 2007).; Michael N. Schmitt, 'The Principle of Discrimination in 21st Century Warfare' (1999) 2 *Yale Hum Rts & Dev LJ* 143.

[12] Gabriel Swiney, 'Saving Lives: The Principle of Distinction and the Realities of Modern War' (2005) 39 *International Lawyer* 733.

[13] Ibid., 733.

the laws of armed conflict because to do otherwise would mean defeat. Major powers bend the principle to suit their needs by utilizing the civilian sector as contractors and using civilian settlers to effect their occupations (Swiney cites as examples, Israel and Sri Lanka).[14] Both the approaches advocated by Dunlap and Swiney seek to undermine the principle of distinction albeit for different reasons.

The principle of distinction has been under threat before. As Stephen Oeter points out, the principle of distinction has always belonged to the basic set of rules which in practice were put into doubt by belligerents who were not willing to restrict their use of violence as soon as such restrictions were perceived as being harmful to their strategies.[15] However the current threat stems from the multiple layers of movement currently happening in relation to armed conflict; many of these are both a product of, and instrumental in, the advance of military technology. One effect which is not, however, is at the politico-societal level where a move from conflicts occurring over resources and territory to conflicts for the purpose of shaping decision-making processes is taking place.[16] This shift in the underlying purposes of conflict is also seen in the changing goals of warfare in the modern era toward influencing political changes rather than outright military victory. An example of such a 'compellance' or 'coercive' campaign was seen in the NATO intervention over Kosovo, where force was applied in order to coerce Milosevic to abandon a policy of ethnic cleansing in the area.[17] At the strategic level, there is a movement in the dominant theory of warfare in the West from attrition warfare towards effects-based operations which are designed for coercive campaigns. Effects-based operations represent the operationalisation of network-centric warfare.[18] In attrition warfare the purpose is to

---

[14] Ibid., 750.

[15] Stefan Oeter, 'Comment: Is the Principle of Distinction Outdated?' in W H v Heinegg and V Epping (eds), *International Humanitarian Law Facing New Challenges* (Springer, Berlin; New York, 2007) 53-65, 55.

[16] Gray, *Another Bloody Century;* Smith, *Utility of Force*, 270.; Chapter 1 *supra.* Although this may not represent a permanent trend as predictions are that conflicts based on resources, particularly water, are expected to increase with environmental changes brought about by global warming. See generally, Klare, *Resource Wars: The New Landscape of Global Conflict.*

[17] Schmitt, 'Asymmetrical Warfare', 36-38. Attacks on industrial facilities in Bor and Smederevo were designed to put pressure on cronies of President Milosevic to influence him to withdraw his troops. Arkin and Windrem, 'The Other Kosovo War'; Marc J. Romanych and Kenneth Krumm, 'Tactical Information Operations in Kosovo' (2004) September-October 2004 *Military Review* 56.

[18] See generally, Smith, *Effects Based Operations*, 1.

significantly weaken the military forces of the opposing side in order to destroy their physical capacity to wage war. In effects-based operations, the purpose is to coerce the other side using a combination of force and other non-forceful methods such as diplomacy to effect change at the political level.[19] This tempts military commanders to attack any target which will achieve the aims of the operation, and hence end the war, in the most effective manner possible; many times these will be civilian targets.[20] At the technological level, advancement of weapons technology allows technologically advanced militaries to strike almost any target they choose in the battlespace. On top of this uneasily shifting structure sits computer network attack. Computer network attacks not only increase the number of targets that it is possible to attack by reducing the collateral damage and hence the proportionality equation in target selection, they also allow the possibility of operations which cause no physical damage but nonetheless destroy or merely neutralize the object or system in question. This is an attractive option for States, particularly in conflicts which will necessitate the reconstruction of the battlespace at the conclusion of hostilities; it is inefficient to bomb a power generating station, if you can simply turn it off.

2. Legitimate Military Objectives

The principle of the military objective has become part of the customary international law for armed conflict, at sea as well as on land or in the air.[21] In 1977 the principle was codified and a definition of the term 'military objectives' was included in Article 52(2) of Additional Protocol I:[22]

> Attacks shall be limited strictly to military objectives. In so far as objects are concerned, military objectives are limited to those objects which by their nature,

---

[19] Effects-based operations are not new. Their roots can be traced back for centuries and are what good generals and statesmen have always attempted to do. When combined with network-centric thinking and technologies, however, such an operational approach offers a way of applying the power of the network to the human dimension of war and to military operations in peace and crisis, as well as combat. Ibid., xxiii.

[20] Schmitt, *High and Low-Tech Warfare*, 8.

[21] Horace B. Robertson, 'The Principle of the Military Objective' (1997-1998) 8 *US AF Acad J Legal Stud* 35, 46.; See also Yoram Dinstein, 'Legitimate Military Objectives under the Current Jus in Bello' in A E Wall (ed) *Legal and Ethical Lessons of NATO's Kosovo Campaign* (Naval War College, Newport, Rhode Island, 2002) 139-173, 140.

[22] The definition of military objectives also appears in several subsequent instruments: Additional Protocols II & III, Annexed to the 1980 Conventional Weapons Convention, and the second protocol to the Cultural Property Convention. See Dinstein "Legitimate Military Objectives", 141.

> location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.

The definition contains several elements which raise interesting questions in relation to computer network attacks. The first is easily dealt with, the definition relates to objects (or in the French text 'biens'), which the ICRC commentary notes refers to something visible and tangible.[23] It could be argued that only material tangible things can be targets,[24] and thus the intangible nature of many computer network attack targets exclude them from that definition. However, it is clear from the text of the commentary that this definitional point is being made to distinguish the term object as a 'thing' from its use in the sense of 'aim or purpose of an operation', rather than to exclude an intangible object from the definition. Thus any computer program, database, system, or virtual network would still be a legitimate target if it meets the above definition, regardless of whether it has a tangible component or exists purely as lines of code.

2.1. Nature, Location, Purpose & Use

The criteria imposed by Article 52(2) is that the prospective target must by its nature, location, purpose, or use make an effective contribution to military action.[25] Objects which by their nature make a contribution to military action comprise all objects directly used by the armed forces: weapons, equipment, transports, fortifications, depots, buildings occupied by the armed forces, staff headquarters, communications centres etc.[26] To meet this yardstick they must have something in their intrinsic

---

[23] Pilloud, et al., *Commentary*, para 2008-2010.

[24] Marco Sassòli, 'Targeting: The Scope and Utility of the Concept of "Military Objectives" for the Protection of Civilians in Contemporary Armed Conflicts' in D Wippman and M Evangelista (eds), *New Wars, New Laws?: Applying the Laws of War in 21st Century Conflicts* (Transnational Publishers, Ardsley, N.Y., 2005) 181-210, 185.

[25] The formulation was influenced by that proposed in Art. 2 of the Edinburgh resolution of the Institute of International Law, which defined military objectives as facilities which by their "very nature or purpose or use, make an effective contribution to military action, or exhibit a generally recognised military significance, such that their total or partial destruction in the actual circumstances gives a substantial, specific and immediate military advantage to those who are in a position to destroy them". Bothe, et al., *New Rules*, 321.

[26] Pilloud, et al., *Commentary*, para 2020.

character, an inherent attribute which contributes to military action.[27] In terms of targets for computer network attack this would include all weapons systems, sensor arrays, battlefield devices, military networks and databases, digital communications systems and any other military specification digital device or system.[28]

Location is the second criterion set out by the article. As noted by the ICRC commentary, there are objects which by their nature have no military function but which by virtue of their location make an effective contribution to military action. Examples relating to computer network attack are not easily come by given the inherent nature of networks. The existence of multiple pathways to the same destination provides a network with its efficiency and robustness, and in the case of the Internet, the physical location of nodes in the network is not of primary importance. However there may be circumstances where location plays a role in computer network attacks where it may be important to deny a network or other object to the enemy. For example, a civilian wireless network may exist in a particular area that would enable the adversary's military located in the area to piggy-back military communications off the signal in the event of the military network being disabled or to usurp the use of the network entirely.[29] The primary connection nodes of a State's internal telecommunications network to the Internet backbone would make attractive targets, depending on the level of connectivity of the particular State.[30]

---

[27] Dinstein, *Conduct of Hostilities*, 88.

[28] Note that this would not include medical devices, databases or networks which are subject to measures of special protection. See Chapter 7 *infra*.

[29] For example, some areas have entire cities connected with wireless networks i.e. Toronto. These are not restricted to developed areas, wireless communications technology is fast becoming one of the steps in developing communications infrastructure in parts of Africa. See for example Mark Cieslak "Bridging an African Digital Divide" BBC Click Online, 7 September 2007 Available at http://news.bbc.co.uk/1/hi/programmes/click_online/6983397.stm (last accessed 10 September 2007).

Art. 53 of the Hague Regulations allows an army of occupation to take possession of "Railway plant, land telegraphs, telephones, steamers and other ships, apart from cases governed by maritime law, as well as depots of arms and, generally, all kinds of munitions of war, even though belonging to companies or to private persons, are likewise material which may serve for military operations, but they must be restored at the conclusion of peace, and indemnities paid for them." This allows an occupying force to take control of all lines of communication including all networks.

[30] For example, New Zealand connects to the Internet backbone through primary nodes which provide connections through three undersea cables, the Pacrim, Tasman 2 and Southern Cross fibre-optic cables. Disabling these nodes would effectively cut New Zealand off from all but satellite communications. Many countries have similar limited connections to the backbone. For example, the Eastern African Submarine Cable System provides fibre-optic cable links for South Africa, Sudan, Mozambique, Madagascar, Tanzania, Kenya and Djibouti. Each of the nodes connecting to the

The criteria of purpose and use are linked – purpose is concerned with the intended future use of an object, while use is concerned with its present function.[31] Dinstein notes that military purpose should be deduced from an established intention of a belligerent as regards future use.[32] He warns it must be predicated on intentions known to guide the adversary, not on those figured out hypothetically in contingency plans based on a 'worst-case scenario'.[33] Actual use of an object which makes an effective contribution to military action will likewise render the object a military objective and thus liable to attack. In the event that there is any doubt over whether an object which is normally a civilian object is being used to make an effective contribution to military action, Article 52(3) provides a presumption that it is not being so used. Should a computer network attack be launched from a civilian computer system or network, that network would become a legitimate military objective and may be attacked (presuming that its destruction, capture or neutralisation also provides a definite military advantage to the attacking State).[34] This is significant for countries such as the United States where a large percentage of all military communications are transmitted over civilian networks,[35] making them a potential target for computer network attacks.

2.2. Effective Contribution to Military Action

The second part of the definition requires that the object must make an effective contribution to military action. While all parties accept this provision as a statement of customary international law, there is some variation in the interpretation of the scope of the contribution to military action required. Bothe et al point out in their

---

national networks would present an attractive target. IRIN News Report "Africa: Getting Connected at Last" 24 January 2006.

[31] Pilloud, et al., *Commentary*, para 2022.

[32] Dinstein, *Conduct of Hostilities*, 89-90.

[33] Ibid. Dinstein cites the example of the Abbey of Monte Cassino as a warning against reliance on supposition backed by flimsy intelligence.

[34] In much the same way, civilian taxis commandeered by the military governor of Paris to transport reservists to the front in 1914 became military objectives.

[35] In 1995 more than 95% of all U.S. military communications were sent across civilian networks. A more recent figure has not been made publically available. Aldrich, 'International Legal Implications', 105.citing Science Applications International Corporation, "Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance," research report for the chief, Information Warfare Division (J6K), Command, Control, Communications and Computer Systems Directorate, Joint Staff, The Pentagon, Washington, D.C., 4 July 1995.

commentary to the Protocol, that the requirement of effective contribution relates to military action in general, and there need be no 'direct connection' with specific combat operations such as that required of civilians who lose their immunity for directly participating in hostilities.[36] Despite being a broader requirement than 'direct participation', there remains disagreement over the level of connection to military action required.

The United States substitutes the words "war-fighting or war-sustaining capability" for the term 'military action' as used in the Protocol.[37] Using the targeting of Confederacy cotton production in the American Civil War as an example, it argues that "[e]conomic targets of the enemy that indirectly but effectively support and sustain the enemy's war-fighting capability may also be attacked".[38] The report on U.S. practice provided for the ICRC work on customary international law explains that while the U.S. accepts the customary nature of Article 52(2), the alternative formulation reflects its position that this definition is a wide one which includes areas of land, objects screening other military objectives and war-supporting economic facilities.[39] Other authors disagree with this position; for example Dinstein argues that the reference to 'war-sustaining capability' goes too far, opening a slippery slope in which just about every civilian activity could be construed as indirectly sustaining the war effort.[40] The present author agrees, taken to its logical conclusion the U.S. position means that any goods or services which support the economy of the country (and thus the ability of the government to wage war) would become legitimate targets. As Stefan Oeter has pointed out, the U.S. targeting of war-sustaining capabilities moves the target of military operations away from the military effort of the enemy and onto the political command and control system and

---

[36] Bothe, et al., *New Rules*, 324.

[37] The latest military manual to be released in the United States is the *U.S. Commander's Handbook on the Law of Naval Warfare* NWP 1-14M it is useful as the most current expression of U.S. policy in this area. The reference to war-sustaining capability is set out in paragraph 8.2.

[38] Michael N. Schmitt, 'Fault Lines in the Law of Attack' in S Breau and A Jachec-Neale (eds), *Testing the Boundaries of International Humanitarian Law* (British Institute of International and Comparative Law, London, 2006) 277-307.

[39] Jean-Marie Henckaerts and Louise Doswald-Beck, *Customary International Humanitarian Law* (Cambridge University Press, Cambridge, 2005), 31.

[40] Dinstein, *Conduct of Hostilities*, 87. For an extreme application of the U.S. position and an example of Dinstein's concerns regarding a slippery slope see Dunlap, 'The End of Innocence: Rethinking Non-Combatancy in the Post-Kosovo Era'. Dunlap suggests that any object, civilian or military, not indispensable to the civilian population should be fair game.

its resource base; this approach gives up the requirement of a close nexus between the target and ongoing military operations.[41]

This disparity in interpretation will have particular relevance in respect of computer network attacks against highly developed information societies where the propensity for damage is higher. Consider for example the damage which could be inflicted on a State which is dependant on the export of a natural resource such as oil or minerals. Destruction of the immediate processing plants of the State can be justified as making an effective contribution to the military effort, however destruction of the resource itself would effect the long-term economic welfare of the State and be too far removed from military action to justify the attacks.[42] Contrast that with the economic meltdown which would be achieved in attacks aimed at the commercial heart of an information-based economy such as Taiwan. Taiwan is one of the most information technology dependant economies in the world; one of their greatest fears is that China will unleash a wave of computer network attacks which will completely shut down political and economic institutions in a matter of days.[43] Under the U.S. interpretation such attacks would be permissible as the economy and therefore war-sustaining capability of the target state would be affected. There is also a question about what would constitute an attack which is dealt with in section 4.1 *infra.*

However a balance must be struck between legitimate economic measures in wartime, for example a sanctions regime or measures which destabilise or devalue a State's currency or credit,[44] and military operations targeting legitimate military objectives. This is particularly so in the case of coercive campaigns where measures are designed to effect a change in the decision-making behaviour of the adversary. A similar effect, albeit on a smaller scale, was seen in the cyber attacks against Estonia

---

[41] Oeter, 'Comment: Is the Principle of Distinction Outdated?' 56.

[42] Schmitt, 'Fault Lines', 281.

[43] 'Taiwan Plays Cyber War Games', *BBC News* 7 August 2000, <http://news.bbc.co.uk/1/hi/world/asia-pacific/870386.stm> (last accessed 15 September 2007). See also David Lague, 'Chinese See Military Dependence on Computers as Weakness', *International Herald Tribune* (Paris), 29 August 2007, Asia Pacific <http://www.iht.com/articles/2007/08/29/news/cyber.php> (last accessed 15 September 2007). Although some analysts argue that Taiwan's advanced computing and information technology industry would allow the islands military to resist cyber attack more readily than China's mounting conventional firepower.

[44] For example the United States refusal to back the pound sterling during the Suez Crisis in 1956 led to a monetary crisis for the British economy, forcing it to call off its campaign.

in April and May 2007.[45] The prolonged distributed denial of service attacks, which lasted over a month, came close to shutting down the country's digital infrastructure, clogging the websites of several government agencies, several newspapers and forcing the country's main bank to cease operations. Estonia is one of the most wired societies in Europe, using the Internet for everything from voting, filing taxes and paying for parking.[46] Under U.S. targeting analysis such measures would be legally justified if they were to take place during the course of an armed conflict.

2.3. Definite Military Advantage

The definition of military objective in Article 52 also requires that the destruction, capture or neutralisation of the object in question must provide a "definite military advantage". Although there was much discussion in the working group that drafted the provision regarding the appropriate adjective to be applied to the term 'military advantage', on reporting back to the conference the Rapporteur commented that he was unable to draw any significance from the particular choice of 'definite'; Bothe et al conclude that the adjective is a word of limitation denoting in this context a concrete and perceptible military advantage rather than a hypothetical and speculative one.[47]

The advantage gained must also be military in nature and not, for example, purely political.[48] Thus as Dinstein notes, forcing a change in the negotiating attitudes of the adverse Party cannot be deemed a proper military advantage. That is not to say that once a potential target has met the criteria as a military objective, the choice between two competing objectives cannot be motivated by which one would produce a favourable political result. The targeting choices made by NATO forces in the Kosovo campaign as the conflict progressed provide a good illustration of politically directed target selection process aimed to force Milosevic to capitulate to NATO

---

[45] See Chapter 1 *supra* and Appendix 1 for further details.

[46] Mark Landler and John Markoff, 'Digital Fears Emerge after Data Seige in Estonia', *New York Times* 29 May 2007, <www.nytimes.com/2007/05/29/technology/29estonia.html> (last accessed 20 August 2007); Traynor, 'Russia Accused of Unleashing Cyberwar to Disable Estonia'.

[47] Bothe, et al., *New Rules*, 326.

[48] Dinstein, *Conduct of Hostilities*, 86.

demands.[49] Dinstein also notes that the scope of the advantage should be wider than purely tactical.[50] Australia, Canada and New Zealand have stated that the term 'military advantage' includes the security of the attacking forces.[51] In an age of coalition warfare, it should also be noted that the military advantage gained may also constitute a benefit for an allied force or the alliance as a whole.[52]

A further question that arises is whether the military advantage gained must result from a single attack. In an age of network centric warfare the individual targeting of small parts of an integrated system will accrue to contribute to a military advantage that would not necessarily be apparent from neutralising a single part of the system. For example, in order to incapacitate a communications network it may be necessary to neutralise all nodes in the network to achieve the anticipated military advantage. Each node must be attacked separately, but without the neutralisation of all parts, the advantage will not be gained. The attack on the Radio-Television Serbia (RTS) television centre in Belgrade as part of an attack on the Federal Republic of Yugoslavia (FRY) communications network during the Kosovo conflict was an example of this approach.[53] According to NATO reports the FRY command and control network was a complex web and could not be disabled in one strike. In actual

---

[49] Although all targets selected were military objectives (under the U.S. definition), the later part of the bombing campaign focused on industrial targets belonging to Milosevic's cronies. See generally Judith Millers Comments in Andru E. Wall, *Legal and Ethical Lessons of NATO's Kosovo Campaign* (Naval War College, Newport, R.I., 2002), 110. Stephen T. Hosmer, *The Conflict over Kosovo: Why Milosevic Decided to Settle When He Did* (RAND, Santa Monica, 2001) <http://www.rand.org/publications/MR/MR1351/> (last accessed 1 September 2007); Benjamin S. Lambeth, U.S. Air Force and Project Air Force, *NATO's Air War for Kosovo: A Strategic and Operational Assessment* (RAND, Santa Monica, 2001), 13 <http://www.rand.org/publications/MR/MR1365/> (last accessed 15 September 2008).

[50] Dinstein, *Conduct of Hostilities*, 86.

[51] Henckaerts and Doswald-Beck, *Customary International Humanitarian Law*, 50.

[52] Dinstein, *Conduct of Hostilities*, 86. Citing H Meyrowitz "Le Bombardement Stratégique d'après le Protocole Additionnel I aux Conventions de Genève" (1981) 41 ZaöRV 1, 41.

[53] The bombing of the TV studio was part of a planned attack aimed at disrupting and degrading the C3 network. In co-ordinated attacks, on the same night, radio relay buildings and towers were hit along with electrical power transformer stations.... The FRY command and control network was alleged by NATO to comprise a complex web and that could thus not be disabled in one strike. As noted by General Wesley Clark, NATO "knew when we struck that there would be alternate means of getting the Serb Television. There's no single switch to turn off everything but we thought it was a good move to strike it and the political leadership agreed with us" ICTY, *Final Report to the Prosecutor of the Committee Established to Review the NATO Bombing Campaign against the Federal Republic of Yugoslavia*, ICTY (2000) paras 72 & 78 <www.un.org/icty/pressreal/nato061300.htm> (last accessed 16 September 2007).

fact, RTS was broadcasting again in just over three hours.[54] The investigating committee found that:[55]

> With regard to these goals, the strategic target of these attacks was the Yugoslav command and control network. The attack on the RTS building must therefore be seen as forming part of an integrated attack against numerous objects, including transmission towers and control buildings of the Yugoslav radio relay network which were "essential to Milosevic's ability to direct and control the repressive activities of his army and special police forces in Kosovo" (NATO press release, 1 May 1999) and which comprised "a key element in the Yugoslav air-defence network" (*ibid,* 1 May1999).

Oeter points out that although Additional Protocol I relies on a specific concept of 'attack' as an "isolated ground operation by a specific unit", such an approach ignores the problems resulting from modern strategies of warfare which are based on an integrated series of separate actions forming one ultimate compound operation.[56] Rogers addresses this point, noting that although a particular offensive may combine infantry, tanks, artillery, helicopters and other close support aircraft in coordinated actions, each would amount to an attack, as would the whole.[57] Several States have made statements on ratification of the Protocol stating that the military advantage anticipated from an attack is intended to refer to the attack as a whole and not from isolated or particular parts of the attack.[58] The ICRC commentary to the Article suggests that such a statement is redundant: "it goes without saying that an attack carried out in a concerted manner in numerous places can only be judged in its entirety" the commentary goes on to say "this does not mean that during such an attack actions may be undertaken which would lead to severe losses among the civilian population or to extensive destruction of civilian objects".[59]

---

[54] Raising the issue of the importance of the military advantage gained by the attack *vis-à-vis* the civilian casualties. Ibid., para 78.

[55] Ibid.

[56] Stefan Oeter, 'Methods and Means of Combat' in D Fleck (ed) *The Handbook of Humanitarian Law in Armed Conflicts* (Oxford University Press, Oxford, 1995) 105-207, 162, §444.

[57] Rogers, *Law on the Battlefield*, 29.

[58] See statements made by Australia, Belgium, Canada, France, Germany, Italy, the Netherlands, New Zealand, Nigeria, Spain and the United Kingdom.

[59] Pilloud, et al., *Commentary*, para 2218. cited in Rogers, *Law on the Battlefield*, 29.

As the ICRC *Customary International Humanitarian Law* study indicates, numerous States have pointed out that those responsible for planning, deciding upon or executing attacks necessarily have to base their decisions on the assessment of the information from all sources which is available to them at the time.[60] How much information is necessary for a computer network attack and how sophisticated the network intelligence should be, is addressed *infra* under precautions in attack.

3. Dual Use Technology

The term dual use target is not a term of international humanitarian law. It is a term which has become popular in various quarters to refer to an object that has concurrent civilian and military uses. In terms of international humanitarian law however, once an object is used in such a way that it meets the definition of a military objective, it loses its civilian status and becomes liable to attack. The discussion of any civilian aspect or purpose of that piece of technology should therefore be considered under the proportionality equation rather than confusing the distinction question.

One of the often cited examples of the attack of a so-called dual use target is the coalition bombing of the Iraqi electrical grid in the 1991 Gulf War. Yoram Dinstein effectively reviews the outcome of that campaign as follows:[61]

> Since the electrical grid in Iraq was totally integrated, attacks against it – and its installations – resulted not only in a tremendous military advantage (shutting down radar stations, military computers, etc.), but also extensive damage to civilians: hospitals stopped operating, water pumping facilities came to a standstill, etc. From a legal point of view, a "dual use" of Iraq's electrical grid did not alter its singular and unequivocal status as a military objective. There was, as usual with military objectives, the question of proportionality where collateral damage to civilians is concerned. But the extensive damage to civilians was not excessive in relation to the military advantage anticipated.

---

[60] Henckaerts and Doswald-Beck, *Customary International Humanitarian Law*, 50.

[61] Comment by Yoram Dinstein in 'Discussion' in A E Wall (ed) *Legal and Ethical Lessons of NATO's Kosovo Campaign* (Naval War College, Newport, Rhode Island, 2002) 211-222, 219.

In terms of computer network attack however, most computer technology, hardware and software, has become dual-use. Some systems initially designed for military use have become so integrated into civilian society that any interference or disruption caused by computer network attacks would have serious effects on civilians. The Global Positioning System (GPS), for example, is a U.S. military system which has become integrated into many civilian applications from aircraft traffic control to cell phones and laptops and even the Internet itself.[62] Disruption of the service through jamming or blocking,[63] or spoofing the signal via computer network attack would cause massive disruption and potentially endanger civilian lives.[64] Other countries operate (or are in the process of developing) similar systems which would exhibit similar vulnerabilities.[65]

In the modern era of effects-based operations dual use targets become particularly attractive targets precisely because of their ties to both military and political objectives.[66] The attacker not only benefits from the destruction or neutralisation of the target's military value, but also from cumulative effects on the civilian population.[67]

4. Civilian Objects

In addition to Article 48 of Additional Protocol I outlined above which provides the basic rule, Article 52(1) provides that "civilian objects shall not be the object of

---

[62] GPS uses two levels of signal, the military signal (Y-code) is more accurate and encrypted, the less secure civilian code (or P-code) is not and thus makes it more susceptible. The precision timing provided by the GPS system is needed to the accurate routing of information packets through computer networks.

[63] Both are methods of electronic attack which will not be covered by this thesis.

[64] Spoofing the GPS signal involves feeding a GPS receiver a fake signal so that it computes the wrong time or location of the receiver. Spoofing can occur either through electronic means (such as broadcasting a fake GPS signal with a higher signal strength than the true signal via a GPS satellite simulator) or through the network to GPS receivers. Note that the military has specific anti-spoofing measures in place which encrypt the general civilian P-code signal into a more secure Y-code which only military receivers can use. All military GPS acquisitions post 2006 are required to have the Selective Availability Anti-Spoofing Module (SAASM) attached. See generally, Scott Pace, et al., *The Global Positioning System: Assessing National Policies* (RAND, Santa Monica, 1995) <http://www.rand.org/publications/MR/MR614/> (last accessed 13 September 2008); Symmetricon, *Why Convert to a SAASM Based Global Positioning System (GPS)?*, (2006) <http://www.symmttm.com/pdf/gps/SAASM_2006_wp.pdf> (last accessed 25 September 2007).

[65] For example, the Russian GLOSNASS system, Chinese Beidou system or the European Galileo system.

[66] Schmitt, 'Targeting', 65.

[67] Ibid.

attack or of reprisals". The International Court of Justice stated in its *Nuclear Weapons* Advisory Opinion that "States must never make civilians the object of attack".[68] The Rome Statute makes it a war crime to intentionally direct attacks against the civilian population as such, individual civilians or civilian objects.[69] Civilians are non-combatants, and are neither members of the armed forces nor do they directly participate in conflict.[70] The civilian population is defined in Article 50(2) of Additional Protocol I as comprised of "all persons who are civilians"; the presence of persons who are not civilians in the population does not deprive the population of its civilian character.[71] Civilian objects are defined as all objects which are not military objectives.[72] Where there is doubt over the civilian character of a person or an object, the doubt is resolved in favour of finding civilian status.[73] The problem of civilians directly participating in conflict, a particular problem in relation to modern warfare and computer network attacks in particular is dealt with in Chapter 5 *supra.*

As a general proposition, it is prohibited to direct computer network attacks against civilian objects in the same manner that a conventional attack would be prohibited. Thus attacks against oil pipelines, civilian air traffic control or rail networks, emergency response networks, financial institutions and other civilian objects are prohibited. During the NATO action over Kosovo, there were legal concerns expressed inside the U.S. administration regarding proposals to conduct information operations such as inserting viruses into Serbian computer systems or hacking bank accounts thought to contain funds plundered from Serbian businesses by Milosevic's cronies.[74] However, the nature of computer network attacks raises some interesting dilemmas for modern armed forces. In addition to the issues raised by the 'war-

---

[68] *Nuclear Weapons Case*, para 78.

[69] Art. 8(2)(b)(i)-(ii) Additional Protocol I.

[70] Art. 50(1) Additional Protocol I provides "A civilian is any person who does not belong to one of the categories of persons referred to in Article 4 A (1), (2), (3) and (6) of the Third Convention and in Article 43 of this Protocol. In case of doubt whether a person is a civilian, that person shall be considered to be a civilian".

[71] Arts. 50(2) & (3) Additional Protocol I.

[72] Art. 52(1) Additional Protocol I.

[73] Arts. 50(1) & 52(3) Additional Protocol I.

[74] Arkin and Windrem, 'The Other Kosovo War'.

sustaining' phraseology of the United States' interpretation which are discussed above, computer network attacks raise some issues for the law of targeting. First, computer network attacks do not necessarily result in physical damage, death or injury, thus opening a range of possible targets for attack which might otherwise be unreachable due to excessive collateral damage. A second and related point is that computer network attacks can be designed to result in a range of outcomes, allowing the attacker to merely disable or neutralise a particular target without causing permanent damage or destruction. Such computer network operations may not even rise to the level of an 'attack' at all.

4.1. Attacks and Operations

The ability of a computer network attack to neutralise or destroy target systems without causing physical damage raises an interesting question with regard to the legitimate targets of such attacks. Although the basic rule laid down in Article 48 of Additional Protocol I is general in nature,[75] the majority of the provisions relating to targeting of civilians and civilian objects are phrased in terms of the prohibition of 'attacks'. Attacks are defined in Article 49 of Additional Protocol I as "acts of violence against the adversary, whether in offence or defence".[76] Bothe et al's commentary to Article 49 states that the term 'acts of violence' denotes physical force and thus the concept of attacks does not include dissemination of propaganda, embargoes or other non-physical means of psychological, political or economic warfare.[77] However it should be noted that any act of violence fills this requirement: not only massive air attacks or artillery barrages but also small scale attacks such as a sniper firing a single round.[78] This has led to a disagreement between commentators, particularly in the area of computer network attacks, regarding the legality of directing non-violent computer network attacks against civilian objects. The problem is particularly relevant in respect of modern armed conflicts, not only

---

[75] Art. 48 provides: "In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives."

[76] Note that this only applies to objects on land.

[77] Bothe, et al., *New Rules*, 289.

[78] Dinstein, *Conduct of Hostilities*, 141.

because of the technology now available to modern militaries but also because of the transformation in the character of warfare towards effects-based operations and the increased importance in the use of force to influence decision-making patterns rather than for territorial gain or control of resources.[79]

It is common ground that computer network attacks which result in physical damage to civilian property, injury or death to civilians constitute attacks under international humanitarian law and are thus prohibited.[80] However, the status of computer network attacks that do *not* result in such deleterious effects remains the subject of debate. Knut Dörmann argues that physical damage is not a requirement of an attack.[81] He points out that the definition of a military objective refers to neutralization of an object as the possible outcome of an attack. He thus concludes that the mere disabling of an object, such as shutting down an electricity grid, without destroying it should also qualify as an attack.[82] Dörmann's argument relies on the location of the definition of 'military objective' in the section dealing with attacks against civilian objects. However the argument fails to acknowledge that the use of the term 'military objective' in Additional Protocol I is not restricted to articles and paragraphs detailing the permissible objects of attacks.[83] Further, the term 'neutralization' was added to the definition by the drafting committee without much explanation. However it is clear that an object may also be neutralised by a conventional attack, that is, one which causes death, injury or destruction, therefore

---

[79] See Chapter 1 *supra*, also see generally, Gray, *Another Bloody Century;* Smith, *Utility of Force.* This is by no means to suggest that the use of force against civilians or civilian objects to influence their governments is a creation of the modern military. WWII bombing campaigns are a prime example of operations specifically targeting civilian morale.

[80] See the discussion in Chapter 3 *supra* regarding armed attacks.

[81] Dörmann, 'Additional Protocols', 142-143.

[82] Ibid. Dörmann uses Bothe et al's commentary which provides (in full): "The term "neutralization", insofar as it deals with bombardment, refers to an attack for the purpose of denying the use of an object to the enemy without necessarily destroying it. For example, a specific area of land... might be neutralised by laying landmines on it, thus denying its use to the enemy. Enemy artillery or surface-to-air missiles may be neutralized for a sufficient time to prevent their interference with a planned operation by firing antipersonnel munition at such targets in an attempt to force gun crews to take shelter. Such an attack would not be likely to destroy their intended target, but it would neutralize the target for the limited time required by the attacker." Bothe, et al., *New Rules,* 325.

[83] Art. 48 refers to military operations directed against military objectives; Arts. 51(7) also refers to military objectives in the context of military operations.

the inclusion of the term cannot shed any light on whether or not an operation which does not cause such effects meets that definition.

Bothe et al's commentary's conclusion that the concept of attacks does not include dissemination of propaganda, embargoes or other non-physical means of psychological, political or economic warfare, is supported by state practice.[84] Michael Schmitt expands on this argument, noting the different wording between Article 48 which relates to 'military operations' and Article 52(2) and surrounding which are all framed in terms of 'attacks'.[85] Schmitt argues that the disparity in the terminology means that CNA operations which are not designed to, nor would foreseeably cause, injury, death, damage, or destruction, may be directed against non-military objectives.[86] Should this be the case, it opens up a range of targets for the military which may not be attacked but may be targeted in other ways; computer network attack technology could open up large swathes of permissible targets which may better serve the coercive element of effects based operations. However, the assertion that the distinction allows States to deliberately target, but not 'attack', civilian objects in ways not designed to cause injury, death etc must be examined further.

The present author agrees that there is a distinction between military operations and attacks, however it does not follow that non-violent computer network attacks may be therefore conducted against civilian objects. Article 48, setting out the basic rule, prohibits 'operations' rather than attacks, and while it is agreed that the term operations should refer to *military* operations (as opposed to any other activity supporting the war effort), the term is in no way synonymous with attacks. The ICRC Commentary to Article 48 sets out that the word operations should be understood in the context of the whole of the section; it goes on to set out the dictionary definition of military operation which "refers to all movements and acts

---

[84] Bothe, et al., *New Rules*, 289. See for example the U.S. intervention in Suez as an example of economic warfare; examples of propaganda from WWII onwards; sanctions etc as acts of political warfare.

[85] Schmitt, 'Wired Warfare', 194.

[86] Ibid.

related to hostilities that are undertaken by the armed forces".[87] This interpretation is echoed by the commentary provided by Bothe et al who note:[88]

> "As used in Protocol I, this term deals generally with those aspects of military operations that are likely to cause civilian casualties or damage to civilian objects. Generally, the provisions of this section regulating attacks and other violent phases of military operations do not necessarily affect movement or manoeuvres by which a military unit secures or exercises dominion and control over key terrain features, lines of communication and avenues of approach. ...The discussion in the preceding paragraph of the operation to take a non-defended place which is open to occupation without resistance is equally relevant to the term "military operation". Nevertheless, such operations when carried out in areas containing a dense concentration of civilians present the adverse Party with a military target and invoke the obligation of Art. 58 to take feasible and appropriate precautions"

The reference to the discussion in the preceding paragraph refers to a discussion on the permissibility of entering and occupying a non-defended locality and exercising 'dominion and control' over such an area without contravening the prohibition on 'attacks by any means whatsoever'. Thus the commentary states the need to take precautions in attack when conducting military operations in dense concentrations of civilians. Schmitt argues that the general acceptance by the international community of psychological operations as an element of warfare, operations which he describes categorically as 'military operations', suggests that the term is shorthand for attacks in which physical violence is the consequence. The commentaries would appear to suggest otherwise. The fact that acts associated with the application of violence, such as movement and manoeuvre, do not necessarily result in violent consequences of their own does not exempt them from the requirement to take precautions in attack when they take place in dense concentrations of civilians, a requirement of a military operation, not just an attack. Article 57(1) sets out the general rule relating to military operations and continues in Article 57(2) which relates specifically to attacks. The commentary to Article 57 states "The term 'military operations' should be understood to mean any movements, manoeuvres and other activities whatsoever

---

[87] Pilloud, et al., *Commentary*, para 1875. This is also reiterated in the commentary to Article 51 (Protection of the Civilian Population).

[88] Bothe, et al., *New Rules*, 286.

carried out by the armed forces with a view to combat".[89] Therefore, wherever an act takes place in conjunction with the application of force it must be restricted to military objectives. Such an approach is also consistent with the position adopted by several State Parties to the Protocol which made reservations or declarations interpreting the military advantage to be gained from an attack as a whole not merely a part.[90] Thus to be a prohibited military operation the computer network attack must be associated with the use of physical force, but it does not have to result in violent consequences itself. The proximity calculation is similar to that used to determine direct participation in hostilities for civilians but is not as strict.[91] As with all computer network operations, the legality of the particular attack will depend on what it is designed to do. However this does raise the question of whether, if a civilian object is targeted by computer network attack in order to achieve a physical force strike, it was making a sufficient contribution to military action to become a military objective in its own right.

This difference between attacks and operations leaves a lacuna in the law and may place the military in the unenviable situation of having a course of action available to it before an armed conflict is embarked upon, only to have that same course of action denied during the course of conflict. Although Schmitt's analysis, that the meaning of the general provision is to be taken from the specific provisions relating to attack which follow it, is appealing in order to avoid this problem, at present it is not correct in law and is not without difficulty of its own. Once the ability to target civilian objects is permitted, it crosses the fundamental philosophical line enshrined in the 1868 Declaration of St Petersburg which states "the only legitimate object which States should endeavour to accomplish during war is to weaken the *military forces* of the enemy". While the argument has been made that the character of war has changed in the twenty-first century such that this bright-line distinction between

---

[89] Pilloud, et al., *Commentary*, para 2191.

[90] Several States have indicated that in their target selection they will consider the military advantage to be anticipated from an attack as a whole and not from parts thereof. See for example, the statements of Australia, Canada, France, Germany, Italy, New Zealand, Spain and the United States. Certain military manuals also consider that the anticipated military advantage can include increased security for the attacking forces or friendly forces. Henckaerts and Doswald-Beck, *Customary International Humanitarian Law*, 31.

