1 The world in which we live and fight

On 16 May 1943 one of the most famous missions of World War II, 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; however it was at the cost of eight bomber crews lost during the mission.[1] Fifty-five years later, according to some reports, 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 that are dependent on critical infrastructures that are not adequately protected against this new method of attack.

[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*, www.nationalarchives.gov.uk/dambusters/legacy.htm (last accessed 15 July 2011).

[2] Barton Gellman, 'Cyber-Attacks by Al Qaeda Feared', *Washington Post* (Washington DC), 27 June 2002, A01. Although 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

The most recent example is the Stuxnet worm which is widely believed to have caused significant damage to approximately 1,000 centrifuges at Iran's Natanz nuclear enrichment facility in June 2010.[3] For commentators who had questioned the veracity or significance of previous incidents circulating in the public domain, Stuxnet served as a declaration that cyber warfare had finally come of age. Although widely touted as the first cyber war in the media, the denial of service attacks, which took place against Estonia in 2007 and Georgia in 2008, did not cause physical damage and later came to be seen as criminal attacks. However, the incidents offered concrete examples to analysts and commentators working in the field and focused the minds of national policy makers. In recent years states and international organisations have become increasingly aware of the threats and challenges presented by cyber security and the urgency with which these issues need to be addressed. The national security strategies of states such as the United States and the United Kingdom now reflect the central role of cyber security in their planning;[4] likewise, each of these countries has recently created cyber commands within either the armed forces or intelligence agencies to address the threat.

This book examines the laws governing the resort to force and the conduct of hostilities as they relate to one of the newest forms of warfare, computer network attacks. Computer network attacks 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 networks themselves'.[5] The book is divided into two parts. Part I addresses the *jus ad bellum*; it examines computer network attacks as prohibited acts and the permitted responses to such acts under international law. Chapter 2 first looks at the qualification

hacker (detailed in Appendix 1), the example serves to illustrate the change in the method of warfare, and the comparative ease of achieving the same effect.

[3] See, for example, Kim Zetter, 'Surveillance Footage and Code Clues Indicate Stuxnet Hit Iran', *Wired* 16 February 2011, Threat Level, www.wired.com/threatlevel/2011/02/isis-report-stuxnet/# (last accessed 10 April 2011); David Albright, Paul Brannan and Christina Walrond, *Did Stuxnet Take out 1,000 Centrifuges at the Natanz Enrichment Plant?* Institute for Science and International Security (2010) (hereafter ISIS Stuxnet Report).

[4] UK Cabinet Office, *A Strong Britian in an Age of Uncertainty: The National Security Strategy* (Cmd 7935 ed., The Stationery Office, London, 2010); White House, *National Security Strategy* (2010), www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf (last accessed 15 July 2011).

[5] US Department of Defense, *Dictionary of Military and Associated Terms, 8 November 2010 (as amended through 31 January 2011)* (Washington DC, 2010).

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 then 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 complex issue of the attribution of attacks, a particular problem for a method of warfare that generally relies on anonymity, and the right of states to act in self-defence against non-state actors. The chapter also addresses other possible responses to computer network attacks that do not allow for self-defence, namely countermeasures, and considers the role of computer network attacks both as threats to the peace and possible responses under the collective security regime of the United Nations. Part II of the book 