[91] Bothe, et al., *New Rules*, 324.

civilian and military is no longer appropriate,[92] until a legitimate forum decides that it is appropriate, then it is the present author's opinion that targeting civilian objects as part of a military operation remains prohibited by Article 57. This is also in conformity with the approach of the Appeals Chamber of the ICTY in *Kupreškić* which held that the Martens Clause should be used to interpret Articles 57 & 58 to protect civilians and limit attacks.[93] It is possible that the issue will be circumvented by the use of civilian contractors (or government operatives) engaging in those parts of the overall strategy which require that undertaking anyway.

4.2. Indiscriminate Attacks

While in general, computer network attacks allow for great precision in their application, some forms of malicious code are designed to spread from computer to computer without discrimination. The prohibition against indiscriminate attacks is a rule of customary international law and is expressed in Article 51(4) of Additional Protocol I:

> Indiscriminate attacks are prohibited. Indiscriminate attacks are:
> (a) those which are not directed at a specific military objective;
> (b) those which employ a method or means of combat which cannot be directed at a specific military objective; or
> (c) those which employ a method or means of combat the effects of which cannot be limited as required by this Protocol; and consequently, in each such case, are of a nature to strike military objectives and civilians or civilian objects without distinction.

As Dinstein points out, indiscriminate attacks differ from direct attacks against civilians in that 'the attacker is not actually trying to harm the civilian population', the injury to the civilians is merely a matter of 'no concern to the attacker'.[94] Viruses and worms are two methods of computer network attack which would fall into this category as their effects are not usually limited.[95] Both forms of malicious

---

[92] See section 1 *supra*.

[93] *Prosecutor v Kupreškic* (2000) Case No: IT-95-16-T, International Criminal Tribunal for the Former Yugoslavia.

[94] Dinstein, *Conduct of Hostilities*, 117.

code can be designed to carry a payload which may cause a variety of effects from mere annoyance, to compromising the system by leaving a backdoor for an attacker (in order to access or control the computer), or deleting or rewriting code on the infected system to varying effect.[96] Where the payload is designed to cause effects of such a magnitude to constitute an attack, both viruses and worms would fall foul of paragraph (b) of Article 51(4) above as they are methods of distribution which do not discriminate between civilian and military computers.[97]

Article 57(5) then sets out two examples of indiscriminate attacks; target area bombing and disproportionate attacks causing excessive collateral damage.[98] It is difficult to envisage a computer network attack equivalent of target area bombing as each attack must be conducted against a specific system or node in that system. No matter how 'high-level' the target system or node is in the victim network, and whatever the subsequent effects of its destruction or neutralisation, each node must be assessed on its own merits to qualify, or not, as a military objective. For example, the DNS root servers which run the Internet have come under attack twice in recent years.[99] The denial of service attacks used in those incidents merely shut down the

---

[95] Viruses are programs or bits of malicious code which are attached to a program or file and spread from computer to computer as they are passed between users. Generally they cannot infect computers without being opened or run by the user. Worms, although similar in design, are self-replicating and take advantage of mail or other information transport systems on the system to travel unaided. For example the worm may replicate and send itself to everyone on the users email contacts list, this is how several of the more high profile email worms of the past few years (Slammer/Sapphire, Mydoom & Nimda) have propagated.

[96] Obviously rewriting the code which controls value pressure on an oil pipeline system will have far more serious effects than the 'nuisance' viruses which generally circulate.

[97] From a technical standpoint it is possible to create a virus with a specific dialling protocol which will only dial specific IP address ranges. The IP address ranges of U.S. and other military and intelligence agencies are freely available on the Internet. However most virus writers are trying to get the maxim coverage possible, therefore the Slammer worm utilized a random dialling algorithm.

[98] Art. 57(5) provides: Among others, the following types of attacks are to be considered as indiscriminate:
(a) an attack by bombardment by any methods or means which treats as a single military objective a number of clearly separated and distinct military objectives located in a city, town, village or other area containing a similar concentration of civilians or civilian objects; and
(b) an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.

[99] In both 2002 & 2007 attacks were launched against the DNS root servers. In 2002 all 13 root servers were attacked, however in 2007 the attacks were limited to three of the servers including the server operated by the U.S. Department of Defense. Ryan Naraine, *Massive DDoS Attack Hit DNS Root Servers* <www.internetnews.com/bus-news/article.php/1486981> (last accessed 6 September 2007); Roger A. Grimes, 'Security Adviser: DNS Attack Puts Web Security in Perspective' (2007) 29(8) *InfoWorld* 19 February 2007 <http://www.infoworld.com/article/07/02/16/08OPsecadvise_1.html> (last accessed 1 October 2007).

servers (or slowed them) however in both incidents the individual servers targeted are either military objectives (for example the case of root server G, maintained by the U.S. Department of Defense) or civilian objects. Where the particular node (in this case a server) is the reference for both military and civilian sources, it is a so-called dual use target; the question of the effects of the attack will consequently become more important.[100]

One of the problems brought on by the interconnectedness of the Internet is that the knock-on effects of computer network attacks may have even further reaching consequences than they do with conventional kinetic attacks. For example, it has been reported that U.S. officials may have rejected launching a planned cyber attack against Iraqi financial computers because Iraq's banking network is connected to a financial communications network also located in Europe.[101] Similarly, the Iraqi oil pipeline communications network is reportedly cross-linked with the fibre-optic Tiger Song air defence network.[102] Such close linkages reportedly frustrated attempts by U.S. Forces to design a computer network attack that could be limited to military objectives solely in Iraq.[103] Although exacerbated by computer network technology, this problem is certainly not unique to computer network attacks. As noted above, both the 1991 Gulf War and the NATO campaign over Kosovo faced similar problems when the attacks on the power supply networks resulted in water pumping stations being closed.[104]

5. Precautions in Attack

Article 57 of Additional Protocol I requires attackers to take precautionary measures in carrying out military operations and attacks. The ICTY has recognised the customary nature of these precautions in both the *Kupreškić* and *Tadic* cases.[105] The

---

[100] See section 3 *supra.*

[101] Clay Wilson, *Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues*, Congressional Research Service, RL31787 (2007) 5.

[102] Charles R Smith, 'U.S. Information Warriors Wrestle with New Weapons' (2003) *NewsMaxcom* 13 March 2003 <http://www.newsmax.com/archives/articles/2003/3/12/134712.shtml> (last accessed 4 October 2007).

[103] Ibid.

[104] In the case of the attacks on Iraqi power networks knock-on effects affected hospitals, refrigeration as well as water supplies. 'NATO Denies Targeting Water Supplies', *BBC News* 24 May 1999, <http://news.bbc.co.uk/1/hi/world/europe/351780.stm> (last accessed 5 October 2007).

[105] *Tadic (Interlocutory Appeal)*, para 111-112; *Kupreškic*, para 524.

Appeals Tribunal in *Tadic* cited with approval the UN General Assembly Resolution 2675 that "all necessary precautions should be taken to avoid injury loss or damage to civilian populations" stating that the resolution represented customary international law "in armed conflicts of any kind".[106] The judgement confirms that the rule extends to non-international armed conflicts despite a lack of provisions in Common Article 3 or Additional Protocol II.

In the conduct of military operations, constant care must be taken to spare the civilian population, civilians and civilian objects.[107] As discussed in section 4.1 *supra*, military operations are a broader concept than attacks and the general rule thus applies more widely than the specific rules which follow relating to that part of the operation which constitutes an attack. Boivin usefully summarises the measures to be taken by those who plan or decide on attacks as follows:[108]

(i) do everything feasible to verify that the objectives to be attacked are military objectives;[109]

(ii) take all feasible precautions in the choice of means and methods of warfare;[110]

(iii) do everything feasible to assess whether the attack may be expected to cause excessive collateral damage;[111]

(iv) do everything feasible to cancel or suspend an attack if it becomes apparent that the proportionality rule will be breached, or that the target is not a military objective or that it is subject to special protection;[112]

(v) give effective advance warning prior to an attack that is likely to affect the civilian population, unless the circumstances do not permit;[113] and

(vi) where a choice between several military objectives is possible, choose the one that will cause the least danger to civilian lives and civilian objects.[114]

---

[106] *Tadic (Interlocutory Appeal)*, para 111-112. citing GA Res 2675 (XXV) Basic Principles for the Protection of Civilian Populations in Armed Conflicts UN GAOR, 25th Sess., Supp No. 28, 76, UN Doc. A/8028 (1971) of 1 December 1970.

[107] Art. 57(1), Additional Protocol I.

[108] Alexandra Boivin, *The Legal Regime Applicable to Targeting Military Objectives in the Context of Contemporary Warfare*, University Centre for International Humanitarian Law, 2 (2006) 36 <http://www.cudih.org/recherche/objectif_militaire_recherche.pdf> (last accessed 10 October 2007).

[109] Art. 57(2)(a)(i), Additional Protocol I.

[110] Art. 57(2)(a)(ii), Additional Protocol I.

[111] Art. 57(2)(a)(iii), Additional Protocol I.

[112] Art. 57(2)(b), Additional Protocol I.

[113] Art. 57(2)(c), Additional Protocol I.

Computer network attacks raise several issues with regard to the requirement to take precautions in attack. However two general matters should be dealt with before addressing these specific concerns. First, it should be noted that as with obligations regarding targeting set out in Article 49 and following, the majority of provisions relating to the precautions in attack refer to 'attacks'. That is, other than the general rule expressed in Article 57(1) requiring that constant care be taken to spare the civilian population, individual civilians and civilian objects in the course of military operations, the specific obligations will only apply to those computer network attacks which result in physical damage, injury or death.[115]
Secondly, the first four precautionary measures all refer to 'feasibility', a measure which has been interpreted by many States, and defined in the Commentary, as "those precautions that are practicable or practically possible, taking into account all the circumstances ruling at the time, including humanitarian and military considerations".[116]

5.1. Verification of military objectives

The law requires that commanders do everything feasible to verify that the target is not protected from attack and that it is a military objective.[117] As most targeted computer network attacks (as opposed to mass disruption attacks like worms and viruses) require fairly extensive system surveillance and scanning to determine an entry point to the system, this obligation should not prove difficult for preselected targets. However so-called 'targets of opportunity' may prove more difficult.
Attacks refer to acts of violence both in offence and in defence. Where a commander wishes to respond to an adversary's computer network attack they must verify first, the source of the attack, and secondly, that it is a military objective. As discussed in Chapter 3, the problem of accurate attribution of computer network attacks is made difficult by the tendency of attackers to spoof the origin of the attack, that is, to deliberately mislead the adversary as to the source of the attack. Note that the

---

[114] Art. 57(3) Additional Protocol I.

[115] For a discussion of the difference between attacks and operations and what this may mean for computer network attacks, see section 4.1, *supra.*

[116] UK Declaration of Understanding. This wording has been adopted by Protocols II, III and amended Protocol II to the Conventional Weapons Treaty.

[117] Art. 57(2)(a)(i), Additional Protocol I.

deception must not extend to a violation of Article 51(7) by the dissemination of false intelligence reports intended to induce the enemy to attack civilians and civilian objects in the mistaken belief that they are military objects.[118]

The extent of knowledge to be expected from the commander in assessing possible targets may prove problematical, and echoes the concerns held by many parties to Additional Protocol I regarding the level at which commanders' decisions were to be taken. Michael Schmitt raises this issue, querying to what extent computer expertise must be available during the targeting process to assess possible collateral damage and incidental injury.[119] However, military commanders are not expected to have personal knowledge of every target they attack and rely on intelligence reports for much of their information in regard to conventional attacks. Military commanders have to make their decisions on the basis of the information from all sources which is available to them at the time.[120] Many military manuals stress that the commander must obtain the best possible intelligence, including information on concentrations of civilian persons, important civilian objects, specifically protected objects, the natural environment and the civilian environment of military objectives.[121] In its Final Report to the Prosecutor, the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia described the obligation thus:[122]

> A military commander must set up an effective intelligence gathering system to collect and evaluate information concerning potential targets. The commander must also direct his forces to use available technical means to properly identify targets during operations. Both the commander and the aircrew actually engaged in operations must have some range of discretion to determine which available resources shall be used and how they shall be used.

---

[118] Bothe, et al., *New Rules*, 363. Giving the example of WWII British intelligence sending out false intelligence reports which induces the Luftwaffe to bomb civilian areas believing they were bombing strategic military objectives.

[119] Michael N. Schmitt, 'CNA and the Jus in Bello: An Introduction' (Paper presented at the International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, Stockholm, 17-19 November 2004) 101-125, 117.

[120] Henckaerts and Doswald-Beck, *Customary International Humanitarian Law*, 50, 54. Citing the military manuals of Algeria, Australia, Austria, Belgium, Canada, Equador, Egypt, Germany, Ireland, Italy, the Netherlands, New Zealand, Spain, the United Kingdom & the United States.

[121] Ibid., 55.

[122] ICTY, *Final Report to the Prosecutor*, para 29.

It follows that the same level of reliance on information must occur in respect of computer network attacks. In practical terms, it is also unlikely that any computer network attacks will be organised from a field position located in a combat zone, but would be the task of dedicated teams of computer technicians elsewhere in the battlespace where the requisite expertise is available.

5.2. Choice of Weapons

Ironically, the requirement for an attacker to take all feasible precautions in the choice of means and methods of warfare may require States who have the ability to launch computer network attacks to use that ability in preference to more traditional means. A similar argument has been advanced in relation to the use of precision-guided missiles, particularly with respect to warfare in urban environments.[123] Article 57(2)(a)(ii) of Additonal Protocol I requires those deciding on attacks to take all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event to minimizing, incidental loss of civilian life, injury to civilians and damage to civilian objects. The ICRC study has concluded that state practice establishes this as a norm of customary international law applicable in both international and non-international armed conflicts.[124] As Kalshoven points out, the primary obligation in the provision is to 'avoid' damage to the civilian population; the goal of 'minimizing' such damage will come into play only when total avoidance is not feasible.[125] These factors tend to promote the use of computer network attack methods which do not have an inherent risk to civilian objects and do not necessarily cause destruction. As Schmitt notes:[126]

> Whereas in the past physical destruction may have been necessary to neutralize a target's contribution to the enemy's efforts, now it may be possible to simply "turn it off". For instance, rather than bombing an airfield, air traffic control can be

---

[123] See generally, Stuart Walters Belt, 'Missiles over Kosovo: Emergence, Lex Lata, of a Customary Norm Requiring the Use of Precision Munitions in Urban Areas' (2000) 47 *Naval Law Review* 115.or an alternative view see also, D. L. Infeld "Precision guided Munitions" cited in Dinstein, *Conduct of Hostilities*, 126.

[124] Henckaerts and Doswald-Beck, *Customary International Humanitarian Law*, 57.

[125] Frits Kalshoven and Liesbeth Zegveld, *Constraints on the Waging of War* (ICRC, Geneva, 2001), 108.

[126] Schmitt, 'Wired Warfare', 394.

> interrupted. The same is true of power production and distribution systems, communications, industrial plants, and so forth.

One of the difficulties of certain computer network attack techniques is the fact that once they have been used once, they may be guarded against and may not work again.[127] Does this impact on a commander's obligation to field such weapons? The limited availability of weapons has been discussed with respect to the use of precision-guided munitions. Thus, Dinstein argues that the legal position is quite simple: the law of armed conflict instructs the planners to take whatever steps are necessary, in order to avoid or minimize collateral damage to civilians.... The availability of precision-guided munitions by no means forecloses alternative precautions in attack.[128]

Can such weapons be held in reserve in case they are needed further down the line? With regard to the Gulf conflict of 1990-91, Christopher Greenwood has noted that the United States did not invariably use precision-guided munitions whenever an attack involved a risk of collateral damage, on the grounds that supplies of these weapons were limited and they might have to be conserved for attacks on other objectives later in the campaign. Greenwood states that this approach involves a broad (though not untenable) interpretation of the duty to take 'feasible' precautions.[129] Certainly, the position is stronger where the weapons are held in reserve for an attack which is definitely planned down the line. The U.S. Department of Defense Final Report to Congress on the conduct of the Gulf War 1990-1991 makes it clear that the United States did not regard itself as bound always to select the method or means of attack which would cause the least danger to civilians, but was entitled to take account of the risk to coalition aircrews and the likelihood of successfully destroying the target. The report states:[130]

---

[127] In the same way that security flaws in software may be patched for domestic applications, ports may closed, patches installed and anti-virus software updated.

[128] Dinstein, *Conduct of Hostilities*, 126-127.

[129] Christopher Greenwood, 'Customary International Law and the First Geneva Protocol of 1977 in the Gulf Conflict' in P J Rowe (ed) *The Gulf War 1990-1991 in International and English Law* (Routledge, London, 1993) 63-88, 85-86.

[130] U.S. Department of Defence, *Conduct of the Persian Gulf War: Final Report to Congress*, U.S. Department of Defence, (1992) 697-698.

> To the degree possible and consistent with allowable risk to aircraft and aircrews, aircraft and munitions were selected so that attacks on targets within populated areas would provide the greatest possible accuracy and the least risk to civilian objects and the civilian population. Where required, attacking aircraft were accompanied by support mission aircraft to minimize attacking aircraft aircrew distraction from their assigned mission.

Greenwood argues that this approach is consistent with the interpretation placed on the word 'feasibility' in Article 57 by several States on signature or ratification of the Protocol and that it is inconceivable that any State would fail to take such factors into account.[131] Certainly the United Kingdom, which interprets the term 'feasible' to mean 'all measures practicable under the circumstances ruling at the time', lists the risks to a commander's own troops under the various options open to him as a factor to be considered when choosing what means and methods of warfare to employ.[132]

It must also be noted that the choice of weapons available to the war-fighter will vary depending on the level of the decision making. A military commander will have a greater ability to choose between various methods of attack than a unit commander located in the battlespace or an individual combatant. As Kalshoven has pointed out, a combatant simply cannot be equipped with a wide array of weapons for all kinds of situations, as the golf player is with his bag of clubs.[133] Interestingly, the advent of networked militaries and the concept of network-centric warfare actually allows a unit on the ground access to more technologies than has been previously available. Real-time communications allow the soldier on the ground to call in air strikes,

---

[131] Greenwood, 'Customary International Law in the Gulf', 85, 375, n117.

[132] U.K. Ministry of Defence, *UK Manual*, 83-84, . The factors are as follows: (1) the importance of the target and the urgency of the situation; (2) intelligence about the proposed target – what it is being, or will be used for and when; (3) the characteristics of the target itself, for example, whether it houses dangerous forces; (4) what weapons are available, their range, accuracy and radius of effect; (5) conditions effecting the accuracy of the targeting, such as terrain, weather, and time of day; (6) factors affecting incidental loss or damage, such as the proximity if civilians or civilian objects in the vicinity of the target or other protected objects or zones and whether they are inhabited, or the possible release of hazardous substances as a result of the attack; (7) the risks to his own troops under the various options open to him.

[133] Frits Kalshoven, 'The Soldier and His Golf Clubs' in C Swinarski (ed) *Studies and Essays on International Humanitarian Law and Red Cross Principles in Honour of Jean Pictet* (Martinus Nijhoff, The Hague; Boston, 1984) 369-385, 385.

'paint' targets with laser sights for laser guided missiles or plant GPS locator beacons, all increasing the options available to them rather than being limited to the contents of their backpack. These increased options will require commanders in the field to assess the appropriate options for attack.

Even more than the military commanders, the authorities who decide on the armament of the armed forces have the option to select suitable weapons. Although Kalshoven has noted that considerations of military efficiency will tend to preponderate in the deliberations of those authorities, he considers that "at the same time they will fail in their duty if they lose sight of the humanitarian requirement of minimisation of human suffering".[134] However, humanitarian law does not contain any obligation to acquire military capabilities that provide civilians greater protection; instead, it limits itself to imposing a duty to use capabilities once in the inventory.[135]

5.3. Proportionality

The principle of proportionality is part of customary law of armed conflict, however its codification and exact scope has not been without debate.[136] Article 57(2)(iii) of Additonal Protocol I codifies the principle of proportionality which requires those planning an attack to:

> "refrain from deciding to launch any attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated"

The wording is repeated in Article 51(5)(b) which considers such attacks to be indiscriminate; indiscriminate acts in violation of the rule of proportionality constitute 'grave breaches' under Article 85 of Additional Protocol I.

Ruth Wedgwood has addressed the proportionality equation for computer network attacks and suggested that greater damage to civilian objects may be tolerated in

---

[134] Ibid.

[135] Schmitt, *High and Low-Tech Warfare*, 11.

[136] *Nuclear Weapons Case.*, per Higgins J in her dissenting opinion (dissenting on other grounds); Henckaerts and Doswald-Beck, *Customary International Humanitarian Law*, 46.

order to eliminate a security threat, so long as that damage is reversible.[137] This view seems to be based on the idea that an attack may not cause destruction but mere incapacity. Although this view corresponds with Knut Dormann's approach outlined in section 4.1 *supra*,[138] it does not accord with the requirement of the Protocol's definition of attacks as 'acts of violence'. Taken to its logical conclusion, Wedgewood's argument would seem to infer that any damage is permissible as long as the damage can be reconstructed at the conclusion of the conflict.
Michael Schmitt has also queried the extent to which specialised computer expertise must be available during the targeting process to assess possible collateral damage and incidental injury.[139] As he points out, in traditional kinetic attacks, properly trained mainstream military officers can usually conduct reliable estimates. However in computer network attacks highly specialised expertise would be required.[140] This argument is essentially the same argument that occurs in terms of verification of military objectives, and can be addressed in the same manner.

Two major problems for modern proportionality judgements, especially with respect to computer network attacks, are the extent to which the knock-on effects of attacks must be incorporated into the calculation and the effects of increasingly dual use technological systems on that calculation.

Knock-on effects

As Christopher Greenwood has noted, the Gulf Conflict of 1990-91 has highlighted the fact that knock-on effects of attacks cause more harm to civilians than the direct effect of the attack itself.[141] Application of the proportionality test today, at least at the strategic level, requires that less immediate damage of this kind must also be

---

[137] Ruth G. Wedgwood, 'Proportionality, Cyberwar, and the Law of War' in M N Schmitt and B T O'Donnell (eds), *Computer Network Attack and International Law* (Naval War College, Newport, RI, 2002) 219-232, 228.

[138] Dörmann, 'Additional Protocols', 142-143.

[139] Michael N. Schmitt, 'CNA and the Jus in Bello: An Introduction'Ibid., 101-125, 117.

[140] Ibid.

[141] Christopher Greenwood, 'The Law of Weaponry at the Start of the New Millennium' in M N Schmitt and L C Green (eds), *The Law of Armed Conflict: Into the Next Millennium* (Naval War College, Newport, Rhode Island, 1998) 185-231, 202.

taken into account, although the difficulty of doing so is apparent.[142] While this problem is not unique to computer network attacks, both the 1991 Gulf Conflict and the NATO action in Yugoslavia illustrated the knock-on effects of targeting the electricity networks,[143] the problem is exacerbated by the nature of computer systems and linkages between military and civilian systems. Certainly the attacker will be required to have conducted some sort of mapping of the target network or system to ascertain what ancillary networks or systems are connected to the target. It is unclear how many levels of these cascading effects will need to be taken into account by the planners of the attacks and those executing them. Michael Schmitt argues that those effects that are reasonably foreseeable, no matter what 'tier' of effect they may be must be factored into the proportionality calculation.[144] This fits with the language of the article which refers to the *expected* consequences. Ironically, the move towards militaries buying off-the-shelf technology and systems may aid attackers in correctly predicting the effects of certain attacks.

Dual Use Systems

To what extent does that fact that a State has deliberately integrated civilian and military systems together impact the proportionality calculation? For example, the Iraqi Tiger Song air defence network was cross-wired with the Iraqi oil pipeline communications network,[145] additionally a large majority of U.S. military communications travel across civilian networks. While such actions undoubtedly expose the networks to attack as military objectives, can the argument be made, as with the case of voluntary human shields,[146] that if the defenders have integrated their military and civilian systems such that the military system may not be attacked without impacting the civilian, that the civilian impact should be excluded from the

---

[142] Ibid.

[143] In the Gulf Conflict of 1990-1991, Allied forces disabled the Iraqi power distribution networks using a variety of tactics including carbon-fibre filament munitions. The unintended (and apparently unexpected) side effects of these attacks were to deny electricity to the sewerage and water treatment facilities supplying the civilian population: William M Arkin, 'Cyber Warfare and the Environment' (2001) 25 *Vermont Law Review* 779, 781.citing Daniel T Kuehl, 'Airpower vs Electricity' (1995) 18 *Journal of Strategic Studies* 28. Similarly, when NATO forces attacked Yugoslavia's electrical supply network, water pumping stations were affected: 'NATO Denies Targeting Water Supplies'.

[144] Schmitt, *High and Low-Tech Warfare*, 10; Schmitt, 'Fault Lines', 296.

[145] Smith, 'U.S. Information Warriors Wrestle with New Weapons'.

[146] Schmitt, 'Fault Lines', 298.

proportionality calculation. The answer must be negative, as the protection only exists for civilians not civilian objects. In addition, for the most part civilians would be unaware that the systems were so intertwined; thus the parallel would be drawn with involuntary human shields which must definitely be taken into account when conducting the targeting analysis. Further as Schmitt points out, there are instances where protected objects lose their protected status due to the adversary's misconduct. A hospital housing combatants (who are not otherwise *hors du combat*) may be attacked once a warning to desist has been ignored.[147] Rogers argues that a tribunal that is considering the criminal liability of an attacker in respect of death or injury to civilians, would be entitled to consider the extent to which the defenders had flouted their obligations to separate military objects from civilian objects.[148]

5.4. Choice of Targets

Article 57(3) of Additional Protocol I provides that where there is a choice of several military objectives for obtaining a similar military objective, the objective chosen should be the one which causes the least danger to civilian lives and to civilian objects. Christopher Greenwood notes that although this Article may have gone beyond the customary law as it stood at 1977, it certainly represented customary international law by the 1990-1991 Gulf Conflict.[149] The obligation is particularly relevant for computer network attacks as the form of attack opens multiple options to achieve the same effect. For example, a system may be neutralised by disabling an essential component of the system so that it is unable to function, attacking the system as a whole, attacking the network on which that system resides, or by shutting off the electrical supply to the target system. All would achieve the same result, i.e. denying the target system to the adversary. This is, to a certain extent, a natural extension of the obligation to choose means and methods of attack which minimise harm to civilians, however as computer network attacks increase the ability to break target networks into their component systems, the targeting analysis will likewise become more refined. Thus the obligation to choose 'the lesser of two

---

[147] Ibid., 300.

[148] Rogers, *Law on the Battlefield*, 129. Rogers considers this proportionality approach would redress the balance which might otherwise be tilted in favour of the unscrupulous.

[149] Greenwood, 'Customary International Law in the Gulf', 83.

evils'; the example given in the ICRC Commentary is the bombing on railways lines rather than stations which are primarily located in urban areas.[150] Of course the obligation, as with the other precautions in attack, is to take feasible measures, therefore the question will be dependent on the ability to access the networks, the ability to determine the effects of neutralising a particular component, the desired effect of the attack and whether the systems can be cracked in time for the purposes of the operation. Although the specifics of this provision will only apply to those computer network attacks which amount to attacks as discussed *supra*, the general obligation under Article 57(1) would oblige attackers to take these factors into consideration in part of any military operation.

Failure to sufficiently refine the target, particularly in relation to dual use targets, also raises possible parallels with target area bombardment which is prohibited by Article 51(5)(a):[151]

> An attack by bombardment by any method or means which treats as a single military objective a number of clearly separated and distinct military objectives located in a city, town, village or other area containing a similar concentration of civilians or civilian objects.

If a system or network is disrupted too far 'up-stream' from the ultimate objective, it will affect the not only the objective, but all other systems (including any civilian systems) on the network. However the analogy is flawed, as any system attacked will qualify as a military objective or not on its own merits (with the knock-on effects included in the proportionality equation), rather than treating a number of objectives as a single objective.

6. Precautions Against the Effects of Attacks

The main prohibition addressed to defenders in respect of the civilian population or individual civilians is expressed in Article 51(7) of Additional Protocol I which

---

[150] Bothe, et al., *New Rules*, para 2227-2228.

[151] Art. 51(5)(a), Additional Protocol I provides: The presence or movements of the civilian population or individual civilians shall not be used to render certain points or areas immune from military operations, in particular in attempts to shield military objectives from attacks or to shield, favour or impede military operations. The Parties to the conflict shall not direct the movement of the civilian population or individual civilians in order to attempt to shield military objectives from attacks or to shield military operations.

prevents the use of civilians as human shields for military objectives.[152] However this does not raise many issues for computer network attacks, other than to comment that counter attacks against computer network attacks may not necessarily be returned in kind, and the use of civilian contractors to defend against intrusions into military networks does not prevent them from being targeted or attacked by other means. Of more interest is Article 58 which provides that:

> The Parties to the conflict shall, to the maximum extent feasible:
> (a) without prejudice to Article 49 of the Fourth Convention, endeavour to remove the civilian population, individual civilians and civilian objects under their control from the vicinity of military objectives;
> (b) avoid locating military objectives within or near densely populated areas;
> (c) take the other necessary precautions to protect the civilian population, individual civilians and civilian objects under their control against the dangers resulting from military operations.

These rules represent customary international law,[153] however as Christopher Greenwood points out in most conflicts little more than lip service appears to have been paid to this rule.[154] However the wording of the provision clearly indicates that these obligations are weaker than those of the attacker.[155] Unlike the obligations of the attacker, failure to comply with the provision does not constitute a grave breach of the Protocol; defenders obligations only have to be taken "to the maximum extent possible", and the defender has only to "endeavour to remove" the civilian population and "avoid" locating military objectives nearby.

What does this mean for computer network attacks? Paragraph (a) requires that parties endeavour to remove civilian objects from the vicinity of military objectives,

---

[152] Sassòli, 'Targeting', 206.

[153] Henckaerts and Doswald-Beck, *Customary International Humanitarian Law*, 67-76. The Trial Chamber in *Kupreškić* considered that both Art. 57 API (pertaining to precautions in attack) and Art. 58 are now part of customary international law, not only because they specify and flesh out general pre-existing norms, but also because they do not appear to be contested by any State, including those which have not ratified the Protocol. *Kupreškic*, para 524.

[154] Greenwood, 'Customary International Law in the Gulf', 374, n122.

[155] Sassòli, 'Targeting', 207.

to the maximum extent feasible.[156] This would require parties (where practicable) to extricate military systems and networks from civilian ones and to avoid using civilian networks for military communications. However, as has been pointed out throughout this thesis, the increasing civilianisation of the military and widespread networking of modern militaries has led to the opposite happening. The integration of civilian and military technology such as civilian use of the GPS system, and military use of civilian communications satellites and networks. The lack of partitioning between Iraqi military and civilian systems caused difficulties for the U.S. in achieving some of their computer network attacks aims in the 2003 Iraq conflict.[157]

Paragraph (c) also imposes a general obligation to take other necessary precautions to protect the civilian population, individual civilians and civilian objects under their control from dangers resulting from military operations. It is unclear how far this obligation will go in an age of computer network attack. Practice reports submitted to the ICRC customary international humanitarian law study have indicated construction of shelters, digging of trenches, direction of traffic, guarding of civilian property and the mobilisation of civil defence organisations are measures which States have taken. Such measures in relation to digital property may include ensuring that all publicly administered digital property is properly backed up and all systems have built in redundancy, so that any loss of systems or information can be restored. Similar digital disaster planning programs were put in place on a wide scale in preparation for the year 2000 change-over following predictions of catastrophic electronic failures.

---

[156] As with other Articles in the Protocol which incorporate the word 'feasible', a number of delegations have indicated that the word feasible means that which is practicable or practically possible, taking into account all the circumstances at the time, including those relevant to the success of military operations. Bothe, et al., *New Rules*, 373.

[157] Smith, 'U.S. Information Warriors Wrestle with New Weapons'.

Chapter 7 – Measures of Special Protection

Special protection is granted to certain personnel and objects under the laws of armed conflict. Although even the most advanced information society is yet to deploy technology which would enable direct attacks against personnel using computer network attacks, other objects have become sufficiently incorporated into computer networks to make them vulnerable to a computer network attack. The environment, installations containing dangerous forces (namely dams, dykes and nuclear power plants), hospitals and other medical units are all granted particular protection from attack over and above the general protection granted to civilian infrastructure. As much of the developed world's critical infrastructure is now controlled using computer networks, this protection will extend to prohibit computer network attacks against such objects. Dams, power stations, chemical plants, water and sewage, gas and oil pipelines are all controlled by networked systems such as Supervisory Control and Data Acquisition (SCADA) systems, thus making them vulnerable to computer network attacks.[1] In addition, information societies now rely on digital information for fast and reliable access to up-to-date information; this trend is also seen in the medical sector where medical records and other information are stored and transmitted over computer networks, thus also leaving them susceptible to computer network attack. While there is no question that these installations and data remain protected by their status regardless of the means or method of warfare adopted against them, some issues require review in light of the new technology.

1. The Environment

Harm caused to the environment during periods of armed conflict, both directly and as a by-product of war, has been an unfortunate inevitability of conflict throughout the ages; post-modern warfare is no exception. For example, the 2006 armed conflict between Hezbollah and Israel resulted in severe damage to the Lebanon coastline

[1] SCADA systems (Supervisory Control and Data Acquisition) are organisational systems which control other networks and automated processes.

after a power station was damaged by Israeli missile fire;[2] likewise the oil fires resulting from the 1991 Gulf War caused substantial damage to the ecology in Kuwait & Iraq.[3] In the latter incident, the deliberate damage caused to the environment by Iraqi troops shocked the world and prompted a flurry of legal commentary on the degree of protection provided by the law pertaining to environmental warfare.[4]

At the time of writing no reports of incidents of wartime environmental damage using computer network attack exist in the public domain. However, in April 2000 a domestic case emerged in Queensland, Australia, solving a mystery that had perturbed authorities for months, and showing the potential of this new type of attack for environmental damage.[5] Vitek Boden was arrested after being caught using a stolen computer and radio transmitter to gain access to a water sewerage treatment system. Over the previous two month period Boden had accessed the system 46 times, gaining complete control of treatment of the region's sewerage and drinking water facilities and dumping 250 million tonnes of putrid sludge into the area's rivers and parks, killing wildlife and plants. Although Boden was acting for personal reasons in his attacks,[6] the case illustrates the potential for intrusion and establishment of control over infrastructure utilising SCADA systems, a tactic which could easily be adopted for military purposes. Could a repeat of the 1991 Gulf War oil disaster occur as a result of computer network attacks? Based on current technology, the answer is undoubtedly yes. For example, approximately thirty percent of the United Kingdom's oil output runs over one pipeline system in the North Sea, pumping a volume of 2.5 million gallons of oil a day. The Forties

---

[2] Mark Kinver, "Damage Is Done' to Lebanon Coast', *BBC News* 8 August 2006, <http://news.bbc.co.uk/1/hi/sci/tech/5255966.stm> (last accessed 9 January 2007).

[3] Oil well fires were greater in number than all well fires in previous history put together. Oil slicks were more than two to three times the size of the word's previously largest oil spill, the Exxon Valdez. Gushing Oil wells, pipes, and storage tanks left rivers and lakes of spilled oil, more than ninety million barrels covering over fifty percent of Kuwait's land area. This huge amount of exposed oil released toxic substances, heavy metals, and unequalled emissions of hydrocarbons. Arkin, 'Cyber Warfare and the Environment'.

[4] Eric Talbot Jensen, 'The International Law of Environmental Warfare: Active and Passive Damage During Armed Conflict' (2005) 38 *Vand J Transnat'l L* 145.

[5] *R v Boden* (2002) QCA 164, Court of Appeal of the Supreme Court of Queensland (Australia).

[6] Evidence at his trial suggested that Boden was motivated either by a desire for vengeance or that he hoped to be re-employed by the company running the system in a consulting capacity to solve the problem he had caused: Ibid; Gellman, 'Cyber-Attacks by Al Qaeda Feared'.

pipeline is controlled by a SCADA system similar to those that control the Queensland water and sewerage treatment plant infiltrated by Boden. By resetting the valves on the North Sea Forties oil pipeline it may be possible to cause a hammering effect in the lines;[7] the resulting rupture of the pipeline would cause untold damage to the ecology of the area (including an area of special scientific interest), and cripple the U.K. oil supply for weeks.

As with all of the issues outlined in this thesis, the general principles of the laws of armed conflict will continue to apply to computer network attacks despite the application of new technology to cause harm. In addition, those general principles also serve to protect the environment indirectly, even where direct protection is not provided by specific prohibitions relating to the environment.[8] Specific protection of the environment in armed conflict has been rising in prominence since the Vietnam War and it has come to the forefront of legal attention since the 1991 Gulf War.

1.1. Additional Protocol I

Additional Protocol I contains two articles containing measures of direct protection for the environment during international armed conflict, namely Articles 35(3) and 55. There is no equivalent provision in Additional Protocol II relating to non-international armed conflicts.[9] Both Articles contain broad prohibitions against any means or method of warfare which is intended or may be expected to cause damage to the environment;[10] thus computer network attacks which meet the requisite criteria for damage are also prohibited. Both Article 35(3) and Article 55(1) are restricted in terms of the intended or foreseeable consequences of the attack; the effect on the

---

[7] See also the account of the 'farewell dossier' incident in Appendix 1, although an explosion would be unlikely in a predominantly seabed system.

[8] For example, the general protection granted to civilian objects, protection of objects indispensable to the survival of the civilian population and simple application of the principles of proportionality and necessity will provide protection for many parts of the environment.

[9] A proposal was made at the diplomatic conference to introduce into Additional Protocol II a provision analogous to Art. 35(3) and Art. 55 of Additional Protocol I but the idea was ultimately rejected. Antoine Bouvier, 'Protection of the Natural Environment in Time of Armed Conflict' (1991) 285 *IRRC* 567 <www.icrc.org/web/eng/siteeng0.nsf/html/57JMAU> (last accessed 10 January 2007).

[10] Art. 33 states "It is prohibited to employ methods or means of warfare which are intended, or may be expected, to cause widespread, long-term and severe damage to the natural environment".

Art. 55: Care shall be taken in warfare to protect the natural environment against widespread, long-term and severe damage. This protection includes a prohibition of the use of methods or means of warfare which are intended or may be expected to cause such damage to the natural environment and thereby to prejudice the health or survival of the population.

environment must be "widespread, long-term and severe",[11] and in the case of Article 55(1), the subsequent effect of the environmental damage must also be prejudicial to the health or survival of the population.[12] Article 55(1) also contains a general obligation of care to protect the natural environment against "widespread, long-term and severe" damage.

Article 55(2) of the Additional Protocol I also contains a blanket prohibition against any attacks against the natural environment by way of reprisals; this constitutes an absolute standard of zero harm to the environment in the case of reprisals.[13]

1.2. ENMOD Convention

Like Additional Protocol I, the 1977 Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques (ENMOD) does not limit itself to specific means and methods of warfare.[14] Article 1 of the ENMOD Convention prohibits States Party from military or any other hostile use of environmental modification techniques which result in "widespread, long-lasting or severe" effects as a means of affecting any other State party to the Convention.[15]

---

[11] Note that under Additional Protocol I, a means or method of warfare must cause damage which cumulatively fulfils all three conditions to be rendered unlawful. For an examination of the meaning of the terms "widespread, long-term and severe" under the Protocol, see Karen Hulme, *War Torn Environment: Interpreting the Legal Threshold* (Martinus Nijhoff Publishers, Leiden, 2004), 91-100.

[12] The word "health" was included to indicate that the provision was also concerned with acts which could seriously prejudice health, such as congenital defects, degenerations or deformities. Pilloud, et al., *Commentary*, 663-664.

[13] Hulme, *War Torn Environment*, 73.

[14] 18 May 1977, *Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques.*

[15] The terms "widespread, long-lasting or severe" are used deliberately to mirror the terminology in Additional Protocol I which was negotiated in the same time-frame. Note however the use of 'or' rather than 'and' which gives the ENMOD Convention a broader application. Although the terminology is practically identical, the terms are not used synonymously. While not defined in the Convention, the terms have been given definition by a set of "Understandings" which were drafted at the same time by the Committee and are attached to the Convention (although not officially incorporated into it). 'Widespread': encompassing an area on the scale of several hundred square kilometres; 'long-lasting': lasting for a period of months, or approximately a season; severe: involving serious or significant disruption or harm to human life, natural and economic resources or other assets.

Environmental modification techniques are defined broadly as:[16]

> "Any technique for changing – through the deliberate manipulation of natural processes – the dynamics, composition or structure of the Earth, including its biota, lithosphere, hydrosphere and atmosphere, or of outer space".

Possible methods mooted for manipulating the environment are: triggering earthquakes, generating tsunamis, triggering landslides, fluidising thixotropic soils, activating volcanoes, breaching water containments, melting polar ice, disrupting permafrost soils, seeding clouds to create rain & flooding, creating holes in the ozone layer and creating drought conditions.[17] Other than breaching water containment facilities, a topic which is dealt with further in the following section on installations containing dangerous forces, it is difficult to see how a computer network attack could directly manipulate the environment. However, where a computer network attack *is* capable of performing such a function, the provisions of the ENMOD Convention are broad enough to prohibit it.

With the current state of technology, the most likely scenario involves hostile manipulation of existing peacetime environmental modification techniques which have been put in place to combat increasing environmental problems.[18] Such solutions are likely to be controlled by SCADA systems or other networked computer systems and may therefore be susceptible to appropriation and manipulation for hostile purposes. The Thames Barrier, a 523 metre gated barrier across the River Thames in London, is an example of an environmental modification technique used for peaceful purposes. The Barrier was created to protect London and the Thames Estuary from flooding caused by rising tide levels and surge tides.[19] The massive hydraulic gates of the Barrier are ultimately controlled via a computer system and are therefore theoretically vulnerable to manipulation by computer

---

[16] Art. 2, ENMOD Convention.

[17] Ernö Mészáros, 'Techniques for Manipulating the Atmosphere' in A H Westing (ed) *Environmental Warfare: A Technical, Legal and Policy Appraisal* (Taylor & Francis, London, 1984), 13; Hallan C Noltimier, 'Techniques for Manipulating the Geosphere' in A H Westing (ed) *Environmental Warfare: A Technical, Legal and Policy Appraisal* (Taylor & Francis, London, 1984) 25-31.

[18] Peaceful use of environmental modification techniques are specifically excluded from the ambit of the ENMOD Convention under Art. 3(1).

[19] See generally The Environment Agency, *The Thames Barrier: Flood Defence for London* <http://www.environment-agency.gov.uk/regions/thames/323150/335688/341764/> (last accessed 29 November 2006).

network attack. For example, preventing the system from closing the gates during a tidal surge would allow the natural flow of flood waters to cause damage to a substantial part of London. It would also be possible to use the Barrier itself to amplify the deleterious effects of such tides on London. By closing the gates during a surge tide and then opening them at the height of the tide, a wall of water would flood central London causing immense loss of life and property damage.[20] Such damage would certainly meet the 'severe' criteria of the Convention.

The ENMOD Convention is not limited to international armed conflicts. However its application to non-international armed conflicts is limited by the requirement that damage must be caused to another State Party. The Convention would nevertheless cover the situation where an environmental modification technique was used intentionally against a domestic opponent, but caused cross-border environmental damage to another State Party.[21]

1.3. Other Protections

The environment is also protected by general rules relating to the protection of civilian objects, proportionality and military necessity. The relevance of the general principles of proportionality and necessity for the protection of the environment were underscored by the International Court of Justice in its advisory opinion on *Nuclear Weapons*:[22]

> "States must take environmental considerations into account when assessing what is necessary and proportionate in the pursuit of legitimate military objectives. Respect for the environment is one of the elements that go to assessing whether an action is in conformity with the principles of necessity and proportionality".

In addition, the U.N. General Assembly has stated that the destruction of the environment not justified by military necessity and carried out wantonly, is clearly

---

[20] A scenario very similar to this was created by BBC's drama 'Spooks' when the Thames Barrier was overrun by environmental terrorists; the addition of computer network attacks to manipulate the gates is new. *Spooks: Series 5, Episode 10* (BBC, 13 November 2006)

[21] Dinstein, *Conduct of Hostilities*, 189.

[22] *Nuclear Weapons Case*, para 30.

contrary to existing international law.[23] The International Court of Justice cited this passage in the *Nuclear Weapons* case, noting that although General Assembly resolutions are not binding as such, "they provide evidence of the existence of a rule or the emergence of *opinio juris*".[24] This has led commentators to confirm that the protection of the environment is a norm of customary international law applicable in both international and non-international armed conflicts.[25]

The Rome Statute of 1998 incorporates some of the prohibitions contained in Additional Protocol I. For instance, the International Criminal Court has jurisdiction in respect of war crimes that consist of "[i]ntentionally launching an attack in the knowledge that such attack will cause incidental ... widespread, long-term and severe damage to the natural environment which would be clearly excessive in relation to the concrete and direct overall military advantage anticipated".[26]

Protection of the environment is also inferred from the provisions relating to protection of civilian objects and protection of objects indispensable to the civilian population. Civilian objects are defined as all objects which are not military objectives, and while in some cases the environment could by its use constitute a military objective (for example by providing cover for troops), as a general matter it is likely to be considered a civilian object. Indeed, in some circumstances it may be considered an object indispensable to the civilian population (for example natural water reservoirs) and thus be provided protection under Article 54 and Article 14 of Additional Protocol I and Additional Protocol II respectively. Article 14 of Additional Protocol II is perhaps of more importance in protecting the environment as Additional Protocol II, unlike Additional Protocol I, does not protect civilian objects in general.[27] The International Committee of the Red Cross has also issued a set of Guidelines for Military Manuals and instructions on the protection of the

---

[23] Protection of the Environment in Times of Armed Conflict, U.N. GAOR, 47th Sess., Agenda Item 136, UN Doc A/Res/47/37 (1992).

[24] The Court also noted that "Addressing the reality that certain instruments are not yet binding on all States, the General Assembly in this resolution "*[a]ppeals* to all States that have not yet done so to consider becoming parties to the relevant international conventions." *Nuclear Weapons Case*, para 32.

[25] See for example,Dinstein, *Conduct of Hostilities*, 193; Henckaerts and Doswald-Beck, *Customary International Humanitarian Law*, Vol 1, 143.

[26] Art. 8(2)(b)(iv) Rome Statute of the International Criminal Court 1998 (entered into force 1 July 2002). Note that knowledge in this instance means actual knowledge not reasonable forseeability (Art. 30(3) of the Rome Statute).

[27] Pilloud, et al., *Commentary*, para 4794.

environment in times of armed conflict.[28] While not formally approved by the U.N. General Assembly, the Assembly did invite all States to give due consideration to the possibility of incorporating the guidelines into their military manuals and other instructions addressed to their military personnel.[29]

2. Installations containing Dangerous Forces

Until 2002, the idea of a country being attacked through its computer networks as a co-ordinated act of war was considered remote and largely dismissed as panic-mongering.[30] Although United States intelligence agencies were monitoring China, Russia and other Nation States on the threat to U.S. information systems, the threat from non-state actors was largely underestimated.[31] Then in 2002, troops clearing the cave system in the Tora Bora region of Afghanistan uncovered an Al Qaeda laptop which indicated a strong interest in computer network attacks. Computer forensics indicated that the laptop had made multiple visits to sites offering sabotage handbooks, software and programming instructions on SCADA systems, and other 'cracking' tools. In combination with the Mountain View surveillance program which had been uncovered the year before,[32] officials became increasingly concerned about Al Qaeda's computer network attack capabilities. In January 2002, another computer was seized at an Al Qaeda office in Kabul, Afghanistan. The computer contained models of a dam, made with structural architecture and engineering software and included geological soil identification software which would enable the planners of an attack to simulate the dam's catastrophic failure and

---

[28] ICRC, 'Guidelines for Military Manuals and Instructions on the Protection of the Environment in Times of Armed Conflict' (1996) 311 *IRRC* 230 <http://www.icrc.org/Web/Eng/siteeng0.nsf/html/57JN38> (last accessed 11 January 2007).; annex to UN Doc. A/49/323 (1994).

[29] GA Res 49/50, 9 December 1994.

[30] See for example, Interviews with John Hamre and James Lewis, PBS Frontline *Cyberwar!* 24 April 2003 http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/ (last accessed 11 January 2006).

[31] Gellman, 'Cyber-Attacks by Al Qaeda Feared'.

[32] In 2001 Mountain View California police began investigating a suspicious pattern of surveillance against silicon valley computers. The visitors were studying emergency telephone systems, electrical generation and transmission, water storage and distribution, nuclear power plants and gas facilities. While some probes indicated planning for a conventional attack, others honed in on the digital devices which run critical infrastructure. Ibid.

plot the consequences of a breach.[33] Although the authorities declined to say whether the schematics related to a particular targeted dam, the use of cyberspace to infiltrate a dam is not unprecedented. As refered to *supra,* in 1998, a 12-year-old hacker, exploring on a lark, broke into the computer system that controls the Roosevelt Dam in Arizona, U.S.A.[34] Although he was unaware of the fact, federal authorities claim the boy had complete control of the SCADA system which controls the dam's massive floodgates and the 489 billion gallons of water which it contains. Unleashed, the water would course down the Salt River and over a downstream flood plain (home to an estimated population of one million people) before reaching the state capital, Phoenix.

Dams are not the only installations containing dangerous forces to have been compromised via the Internet. In January 2003, the Davis-Besse nuclear power plant in Ohio, U.S.A. was hit by the Slammer worm, disabling a safety system for nearly five hours and a process computer for nearly six hours.[35] Fortunately the power plant was offline at the time; however the incident provided a stark reminder of the vulnerability of such installations, prompting a review of safety protocols. In the UK, the Bradwell nuclear power plant was likewise compromised in June 1999 by a security guard who attempted to alter sensitive information, and succeeded in deleting records from one of the systems.[36] As with the Davis-Besse incident, the Bradwell incident prompted a review of security and change of procedures.

Additional Protocol I to the Geneva Conventions grants special protection to installations containing dangerous forces, namely dams, dykes and nuclear power stations. Article 56(1) provides as follows:

> Works or installations containing dangerous forces, namely dams, dykes and nuclear electrical generating stations, shall not be made the object of attack, even where these objects are military objectives, if such an attack may cause the release of dangerous forces and consequent severe losses among the civilian population. Other

---

[33] Ibid.

[34] Ibid. See also Appendix 1 for queries that have been raised regarding the veracity of some of the facts of this account.

[35] Kevin Poulsen, 'Slammer Worm Crashed Ohio Nuke Plant Network' (2003) *Security Focus* 19 August 2003 <www.securityfocus.com/print/news/6767> (last accessed 31 October 2006).

[36] Kevin Maguire, 'Guard Tried Sabotage at Nuclear Reactor: Security Checks Tightened after High-Level Alert', *The Guardian* (London), 9 January 2001, 2.

> military objectives located at or in the vicinity of these works or installations shall not be made the object of attack if such attack may cause the release of dangerous forces from the works or installations and consequent severe losses among the civilian population.

The first sentence of this Article is repeated verbatim in Article 15 of Additional Protocol II relating to non-international armed conflicts. The provisions represent an innovation in the laws of armed conflict, and are a reflection of the attempt to limit the extent of permissible collateral damage.[37]

An interesting question arises in the respect of computer network attacks as to whether the concept of military objectives "located at or in the vicinity of" such works and installations will extend to network vicinity as well as physical proximity. As has been illustrated in previous chapters, in information age warfare, physical distance is no longer a useful yardstick for the amount of damage which can be inflicted. While a strict reading of the text of Article 56(1) would tend to indicate that the physical location of the objective is the only prerequisite, if the Article is to maintain its utility in the Internet age it would seem that it should extend to network proximity as well. The operative part of the prohibition being "if such an attack may cause the release of dangerous forces...and consequent severe losses among the civilian population". As Yoram Dinstein points out, the guiding consideration is the protection of the civilian population from catastrophic collateral damage.[38] Where a computer network attack is designed to disable an adjacent system or network such that it would have a knock-on effect onto a dam, dyke or nuclear generator, causing that installation to release its forces, it should not matter that the system or network is not physically located in the vicinity of that installation. Where it is reasonably foreseeable - using normal network reconnaissance techniques - that the target system is connected to the installation, such that making the former the object of an attack would affect the latter, the prohibition should stand.[39] The requirement to take suitable precautions in attacks is dealt with in more detail in Chapter 6 *supra*. Note

---

[37] Oeter, 'Methods and Means of Combat', 194.

[38] Dinstein, *Conduct of Hostilities*, 173.; See also Oeter, 'Methods and Means of Combat', 195.

[39] Note for example the loss of civilian water distribution, purification and sewerage facilities which followed the U.S. destruction of the Iraqi electricity grid in 1991. Given U.S. intelligence and reconnaissance capabilities at the time, such a consequence should have been reasonably foreseeable, however it appears that the result was unexpected. Arkin, 'Cyber Warfare and the Environment', 781, citing Kuehl, 'Airpower vs Electricity'.

that this issue will only arise in relation to international armed conflicts as the relevant sentence is omitted from Article 15 of Additional Protocol II.
While the advent of computer network attacks may remove some military objectives from the permissible target list by virtue of their being in close network proximity to a work or installation containing dangerous forces, others may become open to attack. The commentary to Article 56 cites the case of a hydroelectric power station incorporated in a dam or located in the immediate vicinity as an example of a military objective which cannot be attacked because of its proximity to the dam.[40] Computer network attacks may allow the attacking force to disengage the power station from the dam to deny the opposing force the electricity, without running the risk of destroying the dam. Such an action would have severe consequences for those countries where the main source of electricity is hydroelectric power.[41]
It should be noted that, as with dams, dykes and nuclear power generators, military objectives located or in the vicinity of the works or installations lose their special protection only if they are used in regular, significant and direct support of military operations (a higher threshold than that of effective contribution to military effort) and if such an attack is the only feasible way to terminate such support.[42] Parties also have an obligation to endeavour to avoid locating military objectives in the vicinity of works or installations.[43]

3. Objects Indispensable to the Survival of the Civilian Population.

Computer network attacks against systems and networks which are indispensable to the survival of the civilian population are prohibited under Additional Protocols I & II in the same manner that conventional attacks would be prohibited against such objects. Article 54(2) of Additional Protocol I provides:

> It is prohibited to attack, destroy, remove or render useless objects indispensable to the survival of the civilian population, such as foodstuffs, agricultural areas for the production of foodstuffs, crops, livestock, drinking water installations and supplies

[40] Pilloud, et al., *Commentary*, para 2156.

[41] For example, Norway produces virtually all of its electricity from hydroelectric sources, while Iceland (83%), Austria and Canada (both over 70%) would be hugely effected by denial of hydroelectric sources. Notably, China is the world's largest producer of hydroelectric power.

[42] Art. 56(2), Additional Protocol I.

[43] Art. 56(5), Additional Protocol I.

> and irrigation works, for the specific purpose of denying them for their sustenance value to the civilian population or to the adverse party, whatever the motive, whether to starve out civilians, to cause them to move away, or for any other motive.

Article 14 of Additional Protocol II provides equivalent wording. The list is merely illustrative and the Commentary to the provision notes that "it cannot be excluded that as a result of climate or other circumstances, objects such as shelter or clothing must be considered as indispensable".[44] As has been demonstrated by the Australian domestic case of Vitek Boden,[45] drinking water installations are particularly susceptible to computer network attacks, likewise irrigation works have been tampered with in a domestic case,[46] as are any other works primarily controlled by SCADA systems.

Unlike ordinary civilian objects, Michael Schmitt's argument distinguishing the possibility of targeting objects with computer network attacks not severe enough to constitute attacks, would not hold up against objects indispensable to the civilian population;[47] the words 'remove' and 'render useless' were added to 'attack' and 'destroy' in order to cover all possibilities.[48] Attack etc against such objects is only prohibited for the "specific purpose of denying them for their sustenance value to the civilian population".[49] Note that the Rome Statute only considers depriving civilians of objects indispensable for survival a war crime where it constitutes intentional starvation as a method of warfare.[50]

4. Hospitals and other Medical Units

Hospitals, medical units and medical transports (including hospital ships and aircraft) all receive special protection from international humanitarian law. Indeed they form the basis of the origins of the modern laws of armed conflict, and are

---

[44] Pilloud, et al., *Commentary*, para 2103.

[45] *R v Boden.* Boden, a disgruntled employee, accessed the Queensland water treatment facilities 46 times via a stolen laptop and radio transmitter before being caught. See Appendix 1.

[46] Dan Goodin, 'Electrical Supe Charged with Damaging California Canal System' (2007) *The Register* 30th November 2007 <http://www.theregister.co.uk/2007/11/30/canal_system_hack/>.

[47] See Chapter 6, section 4.1 *supra.*

[48] Pilloud, et al., *Commentary*, para 2100-2101.

[49] Ibid.

[50] Art. 8(2)(b)(xxv), Rome Statute.

protected by custom as well as specific *lex scripta*. For the most part this protection does not raise any additional issues in the event of computer network attacks, the protection remains regardless of the method of attack. However two issues, the location and access to medical databases and the encryption of communications to and from hospital ships, require some thought in the information age.

4.1. Location and Access to Medical Databases

In line with the trend towards networked services in both civilian and military life, the supply of operational support services to the military, such as medical treatment facilities, have also benefited from increased network connectivity. For example, the United States military has instituted an information system to provide electronic access to medical information and provide the ability to electronically access and update medical records of serving personnel.[51] The system allows for integrated patient care which can keep pace with the patient's progression from the medic located in the field, through combat support hospitals, to medical centres situated far away from the fighting.[52] The handheld devices, laptops and database which comprise the system undoubtedly form part of the material and supplies of the medical units and thus are protected by the Geneva Conventions,[53] Additional Protocols and customary international law.[54] However, protection only remains in place while the system is used exclusively for the treatment of the wounded or sick and for the prevention of disease.[55] Care must be taken therefore that the medical

---

[51] For a description of the system and its component applications see Sandra Basu, 'Military Electronic Medical Records Support Quality Treatment Abroad', *US Medicine* (Washington, D.C.), February 2006, <http://www.usmedicine.com/article.cfm?articleID=1249&issueID=84> (last accessed 7 December 2006).

[52] Field medics are given hand held devices to capture medical data about a casualty in-theatre. The device is then connected to a laptop where it uploads the information to a centralised database. The database can be accessed by treatment facilities anywhere in the world, allowing doctors to see exactly what treatment has been provided and what still needs to be done. Ibid.

[53] Art. 19, Geneva Convention I requires respect and protection for fixed establishments and mobile medical units. Art. 33 provides specific protections for the material and stores of the units, which must remain available to the medical personnel to enable them to perform their functions; they may not be intentionally destroyed.

[54] Art. 12, Additional Protocol I; Art. 11, Additional Protocol II.

[55] Art. 21, Geneva Convention I states: "The protection to which fixed establishments and mobile medical units of the Medical Service are entitled shall not cease unless they are used to commit, outside their humanitarian duties, acts harmful to the enemy. Protection may, however, cease only after a due warning has been given, naming, in all appropriate cases, a reasonable time limit and after

database and the associated information systems are not used for any other purpose. For example, in addition to the standard access to medical records for treatment, commanders also use the system for medical situational awareness (for instance, to access information on incidents of illness in order to assess the need for vaccinations) a use which is covered by the disease prevention arm of the protections. However, the same broad spectrum use of the database for other purposes would not be covered by the Conventions. Using the database to research the effects of new weapons systems for example, a standard part of weapons development research,[56] would risk discontinuance of protection of the systems and expose the database to targeting by computer network attack.

In addition, paragraph two of Article 19 of Geneva Convention I contains an obligation on parties to ensure that medical units are, as far as possible, situated away from military objectives. Bearing in mind that military networks have become targets for computer network attack, medical databases and associated information systems will need to be isolated from systems which are now considered legitimate targets. Marking such systems as medical systems and informing the opposing side of their existence would also be required.[57] The problem of adapting identification techniques to modern methods of warfare is not new. The problem was previously struck at the time of drafting the Additional Protocols in respect of medical aircraft. Methods of electronic marking of aircraft were discussed and a secondary radar system of transponders (to automatically transmit an allocated identification code) was adopted.[58] This system appears easily adaptable to the computer environment. The communications standard over the Internet revolves around the TCP/IP protocol. Under this system every packet communicated over the Internet contains data about

---

such warning has remained unheeded." Art. 34, Geneva Convention II relating to hospital ships has similar wording, as does Art. 19, Geneva Convention IV relating to civilian hospitals.

[56] Data on the effects of new weapons are used as part of the so-called Solferino cycle, a development cycle which includes providing the observation and documentation of the effects of weapons both to weapons designers and to international humanitarian lawyers. See generally Robin M Coupland, 'The Effects of Weapons and the Solferino Cycle: Where Disciplines Meet to Prevent or Limit the Damage Caused by Weapons' (1999) 319(7214) *BMJ* 864 <http://www.bmj.com/cgi/content/full/319/7214/864> (last accessed 14 December 2006).

[57] Art. 39 Geneva Convention I requires the emblem to be displayed on all equipment employed in the medical service.

[58] Pilloud, et al., *Commentary*, paras 4203-4205.

the originating network and destination network, as well as multiple layers of information about the data itself.[59] Incorporating information regarding the medical nature of the data would not be difficult. Another alternative discussed in Chapter 5 *supra* is the designation of certain IP addresses as military networks, although as discussed, this proposal is not without difficulty as it marks a network for targeting.[60] The idea may translate more easily for networks that are specifically protected such as medical networks. It would however, depend on the network having a fixed IP address, a situation which may not prove technologically practical in modern-day field operations.

4.2. Hospital Ships

Article 34(2) of Geneva Convention II states that hospital ships may not possess or use secret codes for their wireless or other means of communication. Dinstein points out that this injunction against secret codes (forcing hospital ships to send and especially receive all messages in the clear) has severe practical problems.[61] As J Ashley Roach notes, technology has changed since 1949; all messages to and from warships, including unclassified messages, are now automatically encrypted when sent and decrypted when received by communications equipment that includes the cryptographic function.[62] This is also true for all network communications with naval craft and thus leaves hospital ships with the unattractive alternatives of being precluded from reports of movements of the fleet (and particularly advance notice of military operations likely to require their services),[63] or being in breach of their obligations under the second Geneva Convention. The San Remo Manual now moves in the direction of allowing hospital ships to use cryptographic equipment while prohibiting the transmission of intelligence data.[64] Without such encryption the

---

[59] For further explanation see the entry for 'TCP/IP' and 'Communication Protocol' in the techweb encyclopedia.; J. Ashley Roach, 'The Law of Naval Warfare at the Turn of Two Centuries' (2000) 94 *AJIL* 64.

[60] See Chapter 5, section 1.1 *supra.*

[61] Dinstein, *Conduct of Hostilities*, 171.

[62] Roach, 'The Law of Naval Warfare at the Turn of Two Centuries', 75.

[63] Louise Doswald-Beck, 'Vessels, Aircraft and Persons Entitled to Protection During Armed Conflicts at Sea' (1994) 65 *BYBIL* 211, 251; Dinstein, *Conduct of Hostilities*, 171.

[64] Dinstein, *Conduct of Hostilities*, 171.

hospital ships would prove a dangerous backdoor into military networks, allowing an attacker to gain access to other networks to which the ship is connected.

5. Non-defended Localities & Demilitarised Zones

Article 59 of Additional Protocol I prohibits parties to a conflict from attacking any non-defended locality by any means whatsoever. Article 60 prohibits the extension of military operations to zones which have been agreed between the parties as demilitarised zones. While these provisions are undoubtedly broad enough to apply to computer network attacks against physical areas, the characterization of non-defended localities or demilitarised zones raises an interesting issue in the computer age. Can a computer system or network ever be considered in itself a non-defended locality or be designated a demilitarized zone?

Non-defended Localities

Article 59 codifies and confirms customary international law and reiterates almost entirely Article 25 of the Hague Regulations.[65] Article 59 defines the concept of a non-defended location as an "inhabited place" near or in a zone where armed forces are in contact and which is open for occupation. Likewise the Hague Regulations refer to "towns, villages, dwellings, or buildings", all places of human occupation, which cannot easily be equated with computer systems. Traditional customary international law refers to open towns and undefended areas,[66] and may provide more scope for translation to a computer network. However, given the ambiguous nature of the characterisation, the parties would be wise to agree between themselves that a particular computer system or network constituted such a locality and what existing network protections may remain in place without compromising its designation as non-defended. The customary law prohibition of attacks against non-defended localities is also applicable in non-international armed conflicts.[67]

---

[65] Pilloud, et al., *Commentary*, para 2263.; Art. 25, Hague Regulations states "The attack or bombardment, by whatever means, of towns, villages, dwellings, or buildings which are undefended is prohibited".

[66] Henckaerts and Doswald-Beck, *Customary International Humanitarian Law*, 124.

[67] For example, Art. 3, Statute of the International Criminal Tribunal for the former Yugoslavia provides for prosecution of the violations of the laws and customs of war including "attack, or bombardment, by whatever means, of undefended towns, villages, dwellings, or buildings".

Demilitarized Zones

Of greater interest in computer-age conflict is the parties' ability to agree to grant particular zones the status of demilitarised zones.[68] The subject of the agreement can be any zone expressly agreed by the parties, although the Commentary to the Additional Protocols states that the essential character of the zones is humanitarian and not political – they are specially intended to protect the population living there against attacks.[69] While the concept was designed for physical locations, there is no reason why the parties could not agree to designate a particular network or system as a demilitarised zone.[70] Once designated as a demilitarised zone, Article 60(1) of Additional Protocol I prohibits parties to the conflict from "extend[ing] their military operations to zones on which they have conferred by agreement the status of demilitarized zone, if such extension is contrary to the terms of this agreement". This wording is broader than the protection provided under Article 59 relating to non-defended localities, discussed *supra*, which only prohibits attacks against the locality. The Commentary to the Additional Protocols states that the expression "military operations" should be understood as all movements and activities related to hostilities, carried out by armed forces.[71] Thus all use of a particular system for *any* activity relating to hostilities would be prohibited.

---

[68] Art. 60, Additional Protocol I.

[69] Pilloud, et al., *Commentary*, para 2303.

[70] Art. 60(3) sets out the general outline for the terms of such an agreement, however as indicated by the inclusion of the term 'normally', it can be adapted for specific situations. Art. 60(3) provides "The subject of such an agreement shall normally be any zone which fulfils the following conditions: (a) all combatants, as well as mobile weapons and mobile military equipment, must have been evacuated; (b) no hostile use shall be made of fixed military installations or establishments; (c) no acts of hostility shall be committed by the authorities or by the population; and (d) any activity linked to the military effort must have ceased".

[71] Pilloud, et al., *Commentary*, para 2304.

Chapter 8 – Protection of Cultural Property

It may seem odd, in a thesis about the most modern of methods of warfare, to incorporate a chapter dealing with the protection of some of the most enduring and profound symbols of humanity's accomplishments. After all, a computer network attack is scarcely likely to bring down the Sphinx, destroy a Rembrandt or delete the Great Mosque at Mecca. Further, where it *is* possible to cause physical damage to such creations, the mere fact of the use of technology to undertake the attack does not detract from the illegality of the action under the laws of armed conflict.
However in the modern era, more and more cultural monuments, libraries, and scientific collections are digitised and stored on information systems, in some cases becoming the only surviving record of a lost art, language or culture. Where digitisation takes place, these records and collections become vulnerable to the effects of computer network attacks, either through destruction or damage, or by misappropriation of cultural works.
The question also arises as to what the cultural legacy of those peoples living in States that have fully embraced the information age will be and how the protection of that cultural property or heritage will take place. Modern society has utilised the networking power of the Internet for almost every aspect of human cultural endeavour; from religion to art, science to education. Will the backbone servers of the Internet be protected during armed conflicts as the 'cultural heritage of every people'? Will online prayer wheels and other religious networks be protected as places of worship?

1. The Legal Framework

The destruction and looting of cultural property has taken place in almost every conflict since ancient times; sometimes it occurs as an incidental result of the conduct of military operations, other times it is a deliberate attack on the morale and culture of a particular people as a show of dominance and subjugation. For a long time this was an accepted reality of warfare, however the idea of protecting cultural property during times of war began to find favour in the eighteenth century and has

developed over time, and through the devastation of many wars.[1] Cultural property is now protected by both specific cultural property conventions and the more general framework of the laws of armed conflict. In all cases, the principle of distinction applies and cultural property remains protected by virtue of being civilian property.

1.1. Hague Regulations and Geneva Conventions

The Hague Regulations contain the first formal treaty protection for cultural property during armed conflict, although the term is not so defined:[2]

> Art. 27. In sieges and bombardments all necessary steps must be taken to spare, as far as possible, buildings dedicated to religion, art, science, or charitable purposes, historic monuments, hospitals, and places where the sick and wounded are collected, provided they are not being used at the time for military purposes.
>
> It is the duty of the besieged to indicate the presence of such buildings or places by distinctive and visible signs, which shall be notified to the enemy beforehand.
>
> Art. 28. The pillage of a town or place, even when taken by assault, is prohibited.
>
> Art. 56. The property of municipalities, that of institutions dedicated to religion, charity and education, the arts and sciences, even when State property, shall be treated as private property.
>
> All seizure of, destruction or wilful damage done to institutions of this character, historic monuments, works of art and science, is forbidden, and should be made the subject of legal proceedings.

The Hague Regulations thus express an obligation to protect, although protection is qualified, by the inclusion of the words "as far as possible", by the dictates of military necessity. Protection is accorded to buildings rather than their contents,[3] and

---

[1] For a more complete historical background to the development of the laws relating to the protection of cultural property during armed conflict than is possible here, see generally Patrick J. Boylan, *Review of the Convention for the Protection of Cultural Property in the Event of Armed Conflict* (UNESCO, 1993), 28; Jirí Toman, *The Protection of Cultural Property in the Event of Armed Conflict* (Dartmouth : UNESCO, Aldershot; Brookfield, Vt., 1996), 71; Kevin Chamberlain, *War and Cultural Heritage: An Analysis of the 1954 Convention for the Protection of Cultural Property in the Event of Armed Conflict and Its Two Protocols* (Institute of Art & Law, Leicester, 2004).

[2] 18 October 1907, *Convention Respecting the Laws and Customs of War on Land and Its Annex: Regulations Concerning the Laws and Customs of War on Land.*

[3] Chamberlain, *War and Cultural Heritage*, 28.

the buildings are defined in terms of their purpose rather than their cultural importance.[4]

Although the Geneva Conventions do not specifically address the status of cultural property, they do provide some protection to cultural property by virtue of it being civilian property. Article 53 of Geneva Convention IV prohibits an occupying power destroying real or personal property owned by private persons, the State, public authorities or social or co-operative organisations. The provision is subject to the requirements of military necessity where "destruction is rendered absolutely necessary by military operations".[5]

Additional Protocol I continues the protection of civilian objects, defined as all objects which are not military objectives, by prohibiting all attacks and reprisals against such objects.[6] The Protocol also includes specific protections for cultural property. Article 53 of Additional Protocol I provides:

> Without prejudice to the provisions of the Hague Convention for the Protection of Cultural Property in the Event of Armed Conflict of 14 May 1954, and of other relevant international instruments, it is prohibited:
>
> (a) to commit any acts of hostility directed against the historic monuments, works of art or places of worship which constitute the cultural or spiritual heritage of peoples;
>
> (b) to use such objects in support of the military effort;
>
> (c) to make such objects the object of reprisals.

Article 16 of Additional Protocol II provides almost identical wording.[7]

Both Article 53 and Article 16 are expressed without prejudice to the 1954 Hague Convention for the Protection of Cultural Property in the Event of Armed Conflict (Cultural Property Convention), and in the case of Additional Protocol I, any other

---

[4] Ibid.

[5] Art. 53, Geneva Convention IV.

[6] Art. 52, Additional Protocol I. Any doubt as to the status of objects normally dedicated to civilian purposes is to be resolved in favour of finding that the are civilian objects.

[7] Art. 16, Additional Protocol II provides: "Without prejudice to the provisions of the Hague Convention for the Protection of Cultural Property in the Event of Armed Conflict of 14 May 1954, it is prohibited to commit any acts of hostility directed against historic monuments, works of art or places of worship which constitute the cultural or spiritual heritage of peoples, and to use them in support of the military effort".

relevant international instrument.[8] In the event of a conflict between the provisions of the Additional Protocols and the Cultural Property Convention, or in cases where the Cultural Property Convention provides greater detail, the provisions of the Cultural Property Convention (or other relevant instrument) take precedence. This is particularly important in relation to the exception for instances of military necessity, as the Additional Protocols do not allow derogation in the case of imperative military necessity as contained in the Cultural Property Convention.[9] Although the counterpoint to the respect due to the specified cultural objects is a prohibition against using such objects "in support of the military effort", any right to such attacks could only be justified where the objects in question were a military objective under Article 52(4).[10] As the commentary to the Additional Protocol points out, the military effort is a very broad concept, encompassing all military aspects connected with the conduct of the war. Attacks against historic monuments, works of art or places of worship may constitute a grave breach where they result in "extensive destruction".[11]

Both Article 53 and Article 16 prohibit "acts of hostility directed against" cultural objects. Accordingly, it is not necessary to cause damage or other deleterious effects to the objects for this provision to be violated, it is enough merely to direct attacks against them.[12]

1.2. Cultural Property Convention 1954 and its Protocols

The Hague Convention for the Protection of Cultural Property in the Event of Armed Conflict of 1954 (Cultural Property Convention) is, and remains, the primary

---

[8] The omission of "any other relevant international instrument" from the text of Art. 16, Additional Protocol II reflects the fact that the Hague Conventions are not specifically applicable to non-international armed conflicts and the Roerich Pact applies in peace as well as war. Although this does exclude two UNESCO conventions, the omissions have no material consequences on protection. Pilloud, et al., *Commentary*, 1468, para 4837.

[9] Rogers notes that this is suprising given the English-speaking States' insistence on such a derogation in the Cultural Property Convention, but suggests that it may be covered by the principle of necessity. Rogers, *Law on the Battlefield*, 154.

[10] For this to take effect the object would by its "nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage"

[11] Art. 85(4)(d), Additional Protocol I; Pilloud, et al., *Commentary*, 648, para 2074.Note that to constitute a grave breach, an attack against cultural objects must cause "as a result extensive destruction thereof".

[12] Ibid., 647 para 2070, 1470 para 4845.

convention for the protection of cultural property in times of war.[13] Both the subsequent 1999 Protocol II to the Convention and the relevant sections of both Additional Protocols to the Geneva Conventions are drafted "without prejudice" to its terms.[14]

Drafted in reaction to the terrible damage to and systematic pillage of cultural property during WWII, the Convention contains obligations on States to both safeguard their cultural property in times of peace and respect such property in the event of armed conflict.[15] Article 3 requires States to take measures to safeguard the cultural property situated in their territory against the foreseeable effects of armed conflict. The Convention does not specify the form which such safeguarding should take, it merely imposes an obligation on the Parties to take such measures as they consider appropriate in peacetime. Article 4(1) of the Convention balances the obligation of the attacking State not to make cultural property the target of an attack and the receiving State's obligation not to use such property in a manner that might expose the property to destruction or damage:

> The High Contracting Parties undertake to respect cultural property situated within their own territory as well as within the territory of other High Contracting Parties by refraining from any use of the property and its immediate surroundings or of the appliances in use for its protection for purposes which are likely to expose it to destruction or damage in the event of armed conflict; and by refraining from any act of hostility directed against such property.

The obligations may be waived only in cases "where military necessity imperatively requires such a waiver".[16] Paragraph three of the Article further provides:

> The High Contracting Parties further undertake to prohibit, prevent and, if necessary, put a stop to any form of theft, pillage or misappropriation of, and any

---

[13] 14 May 1954, *Convention for the Protection of Cultural Property in the Event of Armed Conflict,* 249 UNTS 240.

[14] Art. 53, Additional Protocol I; Art. 16, Additional Protocol II; Roger O'Keefe, 'The Meaning of 'Cultural Property' under the 1954 Hague Convention' (1999) XLVI *NIL Rev* 26, 31.

[15] Art. 2, Cultural Property Convention.

[16] Art. 4(2), Cultural Property Convention. The reservation of imperative military necessity was debated over several meetings and discussed several options. In the end the proposal to delete the reference to military necessity was defeated by 22 votes to eight with eight abstentions. See Toman, *Protection of Cultural Property*, 72-79.

> acts of vandalism directed against, cultural property. They shall, refrain from requisitioning movable cultural property situated in the territory of another High Contracting Party.

The phrase 'misappropriation' was deliberately chosen instead of 'removal of property' as some property may need to be removed for its safeguarding and the word misappropriation better reflects the intention of the drafters.[17] It should also be noted that, unlike the obligations contained in paragraph one of the Article, the obligation to prevent theft, pillage and misappropriation, may not be waived as a matter of military necessity. The Article also bans any reprisals against cultural property.[18] Another point of note, particularly in relation to precautions in attack as we will see with computer network attacks, is the provision in Article 4(5):

> No High Contracting Party may evade the obligations incumbent upon it under the present Article, in respect of another High Contracting Party, by reason of the fact that the latter has not applied the measures of safeguard referred to in Article 3.

Articles 8 and 9 of the Convention provide that certain property may also be granted special protection where it is a refuge intended to shelter movable cultural property or a centre containing monuments or other immovable cultural property of very great importance. These refuges and centres must be located an adequate distance away from industrial centres and other military objectives and not be used for military purposes, although location does not matter to the granting of special protection as long as the refuge is constructed so that in all likelihood it will not be damaged by bombs. Cultural property under special protection is designated as such by registering the property in the International Register of Cultural Property under Special Protection, from which time the property will enjoy immunity from attack and use for military purposes.[19] Notably, immunity for cultural property under special protection can only be waived in situations of "exceptional cases of unavoidable military necessity, and only for such time as that necessity continues".[20] A cultural centre is deemed to be used for military purposes if it is used for the

---

[17] Ibid., 71.

[18] Art. 4(4), Cultural Property Convention.

[19] Arts. 8 & 9, Cultural Property Convention.

[20] Art. 11, Cultural Property Convention.

movement, even transit, of military personnel or supplies, activities directly concerned with military operations, stationing of military personnel or the production of war material.[21]

The Protocol for the Protection of Cultural Property in the Event of Armed Conflict (Protocol I) was adopted at the same time as the Cultural Property Convention and deals mainly with the protection of cultural property in occupied territory. Boylan and Toman both point out that the non-existence of examples of States Parties taking actions to bring its provisions into practical effect.[22] The almost universal disregard for the principles of the Protocol is one of the most serious breaches of the Cultural Property Convention.[23]

The Second Protocol to the Cultural Property Convention (Protocol II) is additional to the Convention and does not modify its terms.[24] The protocol does however clarify that cultural property may only be attacked on the basis of imperative military necessity where that property has, by its function, been made into a military objective and where there is no feasible alternative available; this change reflects the evolution of international humanitarian law with respect to military necessity which had occurred between the time of drafting of the Cultural Property Convention in 1954 and the drafting of the Additional Protocols to the Geneva Conventions in 1977.[25] Likewise the exception allowing the use of cultural property in cases of imperative military necessity, is further elucidated by allowing the use of cultural property for military action "when and for as long as no choice is possible between such use of the cultural property and another feasible method for obtaining similar military advantage".[26]

Protocol II also adds an additional level of 'enhanced' protection for property where it meets the following three conditions:[27]

a. it is cultural heritage of the greatest importance for humanity;

---

[21] Art. 8(3), Cultural Property Convention.

[22] Boylan, *Review*, 101; Toman, *Protection of Cultural Property*, 349.

[23] Boylan, *Review*, 101; Toman, *Protection of Cultural Property*, 349.

[24] *Second Protocol to the Hague Convention of 1954 for the Protection of Cultural Property in the Event of Armed Conflict,* 26 March 1999, UNESCO Doc. HC/1999/7.

[25] Art. 6, Second Cultural Property Protocol; Jean-Marie Henckaerts, 'New Rules for the Protection of Cultural Property in Armed Conflict' (1999) 835 *IRRC* 593, 601.

[26] Art. 6(b), Second Cultural Property Protocol.

[27] Art. 10, Second Cultural Property Protocol.

b. it is protected by adequate domestic legal and administrative measures recognising its exceptional cultural and historic value and ensuring the highest level of protection;
c. it is not used for military purposes or to shield military sites and a declaration has been made by the Party which has control over the cultural property, confirming that it will not be so used.

Interestingly, enhanced protection status does not provide cultural property with any additional protection from attack; the enhanced status refers to the difference in the obligations of the holder of the cultural property.[28] In the case of general protection, the holder of the property has the right, if need be, to convert the property into a military objective by using it for military action; property under enhanced protection may never be so used. Doing so would amount to a serious violation of the Protocol and render the offender liable to criminal sanction as a war criminal.[29]
The Protocol also attaches individual criminal responsibility for the following offences against cultural property protected under the Convention: attacking; extensive destruction or appropriation; theft, pillage or misappropriation; and acts of vandalism.[30] The Protocol also provides for specific sanctions for serious violations of cultural property, and requires States to take necessary measures to establish jurisdiction over, and criminalise the offences.[31] It should also be noted that Protocol II applies equally to international and non-international armed conflicts.[32]

1.3. Definition of Cultural Property

Defining just what constitutes protected cultural property is a complex task. Many of the treaty regimes covering the protection of cultural property in the event of armed conflict use different definitions, so that some objects which are protected under one regime may not be granted protection under others.

---

[28] Henckaerts, 'New Rules', 610.

[29] Ibid.

[30] Art. 15, Cultural Property Protocol. Note that the offence of theft, pillaging and misappropriation is against property protected by the Convention only, rather than "the Convention and this Protocol", unlike the other general offences.

[31] Arts. 15(2) and 16, Cultural Property Protocol.

[32] Arts. 3 & 22, Second Cultural Property Protocol. The application of the Protocol to all parties to a non-international armed conflict, whether governmental or insurgent, was clearly acknowledged at the final plenary session. Henckaerts, 'New Rules', 617.

As noted previously, the Hague Regulations do not use the term 'cultural property' but extend their protections to "buildings dedicated to religion, art, science, or charitable purposes and historic monuments" provided that they are not being used at the time for military purposes.[33] Further property belonging to municipalities and that of institutions dedicated to religion, charity and education, the arts and sciences are protected, as are historic monuments and works of art and science.[34] It is widely accepted that the Hague Regulations, and therefore its classification of cultural property for the purposes of the convention, has the force of customary international law.[35]

The 1954 Cultural Property Convention defines cultural property (irrespective of origin or ownership) as "movable or immovable property of great importance to the cultural heritage of every people".[36] The definition includes "monuments of architecture, art or history, whether religious or secular; archaeological sites; groups of buildings which, as a whole, are of historical or artistic interest; works of art; manuscripts, books and other objects of artistic, historical or archaeological interest; as well as scientific collections and important collections of books or archives or of reproductions of the property defined above". The definition also includes "buildings whose main and effective purpose is to preserve or exhibit the movable cultural property" defined above,[37] and "centres containing a large amount of cultural property".[38]

The Protocols to the Cultural Property Convention and the two Additional Protocols to the Geneva Conventions all refer to the definition in the Cultural Property Convention.

---

[33] Art. 27, Hague Regulations.

[34] Art. 56, Hague Regulations.

[35] Note that the definition does not extend to archives and it has been concluded that the occupying power had the right to seize archives and military plans. Toman, *Protection of Cultural Property*, 47.

[36] Art. 1(a), Cultural Property Convention.

[37] Such as museums, large libraries and depositories of archives, and refuges intended to shelter cultural property in the event of armed conflict. Art. 1(b) Cultural Property Convention.

[38] Art. 1(c), Cultural Property Convention.

2. The Digital Millennium and Protection of Cultural Property

Cultural property may be covered by two types of protection, the general protection provided to civilian objects and specific cultural property protections. Any cultural property covered by those protections will be protected from computer network attacks as it would be from any other attack. However the evolution of societies into the digital age has created a new genus of property, namely digital cultural property; some of which will constitute 'property of great importance to the cultural heritage of all peoples'. UNESCO adopted the Charter on the Preservation of the Digital Heritage in 2003, recognising that the digital heritage consists of resources which have "lasting value and significance, and therefore constitute a heritage that should be protected and preserved for the current and future generations".[39] The Charter does not refer to the protection of the digital heritage in armed conflict, however it sets out measures for protection and preservation of digital heritage and emphasises the threat of loss and need for action in protecting it.[40] It should be noted that cultural heritage is a broader concept than cultural property,[41] and any digital property for which protection is claimed would need to meet the definition of cultural property set out above. Like traditional forms of cultural property, most digital cultural property will be covered by the protections afforded to civilian property; some however will also be covered by the provisions of the Cultural Property Convention and other cultural property instruments. Two main types of digital cultural property may be at risk from computer network attacks; works which are digital reproductions of pre-existing cultural property and those which are 'born-digital' and exist only in digital form.[42]

---

[39] Art. 1, Charter on the Preservation of the Digital Heritage, Adopted at the 32nd session of the General Conference Paris, France, 17 October 2003.

[40] Arts. 3-9, Charter on the Preservation of the Digital Heritage.

[41] See generally, Manlio Frigo, 'Cultural Property *v.* Cultural Heritage: A "Battle of Concepts" in International Law?' (2004) 86(854) *IRRC* 367.The Cultural Property Convention notes "damage to cultural property belonging to any people whatsoever means damage to the cultural heritage of all mankind, since each people makes its contribution to the culture of the world." Thus cultural property is a subset of cultural heritage.

[42] Jean-Michel Rodes, Geneviève Piejut and Emmanuèle Plas, *Memory of the Information Society* (UNESCO, Paris, 2003), 39.

2.1. The Digitisation of Cultural Property

A significant part of the current digital heritage consists of the products of digital reproduction of pre-existing works.[43] Where the original works represent cultural property covered by the conventions above, their digital counterparts are to be considered reproductions and will be covered by the Cultural Property Convention where they are held in important collections. In discussions regarding the protected status of reproductions of cultural property at the conference which adopted the Convention, the French and Swiss delegates point out that reproductions become of even more importance where the original is destroyed.[44] However not all reproductions are intended to be protected by the Conventions; no-one would suggest that the millions of souvenir copies of Michelangelo's David sold in Florence each year are protected under the Convention despite the undoubted protected status of the original. An additional problem is that not all digital reproductions reproduced for the purpose of conservation form part of collections, but are nonetheless important reproductions of protected and highly fragile cultural objects. A number of examples of objects reproduced for particular projects will illustrate the problem.

Monuments

In 1995 the Getty Conservation Unit sponsored a virtual reality reconstruction of the tomb of Queen Nefertari in an effort to prevent further deterioration to the original tomb. Now, anyone with a ten-thousand dollar Silicon Graphics computer can "walk through" her final resting place miles away from the Theban necropolis in Luxor.[45] Likewise, the Great Sphinx at Giza has been digitally recreated in its original form,

---

[43] Ibid., 37.

[44] Intergovernmental Conference on the Protection of Cultural Property in the Event of Armed Conflict, *Records of the Conference Convened by the United Nations Educational, Scientific and Cultural Organisation and Held at the Hague from 21 April to 14 May 1954* (Government of the Netherlands, The Hague Staatsdrukkerij en Uitgeverijbedrijf, 1961). paras 214-215, cited in Toman, *Protection of Cultural Property*, 134.

[45] The reconstruction was made for the exhibition "Nefertari, Light of Egypt" organized by the Getty Conservation Institute and Fondazione Memmo. The tomb was discovered in 1904 and closed in the 1950s to avoid further degradation of the frescoes. Restored between 1986 & 1992, the Tomb was re-opened in 1995 with strict controls on visitor access. The authority is still try to find a way to permit visitors inside the tomb without damaging it; virtual reality gives the visitor this opportunity. See http://www.infobyte.it/vartcollection/contenuto_uk.htm#; Alexander Stille, *The Future of the Past: How the Information Age Threatens to Destroy Our Cultural Heritage* (Picador, Oxford, 2002), 3.

nose, royal beard and headdress intact, by computer generation from careful scientific measurements;[46] scientists are studying erosion patterns on the monument to help study and restore the giant edifice. As some of the great monuments of the world are being gradually destroyed, both through the natural process of erosion and the increased effects of human intervention,[47] the digital versions are becoming more and more important to researchers and the public alike. However because of the nature and scope of the projects involved, and the sheer scale of the projects, it is unlikely that any institution will have more than a few such projects at a time. Thought will need to be given to the status of these projects and their inclusion as part of a collection.[48]

Digitised libraries & museums

The number of digitisation projects at the world's libraries and museums has exploded over the past 10 years. Museums are intensely engaged in the creation of digital reproductions from the museums' collections, which are then archived, reproduced and disseminated either through digital media (such as CDs) or via other communication technology such as the Internet.[49] In fact, the number of visitors to New York's Metropolitan Art Museum collections is now higher over the Internet than in person.[50] Many art museums also have websites with virtual exhibition space in which they display their collections.[51] Collections of digital reproductions of

---

[46] Coupled with the data from a fully automated, solar powered monitoring station placed behind the Sphinx, the reconstruction relies on the data and images collected by Dr Mark Lehner of the Sphinx Mapping Project (http://www.aeraweb.org/sphinx_home.asp), a project designed to survey and record the Sphinx using photogrammetric cameras. Ibid.

[47] The monuments are gradually being damaged both through pollution and accelerated salt crystallisation from increasing numbers of people accessing the sites.

[48] The Getty Conservation Unit, forms part of the Getty Institute which possesses a collection of art works in its own right, however the example illustrates the point that Institutes involved in digital reproductions may not have a collection per se, let alone an 'important collection' for the purposes of the Cultural Property Convention. The reconstruction of Nefertiti's tomb forms part of the collection by Infobyte, along with reconstructions of the Colosseum in Rome, the Basilica of Assisi and other important cultural property. See http://www.infobyte.it/vartcollection/contenuto_uk.htm#.

[49] Guy Pessach, *Digital Art Museums - Legal Perspectives*, (2006) <http://islandia.law.yale.edu/isp/writing%20paper/digital_art.htm> (last accessed 9 June 2006).

[50] Carol Vogel, '3 out of 4 Visitors to the Met Never Make It to the Front Door', *New York Times* 29 March 2006, Section G 18 <www.nytimes.com/2006/03/29/arts/artsspecial/29web.html?pagewanted=print> (last accessed 12 August 2006).

[51] Pessach, *Digital Art Museums - Legal Perspectives*.

major artistic works, architecture and artefacts are also collected and presented for educational use in digital collections such as ARTstor.[52]

Major depository libraries such as the British Library, U.S. Library of Congress and the Vatican Library are all undergoing extensive digitisation projects in order to conserve their collections and increase access to some of their most important and fragile works. A study commissioned by the British Library and conducted by Electronic Publishing Services found that by 2020, ninety percent of all research materials in the United Kingdom will be available digitally; half will be available in both print and digital format and forty percent will be digital only.[53]

Databases, lost languages & other intangible property

Records of languages which have been subsequently lost or are in the process of extinction also exist in digital format transferred from tape onto digital media as part of preservation efforts. In many cases these are the only surviving records of a language or even an entire culture. As more societies feel the effects of globalisation increasing numbers of languages will be lost.[54] UNESCO has stated that these languages form part of the intangible cultural heritage of humanity.[55] Other projects designed to record and preserve intangible cultural property such as the traditional ecological knowledge prior art database (TEK*PAD) have been created with the dual purpose of preventing Western pharmaceutical and other companies from taking patents over traditional preparations and preventing traditional uses of these remedies, as well as forming a world repository of traditional knowledge.[56] Although

---

[52] http://www.artstor.org/info/

[53] Sylvia Carr, 'British Library Prepping for Digital Future' (2005) *Siliconcom* 30 June 2005 <http://networks.silicon.com/webwatch/0,39024667,39131513,00.htm> (last accessed 9 June 2006).

[54] There are roughly 6,000 languages in the world, yet 95% of the population speaks just 15 of them. Economic imperialism has gone hand-in-glove with linguistic imperialism, as people abandon their mother tongues in favour of the globally dominant English, French, Spanish, Arabic, Chinese and Russian. As a result, hundreds of languages have disappeared in the past 50 years, and experts predict there will be fewer than 3,000 languages left by the turn of the next century. John Crace, 'Silence Falls: Documenting the Extinction of Languages', *The Guardian* (London), 5 November 2002, Education <http://education.guardian.co.uk/egweekly/story/0,,825613,00.html> (last accessed 28 June 2006).

[55] *Convention for the Safeguarding of the Intangible Cultural Heritage,* 17 October 2003, UNESCO General Conference UNESCO MISC/2003/CLT/CH/14.

[56] TEK*PAD is a database of publicly available information concerning indigenous knowledge and plant species' uses intended to assist in research into prior art in the patent process and also to act as a

as noted above, care must be taken not to confuse the term cultural heritage with cultural property protected under the Cultural Property Convention,[57] archives of these materials are nevertheless archives which would be protected under the Convention.

2.2. 'Born Digital' - The Cultural Property of the Digital Age.

A second question which arises is what will constitute the cultural property of digital societies. Works which exist only in digital form are generally referred to as 'born digital'. These works result from an all digital process of initial production, the work being digitally encoded at the moment of its creation – for example a collection of digital photographs of planet earth.[58] Born digital works include art works completed and shown in digital format,[59] documents and archives stored only in electronic format, digital recordings, etc. It incorporates those digital works associated with a physical medium on which the file is recorded and stored, and also those works whose constituent parts are stored on physical media but where the work in question only reconstitutes itself in the digital environment.[60] Art museums are now exhibiting new digital art works by artists who specialise in the digitized virtual medium,[61] and many film makers now shoot only in digital mediums.

2.3. Attacks on, and Damage to, Digital Works

International humanitarian law prohibits attacks on, and damage to, cultural property except in cases of imperative military necessity.[62] This prohibition will apply despite translation to a digital environment. However, while digital works may still constitute cultural property, the digital environment operates in a different way to the physical one. The degree and necessary consequences of the attacks required to

---

resource for anyone researching traditional ecological knowledge, including scientists, health professionals: http://ip.aaas.org/tekindex.nsf (last accessed 26 June 2006).

[57] See generally Frigo, 'Cultural Property *v.* Cultural Heritage: A "Battle of Concepts" in International Law?'

[58] Rodes, Piejut and Plas, *Memory of the Information Society*, 39.

[59] See for example the works of artists submitted for the UNESCO digital art awards http://portal.unesco.org/culture/en/ev.php-URL_ID=29021&URL_DO=DO_TOPIC&URL_SECTION=201.html

[60] Rodes, Piejut and Plas, *Memory of the Information Society*, 39.

[61] Pessach, *Digital Art Museums - Legal Perspectives.*

[62] Art. 51, Hague Regulations; Art. 51, Additional Protocol I; Art. 4, Cultural Property Convention.

constitute an infringement may need reanalysis. The integrity of digital records is more fragile than that of their physical counterparts thus making the risk, and consequences, higher. The digital environment provides a forum in which records can be restored to their original form from backups without any trace that the record was ever changed. While this is one of the great strengths of digital media, it also represents one of its greatest threats; it means that records may also be changed unnoticed without leaving a trace of their amendments, leaving open the possibility of an Orwellian rewriting of history.[63] The defacement of websites has occurred on an increasing scale during diplomatic incidents over the past decade. While such actions would not be sufficient to constitute an attack, could drawing a moustache on a digital copy of the Mona Lisa be sufficient to breach the cultural property conventions? Will altering the work constitute damage – is it still an offence when digital property is not harmed permanently but can easily be restored to the original standard using backups? As seen in Chapter 6 *supra*, it is no defence to argue that the work or site in question was not protected.

The wording contained in the relevant conventions is fairly broad. Article 56 of the Hague Regulations provides that property belonging to institutions dedicated to religion, charity and education, and the arts and sciences are protected as private property and further "seizure of, destruction or wilful damage" to these institutions, historic monuments, works of art and science is forbidden.[64] The protection is part of customary international law, and presumably extends to the digital assets of those institutions and to digital monuments, works of art and science as well as any tangible works.

Article 4(1) of the Cultural Property Convention and both Article 53 of Additional Protocol I and Article 16 of Additional Protocol II, require State Parties to the Conventions to refrain from "any act of hostility" directed against cultural property. The obligation under the Cultural Property Convention may be waived only when military necessity imperatively requires such a waiver.[65] The broad language

---

[63] George Orwell's dystopian novel *1984* describes a department of a government ministry (the Ministry of Truth) which is responsible for rewriting segments of history (for example newspaper reports) which no longer fit with official policy. The slogan of the regime being "Who controls the past controls the future; who controls the present controls the past".

[64] Art. 56, Hague Regulations.

[65] Art. 4(2), Cultural Property Convention. It should also be noted that the territoriality principle was specifically removed from the article in order to affirm that cultural property is to be respected

contained in the Additional Protocols was discussed in the ICRC commentary on the Additional Protocols and confirmed by the Trial Chamber in *Jokic* which held that, according to the Additional Protocols, it is prohibited to direct attacks against "historic monuments, works of art or places of worship which constitute the cultural or spiritual heritage of peoples" whether or not the attacks result in actual damage.[66] However, the Appeals Chamber in *Kordic & Cerzec* subsequently held that, while recognising that attacks in violation of Articles 51 and 52 of Additional Protocol I are clearly unlawful even without causing serious harm,[67] the broad wording used in the above articles has been tempered by attaching individual criminal liability only to those acts which result in damage or destruction of the property. [68]

> "...deliberate attacks on civilian objects such as historic monuments, works of art and places of worship are considered to be grave breaches of the Additional Protocol only insofar as the attack results in extensive destruction."

It would appear that while attacks on digital works would constitute a breach of the Convention and/or Protocols, they would not rise to the level of grave breaches (and thus incur individual criminal liability) without resulting in substantial damage. However, one of the defining aspects of digital works is that a copy, for example a backup copy, is identical to the original, meaning that in many instances a digital work may be restored completely with no lasting damage. It remains to be seen whether damage to a digital work must be irreparable, but it would seem in line with the reasoning of the Appeals chamber in *Kordic & Cerzec* that it would not constitute a grave breach to damage a digital work which can be completely and

---

wherever it is situated. The amendment was tabled by Belgium, France, the Netherlands and Switzerland "Our amendment has been designed to break with the territorial concept and to affirm the principle that cultural property, wherever situated, must be respected by all States. It is important to break away from the notion of frontiers as, in time of war, military vicissitudes may lead to a State's overflowing its frontiers" Records, 136, para 247, cited in Toman, *Protection of Cultural Property*, 69.

[66] ICRC Commentary to Additional Protocol I, para 2067, 2069-72; *Prosecutor v Miodrag Jokic (Sentencing Judgement)* (2004) Case No IT-01-42/1-S, International Criminal Tribunal for the Former Yugoslavia - Trial Chamber I, §50.

[67] *Prosecutor v Dario Kordic and Mario Cerkez (Appeal)* (2004) Case No IT-95-14/2-A, International Criminal Tribunal for the Former Yugoslavia, Appeals Chamber, §65.

[68] Ibid., para 65.; Art. 85(4)(d), Additional Protocol I; Art. 3(d), Statute of the International Criminal Tribunal for the Former Yugoslavia.

identically restored from backup copies.[69] The maintenance of such backups would presumably fall within the measures taken by the victim State under its obligation to safeguard cultural works.[70] Whether or not those measures had been taken by the victim State would have to fall within the foreseeable harm analysis of the attacking State. Recent domestic criminal hacking cases have attempted to raise the lack of security on compromised systems in mitigation of the expected severity of the sentence.[71] However such a defence would have the opposite effect in the case of cultural property. Article 85 of Additional Protocol I makes it a grave breach of the Protocol to make a non-defended locality the object of an attack.

2.4. Theft, Pillage or Misappropriation of Digital Works

The Cultural Property Convention 1954 and its later protocol contain absolute prohibitions against "any form of theft, pillage or misappropriation" of cultural property;[72] the prohibition may not be derogated from through military necessity. Further, the Hague Regulations make all property belonging to cultural institutions private property and forbids the seizure of any such institution, historic monument or work of art or science; pillage is prohibited absolutely.[73]

As discussed in Chapter 9 *infra* regarding pillage generally, the intangible nature of digital works will not create an issue for international law; courts and tribunals have had no problem in finding pillage involving intangible property such as shares and property rights.[74] Thus where a State has digital reproductions of cultural property or born-digital works which constitute cultural property, those works would also be subject to the prohibition against theft, pillage and misappropriation.

---

[69] Ibid.

[70] Art. 3, Cultural Property Convention.

[71] 'UK Hacker 'Should Be Extradicted", *BBC News* (London), 10 May 2006, Technology <http://news.bbc.co.uk/1/hi/technology/4757375.stm> (last accessed 6 July 2006).

[72] Art. 4(3), Cultural Property Convention; Art. 15, Second Cultural Propery Protocol.

[73] Arts. 47 & 56, Hague Regulations.

[74] See for example, *Trial of Carl Krauch and Twenty-Two Others (I.G. Farben Trial)* (1948) X Law Reports of Trials of War Criminals 1, United States Military Tribunal, Nuremburg; *Trial of Alfied Felix Alwyn Krupp Von Bohlen Und Halbach and Eleven Others (the Krupp Trial)* (1948) X Law Reports of Trials of War Criminals 69, United States Military Tribunal, Nuremburg.

2.4.1. Unauthorised Copying of Works

Once stored in digital format, not only do works constituting cultural property become exposed to the risk of damage from computer network attacks as seen above, they may also be copied for use for the attacking State's own purposes. As the *Titan Rain* incidents show, vast amounts of such copying can occur in minutes. One of the defining characteristics of digitally stored information is that any number of copies may be made, at negligible cost, without in any way degrading the original.[75] This feature makes unauthorised copying of digital cultural property perhaps the most likely form of theft or misappropriation to affect digital works. Not only is it now possibile that the reproduction of Nefertiti's tomb may be copied in its entirety to be reproduced and displayed in a museum somewhere else, a more mundane use may be made of such digital works. Take the following hypothetical example, Arcadia is at war with Mesopotamia and subsequently occupies a portion of the territory of Mesopotamia. During the occupation, an enterprising group of soldiers copy digital art works from Mesopotamia's national gallery collection and place them on carpets, selling them in Arcadia. The art works copied are some of the most sacred and important cultural works of Mesopotamia's indigenous people and the resulting carpets cause great offence by having the 'enemy' literally walk on the spiritual traditions of the occupied territory.[76]

Leaving aside the issue of residual copyright in a digital reproduction as a work itself,[77] the question must be asked whether mere copying of a digital work, original or reproduction, leaving the digital 'master' unaltered and unharmed will constitute theft, pillage or misappropriation. Understandably, the conference which drafted the Convention did not consider the meaning of the words theft, pillage and

---

[75] In fact, one of the greatest paradoxes of digital cultural property is that preservation relies on multiple copies being made. Computing reverses those very propositions which seemed the most certain: the survival of a document is not dependant on how long the medium carrying it will last, but on the capacity of that document to be transferred from one medium to another as often as possible: Rodes, Piejut and Plas, *Memory of the Information Society*, 35.

[76] This example is a variant on the facts of an Australian copyright case of *Milpurrurru v Indofurn Pty Ltd* (1994) 54 FCR 240 in which Indofurn appropriated and simplified sacred aboriginal designs and reproduced them on carpets manufactured in Vietnam.

[77] A digital work is likely to have the protection of the relevant intellectual property act of the jurisdiction of origin. The unauthorised copying of the work would thus be considered a breach of copyright and be actionable under the domestic jurisdiction of the relevant State. However this section will deal only with the digital work's relevance as cultural property for the purposes of the laws of armed conflict.

misappropriation – all presumably deemed self explanatory.[78] In determining whether illegal copying may amount to theft, pillage or misappropriation, two questions must be answered. First, must the owner of the property be deprived of it entirely, or is it sufficient that the owner's property rights, namely the right to control the use made of the work, are infringed? And second, with regard to pillage, must the property be acquired through threats or use of violence?

The International Criminal Tribunal for the Former Yugoslavia held in the *Celebici* case stated that "the prohibition against the unjustified appropriation of public and private enemy property is general in scope, and extends both to acts of looting committed by individual soldiers for their private gain, and to the organized seizure of property undertaken within the framework of a systematic economic exploitation of occupied territory."[79] The Nuremburg cases, applying the Hague Regulations, tended to group property crimes together under a general heading of spoliation, and in some case it can be very difficult to establish which crime forms the basis of the charges.[80] However the phrase 'other misappropriation' contained in the Cultural Property Convention is a similarly broad based charge which would encompass the crimes set out by the military tribunals which included the offence contained in Article 46 of the Hague Regulations, namely respect for private property.

The Flick Trial convicted Friedrich Flick of crimes against property in a case which perhaps maps most closely to unauthorised copying of a digital work. Flick's offence consisted of operation of a plant in occupied territory of which he was not the owner

---

[78] The word misappropriation was added to replace the term 'removal of property' in regard to a party's obligation not to requisition property however its basic meaning was not discussed. Toman, *Protection of Cultural Property*, 71.

[79] *The Prosecutor v. Zejnil Delalic et al. (Celebici)* (1998) Case No. IT-96-21-T, International Criminal Tribunal for the Former Yugoslavia, para 590.

[80] For example, it is not completely clear which offence against private property Flick is found guilty of. The acts in question related to the seizure and operation of the Rombach plant in occupied France; however the Tribunal held that none of the defendants were shown to have been "responsible for any act of pillage as that word is commonly understood...Flick's acts and conduct contributed to a violation of Hague Regulation 46, that is that private property must be respected. Of this there can be no doubt. But his acts were not within his knowledge intended to contribute to a programme of 'systematic plunder' conceived of by the Hitler regime..."80 the analysis concludes that Flick must therefore have been found guilty either of an offence other than spoliation or a particular type of pillage. ... it may be that Flick's offence is to be regarded as an offence against property in occupied territories other than plunder or spoliation. *The Trial of Friedrich Flick and Five Others (the Flick Trial)* (1947) IX Law Reports of Trials of War Criminals 1, United States Military Tribunal, Nuremburg, 40.

and without the consent of the owner.[81] It is interesting to note that the Tribunal regarded his acts as illegal despite the fact that *(a)* "the original seizure may not have been unlawful; *(b)* Flick had nothing to do with the expulsion of the owner; *(c)* the property was left "in a better condition than when it was taken over"; *(d)* there was no exploitation either for Flick's personal advantage or to fulfil the aims of Goering", there being no proof that the output of the plant went to countries other than those who benefited before the war.[82] In a situation such as the hypothetical scenario above, where the property is exploited for the personal benefit of the perpetrators, it seems certain that a court would have no difficulty in finding that the work had been misappropriated. Indeed the commentary to the *Krupp Case* states that the prosecution was probably correct in claiming that violation of Article 46 of the Hague Convention [respect for private property] "need not reach the status of confiscation. Interference with any of the normal incidents of enjoyment of quiet occupancy and use, we submit is forbidden. Such incidents include, *inter alia*, the right to personal possession, control of the purpose for which the property is to be used, disposition of such property, and the right to the enjoyment of the income derived from the property".[83]

3. Case Study: Places of Worship & Religion on the Web

Places of worship are one of the earliest forms of protected cultural property. The digital environment has also allowed places of worship to become established on the Internet in both digitised and born digital forms. While some sites merely use the web as a broadcast tool, providing access to religious services over the Web and making information available to a global audience, other sites seek to create purely virtual churches,[84] where web casts of services are available live,[85] and prayer circles

---

[81] Ibid.

[82] Ibid. (footnotes removed)

[83] *The Krupp Trial*, 16, fn 15.

[84] See for example http://www.stpixels.com. St Pixels was, at the time of writing, in the process of being constructed as the successor site to Church of Fools which closed its virtual doors in May 2006 (http://www.churchoffools.com). See also The Godweb (http://www.godweb.org/) which is the successor to the First Church of Cyberspace.

[85] See for example http://www.hotworship.com/ (The site provides links to both live and recorded services).

and Quaker meetings meet in online forums to pray together.[86] Are these protected by cultural property laws? The capacity of a particular religion to use the Internet as sacramental space (and therefore as a place of worship which may be subject to protection in times of armed conflict) is, of course, dependent on the particular religion's conceptualisation of the Internet. Heidi Campbell has explored these different conceptualisations in her 2005 paper "Spiritualising the Internet".[87] Two of the discourses she outlines in particular are useful as a foundation for viewing these sites as a protected place of worship: the first, as a spiritual network, a conduit for the sacred created by the wires and connections of the technology itself;[88] or secondly as a worship space with the potential to be constructed and consecrated for religious use by its users.[89] The latter concept is illustrated by the examples of virtual churches above and is the approach adopted by most mainstream religions utilising this technology.[90] This view sees the potentially sacred space located at a particular website or IP address although the entire Internet may be consecrated or blessed as part of the process. According to Jeff Zaleski, Buddhists were the first members of a major world religion to both consecrate the Internet as a sacramental space and to duplicate online and in full a traditional form of religious practice.[91] Since then, other religious groups have also conducted rituals to consecrate cyberspace as holy space.[92]

---

[86] http://worship.quaker.org/ (Online Quaker Meeting); http://www.myprayercircle.com/ (Online Prayer Circle); although the above examples are all based on Christian traditions of worship, other religions also utilise the Internet for worship. (all sites last accessed 14 July 2006)

[87] Heidi Campbell, 'Spiritualising the Internet: Uncovering Discourses and Narratives of Religious Internet Usage' (2005) 1(1) *Online - Heidelburg Journal of Religions on the Internet* 1 <http://www.ub.uni-heidelberg.de/archiv/5824> (last accessed 27 January 2007).

[88] See Jennifer J. Cobb, *Cybergrace: The Search for God in the Digital World* (Crown, New York, 1998). cited in Campbell, 'Spiritualising the Internet'. These themes have been explored by Heidi Campbell in discussing how the Internet is written about and used in practice for religious purposes.

[89] See Margaret Wertheim, *The Pearly Gates of Cyberspace: A History of Space from Dante to the Internet* (W.W. Norton, New York, 1999). cited in Campbell, 'Spiritualising the Internet'.

[90] Note that not all mainstream religions are comfortable with virtual churches, requiring the physical presence of people to perform rituals. Further, those religions which require an intermediary between the individual and God (for example Roman Catholicism) struggle with the distinctly non-hierarchical nature of the Internet. Jeffrey P. Zaleski, *The Soul of Cyberspace: How New Technology Is Changing Our Spiritual Lives* (HarperEdge, San Francisco, 1997).

[91] The Buddhists interviewed by Zaleski engaged in Dharma Combat online. Dharma Combat is an unrehearsed dialogue in which Zen practitioners test and sharpen their understanding of Zen truths. Ibid., 160.

[92] Campbell, 'Spiritualising the Internet', 16.

However, in the same way that artisans have created born digital works, other religious traditions have used the power of the Internet to create new forms of ritual, incorporating the nature of the Internet into the ritual itself. For example, in 1995 a group of technopagans celebrated a CyberSamhain,[93] utilising the networking power of the web to create a sacred space online; other pagans may code their workings in HTML.[94] Where as the mainstream religions focus the creation of sacred space online, the pagan traditions (and hence the technopagans) view the connection between members as the essential element, although each member creates their own personal sacred space, the spirituality of the group comes from the flow of energy around the circle.[95] A similar view of the importance of connection and the flow of energy can be found in other spiritualist traditions such as Sufism, the mystical branch of Islam.[96]

So what does this online spirituality mean for the protection of these places of worship from computer network attack; are they entitled to special protection as cultural property?

The Hague Regulations state that all necessary steps must be taken to spare buildings dedicated to religion in sieges and bombardments.[97] The term 'buildings dedicated to religion' covers buildings of all religious persuasions, both Christian and non-Christian, churches, places of worship, mosques, synagogues and so forth.[98] Further, in relation to occupied territories, the property of institutions dedicated to religion is to be treated as State property, and all seizure, destruction or wilful damage done to institutions of this character is forbidden.[99] While the websites, servers and other property used for conducting online worship would undoubtedly be protected in

---

[93] Zaleski, *The Soul of Cyberspace*, 262. Technopaganism is a belief or cultural movement which combines an engagement with applied (esp. computer) technologies with spiritual and religious elements, typically derived from pre-Christian nature worship: Oxford English Dictionary; Samhain is the Pagan new year celebrated on 31 October.

[94] Lisa McSherry, *The Virtual Pagan: Exploring Wicca and Paganism through the Internet* (Red Wheel/Weiser, 2002). Interestingly, this is not a concept which is accepted by other religions. For example Judaism requires the physical presence of 10 adult males to create the minyam (or quorum) to create the 'higher level of godliness' for worship. Zaleski, *The Soul of Cyberspace*, 18-19.

[95] McSherry, *The Virtual Pagan*, 64.

[96] Zaleski, *The Soul of Cyberspace*, 61-68.

[97] Art. 27, Hague Regulations.

[98] Toman, *Protection of Cultural Property*, 11.

[99] Art. 56, Hague Regulations. Note that this protection is absolute without any reservations on the grounds of military or other necessity: Ibid.

occupied territories, the case for their general protection is harder to make. In short, servers are not buildings. Even by analogy, the difficulties are numerous. Where the place of worship sought to be protected is situated on one particular site, these sites are generally hosted by an ISP, on servers which host multiple sites, not merely religious ones. While these individual sites may qualify for protection, the server itself would not.

Under the theory of networked spirituality advanced by Cobb and practised by the technopagans, the sacred space is formed by the network created between individuals (and their own technology) rather than any one site. Thus the protected space would come into existence only when the members are online for spiritual purposes and would only relate to those connections which make up the circle at any one time; those connections change with each meeting.

While some religions have purported to consecrate the whole of cyberspace (an act which would presumably incorporate all connections to the Internet), as a matter of practicality this cannot literally be the case.[100] Indeed even within religions, and within denominations of those religions, there is no agreement as to the validity of any act of consecration or of the resulting sacredness of any online religious site.[101]

Under the Cultural Property Convention, places of worship are only protected where they amount to a monument of historic or artistic interest, or where they contain objects of historic or artistic interest.[102] Online religious forums do not fit comfortably into either category. The mere fact of their consecration for religious purposes does not automatically provide special protection from attack. During the preparatory work for the conference which resulted in the Convention it was proposed to classify all religious buildings as cultural property, regardless of their artistic or historic interest. This idea was abandoned in the UNESCO draft, as there was no wish to broaden the framework of protection to include other elements such as schools and laboratories.[103] Similar reasoning was also used in the drafting of the Additional Protocols to the Geneva Conventions. Although Article 53 of Additional

---

[100] The act of consecration is to dedicate or set something (or somewhere) apart for a sacred purpose. Given the ubiquitous nature of the Internet it is impossible that the whole of the Internet is consecrated.

[101] See generally Zaleski, *The Soul of Cyberspace.*

[102] Art. 1, Cultural Property Convention.

[103] Toman, *Protection of Cultural Property*, 48.

Protocol I refers only to places of worship (and not to buildings specifically), special protection is only granted to those places of worship which possess cultural or spiritual value independently of their consecrated status and thus constitute the "spiritual heritage of people".[104]

> "The conference rejected the idea which was put forward by some delegations of including any and all places of worship, as such buildings are extremely numerous and often have only a local renown of sanctity which does not extend to the whole nation. Thus the places referred to are those which have the quality of sanctity independently of their cultural value and express the conscience of the people.

Interestingly, it was stated that the cultural or spiritual heritage covers objects whose value transcends geographical boundaries, and which are unique in character and are intimately associated with the history and culture of a people.[105] While these new forms of online worship certainly transcend boundaries and are a unique form of worship, in the decade since the first consecration of cyberspace, they have yet to become entrenched in the history and culture of any particular people. It would seem that under these provisions, places of worship on the Internet are not yet at a stage where they receive special protection.

---

[104] Pilloud, et al., *Commentary*, 647, para 2067.

[105] Ibid., para 2064.

Chapter 9 – Means & Methods of Warfare

While predominately viewed as a method of attack, computer network attack scenarios may represent both means and method of attack depending on the attack being executed. According to the ICRC Commentary to the Additional Protocols the term "means of combat" or "means of warfare" generally refers to the weapons being used, while the expression "methods of combat" generally refers to the way in which such weapons are used.[1] For example, a worm in and of itself is usually a method of attack, it is designed as a means to distribute malicious code, or alternatively to cause generalised damage by overwhelming the networks with packets of information causing massive denial of service. To take one instance, the Slammer/Sapphire worm contains an algorithm designed to self-replicate and randomly generate addresses in order to spread itself as rapidly as possible.[2] Other forms of attack contain specific malicious code which is designed to cause damage to the computer, system or network directly. Trojans designed specifically to destroy hard drives or information are examples, a more indirect example is the code inserted into the Canadian pipeline software which resulted in the 'Farewell Dossier' incident, a huge explosion involving the Soviet Trans-Siberian gas pipeline.[3] Such malware fits the definition of a weapon far more closely than merely a method of attack. The more recent attacks have combined malicious code with a means of propagation such as a worm to form blended attacks. For example the Storm worm which was discovered in the wild in January 2007, combines multiple components; a component to steal email addresses and redistribute itself, a backdoor Trojan to allow subsequent access to the compromised machine, a bot recruiter to incorporate the machine into the Storm botnet, coding to allow remote control of the compromised machine across peer-to-

---

[1] Ibid., para 1957. Note however that the term method and means of warfare includes weapons in the widest sense, as well as the way in which they are used; para 1402.

[2] The Slammer/Sapphire worm hit the Internet in January 2003 and to date is the fastest spreading worm found in the wild. It infected more than 90% of vulnerable hosts (at least 75,000 hosts) in ten minutes. David Moore, et al., *The Spread of the Sapphire/Slammer Worm*, (2003) <http://www.caida.org/publications/papers/2003/sapphire/sapphire.html> (last accessed 9 November 2007). Other viruses may have different propogation techniques.

[3] See Appendix I.

peer networks (which morphs every few minutes to avoid detection), and a denial of service attack tool in a rootkit payload.[4]

1. Law of Weaponry

Article 22 of the Hague Regulations sets out the basic principle that "the right of belligerents to adopt means of injuring the enemy is not unlimited".[5] This concept of limited warfare, repeated almost verbatim in Additional Protocol I and the Conventional Weapons Convention,[6] constitutes the basis for the legal regulation of means and methods of warfare employed. As with the rest of the laws of armed conflict, the law of weaponry represents a balancing act between the principle military necessity, that is, what is required to efficiently conduct military operations, and what is required by humanitarian considerations; in the words of the St Petersburg Declaration of 1868 to fix 'the technical limits at which the necessities of war ought to yield to the requirements of humanity'.[7] The law of weaponry consists of general principles, such as those prohibiting indiscriminate weapons or unnecessary suffering, and a number of specific rules prohibiting or limiting the use of certain weapons or methods of warfare.[8] As Christopher Greenwood has remarked, the general principles tend to refer to the effects produced by the use of weapons or methods of warfare, whereas the specific provisions usually concentrate on the means employed.[9] Although only a few of the specific provisions are relevant to computer network attacks, the same general principles apply regardless of the style of weapon employed. As demonstrated by the discussion of the legality of nuclear weapons by the International Court of Justice, these principles established in

---

[4] For further details of the Storm worm see Joe Stewart, *Storm Worm DDoS Attack*, Secure Works (1997) <http://www.secureworks.com/research/threats/storm-worm> (last accessed 23 November 2007). Thorsten Holz, et al., 'Measurements and Mitigation of Peer-to-Peer-Based Botnets: A Case Study on Stormworm' (Paper presented at the First USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET '08), San Francisco, <http://honeyblog.org/junkyard/paper/storm-leet08.pdf> (last accessed 31 August 2008).

[5] Art. 22, Hague Regulations.

[6] Art. 35(1), Additional Protocol I; Preamble, Conventional Weapons Convention.

[7] Preamble, St Petersburg Declaration.

[8] Greenwood, 'Law of Weaponry', 192.

[9] Ibid.

the last century are capable of being applied well into the next, even to methods of warfare undreamed of when those principles were being formulated.[10]

1.1. General Principles

Flowing from the principle of 'limited warfare' several sub-principles have developed historically, giving the rule of military necessity its specific contours.[11] Not all of these will raise specific issues for computer network attacks, however a number require additional consideration as to their interpretation in the modern battlespace. In particular, the principle regarding unnecessary suffering and the prohibition against indiscriminate weapons; other general principles which form part of the law of weaponry are examined elsewhere in the relevant sections of this thesis, for example those dealing with environmental protection in Chapter 7 *supra*, and perfidy in section 2 *infra*.

Superfluous Injury & Unnecessary Suffering

The International Court of Justice has confirmed that the prohibition of means and methods of warfare which are of a nature to cause superfluous injury or unnecessary suffering is one of the cardinal principles of international humanitarian law.[12] Article 35(2) of Additional Protocol I represents one of the most recent statements of the prohibition:[13]

> It is prohibited to employ weapons, projectiles and material and methods of warfare of a nature to cause superfluous injury and unnecessary suffering.

It follows and clarifies similar statements in the St Petersburg Declaration of 1868 and Article 23(e) of the Hague Regulations.[14] The prohibition of *methods* of warfare

---

[10] Ibid., 186.

[11] Oeter, 'Methods and Means of Combat', 112.

[12] *Nuclear Weapons Case*, para 238.

[13] Art. 35(2) Additional Protocol I; the language is repeated in the preamble to the Conventional Weapons Treaty.

[14] The wording 'of a nature to cause' clarifies the English translations in previous incarnations of this provisions which used the words 'calculated to' and had occasionally been taken to mean the unnecessary suffering would have to be proved intentional. Hans Blix, 'Means and Methods of Combat' in UNESCO (ed) *International Dimensions of Humanitarian Law* (Martinus Nijhoff, Dordrecht, 1998) 135-151, 138.

which are of a nature to cause superfluous injury or unnecessary suffering was first introduced in Additional Protocol I, however the commentaries note that this change of language does not alter the principle which represents customary international law.[15] The principle is also applicable in conflicts not of an international character.[16] In its advisory opinion in the *Nuclear Weapons* case the Court defines unnecessary suffering as a 'harm greater than that unavoidable to achieve legitimate military objectives".[17] Inescapably, the test is valid only for weapons designed exclusively for anti-personnel purposes, in as much as anti-materiel weapons may be expected to cause injury to personnel in the vicinity of the target that would be more severe than necessary to render the combatants *hors de combat.*[18] In this respect, it is the use of computer network attacks as a method of warfare which must be assessed, as malicious code cannot (at the current state of technology) act directly on an individual, but rather on the physical and technological environment in which that person is situated. However, even in relation to weapons designed for other than anti-personnel purposes, the application of the unnecessary suffering principle requires a balancing of the military advantage which may result from the use of a weapon with the degree of injury and suffering which it is likely to cause.[19] As computer network attacks are varied as to their use and execution, each attack will need to be assessed separately to ensure that the balance is maintained. Greenwood notes that while there is general agreement that the character and effect of anti-materiel weapons differ from those commonly used against personnel, such weapons do not violate the unnecessary suffering principle, because the advantages they offer (for example, to destroy materiel) means that the additional suffering they may cause cannot be classed as unnecessary.[20]

---

[15] See for example, Bothe, et al., *New Rules*, 194. Pilloud, et al., *Commentary*, para 1417.

[16] The Appeals Chamber of the ICTY has held that the weapons prohibited in international armed conflicts are also prohibited in internal armed conflicts, stating "what is inhumane, and consequently proscribed, in international wars, cannot but be inhumane and inadmissible in civil strife": *Tadic (Interlocutory Appeal)*, para 119.

[17] *Nuclear Weapons Case*, para 238.

[18] Bothe, et al., *New Rules*, 196; Dinstein, *Conduct of Hostilities*, 60. Although the deliberate employment of an anti-materiel weapon against people, might also fall foul of this principle.

[19] Greenwood, 'Law of Weaponry', 195. Although the use of an anti-materiel weapon, employed deliberately against people might also fall foul of this principle.

[20] Ibid., 196. In this respect, Greenwood notes the use of inflammable bullets which came to be accepted as lawful against aircraft, despite the effect that they may have on an aircrew, but remain unlawful in a simple anti-personnel role: 225, fn 61.

As it is unlawful to use a weapon which causes more suffering or injury than another which offers the same or similar military advantage, the classification necessarily involves a comparison between different weapons systems.[21] This is perhaps one of the most interesting aspects of law of weaponry in relation to computer network attacks, namely the effect that access to these techniques will have on the legality of the parties' choice of other weapons. One of the advantages of computer network attack is that it allows neutralisation and destruction of targets with fewer casualties and less physical destruction, and in many cases more accuracy, than conventional weapons. For example, there is no need to bomb an electrical grid if you can simply turn it off for the desired period of time. This ability may have the effect of making other, more conventional methods of warfare, illegal as the damage caused by those methods becomes subsequently 'unnecessary'. However as Greenwood points out, it is not enough simply to compare the immediate effects of the two weapons (or methods of warfare);[22] the availability (including the expense) of both types of weapon, the logistics of supplying the weapon and its ammunition at the place where it is to be used, the security of the troops which employ it are all additional factors to be taken into account. While these would tend to resolve in favour of using computer network attack methods, there are also factors which may advocate against using such techniques in a given situation. As discussed in Chapter 6 *supra*, given that some computer network attack methods can only be used once before effective counter-measures are put in place, the likely future need for such an attack will also be a factor to be considered by commanders, as would the difficulty in ascertaining knock-on effects of a particular attack.

Indiscriminate weapons

The International Court of Justice in its advisory opinion on the *Threat or Use of Nuclear Weapons* held the principle of discrimination as a cardinal principle of international humanitarian law and held that States "must consequently never use weapons that are incapable of distinguishing between civilian and military targets".[23] Although the principle prohibiting the use of weapons which are inherently

---

[21] Blix, 'Means and Methods of Combat', 138-139.

[22] Greenwood, 'Law of Weaponry', 198.

[23] *Nuclear Weapons Case*, para 78.

indiscriminate or the indiscriminate use of any weapon falls mainly in the area of targeting and is discussed in Chapter 6 *supra*, it also has an effect on the law of weaponry.[24] Although many computer network attacks are targeted very specifically against the particular system or network to be attacked, the effects of an attack and the methods by which it is spread may be indiscriminate (for example, most computer viruses currently in the wild are coded to spread in precisely this manner).[25] Computer network attacks that cannot distinguish between civilian and military networks and systems are inherently indiscriminate, therefore where they cause physical injury or destruction, their use in armed conflict is unlawful. Further, malicious code or network attacks which are capable of being utilised in a discriminating manner but are delivered in an indiscriminate way are also prohibited. As with the principle of unnecessary suffering, where the same military advantages can be achieved in different ways, one of which involves likely civilian casualties whereas the other does not, then the choice of the first route will entail a violation of the principle.[26] This means that computer network attacks may in many cases result in the prohibition of other methods of attack.

As Christopher Greenwood points out the 1991 Gulf Conflict illustrates that the proportionality test, at least at the strategic level, requires that less immediate damage such as that inflicted on the Iraqi population by the destruction of the power generating system and other infrastructure, must be taken into account.[27] Such knock-on effects must be taken into effect in the targeting calculations by commanders.

Martens Clause

The Martens Clause was first included in the preambular provisions of the Hague Convention of 1899 and a modern formulation is expressed in Article 1(2) of Additional Protocol I:

---

[24] Greenwood, 'Law of Weaponry', 200.

[25] For example the Storm worm is hard-coded with a sample set of addresses and a random dialling algorithim which enables it to spread from computer to computer.

[26] Greenwood, 'Law of Weaponry', 201.

[27] Ibid., 202.

> In cases not covered by this Protocol or by other international agreements, civilians and combatants remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and from the dictates of public conscience.

As the Court in the *Nuclear Weapons* case noted, the clause has proved to be an effective means of addressing the rapid evolution of military technology.[28] Thus although there is currently no rule or agreement in international humanitarian law which expressly bans or restricts the use of computer network attacks, where a particular type of computer network attack *per se* would have results which violate the principles of humanity or dictates of public consciousness, it would contravene the Martens Clause.[29] As Greenwood notes, one effect of the Clause is that the absence of a specific treaty provision does not mean that a weapon must be lawful; the Clause makes clear that the general principles embodied in customary law still apply and that the use of a weapon contrary to those principles will be unlawful.[30]

1.2. Explicit prohibitions of weapons.

The International Court of Justice in the *Nuclear Weapons* case stated that the illegality of certain weapons is formulated in terms of prohibition rather than absence of authorisation.[31] As noted above, there is currently no rule or agreement in international humanitarian law which explicitly bans or restricts the use of computer network attacks.[32] However because computer network attacks can cause a multiplicity of effects, some attack techniques may fall within the definitions of other weapons conventions which may restrict or ban their use. Care must be taken, however, not to misunderstand the underlying principles behind the prohibitions of

---

[28] *Nuclear Weapons Case*, para 78.

[29] See generally, Isabelle Daoust, Robin Coupland and Rikke Ishoey, 'New Wars, New Weapons? The Obligation of States to Assess the Legality of Means and Methods of Warfare' (2002) 84(846) *IRRC* 345, 351; ICRC, *A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977*, ICRC (2006) 17.

[30] Greenwood, 'Law of Weaponry', 206.

[31] *Nuclear Weapons Case*, para 52.

[32] In 1998, and every year since, the Russian Federation has tabled a draft resolution for the investigation into communications technologies and information security which would address these issues. To date, it has not been adopted. See for example, Draft resolution A/C.1/55/L. 6 Introduced by the Russian Federation, 18th mtg., 19 October 1998.

specific weapons.[33] While the law of weaponry seeks to protect core humanitarian values, it is also used to affect disarmament objectives which are not directly relevant to computer network attacks, and aspects of fair dealing which are discussed in section 2 on perfidy *infra*.[34]

Protocol II and Amended Protocol II of the Conventional Weapons Convention may restrict the use of some forms of computer network attack. The definition of a booby-trap is wide enough to encompass computer network attacks which are 'designed, constructed or adapted to kill or injure'.[35] For example, a file or device may be rigged to execute some form of malicious code on access which would fool the surge protectors into thinking there was a lightning strike and shutting off the power. When the power is restarted the additional power surge would overload the distribution node causing the computer monitor to explode and destroying all data on the computer. While the primary purpose of such a device would be to destroy the data on the system and prevent unauthorised access to information, where it is certain that the computer would explode and cause injury, it may be prohibited by Amended Protocol II.[36] It is important to note however that the Protocols only apply to booby-traps which kill or injure, thus the use of booby-traps which merely destroy information or render a system useless would not be covered by the Conventions. Booby traps are prohibited if, by their nature or employment, their use violates the legal protection accorded to a protected person or object by another customary rule of international law.[37] Thus any code which is capable of falling within the definition which disguises itself as an email from the ICRC for instance, would automatically be banned.[38] It is also prohibited to design and manufacture certain booby-traps to

---

[33] For example, Brown has proposed that certain attacks i.e. logic bombs, are analogous to landmines and should therefore be prohibited: Brown, 'Proposal for an International Convention', 197.

[34] For a discussion of the objectives of the law of weaponry see generally, Greenwood, 'Law of Weaponry', 189.

[35] Art. 2 of both Protocols defines booby-traps as "any device or material which is designed, constructed or adapted to kill or injure, and which functions unexpectedly when a person disturbs or approaches an apparently harmless object or performs an apparently safe act".

[36] Whether or not a computer would in fact explode or otherwise cause injury is dependent on a number of variables, for instance the type of monitor used by the rigged system – a plasma screen would melt rather than explode, or whether back-up generators were in place etc.

[37] Henckaerts and Doswald-Beck, *Customary International Humanitarian Law*, 278.

[38] This would undoubtedly constitute an act of perfidy in any event, and the misuse of protected symbols is covered more fully in section 2 on perfidy *infra*.

look like harmless portable objects, although it is not prohibited to convert an existing harmless object into a booby-trap.[39] However, although the definition of a booby-trap is broad enough to encompass a computer network attack specifically designed to cause injury, the wording of these particular provisions refer expressly to objects constructed to contain explosive material and thus would not be applicable to malicious code. In the event that the principle was applied by analogy, it would mean that rootkit malware (which inserts itself into existing code) would be a valid form of attack whereas a separate file disguised as a harmless email attachment or other such item would not. This would be in keeping with the prohibition which applies to letter bombs.[40] Such prohibitions would be better dealt with in terms of the principle against perfidy and aspects of fair dealing which are discussed in section 2 on perfidy *infra*.[41]

1.3. Article 36 Obligations

Article 36 of Additional Protocol I imposes an obligation on contracting parties to perform legal reviews of new weapons, means and methods of warfare:

> In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party.

Although a new obligation to international humanitarian law, this obligation follows in the footsteps of the St Petersburg Declaration of 1868,[42] and is an 'obvious and indispensable corollary' to Article 23(e) of the Hague Regulations and Article 35(2) of Additional Protocol I.[43] The ICRC Commentary to the Additional Protocol states that the words 'methods and means' include weapons in the widest sense, as well as

---

[39] Art. 6(1) Protocol II, Art. 7(2) Amended Protocol II.

[40] See generally Dinstein, *Conduct of Hostilities*, 65.

[41] For a discussion of the objectives of the law of weaponry see generally, Greenwood, 'Law of Weaponry', 189.

[42] Whereby parties were to come to an understanding about advances in armaments to maintain the principles which they had established and to "conciliate the necessities of war with the laws of humanity": St Petersburg Declaration.

[43] Bothe, et al., *New Rules*, 199.

the way in which they are used.[44] Further, the meaning of the phrase 'some or all circumstances' is to require a determination whether the employment for its *normal or expected use* would be prohibited under some or all circumstances, not to foresee or analyse all possible misuse of the weapon.[45]

The ICRC notes that the faithful and responsible application of its international law obligations would require a State to ensure that the new weapons, means and methods of warfare it develops or acquires will not violate these obligations.[46] This obligation to review undoubtedly also applies to new computer network attack techniques and States will be required to assess the legality of each type of attack as they are developed. As with conventional weapons' development and review, assessment of computer network attacks under this provision will remain largely a matter of trust. As noted previously in this thesis, many computer network attacks will only work once before counter-measures are developed and installed, therefore any international scrutiny of the technique would render them useless before they have been used.

2. Perfidy & Ruses of War

Advanced network technology provides new opportunities for parties to deceive and mislead the adversary. Additional Protocol I confirms that ruses of war are not prohibited. Article 37(2) defines them as:[47]

> acts which are intended to mislead an adversary or to induce him to act recklessly but which infringe no rule of international law applicable in armed conflict and which are not perfidious because they do not invite the confidence of an adversary with respect to protection under that law. The following are examples of such ruses: the use of camouflage, decoys, mock operations and misinformation.

Advances in computer network technology have enabled twenty-first century ruses to develop in twin-step with advancements in attack scenarios. Many of the options available to armed forces for modern day ruses of war fall into the category of

---

[44] Pilloud, et al., *Commentary*, para 1402.

[45] Bothe, et al., *New Rules*, 200.

[46] ICRC, *Legal Review of New Weapons*, 4.

[47] Art. 37(2), Additional Protocol I.

electronic warfare,[48] however militaries are increasingly adopting more sophisticated techniques which utilise computer network attack capabilities in order to mislead and deceive their adversaries. For example, basic jamming of radar signals would constitute an electronic attack, however the recent use of an airborne network attack system by Israel in the air strike against a target in northern Syria shows other possibilities. U.S. aerospace industry and retired military officials have indicated that the Israelis utilised a system like the U.S. 'Suter' system to allow their fighters to approach undetected by Syrian defences.[49] The U.S. Suter system enables users to invade communications networks, see what the enemy sees and even take over as the systems administrator so that sensors can be manipulated into positions where approaching aircraft cannot be seen.[50] An example of a permissible ruse of war would be to infiltrate the targeting data on the adversary's computer and enter false information.[51]

Routing an attack through multiple hosts in multiple countries to disguise the origin of an attack is common practice in computer network attacks outside the military context. Any number of stepping stone hosts (whether routers, servers, or individual computers) may act as conduits for an attack effectively 'laundering' the packets of information and making tracing the path and the ultimate origin of the attack extremely difficult. Because the purpose of such tactics is to obfuscate the source of the attack, use of any stepping stone host which is part of a civilian network or a neutral state network runs the risk of the victim State retaliating against the apparent source. As Michael Schmitt points out, such retaliation may be kinetic in nature.[52] The question is whether this use of civilian networks is analogous to using civilian

---

[48] For example jamming, electromagnetic pulse (EMP), high energy radio frequency weapons are examples of electronic warfare and while raising interesting issues for LOAC will not be dealt with in this thesis. For a general overview of electronic warfare techniques see Wilson, *Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues.*

[49] Fulghum and Barrie, 'Israel Used Electronic Attack in Air Strike against Syrian Mystery Target'.

[50] Ibid. See Appendix 1 for details of the development of Suter system.

[51] For example, all U.S. target data for Operation Allied Force in Kosovo was stored on and accessed through a classified computer system. The information contained imagery, descriptions of the facility and its functions, analysis on impact (military advantage anticipated) if destroyed, possible collateral damage concerns and historical information on the target. Tony Montgomery, 'Legal Perspective from the EUCOM Targeting Cell' in A E Wall (ed) *Legal and Ethical Lessons of NATO's Kosovo Campaign* (Naval War College, Newport, RI, 2002) 189, 192.

[52] Schmitt, 'Wired Warfare', 206.

aircraft or vehicles to transport military cargo, or whether it amounts to feigning civilian status which would be a prohibited act.[53]

Such measures will be permitted ruses of war as long as they do not cross the line into perfidy. The prohibition against perfidy is expressed in Article 23(b) of the Hague Regulations and expanded on by Article 37(1) of Additional Protocol I.[54] Perfidy is defined by the Additional Protocol as:

> [a]cts inviting the confidence of an adversary to lead him to believe that he is entitled to, or is obliged to accord, protection under the rules of international law applicable in armed conflict, with intent to betray that confidence.

The application of the prohibition of perfidy to internal armed conflicts has also been confirmed by the Appeals Chamber in *Tadic*.[55] The prohibition against perfidy has two purposes: first it seeks to protect those who genuinely wish to surrender, possess protected status or who are injured by prohibiting the misuse of them on the understanding that abuse will erode respect for immunity in future cases; it also seeks to impose a minimum level of 'fairness' to dealings between combatants even where the act endangers no one else.[56] Manipulating information systems so that enemy forces wrongly believe that troops are surrendering rather than gathering for an attack would be perfidious, as would causing them to believe that combat vehicles were medical vehicles or those of neutrals.[57] Similarly, manipulating an enemy's targeting database so that it believed that an army division headquarters was a hospital would be wrong.[58] Using protected symbols such as the U.N. Symbol or the

---

[53] Note that this analogy is in respect of the laws of war on land. Naval vessels may fly false colours under certain circumstances without it constituting perfidy. See generally, Dieter Fleck, 'Ruses of War and Prohibition of Perfidy' (1974) 13 *Revue de Droit Penal Militare et de Droit de la Guerre* 269, 292.

[54] Art. 23(b) states that it is especially forbidden "to kill or wound treacherously individuals belonging to the hostile nation or army".

[55] *Tadic (Interlocutory Appeal)*, para 125. citing the Supreme Court of Nigeria in *Pius Nwaoga v The State* (1972) 52 ILR 494, 496-97 (Nig. S. Ct.).

[56] Greenwood, 'Law of Weaponry', 190.

[57] Greenberg, Goodman and Hoo, *Information Warfare and International Law*, 13.

[58] Ibid.

emblem of the Red Cross would be prohibited acts of perfidy as well as constituting a misuse of the symbols under Article 38 of the Additional Protocol.[59]

The feigning of civilian, non-combatant status is one of the examples given in Article 37(1) of perfidious acts. This has led some commentators to state incorrectly that the use of emails purporting to be from Microsoft support which in actuality contain viruses or executable software patch designed to wreck the targeted computer system would be perfidious.[60] This misunderstands the limitations of the prohibition contained in the Additional Protocol. Perfidy is only prohibited in so far as it results in the killing, injuring or capture of an adversary. Although this limitation has been criticized,[61] beyond this restrictive definition, such acts are not prohibited under international law.[62] However, depending on the payload of the virus or other malware, this would not be prohibited by the Additional Protocol. Sabotage or the destruction of property as such, through the use of perfidious deception is not prohibited by the Article; there must be a direct proximate causation between the act of perfidy and the killing, injury or capture of the adversary to breach Article 37.[63]

A further question arises over whether States have legitimate expectation of authenticity of emails. Because of the longstanding view that communications may be disrupted, and because, unlike uniforms, information systems are in no way required by the laws of war but are rather combat aids, such tactics might seem less treacherous than would taking advantage of the requirement that troops wear distinct uniforms to set themselves off from their foes and civilians.[64]

Misuse of Protected Symbols

Article 38 of Additional Protocol I prohibits any improper or deliberate misuse of internationally recognized signs, symbols or signals including those of the Red Cross

---

[59] As well as breaching Arts. 38 & 39 on misuse of protective symbols, see *infra*. Note that use of the U.N. symbol is only considered perfidy where the United Nations is *not* engaged in combat.

[60] Shulman, 'Discrimination in the Laws of Information Warfare', 959. See also Dörmann, 'Additional Protocols', 152.

[61] Oeter, 'Methods and Means of Combat', 202; Knut Ipsen, 'Perfidy' in R Bernhardt (ed) *Encylopedia of Public International Law* (Max-Planck Institute, Amsterdam; New York, 1997) 978-981.

[62] Oeter, 'Methods and Means of Combat', 201.

[63] Bothe, et al., *New Rules*, 204. Although as Bothe et al point out, the saboteur would not be entitled to POW status and may also be guilty of a breach of Art. 44(3) API for failing to distinguish themselves from the civilian population.

[64] Greenberg, Goodman and Hoo, *Information Warfare and International Law*, 13.

and associated symbols, the flag of truce, cultural property or of the emblem of the United Nations except as authorized by the U.N.[65] An equivalent provision relating to the red cross, crescent, lion or sun exists in Article 12 of Additional Protocol II for internal armed conflicts. This is an absolute prohibition which does not require any link to killing, injuring or capture. Thus, a clearer example of a prohibited act would be if the email purported to be from a U.N. representative or Red Cross or Crescent society and misused the protected emblem. By extension it is likely that a spoofed email address would also be protected although it does not fall within the category of protective emblems, signs or signals.

3. Destruction & Seizure of Property

The laws regulating the treatment of an adversary's property in times of armed conflict raise interesting issues for networked societies and knowledge economies. The basic principle is set out in Article 46 of the Hague Regulations which provides that private property must be respected and cannot be confiscated. Further, Article 23(g) provides that it is forbidden to "destroy or seize the enemy's property, unless such destruction or seizure be imperatively demanded by the necessities of war".[66] Article 8(2)(b)(xiii) of the Rome Statute makes such destruction or seizure a war crime.[67] Pillage also is formally prohibited by the Hague Regulations, Geneva Convention IV, Additional Protocol II, and made a war crime under the Rome Statute.[68] However, the protections for property are subject to several exceptions, some of which are particularly relevant to communications networks and digital property.

Before turning to the exceptions, two preliminary matters call for comment. First, as indicated in Chapter 8 *supra* in relation to the protection of cultural property, the fact

---

[65] Note that the emblem of the U.N. is only protected where the U.N. is not a party to the conflict.

[66] Art. 23(g), Hague Regulations.

[67] An almost identical provision exists in Art. 8(2)(e)(xii) of the Rome Statute in relation to armed conflicts not of an international character.

[68] Arts. 28 & 47, Hague Regulations; Art. 33(2), Geneva Convention IV; Art. 4(2)(g), Additional Protocol II; Art. 8(2)(b)(xvi), Rome Statute for international armed conflicts and Art. 8(2)(e)(v) for armed conflicts not of an international character. It is also an offence under Art. 4(f) of the ICTR Statute, Art. 3(e) of the ICTY Statute (referring to plunder, although the French text still refers to pillage) and Art. 3(f) of the SCSL Statute.

that property may be intangible is not a unique issue for armed conflict involving information technology. The Nuremburg war crimes tribunals in both the *Krupp* and *I.G. Farben* trials were in no doubt that the property offences set out by the Hague Regulations were broad enough to encompass the acquisition of intangible property by a number of means.[69]

> "Property offences recognised by modern international law are not, however, limited to offences against physical tangible possessions or to open robbery in the old sense of pillage, but include the acquisition of intangible property and the securing of ownership, use or control of all kinds of property by many ways other than open violence."

The Tribunal in the *I.G. Farben Trial* held that "In our view, the offences against property defined in the Hague Regulations are broad in their phraseology and do not admit of any distinction between 'plunder' in the restricted sense of acquisition of physical properties,...the plunder or spoliation resulting from acquisition of intangible property such as is involved in the acquisition of stock ownership, or of acquisition of ownership or control through any other means...".[70] Further, following the invasion of Germany in the Second World War, Allied Forces had no difficulty with acquiring such intangibles as technical and scientific information and military expertise in varying forms including patents and documentation, both as booty and 'intellectual reparations'.[71]

The second preliminary issue to be dealt with is the concept of seizure. While destruction of property is fairly unambiguous even in respect of computer systems, networks and the information contained on them,[72] what is not clear is what actions will constitute seizure of those items. There are two separate aspects to this issue, the first is the remote appropriation of a system or network while leaving its physical

---

[69] *I.G. Farben Trial*, 46; *The Krupp Trial*, 129. United Nations War Crimes Commission, *Law Reports of Trials of War Criminals* (H.M.S.O. for the United Nations War Crimes Commission, London, 1949), Vol XV, 129. citing the *Krupp Trial* which dealt in part with transfer of shares, transfer of corporate property, contractual transfer of property rights and the like.

[70] *I.G. Farben Trial*, 46.

[71] See generally, John Farquharson, 'Governed or Exploited? The British Acquisition of German Technology, 1945-48' (1997) 32(1) *Journal of Contemporary History* 23.

[72] Although a question may be raised as to whether destruction of information can be established if it can be restored or reconstructed, albeit with effort & expenditure from backups.

components in place, and the second is the copying of information located on that network or system. The issue is relevant both for property captured by a party on the battlefield as booty of war and for property seized in occupied territory; for both questions however it should be noted that it is sufficient that the property in question is located in the battlespace, the location of the actor is not of primary importance.[73] Although the tangible aspects of a system or network may be physically seized,[74] it is possible to assume control of a network without doing so. No formal definition of seizure appears in international instruments or in decisions before international tribunals, however the Military Tribunal in the *Krupp Trial* held that the offence of spoliation was achieved even if no definite alleged transfer of title was accomplished stating:[75]

> "However, if, for example, a factory is being taken over in a manner which prevents the rightful owner from using it and deprives him from lawfully exercising his prerogative as owner it cannot be said that his property 'is respected' under Article 46 as it must be."

William Downey has argued that effective seizure requires that the property is placed under substantial guard and is in the 'firm possession' of the capturing State.[76] Although there is conflicting case law on what is required in order to reduce property to firm possession, Downey cites an opinion by the Legal Advisor of the Office of Military Government for Germany (OMGUS) as the preferable view.[77] The OMGUS opinion concludes:

---

[73] See above discussion on location of offences in section 1.2.1 of Chapter 5, relating to sabotage, 137 *supra.*

[74] It may be questioned whether the cable element of a fibre-optic network would be considered 'movable' property for the purposes of seizure or booty. However it would appear that the distinction is to refer to personal property or chattels (as distinguished from real property) rather than any requirement for actual movability: William Gerald Downey, Jr., 'Captured Enemy Property: Booty of War and Seized Enemy Property' (1950) 44 *AJIL* 488, 489.

[75] *The Krupp Trial*, 623-624 The tribunal was responding to a Defence argument that the laws and customs of war do not prohibit seizure and exploitation of property in belligerently occupied territory, so long as no definite transfer of title is accomplished.

[76] Downey, 'Captured Enemy Property', 492.

[77] Legal Advisor of the Office of Military Government for Germany (OMGUS) IX Selected Opinions, OMGUS, 57, 60, cited Ibid., 493. *Cf.* an alternate opinion cited by Downey which dealt with a case of U.S. Civil War era confederate cannon found at the bottom of a river in Arkansas during WWII. It was held in 1947 that the cannon became the property of the United States when the area in which the cannon were located was captured by Federal forces. i.e. mere seizure and occupation of the territory

> "It appears that 'firm possession' requires some manifestation of intention to seize and retain the property involved and some affirmative act or declaration of a possessory or custodial nature with respect to the property. The circumstances which will satisfy these two elements of firm possession will, of course, vary in each case. It is, however, our conclusion that the general occupation of an area by a belligerent is not of itself sufficient to satisfy either of the two elements of the doctrine of firm possession".

In 1985 the Israeli Supreme Court confirmed this approach in *Al Nawar v Minister of Defence et al*, although the Court noted the practical impossibility of seizing all property at once and stated that in order to effect seizure, it would suffice to arrange for a general guarding or patrolling of the area where the property was located.[78] Following this reasoning, in order to seize a network or other system remotely, it would be necessary to access the system or network and change the access codes in order to prevent the original owner from accessing and controlling their system or network. This already happens to a certain extent with computers which are compromised by malicious software and recruited to a botnet.[79] In the case of criminal use of infected computers the author or controller of the botnet leaves the owner's access and control intact, however once the controller has access to the system or network as an administrator it would be possible to change the access permissions so that the system or network is under the sole control of the accessing party and remove all access rights of the original owner. This appears to satisfy the requirements of firm possession set out above, as the act of excluding the original owner manifests the intention of the controller to retain control of the network or system. Placing the network or system under guard may be as simple as changing passwords and ensuring that the system is running up-to-date virus protection software and that all program updates and patches are installed.

---

was enough to transfer title: 6 Bull JAG (1947) 238-289, cited in Downey, 'Captured Enemy Property', 493.

[78] *Al Nawar v Minister of Defence et al* (1985) 39(3) Piskei Din 449, Israel Supreme Court. Excerpted in English in F Domb, 'Judgements of the Supreme Court of Israel' (1986) 16 *Israel YB Hum Rts* 321, 326.

[79] See for example, the Storm Worm which was first detected in the wild on 17 January 2007.

Mere copying of data and information resident on systems poses a slightly more difficult analysis.[80] The nature of digital information is such that copying renders an identical copy capable of being used by the capturing party for any purpose that the original would have been, thus the requirement of intention to seize and retain would still be met. Generally speaking, property is seized for one of two purposes; either to deprive the opposing forces of its use, or to turn it to the capturing State's advantage.[81] While copied information may fulfil the latter purpose, it would not deny the use of the property to the opposing forces. This 'seizure by copying' is not a new phenomenon, following the invasion of Germany in the Second World War significant documents programs were put in place by the Allied Forces. Vast amounts of technical information, research facilities, and prototypes were confiscated as booty by the American and British authorities, with much of the documentation being acquired by way of extensive microfilming projects that left the original documents in place.[82] Historian John Farquharson notes that by mid 1947, five million pages were available on microfilm in the U.S. to businesses and academic institutions comprised entirely of documents, patents etc found by the occupying powers in Germany.[83] However one of the difficulties that arises with this form of seizure is the differing treatment of seized property under the laws relating to booty and military necessity on the one hand, and that of seizure of property in an occupied area on the other. Both Article 23(g) and Article 53 of the Hague Regulations refer to property being seized but the treatment (inferred in the case of Article 23(g) and specified in the case of Article 53) is very different. Under Article 53 ownership rights are not transferred to the occupying party, the property may be seized but must be returned when peace is made and compensation paid. However, property seized for military operations or under the law of booty becomes the

---

[80] It should be noted that there is considerable disagreement at present in domestic jurisdictions concerning the appropriate property rights, other than intellectual property rights, to be granted over information. See for example the discussion on theft of information in Ian J. Lloyd, *Information Technology Law* (4th ed, Oxford University Press, Oxford, 2004), 315-321. comparing England, Scotland, the United States and Canada. Database rights in particular are particularly contentious.

[81] Lauterpacht (ed) *Oppenheim's International Law*, 152.

[82] Farquharson, Gimbel 60-74. There is controversy over the extent of the documentation programs put in place in respect of the type of information confiscated which included large-scale acquisitions from private industry. However much was taken of purely military usage and was nearly all taken as booty: Farquharson, 'Governed or Exploited', 37.

[83] Ibid., 23.

property of the seizing party. Title passes on effective seizure for purposes of booty and the previous owner is completely divested of all rights in the property.[84] Logically it would seem that in terms of seizure under those conditions, the affirmative action or declaration must incorporate the 'right to exclude' or in some other way deprive the original owner of their rights over the information. Thus, mere copying would not constitute valid seizure as it only succeeds in depriving the original owner of the right to exclude vis-à-vis the seizing State. As this is inconsistent with state practice, it would appear that seizure may mean different things with respect to booty than its does to occupation and that any action with respect to such property would be prohibited if it entailed the party to act in a manner inconsistent with the property rights which continue to vest in the original owner.

3.1. Booty

In accordance with customary international law, all movable State property captured on the battlefield may be appropriated as booty of war. The seized property becomes the property of the capturing State rather than the individual soldier or unit seizing it, and title passes on seizure.[85] Title to the property is acquired automatically by the belligerent State whose armed forces have seized it, irrespective of the military character of the property (not only weapons and ammunition, but also money, food and stores).[86] This would undoubtedly apply to all government owned systems and networks, as the computers, servers and routers would all fall in the category of movable property. Although the issue has not been formally addressed in international law, it would seem that all information resident on such computers, networks and other devices could also be lawfully appropriated in a similar way to the information, technical documents, patents and other intellectual property which were seized by the Allied Powers after World War II.[87] However, as discussed in

---

[84] Yoram Dinstein, 'Booty in Land Warfare' in R Bernhardt (ed) *Encyclopedia of Public International Law* (Max Plank Institute; North Holland, Amsterdam, 1992) 432-434, 432.

[85] Downey, 'Captured Enemy Property', 500; Dinstein, *Conduct of Hostilities*, 215. Dinstein, 'Booty in Land Warfare', 432.

[86] Dinstein, *Conduct of Hostilities*, 215.

[87] Although there was significant discussion over the extent and type of property which could be confiscated (in terms of much of it being from private firms), none of the discussion appears to have focussed on the intellectual nature of the property. Following March 1946, a narrow definition of booty was adopted by the Allied powers limiting booty to 'arms, munitions and implements of war, and all research and development facilities (including documents, material and training devices)

Chapter 8 *supra*, any property which would amount to cultural property would not be subject to seizure.

While private property is generally immune from seizure on the battlefield, any private property actually used for hostile purposes may be appropriated by the belligerent State.[88] In *Al Nawar* the Court held that Article 23(g) of the Hague Regulations does not accord protection to property used for hostile purposes; such property enjoys protection from arbitrary destruction, but it is still subject to the enemy's right of appropriation as booty.[89] The Court also held that the distinction between state and private property should be based on the functional test applied in the 1921 Arbitral Award in the *Cession of Vessels and Tugs for Navigation on the Danube Case* which determines the nature of the property in question based on its actual use.[90] Thus any commercial network, system or computer that is utilised by the opposing State for military operations may also be seized, a significant concern given the large percentage of military communications which travel over civilian networks.[91]

Further, it is permissible to seize any weapons, ammunition, military equipment, military papers and the like, regardless of whether it can be used for military operations or not, even though they constitute private property.[92] In an age of computer network attack this is an extremely broad exception. Practically all networks operating in the battlespace will be liable to be appropriated as well as most systems which are capable of being used in a computer network attack. As the average home computer or laptop with an Internet connection has this capacity, and may already be leveraged as part of a botnet (with or without the owners consent or knowledge), it would seem that any computer would be open to seizure by the armed forces. Likewise any information resident on networks or computers would be able

---

relative thereto': John Gimbel, *Science, Technology, and Reparations: Exploitation and Plunder in Postwar Germany* (Stanford University Press, Stanford, Calif, 1990), 172-175; Farquharson, 'Governed or Exploited', 33.

[88] *Al Nawar*. Excerpted in English in Domb, 'Judgements of the Supreme Court of Israel', 324.

[89] Domb, 'Judgements of the Supreme Court of Israel', 324.

[90] Ibid., 325. citing *Cession of Vessels and Tugs for Navigation on the Danube Case* (1921) 1 RIAA 97.

[91] In 1996 the percentage was quoted at 95% of all military communications passed over commercial networks: Aldrich, 'International Legal Implications', 105.

[92] Downey, 'Captured Enemy Property', 494.

to be seized insofar as it amounts to military papers (in the case of documents or databases) or military equipment (in respect of software).

The term 'battlefield' is commonly used in describing where property may be seized in accordance with the law of booty in warfare; however as Dinstein points out, the term is to be understood very broadly and is perhaps better to be understood in terms of 'combat' or 'military engagement'.[93] The Supreme Court of Israel held in *Al Nawar* that the entire theatre of operations may be regarded as the battlefield for the purposes of the law of booty in land warfare.[94] This raises interesting questions for computer network attack as the battlespace is much larger than traditionally contemplated. Taken to its logical conclusion this would mean that any network, computer, router, server or mobile satellite command station utilised in military operations may be appropriated as booty of war,[95] as well as any information resident on those devices (unless they amount to cultural property). Given the ability to seize such networks remotely, it would appear that a belligerent party could seize systems or networks in the territory of an adversary regardless of the size, or indeed fact of, their physical presence in the adversary State. For example, it is possible that any attacks launched against Iraq from U.S. military bases on United States soil, would open U.S. networks to seizure as booty by Iraq.

---

[93] Dinstein, 'Booty in Land Warfare', 433; Dinstein, *Conduct of Hostilities*, 215.

[94] *Al Nawar*. Excerpted in English in Domb, 'Judgements of the Supreme Court of Israel', 324.

[95] An interesting issue arises over whether the satellite's space architecture would be considered 'movable' property for the purposes of seizure. Where it is possible to access and obtain control of the thrusters and inclination of the satellite it follows logically that it may be moved. As the traditional battlefield is now thought of in terms of battlespace any satellite which is actually used by the parties to the conflict must necessarily form part of that battlespace. Note however the exclusion of this right for occupied territory. See generally, Thomas C. Wingfield, 'Legal Aspects of Offensive Information Operations in Space' (1998) 9 *J Legal Stud* 121; Michel Bourbonnière, 'Law of Armed Conflict (LOAC) and the Neutralisation of Satellites or Ius in Bello Satellitis' (2004) 9 *JC&SL* 43; Michael N. Schmitt, 'International Law and Military Operations in Space' (2006) 10 *Max Planck UNYB* 89.

3.2. Occupied Territory

Exceptions to the prohibition against destruction or seizure of an adversary's property also exist for occupied territories which are of particular relevance for computer networks. Article 53 of the Hague Regulations allows parties to take possession of communications equipment in occupied territory, stating:

> An army of occupation can only take possession of cash, funds, and realizable securities which are strictly the property of the State, depots of arms, means of transport, stores and supplies, and, generally, all movable property belonging to the State which may be used for military operations.
>
> All appliances, whether on land, at sea, or in the air, adapted for the transmission of news, or for the transport of persons or things, exclusive of cases governed by naval law, depots of arms, and, generally, all kinds of munitions of war, may be seized, even if they belong to private individuals, but must be restored and compensation fixed when peace is made.

Computer networks and other IT systems undoubtedly fall within this provision. However, where these means of communication take the form of submarine cables or satellites specific laws apply. Submarine cables (including fibre-optic cables) connecting the occupied territory to a neutral territory may only be seized or destroyed in cases of absolute necessity and must be restored and compensation fixed when peace is restored.[96] Further, the space architecture of satellite communications systems would also fall outside the Article 53 exception. Outer space is not subject to appropriation by any State though occupation,[97] therefore the laws regulating seizure of property in occupied territories does not apply. This would not prevent the seizure of the ground-based control centres however, so the point

---

[96] Art. 54, Hague Regulations. See for example *Eastern Extension, Australasia and China Telegraph Co. Claim* (1923) 6 RIAA 112; *Cuba Submarine Telegraph Co.* (1923) 6 RIAA 118. cited in Leslie C. Green, *The Contemporary Law of Armed Conflict* (2nd ed, Manchester University Press, Manchester, 2000), 152.

[97] Art. 2, *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies,* Vol. 610 No. 8843. Note that the Hague Regulations do not apply *per se* to space-based conflict as they are only applicable to the law of war on land. Their application is based on their status as customary international law; the International Court of Justice has indicated on several occasions the principles contained in the Hague Regulations constitute "intransgressible principles of international customary law": See for example *Nuclear Weapons Case*, para 79.

may be moot, subject to prohibited interference with the physical aspects of the satellite (i.e. the altitude and orbit control subsystems which control the thrusters and inclination of the satellite itself), exclusive control of information passing through the satellite would still be possible.

Article 53 of Geneva Convention IV relating to protection of civilian persons in occupied territory also prohibits the destruction of property, both state-owned and private, except where it is absolutely necessary for military operations.[98] However, this provision only applies to destruction of property not seizure. The occupying authorities have a recognized right, under certain circumstances, to dispose of property within the occupied territory - namely the right to requisition private property, the right to confiscate any movable property belonging to the State which may be used for military operations and the right to administer and enjoy the use of real property belonging to the occupied State.[99] Extensive destruction is considered a grave breach of the Convention and may be prosecuted as a war crime under Article 8(2)(a)(iv) of the Rome Statute.[100]

3.3. Pillage & Plunder

The prohibition against pillage is firmly rooted in both customary international law and treaty law.[101] Traditionally, pillage meant the looting or plundering of enemy property (public or private) by individuals for private ends,[102] and incorporated an element of violence in the appropriation of such property.[103] The trial Chamber of

---

[98] Art. 53, Geneva Convention IV provides: Any destruction by the Occupying Power of real or personal property belonging individually or collectively to private persons, or to the State, or to other public authorities, or to social or cooperative organizations, is prohibited, except where such destruction is rendered absolutely necessary by military operations.

[99] ICRC 'Article 53' Commentary to Geneva Convention IV, 301; Pictet, Commentary.

[100] Art. 147, Geneva Convention IV; 8(2)(a)(iv) Rome Statute.

[101] *"Celebici" Judgement*, para 315. Art. 28, 47 (concerning occupied territory), Hague Regulations 1907; Art. 33(2), Geneva Convention IV; Art. 4(2) of Additional Protocol II; Art. 8(2)(b)(xvi) & Art. 8(2)(e)(v), Rome Statute, make "pillaging a town or place, even when taken by assault" a war crime; The ICTR and SCSL Statutes both include the crime of pillage while the ICTY Statute prohibits plunder. Interestingly the official French version of both the ICTR and ICTY Statutes use the term 'le pillage'.

[102] Armin A. Steinkamm, 'Pillage' in R Bernhardt (ed) *Encyclopedia of International Law* (Max Plank Institute; North Holland, Amsterdam, 1982) 1029-1030, 1029; Dinstein, *Conduct of Hostilities*, 214.

[103] *Trial of Alois and Anna Bommer and Their Daughters* (1947) IX Law Reports of the Trials of the War Criminals 62, Permanent Military Court at Metz.

the ICTY in *Naletilic and Martinovic* found that the Statute proscribes plunder committed on the entire territory of the parties to a conflict.[104] However a number of these elements have been brought into question in recent judgements. There are two particular questions which arise in respect of pillage of digital property. First, must the owner of the property be dispossessed of it entirely, or is it sufficient that certain of the owner's property rights, namely the right to exclude, and the right to control the use made of the property and the profit from it, are infringed? And secondly, with regard to pillage, must the property be acquired through threats or use of violence?

In the *Flick trial*, Flick was found guilty of war crimes for *inter alia* the plunder of public and private property and spoliation in the countries and territories occupied by Germany. However the Tribunal stated that "no defendant is shown by the evidence to have been responsible for any act of pillage as that word is commonly understood".[105] It is not clear from the judgement whether this is was a result of the lack of violence involved, or the fact that the property was returned to the owners in a better condition than when it was appropriated. Other courts have not separated the offences in the same manner.

The trial chamber of the Sierra Leone Special Court in the *Fofana & Kondewa* Case were of the view that the inclusion of the requirement that the appropriation be for personal or private use is an unwarranted restriction on the application of the offence of pillage.[106] However this statement seems to stem from the conflation of the terms 'pillage', 'plunder' and 'spoliation', and the fact that the Statute for the International Criminal Tribunal for the Former Yugoslavia contains the offence of plunder rather than pillage.

Computer network attacks designed to appropriate property are generally non-violent in nature. Noting that the concept of pillage in the traditional sense implied an

---

[104] *Prosecutor v Mladen Naletilic and Vinko Martinovic* (2003) Case No. IT-98-34-T, International Criminal Court for the Former Yugoslavia, para 615., noting that Geneva Convention IV indicates that the prohibition of pillage is not limited to acts committed in occupied territories.

[105] *The Flick Trial.*

[106] *Prosecutor v Moinina Fofana and Allieu Kondewa (Decision on Preliminary Motion Based on Lack of Jurisdiction (Child Recruitment)).* (2004) SCSL-04-14-T, Special Court for Sierra Leone, 49.

element of violence,[107] the Court in the *Celebici* judgement declined to decide whether the terms pillage and plunder were synonymous stating that the term plunder embraces "all forms of appropriation of property in armed conflict for which individual criminal liability attaches under international law, including those acts traditionally described as 'pillage'.[108] However courts have been happy to consider property seized by enemy forces as pillage even when violence is not used.[109]

3.4. Enemy Owned Property on the Territory of a Belligerent

Enemy owned public property in the territory of a belligerent is subject to seizure, although diplomatic buildings are placed under protection.[110] Thus, any State owned websites hosted in the adversary State or other digital assets would be liable to be seized in the event of an armed conflict breaking out between the States. For example, the government of East Timor is hosted on sites in the Republic of Ireland and would be subject to seizure or freezing should the two States engage in an armed conflict with one another. Likewise any work that has been outsourced offshore to a belligerent State would be subject to seizure. In an age of increased civilian outsourcing of government work (including defence acquisitions), and offshore outsourcing in the commercial sector, knowledge and control over where the actual work will be performed will be important. While it may also be possible to argue that information merely passing over a server in a belligerent State is sufficient to qualify as being on the territory of a belligerent and therefore subject to seizure, most information accessed in this manner could presumably be seized as intelligence gathering which is expressly permitted under Article 24 of the Hague Regulations. The situation with regard to private property is more complex. The protections for civilian property provided by Article 23(g) of the Hague Regulations apply equally to property on the territory of both belligerent parties. In addition, Article 38 of Geneva Convention IV provides that "the situation of protected persons shall

---

[107] The requirement of violence in pillage is brought into question by the case of *Trial of Alois and Anna Bommer and their Daughters* (1947) IX Law Reports of the Trials of the War Criminals 62, Permanent Military Court at Metz.

[108] *"Celebici" Judgement*, § 591. citing Law Reports, Vol IX, pg 64.

[109] See for example, *in re Otto Wallemar* [1948] ADIL 619 (removal of goods during occupation), *Mazzoni v Ministry of Finance* [1927-1928] AD Case No. 384 (on seizure of bonds & shares abandoned by the owner in occupied territory).

[110] Green, *The Contemporary Law of Armed Conflict*, 155.

continue to be regulated, in principle, by the provisions governing aliens in time of peace" with the exception of measures of internment, assigned residence or other exceptional measures for control and security necessitated by the war.[111] These measures have been considered by the Eritrea Ethiopia Claims Commission in its partial awards in respect of some of *Eritrea's Civilian Claims* and its claim for *Loss of Property in Ethiopia.*[112] The decision of the Commission in its partial award for *Eritrea's Civilian Claims* noted that belligerents have "substantial latitude to place freezes or other discriminatory controls on the property of the nationals of the enemy State or otherwise to act in ways contrary to international law in time of peace."[113] While observing that the control measures were necessary to deny the enemy access to economic resources which might otherwise be potentially available to support its conduct of the war, the Commission commented that States have not consistently done so, and that where States have vested the assets of enemy nationals it has been done under controlled conditions and for reasons directly tied to higher State interests.[114] The Commission went on to find:[115]

> "a belligerent is bound to ensure insofar as possible that the property of protected persons and of other enemy nationals are not despoiled and wasted. If private property of enemy nationals is to be frozen or otherwise impaired in wartime, it must be done by the State, and under conditions providing for the property's protection and its eventual disposition by return to the owners or through post-war agreement."

The Commission noted that such limitations on the vesting of property have been emphasised by commentators.[116] Digital property or assets in the territory of the

---

[111] Art. 27, Geneva Convention IV.

[112] *Partial Award, Civilians Claims, Eritrea's Claims 15, 16, 23 & 27-32 between the State of Eritrea and the Federal Democratic Republic of Ethiopia* (2004), Eritrea Ethiopia Claims Commission; *Partial Award, Loss of Property in Ethiopia Owned by Non-Residents, Eritrea's Claim 24 between the State of Eritrea and the Federal Democratic Republic of Ethiopia* (2005), Eritrea Ethiopia Claims Commission.

[113] *Partial Award in Eritrea's Civilians Claims*, para 124.

[114] Ibid., para 127-128.

[115] Ibid., para 151.

[116] Ibid., para 128. citing Lauterpacht (ed) *Oppenheim's International Law*, 326-331; Ian Brownlie, *Principles of Public International Law* (6th ed, Oxford University Press, Oxford, 2003), 514. brownlie principles, 514; oppenheims international law, 326-331.

belligerent may be frozen by that party in the same way that tangible property or funds may be frozen, and would be subject to the same conditions to ensure protection of the assets and for reasons of State interest.

4. Conclusion

Of all of the principles which govern modern armed conflict, it is those relating to the means and methods of warfare which have the most uneasy fit in respect of computer network attacks. One thing is certain, the general principles of the law of weaponry will continue to apply however their specific application will only become apparent with the details of a particular computer network attack. The application of Article 36 obligations to assess individual attack techniques should mitigate against these problems.

Perfidy is one of the most difficult concepts to translate into an online environment where anonymity is the norm. However, it must be borne in mind that it only applies to attacks that result in the killing, injuring or capture of the adversary. Because standard practice in computer network attacks is to disguise the origin of the attack, States will need to take particular care to ensure that sure ruses do not cross the line into perfidy.

The changing conceptions of property and the increasing reliance of economies on intellectual property and intangibles raises serious issues in terms of the rules regarding the protection of property in armed conflict. Some issues do not readily fit within the current framework, others reflect the difficulties found in international criminal law in respect of computer crime generally. Concepts such as pillage raise difficulties with the possible requirement that the owner must be permenantly deprived of the property, thus the copying of files (and even their subsequent deletion, in circumstances where back-up copies exist) may mean that liability is avoided. However the frequent conflation of property offences by international courts may mean that this is less of a difficulty in practice.

Concluding Remarks

The advent of computer network attacks poses new challenges for the international law regulating force and international humanitarian law. Not only do computer network attacks represent a fundamentally different method of warfare, they come at a time when the laws of armed conflict are struggling to meet the challenges of greater than ever civilian participation in conflict, increased asymmetry and technological advance. However despite these challenges, the author believes that the underlying framework and general principles of the laws of armed conflict remain applicable to conflicts involving computer network attacks. Some adaptations in detail will be required, as always happens with law over time,[1] however the underlying principles of the laws of armed conflict are aimed at the fundamental nature of war, which remains unchanging. The exact content and contours of the laws will determined by the prevailing principles of the societies that shape them.

At present, examination of the legality of computer network attacks under international law results in a complex picture. Under the *jus ad bellum*, the need for a physical effect, namely death, injury or destruction of physical property appears to remain constant, although it may be achieved indirectly. The perceived intent of the attacker will play a large role in determining the victim State's response. Certainly for a computer network attack to qualify as an armed attack triggering the right of self-defence under international law, the attack must result in consequences of a sufficient scale and effect. Adopting a restrictive approach to computer network attacks in respect of the *jus ad bellum* also serves to act as a restraint on the right to resort to traditional force in self-defence.

It is perhaps the *jus in bello,* which shows more clearly the complex relationship between fundamental principles and specific applications of the laws of armed conflict in regard to computer network attacks. Principles such as the distinction between combatants and civilians, proportionality in attack and the prohibition against causing unnecessary suffering, remain at the core of the commitment to the

[1] Oeter, 'Comment: Is the Principle of Distinction Outdated?' with regard to the changes wrought by increasing asymmetry.

law, regardless of the technology employed. It is in the specific applications of the laws where the effects of technology and the changing values and conceptions brought about by the information revolution are seen. One of the most significant is the increased value that information societies place on intangible property and information. It will have an impact on the application of the laws governing the conduct of hostilities in relation to targeting analysis, protection of cultural property and property offences generally.

Despite the attempt to adopt a comprehensive approach, as always, there remain a few areas which require further research. As stated in the introduction, this thesis does not examine the law of neutrality, or look in any meaningful way at the effects of computer network attacks on the law of naval warfare (other than a brief mention to draw a comparison in the text). There are other questions which have been raised in the course of this thesis and will require future investigation. Some are raised by the nature of digital property and the protection to be provided to it; for example, in a format capable of perfect digital copies, what criteria will be used to determine which copies of cultural property are worthy of protection as reproductions.

Appendix 1 - Selected Computer Network Attack Examples

1982 **Trans-Siberian Pipeline - the 'Farewell Dossier'.**[1] Following the theft of technology from Western powers by the Soviet KGB, the Central Intelligence Agency (CIA) of the United States and a Canadian firm planted a Trojan horse in the control software for the pipeline system which a KGB operative had been sent to steal. Once installed "the pipeline software that was to run the pumps, turbines, and valves was programmed to go haywire, after a decent interval, to reset pump speeds and valve settings to produce pressures far beyond those acceptable to pipeline joints and welds. The result was the most monumental non-nuclear explosion and fire ever seen from space".[2] The explosion happened in a remote area of Siberia and there were no physical casualties from the attack, however it is not clear from the documents publicly available, whether this was by fortunate happenstance or design.

1997 **Eligible Receiver.** Eligible Receiver is the code name of a 1997 internal exercise initiated by the U.S. Department of Defense. A 'red team' of hackers from the National Security Agency (NSA) was organized to infiltrate the Pentagon systems. The red team was only allowed to use publicly available computer equipment and hacking software. Although many details about Eligible Receiver are still classified, it is known that the red team was able to infiltrate and take control of the Pacific command center computers, as well as power grids and 911 systems in nine major U.S. cities.[3] The red team intruded computer networks, denied services,

---

[1] See Gus W. Weiss, 'The Farewell Dossier: Duping the Soviets' (1996) 35(5) *Studies in Intelligence* 121, 269 <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/96unclass/farewell.htm> (last accessed 29 June 2008); Matthew French, 'Tech Sabotage During the Cold War' (2004) *Federal Computer Week* 26 April 2004 <http://www.fcw.com/print/10_12/news/82709-1.html> (last accessed 29 June 2008); Reed, *At the Abyss*.

[2] Reed, *At the Abyss*, 269.

[3] PBS Frontline, *Cyberwar! The Warnings* <http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/> (last accessed 21 September 2008); William M. Arkin, *Code Names: Deciphering US Military Plans, Programs, and Operations in the 9/11 World* (Steerforth Press, Hanover, NH, 2005), 358.

changed removed and read emails, and disrupted phone services; they also gained super user access in over 36 computer systems which meant they could have created new accounts, deleted accounts, turned the system off or reformatted the server hard drives.

In October 2002, a subsequent no-notice mock attack against military computers, titled 'Eligible Receiver 2003' indicated a need for greater coordination between U.S. military and non-military organisations to deploy a rapid military computer counter-attack.[4]

1998 **Solar Sunrise.** In February 1998, a number of U.S. Department of Defence networks were attacked using a well-known vulnerability in the operating system (the UNIX-based Solaris). The attacks were widespread and appeared to come from multiple servers in the U.S. as well as the United Arab Emirates, Israel, France, Taiwan & Germany. Although the targeted systems were all reported as unclassified, many key support systems reside on unclassified networks (for example the global transportation system, Defence Finance System, medical personnel, logistics and email).[5] The attacks came at a time when the U.S. was preparing for potential military action against Iraq due to UN weapons inspection disputes and raised fears that the attacks were aimed at disrupting deployments and operations. Investigators eventually traced the attacks to two California teenagers, directed by an Israeli teenaged mentor, who were subsequently arrested and charged.[6]

1998 **Roosevelt Dam, Arizona.** In 1998 a 12 year-old U.S. hacker, exploring for fun, broke into the computer system that runs Arizona's Roosevelt

---

[4] Clay Wilson, 'Information Operations and Computer Network Attack Capabilities of Today' (Paper presented at the International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, Stockholm, 17-19 November 2004) 28-79, 64. Citing a U.S. DoD Briefing for the Congressional Research Service, 9 January 2003.

[5] 'Solar Sunrise' GlobalSecurity.org <http://www.globalsecurity.org/military/ops/solar-sunrise.htm> (last accessed 23 September 2008).

[6] Ibid; John A. Serabian, Jr, Cyber Threats and the US Economy: Statement for the Record before the Joint Economic Committee on Cyber Threats and the US Economy (23 February 2000), transcript available in <https://www.cia.gov/news-information/speeches-testimony/2000/cyberthreats_022300.html> (last accessed 15 August 2008).

Dam.[7] Although he was unaware of the fact, federal authorities claim he had complete control of the SCADA system which controls the dam's massive floodgates and the 489 billion gallons of water which it contains. Unleashed, the water would course down the Salt River and over a downstream flood plain (home to an estimated population of one million people) before reaching the state capital, Phoenix.

The facts of this incident have since been disputed in an article claiming that although 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.[8]

1998 **Electronic Disturbance Theatre.** Electronic Disturbance Theatre launched denial of service attack on U.S. Department of Defense in support of Mexico's Zapatista rebels. The attack was in protest at alleged support by the U.S. government for the Mexican Government who were accused of serious human rights abuses in the Chiapas region of Mexico. When users logged on to an EDT website, the Zapatista Floodnet software was downloaded to their computer. As with most DDoS attacks, the software is designed to initiate automatic and repeated requests to reload an IP address, in this case the Pentagon's website DefenceLink. As Floodnet performs automatic reloads of the site, it slows or halts access to the targeted server and clogs bandwidth.[9] The attack is interesting primarily for the Pentagon's response to an attack that they knew was coming. On 9 September 1998, the Pentagon responded in kind by sending a java applet back to the originating computer and disabling the browser of the computer initiating the attack.[10] The action caused a storm of

---

[7] Gellman, 'Cyber-Attacks by Al Qaeda Feared'.

[8] ZDNet, 'Cyberterrorism: The Real Risks', 27 August 2002, <http://news.zdnet.co.uk/internet/0,1000000097,2121358,00.htm> (last accessed 21 September 2008).

[9] The Electronic Disturbance Theatre views this act as performance art, hence the term theatre in their title and classifies the FloodNet action as virtual or electronic civil disobedience.Fusco, 'Performance Art in a Digital Age'.; see also Shawhan "Vital Interests, Virtual Threats"

[10] Friel, 'DoD Launches Internet Counterattack'. According to the EDT only 2 computers of the 80,000-plus who participated were crashed by the DoD counterattack.

controversy on the Internet as it involved an offensive attack on civilian servers. The incident sparked a joint task force to investigate the legalities involved.[11]

1998 **Indonesia and East Timor.**[12] East Timor (now Timor Leste), occupied by Indonesia since 1975, declared its virtual independence in 1998 and established its own Country Code Top Level Domain and website hosted by an Irish Internet Service Provider (ISP), Connect-Ireland. Following the launch of the domain, the Indonesian embassy relayed its concerns regarding the launch to the Irish Times, complaining that the site represented misuse of computer freedom to campaign against Indonesia. In January 1999, Connect-Ireland because the focus of a coordinated attack on its servers. Martin Maguire, Founder and managing director of Connect Ireland believed the attacks were perpetrated by the Indonesian Government and complained to the embassy. Maguire asserted "the attacks were systematic and took place over a long period of time, from 18 different locations, and were targeted at the .tp domain name". Attacks took the form of buffer overflow attacks, defacement of web pages, denial of service attacks. A spokesperson for the Indonesian embassy denied the claims.

1999 **Moonlight Maze.** The code name for the investigation into a highly classified incident of early 1999 electronic assault involving hackers based in Russia. In this attack, U.S. officials accidentally discovered a pattern of probing of computer systems at the Pentagon, NASA, Energy Department, private universities, and research labs that had begun in March 1998 and had been going on for nearly two years. Intruders accessed unclassified but highly sensitive DOD science and technology information, systematically marauding through tens of thousands of files - including maps of military installations, troop configurations and military hardware designs. The

---

[11]Seffers, 'Legalities Cloud Pentagon's Cyber Defence', cited in Shawhan "Vital Interests, Virtual Threats", 37

[12] 'Indonesia, Ireland in Info War?' *Wired News* 27 January 1999, <http://www/wired.com/news/print/0,1294,17562,00.html> (last accessed 4 April 2003); Arthur, 'The Day East Timor Was Deleted'; Nuttall, 'Virtual Country 'Nuked' on Net'.

Defense Department traced the trail back to a mainframe computer in the Russian Academy of Science, a government organization that interacts closely with the Russian military,[13] but the sponsor of the attacks is unknown and Russia denies any involvement. Moonlight Maze is still being actively investigated by U.S. intelligence.[14]

1999 **U.K. MOD Satellite Hack.**[15] (March) A group of hackers is alleged to have seized control of British military communications satellite. The hackers apparently intercepted the link between the Skynet satellite's control centre and the ground station and accessed the control system of the satellite, using it to change the characteristics of the channels used to convey military communications, satellite television and telephone calls. As there is only one news report of this incident, care should be taken in relying on this report.

1999 **Kosovo – Operation Allied Force.** The United States used computer network attacks to confuse and disable the Yugoslav air defence systems. Used in combination with jamming and other electronic warfare techniques, computer network attacks were used to insert misleading messages and false targets into the Yugoslav computer systems. While it is not clear what method was used by the U.S. Air Force to do so, they have two aircraft capable of intercepting and amending data before retransmission to the enemy system.[16]

---

[13] Inside Defense, Defense Information and Electronics Report 1 (22 Oct. 1999). In James P. Terry, 'The Lawfulness of Attacking Computer Networks in Armed Conflict and in Self-Defense in Periods Short of Armed Conflict: What Are the Targeting Constraints?' (2001) 169 *Mil L Rev* 70.

[14] PBS Frontline, *Cyberwar! The Warnings* (last accessed 21 September 2008).

[15] 'British Hackers Attack MoD Satellite', *Telegraph* (London), March 1999, <http://www.telegraph.co.uk/connected/main.jhtml?xml=/connected/1999/03/04/ecnhack04.xml> (last accessed 23 September 2008).

[16] For fuller details see William M. Arkin, 'The Cyber Bomb in Yugoslavia', *Washington Post* (Washington D.C.), 25 October 1999, <http://www.washingtonpost.com/wp-srv/national/dotmil/arkin.htm> (last accessed 21 September 2008); David A. Fulghum, 'Yugoslavia Successfully Attacked by Computers' (1999) 151(8) *Aviation Week and Space Technology* 23 August 1999 31; David A. Fulghum, 'Data Link, Ew Problems Pinpointed by Pentagon' (1999) 151(10) *Aviation Week and Space Technology* 6 September 1999 87; Arkin and Windrem, 'The Other Kosovo War'.

2000 **Queensland Water Supplies - Vitek Boden.** In April 2000 Vitek Boden was arrested after being caught using a stolen computer and radio transmitter to gain access to a water sewerage treatment system. Over the previous two month period Boden had accessed the system 46 times, gaining complete control of treatment of the region's sewerage and drinking water facilities and dumping 250 million tonnes of putrid sludge into the area's rivers and parks, killing wildlife and plants.[17]

2001 **Code Red.** Code Red was a worm with multiple variants that first appeared in July 2001 and ultimately affected nearly 300,000 computers in the U.S. Exploiting a hole in Microsoft's IIS Web servers, it was time sensitive based on the date: From days 1-19 of the month the worm would propagate; from days 20-27 it would launch a denial of service attack against a particular site, and from day 27 through the end of the month the worm would "sleep," dormant in the computer. In Code Red's first variation, the affected computers were programmed to launch a denial of service attack against the White House Website at a certain date and time. If the assault worked, the hundreds of thousands of pings would have overwhelmed the Internet in nanoseconds. Richard Clarke, the president's adviser for cyberspace security, worked with the nation's Internet providers to thwart the attack by blocking traffic to the White House site. Other Websites were shut down, however, and replaced by a message that read "Hacked by Chinese".[18]

2001 **Mountain View.** In the summer of 2001, the coordinator for the city of Mountain View, California's website noticed a suspicious pattern of intrusions. The FBI investigated and found similar "multiple casings of sites" in other cities throughout the U.S. The probes were seemingly emanating from the Middle East and South Asia, and the visitors were looking up information about the cities' utilities, government offices, and emergency systems. This information took on a new significance when

---

[17] *R v Boden;* Gellman, 'Cyber-Attacks by Al Qaeda Feared'.

[18] PBS Frontline, *Cyberwar! The Warnings* (last accessed 21 September 2008).

U.S. intelligence officials examined computers seized from Al Qaeda operatives after the 11 September 2001 attacks and discovered what appeared to be a broad pattern of surveillance of U.S. infrastructure.[19]

> "I think the bottom line on the Mountain View case is the ease with which people can do virtual reconnaissance from overseas on our physical infrastructure and on our cyber infrastructure, and the difficulty that we have in knowing what is being done. We were lucky in the case of Mountain View, that there were good people watching. It's probably occurring in lots of other places around the country, and we don't have people who are catching it."[20]

2001 **Houston Port Authority:** Aaron Caffrey, 19, was accused of launching a denial of service attack that hampered operations at the Port of Houston, Texas, on 20 September 2001 by crippling its web-based systems which contained crucial information on navigation, tides, water depths and weather. Caffrey, who allegedly launched the attack against a female internet chatroom user who had insulted his American girlfriend, used a list of unpatched servers downloaded from the Internet to hijack the machines and launch a denial of service attack. But it almost ended in disaster when it crashed the Port of Houston's systems under the weight of 100,000 requests to ping data at the girl's computer, leaving vital navigation and weather data inaccessible.[21]

2002 **Al-Qaeda Laptops.** U.S. troops clearing the cave system in the Tora Bora region of Afghanistan uncovered an Al Qaeda laptop which indicated a strong interest in computer network attacks. Computer forensics indicated that the laptop had made multiple visits to sites offering sabotage

---

[19] Ibid.

[20] PBS Frontline, *Interview with Richard Clarke - Cyberwar!* <http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/clarke.html> (last accessed 21 September 2008).

[21] Rebecca Allison, 'Hacker Attack Left Port in Chaos: Busiest US Port Hit after Dorset Teenager Allegedly Launched Electronic Sabotage against Chatroom User', *The Guardian* (London), 7 October 2003, Home 7; Andy McCue, "Revenge' Hack Downed U.S. Port Systems', *ZDNet News* 7 October 2003, <http://news.zdnet.co.uk/security/0,1000000189,39116978,00.htm> (last accessed 17 March 2008); Rebecca Allison, 'Youth Cleared of Crashing American Port's Computer', *The Guardian* (London), 18 October 2007, Guardian Home Pages 7.

handbooks, software and programming instructions on SCADA systems, and other 'cracking' tools. In January 2002, another computer was seized at an Al Qaeda office in Kabul, Afghanistan. The computer contained models of a dam, made with structural architecture and engineering software and included geological soil identification software which would enable the planners of an attack to simulate the dam's catastrophic failure and plot the consequences of a breach.[22]

2002 **Attack on DNS Root servers.** A massive denial of service attack of unknown origin briefly interrupted traffic on nine of the 13 DNS 'root' servers that control the Internet but the overall threat was dismissed as 'minimal'.[23] The attack took place over a one-hour window and appeared to be the work of experts. It is interesting as it is an attack on the Internet itself, rather than particular websites.

2000-2006 **Suter Systems.**[24] In 2000, 2002 and 2004, the U.S. military tested the capability for U.S. forces to secretly enter an enemy computer network and monitor what their radar systems could detect. Further experiments tested the added capability for U.S. Forces to take over the enemy computers and start manipulating their radar to show false images. Suter 1,2 & 3 progressively enabled information warfare experts to penetrate anti-aircraft defense networks, using radar and radio antennas and microwave relays as portals. Once inside, Suter operators could see what the enemy radars saw, then jam and spoof the flow of information or even take over as system administrator to control movement of radar antennas. By the 2006 joint forces exercise, the Suter series of communications network invasion and exploitation capabilities, were absent. Senior Air Force officials stated that this change in emphasis was because the technology was no longer experimental and had been moved into

---

[22] Gellman, 'Cyber-Attacks by Al Qaeda Feared'.

[23] Naraine, *Massive DDoS Attack Hit DNS Root Servers* (last accessed 6 September 2007)

[24] David Fulghum, 'Sneak Attack' (2004) *Aviation Week & Space Technology* 28 June 2004 34; David Bond, 'The Dog That Didn't Bark' (2006) 164(19) *Aviation Week & Space Technology* 8 May 2006 19.

operational use in Iraq and Afghanistan.

2003 - **Titan Rain.** Titan Rain is the code name given to a series of computer intrusions originating in Guangdong province, China. The attacks were significant for the high speed and technical skill of the intrusions although the motivation behind them remains unknown as does the identity of the perpetrators. It has been speculated that these were Chinese military attacks.[25] The code name has since been changed from Titan Rain but the new designation remains classified.

2004 **Mydoom & Variants.** The original Mydoom virus began circulating around email systems and peer-to-peer networks at the end of January 2004. The original virus contained a mass-mailing worm,[26] which set up a backdoor into the infected computer by opening TCP ports. These backdoors potentially allow an attacker to connect to the computer either to gain access to its network resources, or to make the computer follow remote commands from the attacker to launch attacks on other computers. In the case of the Mydoom virus, it was the latter. The original virus was programmed to launch Denial of Service attacks at US company SCO over a period of 12 days, apparently as part of an ongoing battle over control of Unix source code.[27] The Mydoom variant, Doomjuice launches a similar attack at the Microsoft website. However, unlike the original virus Doomjuice does not travel by email. Instead, both Doomjuice and its counterpart Deadhat,[28] randomly scan net addresses and upload themselves to any infected machines they find, through the backdoor

---

[25] Graham, 'Hackers Attack Via Chinese Web Sites'.

[26] A mass mailing worm arrives an email attachment which sends itself out to all other addresses in the compromised computers address book.

[27] 'Mydoom Cripples US Firm's Website', *BBC News* 1 February 2004, <http://news.bbc.co.uk/1/hi/technology/3449931.stm> (last accessed 10 February 2008).

[28] The Deadhat virus is designed to find machines infected with the Mydoom virus, it removes any copies of Mydoom.A and Mydoom.B that are resident, installs itself and then attempts to stop the computer running anti-virus software or getting updates to protect itself against future infections.

opened by the original virus.[29]

2007 **Attack on DNS Root Servers.**[30] On 6 February 2007 a distributed denial of service attack was launched against three DNS root servers including one operated by the U.S. Defense Department (the others were operated by the Internet's oversight body ICANN (Internet Corporation for Assigned Names and Numbers) and UltraDNS (which manages traffic for websites ending in "org" and some other suffixes) respectively. There was no evidence of damage to the servers.

2007 **'Aurora'.** In March 2007 researchers from the Idaho National Laboratory launched an experimental cyber attack, hacking into a replica of a power plants control system and changing the operating cycle of a generator.[31] The attack sent the generator out of control and ultimately causing the generator to self destruct, alarming the federal government and electrical industry about what might happen if such an attack were carried out on a larger scale.[32]

2007 **DDoS Attacks against Estonia.**[33] In May 2007, Estonia became the victim of a prolonged series of denial of service attacks which brought the banking system, many government services and much of the media to a halt. Although no critical infrastructure was compromised, for a highly technology dependent State like Estonia that depends on the Internet for everything from parking to banking to voting, the attacks caused serious disruption and caused an estimated tens of millions of euros worth of

---

[29] Security firms suspect that Doomjuice was written by the author of the original Mydoom virus. 'Mydoom Mutants Launch New Attacks', *BBC News* 10 February 2004, <http://news.bbc.co.uk/1/hi/technology/3475235.stm> (last accessed 20 February 2008).

[30] 'Hackers Attack Heart of the Net', *BBC News* 7 February 2007, <http://news.bbc.co.uk/1/hi/technology/6338261.stm> (last accessed 21 September 2008).

[31] Meserve, 'Staged Cyber Attack Reveals Vulnerability in Power Grid'.

[32] Ibid., footage of the generator is also available at http://www.youtube.com/watch?v=fJyWngDco3g.

[33] See generally, 'The Cyber Raiders Hitting Estonia'; AFP, 'Cyber Attacks on Estonia Are Security Issue: NATO Chief'; Tony Halpin, 'Putin Accused of Launching Cyber War', *The Times* (London), 18 May 2007, Overseas News 46; Traynor, 'Russia Accused of Unleashing Cyberwar to Disable Estonia'; Traynor, 'Web Attackers Used a Million Computers, Says Estonia'.

damage.[34] Despite earlier explicit accusations that Russia was behind the offensive, the Estonian government backed away from directly accusing the Kremlin of launching the attacks,[35] but requested assistance from its NATO allies under the terms of that alliance.

2007 **Israeli Attack on Suspected Syrian Nuclear Site.** On 6 September 2007 Israel penetrated of Syrian air defences in order to bomb a suspected nuclear site at Dayr az-Zawr, without being engaged or even detected.[36] That attack combined electronic attack techniques in the form of brute-force jamming, precision missiles to eliminate the facility itself, and computer network attack techniques. The ability of non-stealthy Israeli aircraft to penetrate without interference rests in part on technology, carried on board modified aircraft, that allowed specialists to hack into Syria's networked air defence system.[37] "Network raiders can conduct their invasion from an aircraft into a network and then jump from network to network until they are into the target's communications loop".[38]

---

[34] Traynor, 'Web Attackers Used a Million Computers, Says Estonia'.

[35] Ibid. Russia categorically denies any involvement and no concrete evidence has been found to substantiate those claims. While technical data shows that some of the attacks came from IP addresses allocated to the Russian Government, there is no evidence that these computers were involved in initiating the attacks, or that they had not been compromised or spoofed.

[36] Fulghum, Wall and Butler, 'Israel Shows Electronic Prowess'.

[37] Ibid.

[38] Ibid.

Appendix 2 - Glossary of Selected Computing Terms[1]

Applet	A program designed to be executed from within another application (they cannot be executed directly from the operating system). Web browsers, which are often equipped with Java virtual machines, can interpret applets from Web servers. Because applets are small in file size, cross-platform compatible, and highly secure (can't be used to access users' hard drives), they are ideal for small Internet applications accessible from a browser.
Backdoor	Also called a trapdoor. An undocumented way of gaining access to a program, online service or an entire computer system.
Bitstream	A bitstream is a contiguous sequence of bits (0s & 1s), representing a stream of data, transmitted continuously over a communications path, serially (one at a time).[2]
Botnet	Also called a Zombie net. A group of compromised computers controlled by a master computer and used primarily for DDoS attacks or spam. According to the Independent, a reasonable-sized botnet of 8,000-10,000 computers may rented for £200 an hour.[3]

---

1 Definitions are primarily taken and adapted from the *Webopedia: Online Dictionary of Computing & Internet* <http://www.webopedia.com/> (last accessed 30 November 2007). and the *Department of Defense Dictionary of Military and Associated Terms*, (Government Reprints Press, Washington, DC, 2001).

[2] SearchNetworking.com Definitions <http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci213496,00.html> (last accessed 13 August 2008).

[3] Sarah Arnott, 'How Cyber Crime Went Professional', *The Independant* (London), 13 August 2008, <http://www.independent.co.uk/news/business/analysis-and-features/how-cyber-crime-went-professional-892882.html> (last accessed 20 August 2008).

Computer network attack	Operations designed to disrupt, deny, degrade, or destroy information resident in computers or computer networks, or the computer networks themselves.
Denial of Service Attack	A type of attack on a network that is designed to bring the system or network to its knees by flooding it with useless traffic.
Distributed Denial Of Service Attack	An attack where multiple compromised systems (which are usually infected with a Trojan) are used to target a single system causing a Denial of Service attack. Victims of a DDoS attack consist of both the end targeted system and all systems maliciously used and controlled by the hacker in the distributed attack.
DNS Server	Domain Name Service Server. DNS is an Internet service that translates domain names into IP addresses. For example, the domain name *www.example.com* might translate to *198.105.232.4*. If one DNS server in the network doesn't know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.
Electronic warfare	Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy.
Hard coded	A feature which is built into the hardware or software in such a way that it cannot be modified.
In the wild	in order for a virus to be considered *in the wild*, "it must be spreading as a result of normal day-to-day operations on and between the computers of unsuspecting users." Although there are an estimated 47,000 computer viruses, fewer than 600 are said to be circulating outside of laboratories and research

	facilities - hence, in the wild. Experts say these wild viruses pose the most significant threat to computers.[4]
Information	Facts, data or instructions in any medium or form.
Information operations	The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own.
IP Address	An identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255. For example, 1.160.10.240 could be an IP address.
ISP	Internet Service Provider. A company that provides access to the Internet.
Logic bomb	Malicious programming code which is inserted into application software or an operating system. The code lies dormant until a predetermined period of time has elapsed, or a triggering event (or series of events) occurs, at which time the code activates.
Malware	Malicious software, i.e. software designed specifically to damage or disrupt. E.g. Trojan horse, virus etc.

[4] SearchSecurity.com definitions <http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci511204,00.html> (last accessed 2 December 2007).

Peer-to-peer	Peer-to-peer (P2P) architecture is a type of network in which each workstation has equivalent capabilities and responsibilities. Often used to describe one user linking with another user to transfer information and files through the use of a common P2P client to download MP3s, videos, images, games and other software. This, however, is only one type of P2P networking. Generally, P2P networks are used for sharing files, but a P2P network can also mean Grid Computing or Instant messaging.
Rootkit	Type of malicious software that is activated each time a system boots up. Rootkits are difficult to detect because they are activated before the system's Operating System (OS) has completely booted up. A rootkit often allows the installation of hidden files, processes, hidden user accounts, and more in the system's OS. Rootkits are able to intercept data from terminals, network connections, and the keyboard.
Shareware	Software distributed on the basis of an honor system. Usually free of charge, but with the request that if the user likes the program and uses it regularly the author is paid a small fee. This may entitle the user to service assistance and updates. Shareware may be copied and shared with the same fee expectation.
Spoof	To fool or deceive. Although many things can be spoofed, it generally refers to IP spoofing which allows the sender of data to forge the source address in the header of the IP packet. The receiving computer will then send all replies to the forged address rather than the actual computer. This technique is often used in denial of service attacks.

Trapdoor	See 'Backdoor'.
Trojan horse	Malicious programming code disguised to look like a harmless application. Trojans are further broken down in classification based on how they breach systems and the damage they cause.
URL	Universal Resource Locator. A global address of documents and other resources on the world wide web. A web address
Virus	Malicious programming code written to replicate itself and attaches to another file or program in order to spread from one computer to another. They may also cause damage or destruction as they travel. Unlike a worm, a virus cannot travel without human intervention.
Worm	A sub-class of virus which does not require human intervention to spread from host to host. A worm takes advantage of file or information transport features on the computer system, to allow it to travel unaided.

Appendix 3 - Abbreviations Used

ADIL	Annual Digest & Reports of Public International Law Cases
Additional Protocol I *also* API	Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977.
Additional Protocol II *also* APII	Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 8 June 1977.
AFJ Log	Air Force Journal of Logistics
AFL Rev	Air Force Law Review
AJIL	American Journal of International Law
ASIL Proc	American Society of International Law Proceedings
BFSP	British and Foreign State Papers.
BMJ	British Medical Journal
BU Int'l LJ	Boston University International Law Journal
BUJ Sci & Tech L	Boston University Journal of Science & Technology
BYBIL	British Yearbook of International Law
Case W Res J Int'l L	Case Western Reserve Journal of International Law
CNA	Computer Network Attack
Col J Trans L	Columbia Journal of Transnational Law
Conventional Weapons	Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed

Treaty	to Be Excessively Injurious or to Have Indiscriminate Effects, 10 October 1980.
CPU	Central Processing Unit
DCS	Distributed Control System.
DDoS	Distributed Denial of Service.
EJIL	European Journal of International Law
EMP	Electromagnetic Pulse.
FRY	Federal Republic of Yugoslavia.
Geneva Convention I	Geneva Convention for the Amelioration of the Condition of the Sick and Wounded in Armed Forces in the Field of August 12, 1949.
Geneva Convention II	Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea of August 12, 1949.
Geneva Convention III	Geneva Convention relative to the Treatment of Prisoners of War of August 12, 1949.
Geneva Convention IV	Geneva Convention relative to the Protection of Civilian Persons in Time of War of August 12, 1949.
GJIA	Georgetown Journal of International Affairs
GovExec	Government Executive
Hague Convention 1899	Hague Convention Concerning the Laws and Customs of War on Land
Hague Regulations	Regulations Annexed to the 1907 Hague Convention IV Respecting the Laws and Customs of War on Land.

Harv Int'l LJ	Harvard International Law Journal
Hous J Int'l L	Houston Journal of International Law
HPCR	Harvard Program on Humanitarian Policy and Conflict Research
ICJ	International Court of Justice
ICRC	International Committee of the Red Cross
ICTR	International Criminal Tribunal for Rwanda
ICTY	International Criminal Tribunal for the Former Yugoslavia
IFF	Identification Friend or Foe
IO	Information Operations
IP Address	Internet Protocol Address
IRRC	International Review of the Red Cross
Israel YB Hum Rts	Israeli Yearbook of Human Rights
IW	Information Warfare
JC&SL	Journal of Conflict & Security Law
JSTARS	Joint Surveillance Target Attack Radar System
Keesings	Keesings Record of World Events
Ottawa Convention	Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on Their Destruction.
LOAC	Laws of Armed Conflict

NIL Rev	Netherlands International Law Review
NZLR	New Zealand Law Reports
OAU	Organisation of African Unity
PMC	Private Military Company
Recueil des Cours	*Recueil des cours de l'Académie de droit international de La Haye,* Collected Courses of the Hague Academy of International Law (Leyden)
RIAA	Reports of International Arbitral Awards
SCADA	Supervisory Control and Data Acquisition
SCSL	Special Court for Sierra Leone
Stan J Int'l L	Stanford Journal of International Law
Stud Confl & Terror	Studies in Conflict & Terrorism
T. Jefferson L Rev.	Thomas Jefferson Law Review
UAV	Unmanned Aerial Vehicle
U.N.	United Nations
UNCIO Docs.	Documents of the United Nations Conference on International Organisation
UNTS	United Nations Treaty Series
URL	Universal Resource Locator (a web address)
U.S.	United States (of America)
US AF Acad J Legal Stud	U.S. Air Force Academy Journal of Legal Studies

Vand J Transnat'l L	Vanderbilt Journal of Transnational Law
Yale Hum Rts & Dev LJ	Yale Human Rights and Development Law Journal
Yale J Int'l L	Yale Journal of International Law
ZaöRV	Zeitschrift für ausländisches öffentliches Recht und Völkerrecht

Bibliography

Abi-Saab, Georges, 'The Specificities of Humanitarian Law' in Swinarski, C (ed) *Studies and Essays on International Humanitarian Law and Red Cross Principles in Honour of Jean Pictet* (Martinus Nijhoff Publishers, Geneva, The Hague, 1984) 265-280.

AFP, 'Cyber Attacks on Estonia Are Security Issue: NATO Chief', *The Age* (Melbourne), 26 May 2007.

Ago, Roberto, 'Addendum to the Eighth Report on State Responsibilty' (1980) II *UNYB Int'l L Comm'n* 13.

_____, 'State Responsibility' (1980) Vol 1 *UNYB Int'l L Comm'n* 188.

Al Nawar v Minister of Defence et al (1985) 39(3) Piskei Din 449, Israel Supreme Court.

Alberts, David S., Garstka, John and Stein, Frederick P., *Network Centric Warfare : Developing and Leveraging Information Superiority* (2nd ed, National Defense University Press, Washington, D.C., 1999).

Aldrich, Richard W, 'The International Legal Implications of Information Warfare' (1996) *Airpower* 99.

_____, 'How Do You Know You Are at War in the Information Age?' (2000) 22 *Hous J Int'l L* 223.

Alexandrov, Stanimir A., *Self-Defense against the Use of Force in International Law* (Kluwer Law International, The Hague; London, 1996).

Allison, Rebecca, 'Hacker Attack Left Port in Chaos: Busiest US Port Hit after Dorset Teenager Allegedly Launched Electronic Sabotage against Chatroom User', *The Guardian* (London), 7 October 2003, 7.

_____, 'Youth Cleared of Crashing American Port's Computer', *The Guardian* (London), 18 October 2007, 7.

Alvey, Ruth, 'Russian Hackers for Hire: The Rise of the E-Mercenary' (2001) 13(7) *Jane's Intelligence Review* 52.

American Society of International Law, 'The Jurisprudence of the Court in the Nicaragua Decision' (1987) 81 *ASIL Proc* 258.

Aoul, Samia Kazi, et al., *Towards a Spiral of Violence?*, (2000) <http://www.miningwatch.ca/updir/Memorandum-final-en.pdf> (last accessed 18 August 2008).

Arkin, William M, 'Cyber Warfare and the Environment' (2001) 25 *Vermont Law Review* 779.

Arkin, William M and Windrem, Robert, 'The Other Kosovo War', *MSNBC News*, 29 August 2001, <http://www.msnbc.com/news/607032.asp?cp1=1> (last accessed 12 April 2005).

Arkin, William M., 'The Cyber Bomb in Yugoslavia', *Washington Post* (Washington D.C.), 25 October 1999, <http://www.washingtonpost.com/wp-srv/national/dotmil/arkin.htm> (last accessed 21 September 2008).

_____, *Code Names: Deciphering US Military Plans, Programs, and Operations in the 9/11 World* (Steerforth Press, Hanover, NH, 2005).

Arnott, Sarah, 'How Cyber Crime Went Professional', *The Independant* (London), 13 August 2008, <http://www.independent.co.uk/news/business/analysis-and-features/how-cyber-crime-went-professional-892882.html> (last accessed 20 August 2007).

Arquilla, John, 'The Great Cyberwar of 2002' (1998) *Wired Magazine* February 1998 <http://hotwired.wired.com/collections/future_of_war/6.02_cyberwar_20021.html> (last accessed 9 February 2002).

Arquilla, John and Ronfeldt, David, 'Information, Power and Grand Strategy: In Athena's Camp - Section 1' in Arquilla, J and Ronfeldt, D (eds), *In Athena's Camp: Preparing for Conflict in the Information Age* (RAND, Santa Monica, 1997) 141-171.

_____, 'The Advent of Netwar (Revisited)' in Arquilla, J and Ronfeldt, D (eds), *Networks and Netwars* (RAND, Santa Monica, 2001) 1-24.

Arquilla, John, Ronfeldt, David F. and United States. Dept. of Defense. Office of the Secretary of Defense., *Networks and Netwars: The Future of Terror, Crime, and Militancy* (RAND, Santa Monica, 2001).

Arthur, Charles, 'The Day East Timor Was Deleted', *The Independent* (London), 28 February 1999, 8.

Bank for International Settlements, *Trienniel Central Bank Survey: Foreign Exchange and Derivitaves Market Activity in 2007*, Bank for International Settlements (2007) <http://www.bis.org/publ/rpfxf07t.pdf> (last accessed 17 April 2008).

Basu, Sandra, 'Military Electronic Medical Records Support Quality Treatment Abroad', *US Medicine* (Washington, D.C.), February 2006, <http://www.usmedicine.com/article.cfm?articleID=1249&issueID=84> (last accessed 7 December 2006).

Baxter, Richard R, 'So-Called 'Unprivileged Belligerency': Spies, Guerrillas, and Saboteurs' (1951) 28 *BYBIL* 323.

_____, 'The Duties of Combatants and the Conduct of Hostilities (the Law of the Hague)' in UNESCO (ed) *International Dimensions of Humanitarian Law* (Martinus Nijhoff, Dordrecht, 1988) 93-134.

Belknap, Margaret H., *The CNN Effect: Strategic Enabler or Operational Risk?*, Strategy Research Project, U.S. Army War College (2001) <http://www.iwar.org.uk/psyops/resources/cnn-effect/Belknap_M_H_01.pdf> (last accessed 16 April 2008).

Belt, Stuart Walters, 'Missiles over Kosovo: Emergence, Lex Lata, of a Customary Norm Requiring the Use of Precision Munitions in Urban Areas' (2000) 47 *Naval Law Review* 115.

Black, Jeremy, *War in the New Century* (Continuum, London, 2001).

Blix, Hans, 'Means and Methods of Combat' in UNESCO (ed) *International Dimensions of Humanitarian Law* (Martinus Nijhoff, Dordrecht, 1998) 135-151.

Boivin, Alexandra, *The Legal Regime Applicable to Targeting Military Objectives in the Context of Contemporary Warfare*, University Centre for International Humanitarian Law, 2 (2006) <http://www.cudih.org/recherche/objectif_militaire_recherche.pdf> (last accessed 10 October 2007).

Bond, David, 'The Dog That Didn't Bark' (2006) 164(19) *Aviation Week & Space Technology* 8 May 2006 19.

Bond, James, *Peacetime Foreign Data Manipulation as One Aspect of Offensive Information Warfare: Questions of Legality under the United Nations Charter Article 2(4)*, Naval War College (1996) <http://handle.dtic.mil/100.2/ADA310926> (last accessed 18 September 2007).

Bothe, Michael, 'Terrorism and the Legality of Pre-Emptive Force' (2003) 14(2) *EJIL* 227.

Bothe, Michael, et al., *New Rules for Victims of Armed Conflicts* (Martinus Nijhoff Publishers, Leiden, 1982).

Bourbonnière, Michel, 'Law of Armed Conflict (LOAC) and the Neutralisation of Satellites or Ius in Bello Satellitis' (2004) 9 *JC&SL* 43.

Bouvier, Antoine, 'Protection of the Natural Environment in Time of Armed Conflict' (1991) 285 *IRRC* 567 <www.icrc.org/web/eng/siteeng0.nsf/html/57JMAU> (last accessed 10 January 2007).

Bowett, D. W., *Self-Defence in International Law* (University of Manchester Press, Manchester, 1958).

Boyes, Roger, 'China Accused of Hacking into Heart of Merkel Administration', *The Times* (London), <http://www.timesonline.co.uk/tol/news/world/europe/article2332130.ece> (last accessed 26 August 2008).

Boylan, Patrick J., *Review of the Convention for the Protection of Cultural Property in the Event of Armed Conflict* (UNESCO, 1993).

'British Hackers Attack MoD Satellite', *Telegraph* (London), March 1999, <http://www.telegraph.co.uk/connected/main.jhtml?xml=/connected/1999/03/04/ecnhack04.xml> (last accessed 23 September 2008).

Brookings Institution, *Iraq Index*, Brookings Institute (2006) <http://www.brookings.edu/iraqindex> (last accessed 12 September 2008).

Brown, Davis, 'A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict' (2006) 47 *Harv Int'l LJ* 179.

Brownlie, Ian, 'International Law and the Activities of Armed Bands' (1958) 7 *International and Comparative Law Quarterly* 712.

_____, *International Law and the Use of Force by States* (Oxford University Press, Oxford, 1963).

_____, *International Law and the Use of Force by States: Revisited* (Europaeum, Oxford, 2001).

_____, *Principles of Public International Law* (6th ed, Oxford University Press, Oxford, 2003).

Campbell, Heidi, 'Spiritualising the Internet: Uncovering Discourses and Narratives of Religious Internet Usage' (2005) 1(1) *Online - Heidelburg Journal of Religions on the Internet* 1 <http://www.ub.uni-heidelberg.de/archiv/5824> (last accessed 27 January 2007).

The Caroline Case (1837) 29 BFSP 1137-1138, 30 BFSP 195-196.

Carr, Sylvia, 'British Library Prepping for Digital Future' (2005) *Siliconcom* 30 June 2005 <http://networks.silicon.com/webwatch/0,39024667,39131513,00.htm> (last accessed 9 June 2006).

Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda) (2005), International Court of Justice.

Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America) (Merits) (1986) ICJ 14, International Court of Justice.

Case Concerning Oil Platforms (Islamic Republic of Iran v United States of America) (2003), International Court of Justice.

Case Concerning the Gabcikovo-Nagymoros Project (1997) ICJ Reports 3, International Court of Justice.

Case Concerning the Land and Maritime Boundary between Cameroon and Nigeria (Cameroon v. Nigeria: Equatorial Guinea Invervening) (2002) ICJ Reports, International Court of Justice.

Case Concerning the United States Diplomatic and Consular Staff in Tehran (United States v Iran) (1980) 74 AJIL 746, International Court of Justice.

Cassese, Antonio, 'The Status of Rebels under the 1977 Geneva Protocol on Non-International Armed Conflicts' (1981) 30 *International and Comparative Law Quarterly* 416.

_____, *International Criminal Law* (Oxford University Press, Oxford, 2003).

Castrén, Erik, *The Present Law of War and Neutrality* (Suomalaisen Tiedeakatemian Toimituksia, Helsinki, 1954).

Cession of Vessels and Tugs for Navigation on the Danube Case (1921) 1 RIAA 97.

Chamberlain, Kevin, *War and Cultural Heritage: An Analysis of the 1954 Convention for the Protection of Cultural Property in the Event of Armed Conflict and Its Two Protocols* (Institute of Art & Law, Leicester, 2004).

30 April 1948, *Charter of the Organisation of American States*, 119 UNTS 3.

'China Denies Hacking Dalai Lama Computer', *CNN*, 25 September 2002, <http://europe.cnn.com/2002/TECH/internet/09/25/dalailama.hacking.ap/> (last accessed 28 September 2002).

Clausewitz, Carl von, Graham, J. J. and Maude, F. N., *On War* (new and rev. ed, Kegan Paul, Trench, Trubner & Co., London, 1940).

Cobb, Jennifer J., *Cybergrace: The Search for God in the Digital World* (Crown, New York, 1998).

Cody, Edward, 'Chinese Official Accuses Nations of Hacking', *Washington Post* (Washington D.C.), 13 September 2007, A16.

Combacau, Jean, 'The Exception of Self Defence in U.N Practice' in Cassese, A (ed) *The Current Legal Regulation of the Use of Force* (Martinus Nijhoff, Dordrecht, 1986) 9-38.

14 May 1954, *Convention for the Protection of Cultural Property in the Event of Armed Conflict*, 249 UNTS 240.

18 May 1977, *Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques*.

18 October 1907, *Convention Respecting the Laws and Customs of War on Land and Its Annex: Regulations Concerning the Laws and Customs of War on Land.*

Corfu Channel Case (U.K. v Albania) (Merits) (1949) ICJ Reports 4, International Court of Justice.

Corten, Olivier, 'The Controversies over the Customary Prohibition on the Use of Force: A Methodological Debate' (2005) 16 *EJIL* 803.

Coupland, Robin M, 'The Effects of Weapons and the Solferino Cycle: Where Disciplines Meet to Prevent or Limit the Damage Caused by Weapons' (1999) 319(7214) *BMJ* 864 <http://www.bmj.com/cgi/content/full/319/7214/864> (last accessed 14 December 2006).

Crace, John, 'Silence Falls: Documenting the Extinction of Languages', *The Guardian* (London), 5 November 2002, <http://education.guardian.co.uk/egweekly/story/0,,825613,00.html> (last accessed 28 June 2006).

Cuba Submarine Telegraph Co. (1923) 6 RIAA 118.

'The Cyber Raiders Hitting Estonia', *BBC News*, 17 May 2007, <http://news.bbc.co.uk/1/hi/world/europe/6665195.stm> (last accessed 21 September 2008).

Damrosch, Lori Fisler, 'Politics across Borders: Nonintervention and Nonforcible Influence over Domestic Affairs' (1989) 83 *AJIL* 1.

Daoust, Isabelle, Coupland, Robin and Ishoey, Rikke, 'New Wars, New Weapons? The Obligation of States to Assess the Legality of Means and Methods of Warfare' (2002) 84(846) *IRRC* 345.

Davis, Joshua, 'If We Run out of Batteries, This War Is Screwed' (2003) 11(6) *Wired* June 2003 <http://www.wired.com/wired/archive/11.06/battlefield.html> (last accessed 29 April 2008).

De Wet, Erika, *The Chapter VII Powers of the United Nations Security Council* (Hart, Oxford, 2004).

Declaration on Principles of International Law Concerning Friendly Relations and Co-Operation among States in Accordance with the Charter of the United Nations, GA Res. 2625 (XXV) UN GAOR Supp., 25, 18 122, UN Doc. (1970).

Declaration on the Enhancement of the Effectiveness of the Principle of Refraining from the Threat or Use of Force in International Relations GAOR 42nd sess, 73rd plen mtg, UN Doc. A/Res/42/22 (1987).

29 November/ 11 December 1868, *Declaration Renouncing the Use, in Time of War, of Explosive Projectiles under 400 Grammes Weight (St Petersburg Declaration).*

Deibert, Ronald J., *Parchment, Printing, and Hypermedia: Communication in World Order Transformation* (Columbia University Press, New York, 1995).

Denning, Dorothy E., 'Cyber-Security as an Emergent Infrastructure' in Latham, R (ed) *Bombs & Bandwidth: The Emerging Relationship between Information Technology & Security* (Manas Publications, New Delhi, 2004) 25.

Department of Defense Dictionary of Military and Associated Terms, (Government Reprints Press, Washington, DC, 2001).

Dinstein, Yoram, 'Booty in Land Warfare' in Bernhardt, R (ed) *Encyclopedia of Public International Law* (Max Plank Institute; North Holland, Amsterdam, 1992) 432-434.

_____, 'Computer Network Attacks and Self-Defense' in Schmitt, M N and O'Donnell, B T (eds), *Computer Network Attack and International Law* (Naval War College, Newport, RI, 1999) 99-119.

_____, *War, Aggression, and Self-Defense* (3rd ed, Cambridge University Press, New York, 2001).

_____, 'Legitimate Military Objectives under the Current Jus in Bello' in Wall, A E (ed) *Legal and Ethical Lessons of NATO's Kosovo Campaign* (Naval War College, Newport, Rhode Island, 2002) 139-173.

_____, *The Conduct of Hostilities under the Law of International Armed Conflict* (Cambridge University Press, Cambridge, 2004).

'Discussion' in Wall, A E (ed) *Legal and Ethical Lessons of NATO's Kosovo Campaign* (Naval War College, Newport, Rhode Island, 2002) 211-222.

Domb, F, 'Judgements of the Supreme Court of Israel' (1986) 16 *Israel YB Hum Rts* 321.

Dorman, Andrew M., *Transforming to Effects-Based Operations: Lessons from the United Kingdom Experience*, Strategic Studies Institute (2008).

Dörmann, Knut, 'Applicability of the Additional Protocols to Computer Network Attacks' (Paper presented at the International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, Stockholm, 17-19 November 2004) 139-154.

Doswald-Beck, Louise, 'Vessels, Aircraft and Persons Entitled to Protection During Armed Conflicts at Sea' (1994) 65 *BYBIL* 211.

_____, 'Some Thoughts on Computer Network Attack and the International Law of Armed Conflict' in Schmitt, M N and O'Donnell, B T (eds), *Computer Network Attack and International Law* (Naval War College, Newport, RI, 2002) 163-186.

Downey, William Gerald, Jr., 'Captured Enemy Property: Booty of War and Seized Enemy Property' (1950) 44 *AJIL* 488.

Dunlap, Charles J, 'The End of Innocence: Rethinking Non-Combatancy in the Post-Kosovo Era' (2000) Summer *Strategic Review* 9.

Dunnigan, James F, *The Next War Zone: Confronting the Global Threat of Cyber Terrorism* (Citadel Press Books, New York, 2003).

Eastern Extension, Australasia and China Telegraph Co. Claim (1923) 6 RIAA 112.

Evron, Gadi, 'Battling Botnets and Online Mobs' (2008) 9(1) *GLIA* 121.

Ex Parte Quirin et al (1942) 317 US 1, Supreme Court of the United States.

Farer, Tom, 'Political and Economic Aggression in Contemporary International Law' in Cassese, A (ed) *The Current Legal Regulation of the Use of Force* (Martinus Nijhoff, Dordrecht, 1986) 121-132.

Farquharson, John, 'Governed or Exploited? The British Acquisition of German Technology, 1945-48' (1997) 32(1) *Journal of Contemporary History* 23.

Finding of the International Commission of Inquiry Organized under Article 9 of the Convention for the Pacific Settlement of International Disputes, of July 29, 1899 (the Dogger Bank Incident) (1905) 2 AJIL 931-936, The International Commission of Inquiry between Great Britain and Russia arising out of the North Sea incident.

Fleck, Dieter, 'Ruses of War and Prohibition of Perfidy' (1974) 13 *Revue de Droit Penal Militare et de Droit de la Guerre* 269.

Franck, Thomas M., *Recourse to Force: State Action against Threats and Armed Attacks* (Cambridge University Press, Cambridge, 2002).

French, Matthew, 'Tech Sabotage During the Cold War' (2004) *Federal Computer Week* 26 April 2004 <http://www.fcw.com/print/10_12/news/82709-1.html> (last accessed 29 June 2008).

Friedman, Thomas, 'Global Is Good', *The Guardian* (London), 21 April 2005, <http://www.guardian.co.uk/g2/story/0,,1464454,00.html> (last accessed 27 May 2005).

Friedman, Thomas L, 'Syria Says Airman Seized in U.S. Raid Will Not Be Freed', *New York Times*, 6 December 1983, 1.

_____, 'Widened Cabinet Sought in Beirut', *New York Times*, 8 December 1983, 18.

Friel, Brian, 'DoD Launches Internet Counterattack' (1998) *Government Executive* 18 September 1998 <http://govexec.com/dailyfed/0998/091898b1.htm> (last accessed 7 August 2008).

Frigo, Manlio, 'Cultural Property *v.* Cultural Heritage: A "Battle of Concepts" in International Law?' (2004) 86(854) *IRRC* 367.

Frontline, *Interview with James Lewis for Frontline: Cyber War! (Interview Conducted on 18 February 2003)* <http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/lewis.html> (last accessed 16 March 2008).

Frontline, PBS, *Interview with Richard Clarke - Cyberwar!* <http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/clarke.html> (last accessed 21 September 2008).

Frowein, Jochen, 'Article 39' in Simma, B (ed) *The Charter of the United Nations: A Commentary* (2nd ed, Oxford University Press, Oxford, 2002) 717.

Fulghum, David, 'Sneak Attack' (2004) *Aviation Week & Space Technology* 28 June 2004 34.

Fulghum, David A., 'Data Link, Ew Problems Pinpointed by Pentagon' (1999) 151(10) *Aviation Week and Space Technology* 6 September 1999 87.

_____, 'Yugoslavia Successfully Attacked by Computers' (1999) 151(8) *Aviation Week and Space Technology* 23 August 1999 31.

_____, 'Frustrations and Backlogs' (2003) 158(10) *Aviation Week & Space Technology* 10 March 2003 33.

Fulghum, David A. and Barrie, Douglas, 'Israel Used Electronic Attack in Air Strike against Syrian Mystery Target' (2007) *Aviation Week & Space Technology* 8 October 2007 <http://www.aviationweek.com/aw/generic/story_channel.jsp?channel=defense&id=news/aw100807p2.xml> (last accessed 10 October 2007).

Fulghum, David A., Wall, Robert and Butler, Amy, 'Israel Shows Electronic Prowess' (2007) *Aviation Week and Space Technology* 25 November 2007 <http://www.aviationweek.com/aw/generic/story_channel.jsp?channel=defense&id=news/aw112607p2.xml&headline=Israel%20Shows%20Electronic%20Prowess> (last accessed 9 May 2008).

Fusco, Coco, 'Performance Art in a Digital Age: A Conversation with Ricardo Dominguez', 25 November 1999.

Gallagher, David F., 'Hackers; Government Tells Vigilantes Their 'Help' Isn't Necessary', *New York Times*, 20 February 2003, 5.

Gardam, Judith G., 'Proportionality and Force in International Law' (1993) 87(3) *AJIL* 391.

Gellman, Barton, 'Cyber-Attacks by Al Qaeda Feared', *Washington Post* (Washington D.C.), 27 June 2002, A01.

Gerhard, William D. and Millington, Henry W., *Attack on a Sigint Collector, the U.S.S. Liberty*, National Security Agency (1981).

Gimbel, John, *Science, Technology, and Reparations: Exploitation and Plunder in Postwar Germany* (Stanford University Press, Stanford, Calif, 1990).

Goodin, Dan, 'Electrical Supe Charged with Damaging California Canal System' (2007) *The Register* 30th November 2007 <http://www.theregister.co.uk/2007/11/30/canal_system_hack/> (last accessed 16 September 2008).

Gordon, Edward, 'Article 2(4) in Historical Context' (1985) 10 *Yale J Int'l L* 271.

Gorman, Siobhan, 'Georgia States Computers Hit by Cyberattack', *Wall Street Journal* (New York), 12 August 2008, A9.

Graham, Bradley, 'Bush Orders Guidelines for Cyber-Warfare', *Washington Post* (Washington D.C.), 7 February 2003, <http://www.washingtonpost.com/wp-dyn/articles/A38110-2003Feb6.html> (last accessed 21 February 2001).

_____, 'Hackers Attack Via Chinese Web Sites', *Washington Post* (Washington D.C.), 25 August 2005, 1.

Gray, Christine D., *International Law and the Use of Force* (2nd ed, Oxford University Press, Oxford, 2004).

_____, 'The Bush Doctrine Revisited: The 2006 National Security Strategy of the USA' (2006) 5(3) *Chinese Journal of International Law* 555.

Gray, Colin S, *Another Bloody Century: Future Warfare* (Weidenfeld & Nicolson, London, 2005).

Green, Leslie C., *The Contemporary Law of Armed Conflict* (2nd ed, Manchester University Press, Manchester, 2000).

_____, 'The Status of Mercenaries in International Law' in Green, L C (ed) *Essays on the Modern Law of War* (Transnational Publishers, Dobbs Ferry, NY, 2000).

Greenberg, Lawrence T, Goodman, Seymour E and Hoo, Kevin J Soo, *Information Warfare and International Law* (CCRP, Washington D.C., 1998).

Greenwood, Christopher, 'Customary International Law and the First Geneva Protocol of 1977 in the Gulf Conflict' in Rowe, P J (ed) *The Gulf War 1990-1991 in International and English Law* (Routledge, London, 1993) 63-88.

_____, 'Scope of Application of Humanitarian Law' in Fleck, D (ed) *The Handbook of Humanitarian Law in Armed Conflict* (Oxford University Press, Oxford, 1995) 39-63.

_____, 'The Law of Weaponry at the Start of the New Millennium' in Schmitt, M N and Green, L C (eds), *The Law of Armed Conflict: Into the Next Millennium* (Naval War College, Newport, Rhode Island, 1998) 185-231.

_____, 'International Law and the War against Terrorism' (2002) 78 *International Affairs* 301.

_____, 'International Law and the Pre-Emptive Use of Force: Afganistan, Al-Qaida, and Iraq' (2003) 4 *San Diego Int'l LJ* 7.

_____, 'The Law of War (International Humanitarian Law)' in Evans, M D (ed) *International Law* (Oxford University Press, Oxford, 2003) 789-821.

Grimes, Roger A., 'Security Adviser: DNS Attack Puts Web Security in Perspective' (2007) 29(8) *InfoWorld* 19 February 2007 <http://www.infoworld.com/article/07/02/16/08OPsecadvise_1.html> (last accessed 1 October 2007).

Guillory, Michael E., 'Civilianising the Force: Is the United States Crossing the Rubicon?' (2001) 51 *AFL Rev* 111.

'Hackers Attack Heart of the Net', *BBC News*, 7 February 2007, <http://news.bbc.co.uk/1/hi/technology/6338261.stm> (last accessed 21 September 2008).

Halpin, Tony, 'Putin Accused of Launching Cyber War', *The Times* (London), 18 May 2007, 46.

Hanseman, Robert G, 'The Realities and Legalities of Information Warfare' (1997) 42 *AFL Rev* 173.

Happold, Matthew, 'Child Soldiers in International Law: The Legal Regulation of Children's Participation in Hostilities' (2000) 47 *NIL Rev* 27.

Harbom, Lotta and Wallensteen, Peter, 'Armed Conflict, 1989-2006' (2007) 44(5) *Journal of Peace Research* 623.

Hargrove, John, 'The Nicaragua Judgment and the Future of the Law of Force and Self-Defense' (1987) 81 *AJIL* 135.

Harris, D. J., *Cases and Materials on International Law* (6th ed, Sweet & Maxwell, London, 2004).

Hart, Kim, 'Longtime Battle Lines Are Recast in Russia and Georgia's Cyberwar', *Washington Post* (washington D.C.), 14 August 2008, D01 <http://www.washingtonpost.com/wp-

dyn/content/article/2008/08/13/AR2008081303623.html> (last accessed 26 August 2008).

Haslam, Emily, 'Information Warfare: Technological Changes and International Law' (2000) 5(2) *JC&SL* 157.

Heickerö, Roland, 'Electronic Warriors Use Mail Order Equipment' (2005) *Framsyn Magazine* April 2005 <http://www.foi.se/FOI/templates/Page____4554.aspx#> (last accessed 21 September 2007).

Heintschel von Heinegg, Wolff and Epping, Volker, *International Humanitarian Law Facing New Challenges: Symposium in Honour of Knut Ipsen* (Springer, Berlin; New York, 2007).

Held, David and McGrew, Anthony, 'Introduction' in Held, D and McGrew, A (eds), *Governing Globalisation: Power, Authority & Global Governance* (Polity Press, Cambridge, 2002) 1-21.

Henckaerts, Jean-Marie, 'New Rules for the Protection of Cultural Property in Armed Conflict' (1999) 835 *IRRC* 593.

Henckaerts, Jean-Marie and Doswald-Beck, Louise, *Customary International Humanitarian Law* (Cambridge University Press, Cambridge, 2005).

Henderson, Christian M., 'The 2006 National Security Strategy of the United States: The Pre-Emptive Use of Force and the Persistent Advocate' (2007) 15 *Tulsa J Comp & Int'l L* 1.

'Hezbollah Takes over West Beirut', *BBC News*, 9 May 2008, <http://news.bbc.co.uk/1/hi/world/middle_east/7391600.stm> (last accessed 10 May 2008).

Higgins, Rosalyn, *Problems and Process: International Law and How We Use It* (Clarendon Press, Oxford, 1993).

Hoagland, Jim, 'U.S., Iraq to Confer on Air War', *Washington Post* (Washington D.C.), 25 May 1987, 1.

Holland, Jesse J, 'Bush Advisor Warns Cyberterrorists', *Washington Post* (Washington D.C.), 13 February 2002, <http://www.washingtonpost.com/wp-dyn/articles/A6846-2002Feb13.htm> (last accessed 30 September 2002).

Hollis, Duncan B., 'Why States Need an International Law for Information Operations' (2007) 11(4) *Lewis & Clark L Rev* 1023.

Holz, Thorsten, et al., 'Measurements and Mitigation of Peer-to-Peer-Based Botnets: A Case Study on Stormworm' (Paper presented at the First USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET '08), San Francisco, <http://honeyblog.org/junkyard/paper/storm-leet08.pdf> (last accessed 31 August 2008).

Hosmer, Stephen T., *The Conflict over Kosovo: Why Milosevic Decided to Settle When He Did* (RAND, Santa Monica, 2001).

Hulme, George V., 'Taiwan Accuses China of Launching Cyberattack' (2004) *Information Week* 16 June 2004 <http://www.informationweek.com/story/showArticle.jhtml?articleID=22100221> (last accessed 15 September 2007).

Hulme, Karen, *War Torn Environment: Interpreting the Legal Threshold* (Martinus Nijhoff Publishers, Leiden, 2004).

Hundley, Richard O, et al., *The Global Course of the Information Revolution: Recurring Themes and Regional Variations* (National Defense Research Institute, RAND, Santa Monica, 2003).

ICRC, 'External Activities: September-October 1987' (1987) 27(261) *IRRC* 650.

_____, 'Guidelines for Military Manuals and Instructions on the Protection of the Environment in Times of Armed Conflict' (1996) 311 *IRRC* 230 <http://www.icrc.org/Web/Eng/siteeng0.nsf/html/57JN38> (last accessed 11 January 2007).

_____, *Direct Participation in Hostilities under International Humanitarian Law*, ICRC (2003) <http://www.icrc.org/web/eng/siteeng0.nsf/html/participation-hostilities-ihl-311205> (last accessed 18 August 2008).

_____, *Second Expert Meeting - Direct Participation in Hostilities under International Humanitarian Law*, ICRC (2004) <http://www.icrc.org/web/eng/siteeng0.nsf/html/participation-hostilities-ihl-311205> (last accessed 18 August 2008).

_____, *A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977*, ICRC (2006).

ICTY, *Final Report to the Prosecutor of the Committee Established to Review the NATO Bombing Campaign against the Federal Republic of Yugoslavia*, ICTY (2000) <www.un.org/icty/pressreal/nato061300.htm> (last accessed 16 September 2007).

'Indonesia, Ireland in Info War?' *Wired News*, 27 January 1999, <http://www/wired.com/news/print/0,1294,17562,00.html> (last accessed 4 April 2003).

'Information' *A Dictionary of Computing* (Oxford University Press, Oxford, 2004).

Intergovernmental Conference on the Protection of Cultural Property in the Event of Armed Conflict, *Records of the Conference Convened by the United Nations Educational, Scientific and Cultural Organisation and Held at the Hague from 21*

April to 14 May 1954 (Government of the Netherlands, The Hague Staatsdrukkerij en Uitgeverijbedrijf, 1961).

International Convention against the Recruitment, Use, Financing and Training of Mercenaries UN GAOR 44th Sess., Supp No.43, UN Doc. A/RES/44/34 (1989).

Intoccia, Gregory F. and Moore, Joe Wesley, 'Communications Technology, Warfare, and the Law: Is the Network a Weapons System?' (2006) 28 *Hous J Int'l L* 467.

Ipsen, Knut, 'Perfidy' in Bernhardt, R (ed) *Encylopedia of Public International Law* (Max-Planck Institute, Amsterdam; New York, 1997) 978-981.

_____, 'Combatants & Non-Combatants' in Fleck, D (ed) *The Handbook of Humanitarian Law in Armed Conflicts* (Oxford University Press, Oxford, 1999) 65-104.

Jacobsen, Walter L., 'A Juridical Examination of the Israeli Attack on the Uss Liberty' (1986) 36(Winter) *Naval Law Review* 69.

Jacobson, Mark, 'War in the Information Age: International Law, Self Defence and the Problem of 'Non-Armed' Attacks' (1998) 21(3) *Journal of Strategic Studies* 1.

Jennings, Robert Y. and Watts, C. Arthur. H. (eds), *Oppenheim's International Law* (9th ed, Longman, Harlow, 1992).

Jensen, Eric Talbot, 'Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense' (2002) 38 *Stan J Int'l L* 207.

_____, 'The International Law of Environmental Warfare: Active and Passive Damage During Armed Conflict' (2005) 38 *Vand J Transnat'l L* 145.

Kalshoven, Frits, 'The Soldier and His Golf Clubs' in Swinarski, C (ed) *Studies and Essays on International Humanitarian Law and Red Cross Principles in Honour of Jean Pictet* (Martinus Nijhoff, The Hague; Boston, 1984) 369-385.

Kalshoven, Frits and Zegveld, Liesbeth, *Constraints on the Waging of War* (ICRC, Geneva, 2001).

Kanuck, Sean P, 'Information Warfare: New Challenges for Public International Law' (1996) 37 *Harv Int'l LJ* 272.

Kidder, Tracy, *The Soul of a New Machine* (Little, Brown, Boston, 1981).

Kinver, Mark, "Damage Is Done' to Lebanon Coast', *BBC News*, 8 August 2006, <http://news.bbc.co.uk/1/hi/sci/tech/5255966.stm> (last accessed 9 January 2007).

Klare, Michael T., *Resource Wars: The New Landscape of Global Conflict* (Metropolitan Books, New York, 2001).

Kritsiotis, Dino, 'Mercenaries and the Privatisation of Warfare' (1998) 22 *Fletcher Forum of World Affairs* 11.

Krulak, Charles C., 'The Strategic Corporal: Leadership in the Three Block War' (1999) 28(1) *Marines Magazine* January 1999 28-34.

Ku, Raymond, 'Foreword: A Brave New Cyberworld' (2000) 22 *T Jefferson L Rev* 125.

Kuehl, Daniel T, 'Airpower vs Electricity' (1995) 18 *Journal of Strategic Studies* 28.

Lague, David, 'Chinese See Military Dependence on Computers as Weakness', *International Herald Tribune* (Paris), 29 August 2007, <http://www.iht.com/articles/2007/08/29/news/cyber.php> (last accessed 15 September 2007).

Lambeth, Benjamin S., U.S. Air Force and Project Air Force, *NATO's Air War for Kosovo: A Strategic and Operational Assessment* (RAND, Santa Monica, 2001).

Landler, Mark and Markoff, John, 'Digital Fears Emerge after Data Seige in Estonia', *New York Times*, 29 May 2007, <www.nytimes.com/2007/05/29/technology/29estonia.html> (last accessed 20 August 2007).

LaRae-Perez, Cassandra, 'Economic Sanctions as a Use of Force: Re-Evaluating the Legality of Sanctions from an Effects-Based Perspective' (2002) 20 *BU Int'l LJ* 161.

Lauterpacht, Hersh (ed) *Oppenheim's International Law* (7th ed, Longmans, Green & Co., London, 1952).

Legal Consequences of the Construction of a Wall in Occupied Palestinian Territory (2004) ICJ 136, International Court of Justice.

Legality of the Threat and Use of Nuclear Weapons (1996) ICJ 226, International Court of Justice.

Legality of the Use by a State of Nuclear Weapons in Armed Conflicts (1996) ICJ 26, International Court of Justice.

Lessig, Lawrence, *Code and Other Laws of Cyberspace* (Basic Books, New York, 1999).

Lev, Izhar, 'E-Intifada: Political Disputes Cast Shadows in Cyberspace' (2000) 12(12) *Janes Intelligence Review* 16.

Leyden, John, 'France Blames China for Hack Attacks', *The Register* (London), 12 September 2007, <http://www.theregister.co.uk/2007/09/12/french_cyberattacks/> (last accessed 26 August 2008).

Libicki, Martin C., *What Is Information Warfare?* (Center for Advanced Concepts and Technology, Institute for National Strategic Studies, Washington, DC, 1995).

Linzer, Dafna and Witte, Griff, 'U.S. Airstrike Targets Al Qaeda's Zawahiri', *Washington Post* (Washington D.C.), 14 January 2006, A09 <http://www.washingtonpost.com/wp-dyn/content/article/2006/01/13/AR2006011302260_pf.html> (last accessed 16 September 2008).

Livingston, Steven, *Clarifying the CNN Effect: An Examination of Media Effects According to Type of Military Intervention*, The Joan Shorenstein Center on the Press, Politics and Public Policy, John F. Kennedy School of Government, Harvard University, R-18 (1997) <http://www.hks.harvard.edu/presspol/research_publications/papers/research_papers/R18.pdf> (last accessed 16 September 2008).

Lloyd, Ian J., *Information Technology Law* (4th ed, Oxford University Press, Oxford, 2004).

Lopez, C. Todd, 'Military Students Get Lesson in Cyberwarfare', *Air Force Print News*, 3 May 2006, <http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1186049,00.html> (last accessed 11 May 2006).

The Lotus (1927) Series A No.10, Permanent Court of International Justice.

Lyman, Peter and Varian, Hal R., *How Much Information?*, University of California at Berkley (2003) <http://www.sims.berkeley.edu/research/projects/how-much-info-2003/> (last accessed 9 November 2007).

Maguire, Kevin, 'Guard Tried Sabotage at Nuclear Reactor: Security Checks Tightened after High-Level Alert', *The Guardian* (London), 9 January 2001, 2.

Malhotra, Yogesh, 'Measuring the Knowledge Assets of a Nation: Knowledge Systems for Development' (Paper presented at the United Nations Advisory Meeting of the Department of Economic and Social Affairs, Division for Public Administration and Development Management, Ad hoc Group of Experts Meeting - Knowledge Systems for Development, United Nations Headquarters, New York, 4-5 September 2003).

Markoff, John, 'Before the Gunfire, Cyberattacks', *New York Times*, 13 August 2008, <http://www.nytimes.com/2008/08/13/technology/13cyber.html> (last accessed 26 August 2008).

McAfee, *Virtual Criminology Report*, McAfee Inc. (2007).

McCue, Andy, "Revenge' Hack Downed U.S. Port Systems', *ZDNet News*, 7 October 2003, <http://news.zdnet.co.uk/security/0,1000000189,39116978,00.htm> (last accessed 17 March 2008).

McDougal, Myres Smith and Feliciano, Florentino P., *Law and Minimum World Public Order: The Legal Regulation of International Coercion* (Yale University Press, New Haven, 1961).

McSherry, Lisa, *The Virtual Pagan: Exploring Wicca and Paganism through the Internet* (Red Wheel/Weiser, 2002).

Mégret, Frédéric, "War"? Legal Semantics and the Move to Violence' (2002) *EJIL* 361.

Mertl, Steve, 'Cyberspace Experts Await Full-Scale Attack', *Globe & Mail* (Canada), 27 December 2002, A11.

Meserve, Jeanne, 'Staged Cyber Attack Reveals Vulnerability in Power Grid', *CNNcom*, 26 September 2007, <http://edition.cnn.com/2007/US/09/26/power.at.risk/index.html> (last accessed 20 February 2008).

Mészáros, Ernö, 'Techniques for Manipulating the Atmosphere' in Westing, A H (ed) *Environmental Warfare: A Technical, Legal and Policy Appraisal* (Taylor & Francis, London, 1984).

'Military Eyes Electronic Warfare', *Associated Press, South China Morning Post*, 28 September 2002, <http://china.scmp.com/chimain/ZZZH3UK2F6D.html> (last accessed 30 September 2002).

Milliard, Todd S, 'Overcoming Post-Colonial Myopia: A Call to Recognise and Regulate Private Military Companies' (2003) 176 *Mil L Rev* 1.

Moir, Lindsay, *The Law of Internal Armed Conflict* (Cambridge University Press, New York, 2002).

Montgomery, Tony, 'Legal Perspective from the EUCOM Targeting Cell' in Wall, A E (ed) *Legal and Ethical Lessons of NATO's Kosovo Campaign* (Naval War College, Newport, RI, 2002) 189.

Moore, David, et al., *The Spread of the Sapphire/Slammer Worm*, (2003) <http://www.caida.org/publications/papers/2003/sapphire/sapphire.html> (last accessed 9 November 2007).

Morozov, Evgeny, 'An Army of Ones and Zeroes: How I Became a Soldier in the Georgia-Russia Cyberwar' (2008) *Slate* 14 August 2008 <http://www.slate.com/id/2197514/> (last accessed 2 September 2008).

Morth, Todd A., 'Considering Our Position: Viewing Information Warfare as a Use of Force Prohibited by Article 2(4) of the U.N. Charter' (1998) 30 *Case W Res J Int'l L* 567.

'Mydoom Cripples US Firm's Website', *BBC News*, 1 February 2004, <http://news.bbc.co.uk/1/hi/technology/3449931.stm> (last accessed 10 February 2008).

'Mydoom Mutants Launch New Attacks', *BBC News*, 10 February 2004, <http://news.bbc.co.uk/1/hi/technology/3475235.stm> (last accessed 20 February 2008).

Naraine, Ryan, *Massive DDoS Attack Hit DNS Root Servers* <www.internetnews.com/bus-news/article.php/1486981> (last accessed 6 September 2007).

National Archives, *Dambusters: The Legacy* <http://www.nationalarchives.gov.uk/dambusters/legacy.htm> (last accessed 21 August 2008).

'NATO Denies Targeting Water Supplies', *BBC News*, 24 May 1999, <http://news.bbc.co.uk/1/hi/world/europe/351780.stm> (last accessed 5 October 2007).

Nichiporuk, Brian and Builder, Carl H., 'Societal Implications' in Arquilla, J and Ronfeldt, D (eds), *In Athena's Camp* (RAND, Santa Monica, 1997) 295.

Noltimier, Hallan C, 'Techniques for Manipulating the Geosphere' in Westing, A H (ed) *Environmental Warfare: A Technical, Legal and Policy Appraisal* (Taylor & Francis, London, 1984) 25-31.

4 April 1949, *North Atlantic Treaty*, 34 UNTS 243.

Nuttall, Chris, 'Virtual Country 'Nuked' on Net', *BBC News*, 26 January 1999, <http://news.bbc.co.uk/1/hi/sci/tech/263169.stm> (last accessed 4 April 2003).

Nye, Joseph S., Jr, *The Paradox of American Power: Why the World's Only Superpower Can't Go It Alone* (Oxford University Press, Oxford, 2002).

, *OAU Convention for the Elimination of Mercenaries in Africa*, OAU Doc. CM/433/Rev.L Annex 1.

Oeter, Stefan, 'Methods and Means of Combat' in Fleck, D (ed) *The Handbook of Humanitarian Law in Armed Conflicts* (Oxford University Press, Oxford, 1995) 105-207.

_____, 'Comment: Is the Principle of Distinction Outdated?' in Heinegg, W H v and Epping, V (eds), *International Humanitarian Law Facing New Challenges* (Springer, Berlin; New York, 2007) 53-65.

Office of General Counsel, *An Assessment on International Legal Issues in Information Operations*, United States Department of Defense (1999) <http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf> (last accessed 30 January 2007).

O'Keefe, Roger, 'The Meaning of 'Cultural Property' under the 1954 Hague Convention' (1999) XLVI *NIL Rev* 26.

Osman Bin Haji Mohamed Ali and Another v the Public Prosecutor (1969) 1 AC 430, Privy Council.

Pace, Scott, et al., *The Global Positioning System: Assessing National Policies* (RAND, Santa Monica, 1995).

Parks, W. Hays, 'Air War and the Law of War' (1990) 32 *AFL Rev* 1.

Partial Award, Civilians Claims, Eritrea's Claims 15, 16, 23 & 27-32 between the State of Eritrea and the Federal Democratic Republic of Ethiopia (2004), Eritrea Ethiopia Claims Commission.

Partial Award, Loss of Property in Ethiopia Owned by Non-Residents, Eritrea's Claim 24 between the State of Eritrea and the Federal Democratic Republic of Ethiopia (2005), Eritrea Ethiopia Claims Commission.

PBS Frontline, *Cyberwar! The Warnings* <http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/> (last accessed 21 September 2008).

_____, *Interview with Peter Singer - Private Warriors* <http://www.pbs.org/wgbh/pages/frontline/shows/warriors/interviews/singer.html> (last accessed 13 September 2008).

_____, *Interview with Stephen Schooner - Private Warriors* <http://www.pbs.org/wgbh/pages/frontline/shows/warriors/interviews/schooner.html > (last accessed 13 September 2008).

PBS Frontline, *Private Warriors*, 2005.

Pessach, Guy, *Digital Art Museums - Legal Perspectives*, (2006) <http://islandia.law.yale.edu/isp/writing%20paper/digital_art.htm> (last accessed 9 June 2006).

Pictet, Jean S., *The Geneva Conventions of 12 August 1949: Commentary* (International Committee of the Red Cross, Geneva, 1952).

Pilloud, Claude, et al., *Commentary on the Additional Protocols of 8 June 1977* (Martinus Nijhoff, Geneva, 1987).

Poulsen, Kevin, 'Slammer Worm Crashed Ohio Nuke Plant Network' (2003) *Security Focus* 19 August 2003 <www.securityfocus.com/print/news/6767> (last accessed 31 October 2006).

'President's News Conference on Foreign and Domestic Issues', *New York Times*, 21 December 1983, 22.

Priest, Dana, 'Private Guards Repel Attack on US Headquarters', *Washington Post*, 6 April 2004, A01 <http://www.washingtonpost.com/ac2/wp-dyn/A53059-2004Apr5?language=printer> (last accessed 13 May 2006).

Prosecutor v Dario Kordic and Mario Cerkez (Appeal) (2004) Case No IT-95-14/2-A, International Criminal Tribunal for the Former Yugoslavia, Appeals Chamber.

Prosecutor v Dragoljub Kunarac et al (2002) (IT-96-23&23/1), International Criminal Tribunal for the Former Yugoslavia.

Prosecutor v Drazen Erdemovic (1997) IT-96-22-A, International Criminal Tribuanl for the Former Yugoslavia, Appeals Chamber.

Prosecutor v Dusko Tadic (1995) Case No. IT-94-1-AR, International Criminal Tribunal for the Former Yugoslavia, Appeals Chamber.

Prosecutor v Dusko Tadic (1997) 36 ILM 908, International Criminal Tribunal for the Former Yugoslavia.

Prosecutor v Jean-Paul Akayesu (1998) Case No. ICTR-96-4-T, International Criminal Tribunal for Rwanda.

Prosecutor v Kupreškic (2000) Case No: IT-95-16-T, International Criminal Tribunal for the Former Yugoslavia.

Prosecutor v Miodrag Jokic (Sentencing Judgement) (2004) Case No IT-01-42/1-S, International Criminal Tribunal for the Former Yugoslavia - Trial Chamber I.

Prosecutor v Mladen Naletilic and Vinko Martinovic (2003) Case No. IT-98-34-T, International Criminal Court for the Former Yugoslavia.

Prosecutor v Moinina Fofana and Allieu Kondewa (Decision on Preliminary Motion Based on Lack of Jurisdiction (Child Recruitment)). (2004) SCSL-04-14-T, Special Court for Sierra Leone.

Prosecutor v Norman (Decision on Preliminary Motion Based on Lack of Jurisdiction (Child Recruitment)) (2004) SCSL-04-14-AR72(E)-131, Special Court for Sierra Leone.

The Prosecutor v. Zejnil Delalic et al. (Celebici) (1998) Case No. IT-96-21-T, International Criminal Tribunal for the Former Yugoslavia.

Public Prosecutor v Koi et al (1968) AC 829, Privy Council.

Quéguiner, Jean-François, *Direct Participation in Hostilities under International Humanitarian Law*, Program on Humanitarian Policy and Conflict Research at Harvard University (2003) <http://www.ihlresearch.org/ihl/pdfs/briefing3297.pdf> (last accessed 13 September 2008).

R v Boden (2002) QCA 164, Court of Appeal of the Supreme Court of Queensland (Australia).

R v Wilkinson (1999) 1 NZLR 403, Court of Appeal (New Zealand).

Randelzhofer, Albrecht, 'Article 2(4)' in Simma, B (ed) *The Charter of the United Nations: A Commentary* (2nd ed, Oxford University Press, Oxford, 2002).

_____, 'Article 51' in Simma, B (ed) *The Charter of the United Nations: A Commentary* (2nd ed, Oxford University Press, Oxford, 2002) 788.

Reed, Thomas C., *At the Abyss: An Insider's History of the Cold War* (Presidio, New York, 2004).

Reisman, W Michael, 'Criteria for the Use of Force in International Law' (1985) 10 *Yale J Int'l L* 279.

Reuters, 'Cyber-War Rages over Iraq', *ZDNet News*, 31 March 2003, <Http://www.zdnet.com/newstech/security/stoty/0,2000024985,20273268,00.htm> (last accessed 31 March 2003).

'Rice Condemns Ongoing Cyber-Attacks as Estonian Embassy Siege Ends', *earthtimesorg*, 4 May 2007.

Rivard v United States (1967) 375 F 2d 882, U.S Ct. App., 5th Cir.

Roach, J. Ashley, 'The Law of Naval Warfare at the Turn of Two Centuries' (2000) 94 *AJIL* 64.

Robbat, Michael J, 'Resolving the Legal Issues Concerning the Use of Information Warfare in the International Forum: The Reach of the Existing Legal Framework, and the Creation of a New Paradigm' (2000) 6 *BUJ Sci & Tech L* 10.

Roberts, Adam and Guelff, Richard, *Documents on the Laws of War* (3rd ed, Oxford University Press, Oxford, 1999).

Robertson, Horace B., 'The Principle of the Military Objective' (1997-1998) 8 *US AF Acad J Legal Stud* 35.

_____, 'Self-Defense against Computer Network Attack under International Law' in Schmitt, M N and O'Donnell, B T (eds), *Computer Network Attack and International Law* (Naval War College, Newport, RI, 2002) 122-145.

Rodes, Jean-Michel, Piejut, Geneviève and Plas, Emmanuèle, *Memory of the Information Society* (UNESCO, Paris, 2003).

Rogers, A. P. V., *Law on the Battlefield* (2nd ed, Manchester University Press, Manchester, 2004).

Rojas, Peter, 'The Paranoia That Paid Off', *The Guardian* (London), 24 April 2003, 27.

Romanych, Marc J. and Krumm, Kenneth, 'Tactical Information Operations in Kosovo' (2004) September-October 2004 *Military Review* 56.

Sassòli, Marco, 'Targeting: The Scope and Utility of the Concept of "Military Objectives" for the Protection of Civilians in Contemporary Armed Conflicts' in Wippman, D and Evangelista, M (eds), *New Wars, New Laws?: Applying the Laws of War in 21st Century Conflicts* (Transnational Publishers, Ardsley, N.Y., 2005) 181-210.

Saxby, Stephen, *The Age of Information: The Past Development and Future Significance of Computing and Communications* (Macmillan, London, 1990).

Schmitt, Michael N., 'The Resort to Force in International Law: Reflections on Positivist and Contextualist Approaches' (1994) 37 *AFL Rev* 105.

_____, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework' (1999) 37 *Col J Trans L* 885.

_____, 'The Principle of Discrimination in 21st Century Warfare' (1999) 2 *Yale Hum Rts & Dev LJ* 143.

_____, 'Wired Warfare: Computer Network Attack and the *Jus in Bello*' in Schmitt, M N and O'Donnell, B T (eds), *Computer Network Attack & International Law* (U.S. Naval War College, Newport, R.I, 2002) 187-218.

_____, Bellum Americanum Revisited: US Security Strategy and the Jus Ad Bellum (28 February 2003), transcript available in 176 *Mil L Rev* 364-421.

_____, *The Impact of High and Low-Tech Warfare on the Principle of Distinction*, Program on Humanitarian Policy and Conflict Research at Harvard University (2003) <http://www.hpcr.org/publications/papers.php> (last accessed 18 December 2007).

_____, 'CNA and the Jus in Bello: An Introduction' (Paper presented at the International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, Stockholm, 17-19 November 2004) 101-125.

_____, 'Direct Participation in Hostilities and 21st Century Armed Conflict' in Fischer, H et al (eds), *Crisis Management and Humanitarian Protection* (Berliner WissenschaftsVerlag, Berlin, 2004) 505-529.

_____, 'Humanitarian Law and Direct Participation by Private Contractors or Civilian Employees' (2004) 5(2) *Chi J Int'l L* 511.

_____, 'Targeting and Humanitarian Law: Current Issues' (2004) 34 *Israel YB Hum Rts* 59.

_____, 'Fault Lines in the Law of Attack' in Breau, S and Jachec-Neale, A (eds), *Testing the Boundaries of International Humanitarian Law* (British Institute of International and Comparative Law, London, 2006) 277-307.

_____, 'International Law and Military Operations in Space' (2006) 10 *Max Planck UNYB* 89.

_____, 'Asymmetrical Warfare and International Humanitarian Law' in Heintschel von Heinegg, W and Epping, V (eds), *International Humanitarian Law Facing New Challenges: Symposium in Honour of Knut Ipsen* (Springer, Berlin; New York, 2007) 11-48.

Scott, Roger D., 'Legal Aspects of Information Warfare: Military Disruption of Telecommunications' (1998) 45 *Naval Law Review* 57.

Seffers, George I., 'Legalities Cloud Pentagon's Cyber Defence' (1999) *DefenceNews* 25 January 1999 3, 26.

Serabian, John A., Jr, Cyber Threats and the US Economy: Statement for the Record before the Joint Economic Committee on Cyber Threats and the US Economy (23 February 2000), transcript available in <https://www.cia.gov/news-information/speeches-testimony/2000/cyberthreats_022300.html> (last accessed 15 August 2008).

Sharp, Walter G., *Cyberspace and the Use of Force* (Aegis Research Corp., Falls Church, VA., 1999).

Shawhan, Karl J "Vital Interests, Virtual Threats: Reconciling International Law with Information Warfare and United States Security" (2001) School of Advanced Airpower Studies, Air University, Maxwell Air Force Base, Alabama, <http://www.maxwell.af.mil/au/aul/aupress/SAAS_Theses/Shawhan/shawhan.pdf> (last accessed 4 April 2003).

Shulman, Mark R, 'Discrimination in the Laws of Information Warfare' (1999) 37 *Col J Trans L* 939.

_____, *Legal Constraints on Information Warfare*, Center for Strategy & Technology, Air War Center, Occasional Paper No.7 (1999).

Simma, Bruno and Paulus, Andreas L., 'The Responsibility of Individuals for Human Rights Abuses in Internal Conflicts: A Positivist View' (1999) 93 *AJIL* 302.

Singer, P. W., *Corporate Warriors: The Rise of the Privatized Military Industry* (Cornell University Press, Ithaca, 2003).

_____, 'Outsourcing War' (2005) 84(2) *Foreign Affairs* 119.

Singer, Peter W., 'War, Profits, and the Vacuum of Law: Privatized Military Firms and International Law' (2004) 42 *Col J Trans L* 521.

Smith, Charles R, 'U.S. Information Warriors Wrestle with New Weapons' (2003) *NewsMaxcom* 13 March 2003 <http://www.newsmax.com/archives/articles/2003/3/12/134712.shtml> (last accessed 4 October 2007).

Smith, Edward A., *Effects Based Operations: Applying Network Centric Warfare to Peace, Crisis, and War* (DOD-CCRP, Washington, DC, 2002).

Smith, Rupert, *The Utility of Force: The Art of War in the Modern World* (Penguin, London, 2005).

Solf, Waldemar A, 'Comment: Non-International Armed Conflicts' (1981-1982) 31 *Am U L Rev* 927.

Steinkamm, Armin A., 'Pillage' in Bernhardt, R (ed) *Encyclopedia of International Law* (Max Plank Institute; North Holland, Amsterdam, 1982) 1029-1030.

Stewart, Joe, *Storm Worm DDoS Attack*, Secure Works (1997) <http://www.secureworks.com/research/threats/storm-worm> (last accessed 23 November 2007).

Stille, Alexander, *The Future of the Past: How the Information Age Threatens to Destroy Our Cultural Heritage* (Picador, Oxford, 2002).

Streltsov, Anatolij, 'Threat Analysis in the Post Cold-War Order' (Paper presented at the International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, Stockholm, 17-19 November 2004) 21-27.

Swiney, Gabriel, 'Saving Lives: The Principle of Distinction and the Realities of Modern War' (2005) 39 *International Lawyer* 733.

Symantec, *Symantec Global Internet Security Threat Report*, Symantec, Vol XIII (2008).

Symmetricon, *Why Convert to a SAASM Based Global Positioning System (GPS)?*, (2006) <http://www.symmttm.com/pdf/gps/SAASM_2006_wp.pdf> (last accessed 25 September 2007).

'Taiwan Plays Cyber War Games', *BBC News*, 7 August 2000, <http://news.bbc.co.uk/1/hi/world/asia-pacific/870386.stm> (last accessed 15 September 2007).

Terry, James P., 'The Lawfulness of Attacking Computer Networks in Armed Conflict and in Self-Defense in Periods Short of Armed Conflict: What Are the Targeting Constraints?' (2001) 169 *Mil L Rev* 70.

The Environment Agency, *The Thames Barrier: Flood Defence for London* <http://www.environment-agency.gov.uk/regions/thames/323150/335688/341764/> (last accessed 29 November 2006).

Thomas, T, 'Russia's Information Warfare Structure: Understanding the Roles of the Security Council, Fapsi, the State Technical Commission and the Military' (1998) 7 *European Security* 156.

Thornburgh, Nathan, et al., 'The Invasion of the Chinese Cyberspies (and the Man Who Tried to Stop Them)' (2005) 166(10) *Time* 34.

Todd, Bennett, *Distributed Denial of Service Attacks*, (2000) <http://www.linuxsecurity.com/resource_files/intrusion_detection/ddos-faq.html> (last accessed 29 January 2004).

Toffler, Alvin and Toffler, Heidi, *War and Anti-War: Survival at the Dawn of the 21st Century* (Warner Books, London, 1994).

_____, 'Foreword: The New Intangibles' in Arquilla, J et al (eds), *In Athena's Camp: Preparing for Conflict in the Information Age* (RAND, Santa Monica, 1997) xiii-xxiv.

Toman, Jirí, *The Protection of Cultural Property in the Event of Armed Conflict* (Dartmouth : UNESCO, Aldershot; Brookfield, Vt., 1996).

Traynor, Ian, 'Russia Accused of Unleashing Cyberwar to Disable Estonia', *The Guardian* (London), 17 May 2007, 1 <www.guardian.co.uk/print/0,,329864981-103610,00.html> (last accessed 20 August 2007).

_____, 'Web Attackers Used a Million Computers, Says Estonia', *The Guardian* (London), 18 May 2007, 30.

, *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies*, Vol. 610 No. 8843.

Trevelyan, Mark, 'Security Experts Split on "Cyberterrorism" Threat', *International Herald Tribune* (Paris), 16 April 2008, <http://www.iht.com/articles/reuters/2008/04/16/europe/OUKWD-UK-SECURITY-CYBERSPACE.php> (last accessed 19 April 2008).

Trial of Alfied Felix Alwyn Krupp Von Bohlen Und Halbach and Eleven Others (the Krupp Trial) (1948) X Law Reports of Trials of War Criminals 69, United States Military Tribunal, Nuremburg.

Trial of Alois and Anna Bommer and Their Daughters (1947) IX Law Reports of the Trials of the War Criminals 62, Permanent Military Court at Metz.

Trial of Carl Krauch and Twenty-Two Others (I.G. Farben Trial) (1948) X Law Reports of Trials of War Criminals 1, United States Military Tribunal, Nuremburg.

The Trial of Friedrich Flick and Five Others (the Flick Trial) (1947) IX Law Reports of Trials of War Criminals 1, United States Military Tribunal, Nuremburg.

U.K. Cabinet Office, *The National Security Strategy of the United Kingdom: Security in an Interdependent World*, U.K. Cabinet Office, Cm 7291 (2008).

U.K. Ministry of Defence, *The Manual of the Law of Armed Conflict* (Oxford University Press, Oxford; New York, 2004).

U.N. Economic and Social Council, *Report of the Working Group on a Draft Optional Protocol to the Convention on the Rights of the Child on Involvement of Children in Armed Conflicts in Its Sixth Session*, UN Doc. E/CN.4/2000/74 (2000).

U.S. Department of Defence, *Conduct of the Persian Gulf War: Final Report to Congress*, U.S. Department of Defence, (1992).

_____, *Dictionary of Military and Associated Terms*, Joint Publication 1-02 (2001) <http://www.dtic.mil/doctrine/jel/doddict/index.html> (last accessed 22 April 2008).

_____, *Information Operations*, Joint Chiefs of Staff, Joint Publication 3-13 (2006).

U.S. Department of Defense, *Dictionary of Military and Associated Terms (as Amended through 20 March 2006)* (Washington D.C., 2001).

U.S. Department of Homeland Security, *National Infrastructure Protection Plan*, U.S. Department of Homeland Security, (2006) <http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf> (last accessed 28 April 2008).

'U.S. Gov IP Addresses You Should Not Scan' (2007) *Hellbound Hackers* 21 June 2007 <http://www.hellboundhackers.org/articles/721-US-GOV-IP-ADDRESSES-YOU-SHOULD-NOT-SCAN.html> (last accessed 13 September 2008).

U.S. Joint Chiefs of Staff, *Information Warfare: A Strategy for Peace... The Decisive Edge in War*, (1996) <http://handle.dtic.mil/100.2/ADA318379>.

'UK Hacker 'Should Be Extradicted", *BBC News* (London), 10 May 2006, <http://news.bbc.co.uk/1/hi/technology/4757375.stm> (last accessed 6 July 2006).

UN Secretary General, *In Larger Freedom: Towards Development, Security and Human Rights for All*, United Nations, UN Doc. A/59/2005 (2005).

Convention for the Safeguarding of the Intangible Cultural Heritage, 17 October 2003, UNESCO General Conference, UNESCO.

United Nations, *A More Secure World: Our Shared Responsibility Report of the Secretary-General's High-Level Panel on Threats Challenges and Change*, United Nations, UN Doc. A/59/565 (2004).

United Nations War Crimes Commission, *Law Reports of Trials of War Criminals* (H.M.S.O. for the United Nations War Crimes Commission, London, 1949).

Vandewiele, Tiny, *Commentary on the United Nations Convention on the Rights of the Child, 46 Optional Protocol : The Involvement of Children in Armed Conflicts* (Martinus Nijhoff Publishers, Leiden; Boston, 2005).

Verton, Dan, 'Navy Opens Some It Ops to Vendors' (2000) *Federal Computer Week* <www.fcw.com/fcw/articles/2000/0821/pol-navy-08-21-00.asp> (last accessed 15 April 2004).

_____, 'The Prospect of Iraq Conflict Raises New Cyber Attack Fears' (2002) *Computerworld Hong Kong* 30 September 2002 <http://www.idg.com.hk/cw/readstory.asp?aid=20020930004> (last accessed 30 September 2002).

Vogel, Carol, '3 out of 4 Visitors to the Met Never Make It to the Front Door', *New York Times*, 29 March 2006, 18 <www.nytimes.com/2006/03/29/arts/artsspecial/29web.html?pagewanted=print> (last accessed 12 August 2006).

Wall, Andru E., *Legal and Ethical Lessons of NATO's Kosovo Campaign* (Naval War College, Newport, R.I., 2002).

Walzer, Michael, *Just and Unjust Wars: A Moral Argument with Historical Illustrations* (2nd ed, Basic Books, New York, 1992).

Watkin, Kenneth, *Combatants, Unprivileged Belligerents and Conflicts in the 21st Century*, HPCR (2003).

Webopedia: Online Dictionary of Computing & Internet <http://www.webopedia.com/> (last accessed 30 November 2007).

Wedgwood, Ruth G., 'Proportionality, Cyberwar, and the Law of War' in Schmitt, M N and O'Donnell, B T (eds), *Computer Network Attack and International Law* (Naval War College, Newport, RI, 2002) 219-232.

Weisburd, A. Mark, *Use of Force: The Practice of States since World War II* (Pennsylvania State University Press, University Park, Pa., 1997).

Weiss, Gus W., 'The Farewell Dossier: Duping the Soviets' (1996) 35(5) *Studies in Intelligence* 121 <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/96unclass/farewell.htm> (last accessed 29 June 2008).

Wertheim, Margaret, *The Pearly Gates of Cyberspace: A History of Space from Dante to the Internet* (W.W. Norton, New York, 1999).

White House, *The National Security Strategy of the United States of America*, White House (2002) <http://www.whitehouse.gov/nsc/nss.pdf> (last accessed 21 February 2004).

_____, *National Security Strategy of the United States of America*, White House, (2006) (last accessed 30 August 2008).

Wilson, Clay, 'Information Operations and Computer Network Attack Capabilities of Today' (Paper presented at the International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, Stockholm, 17-19 November 2004) 28-79.

_____, *Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues*, Congressional Research Service, RL31787 (2007).

Wingfield, Thomas C., 'Legal Aspects of Offensive Information Operations in Space' (1998) 9 *J Legal Stud* 121.

_____, *The Law of Information Conflict: National Security Law in Cyberspace* (Aegis Research Corp., Falls Church, VA, 2000).

World Bank, *World Development Report: Knowledge for Development*, World Bank (1998).

Zaleski, Jeffrey P., *The Soul of Cyberspace: How New Technology Is Changing Our Spiritual Lives* (HarperEdge, San Francisco, 1997).

Zamparelli, Steven J., 'What Have We Signed up For?: Competitive Sourcing and Privatization - Contractors on the Battlefield' (1999) XXIII(3) *AFJ Log* 9.

Zanardi, Pierluigi L., 'Indirect Military Aggression' in Cassese, A (ed) *The Current Legal Regulation on the Use of Force* (Martinus Nijhoff, Dordrecht, 1986) 111-119.

ZDNet, 'Cyberterrorism: The Real Risks', 27 August 2002, <http://news.zdnet.co.uk/internet/0,1000000097,2121358,00.htm> (last accessed 21 September 2008).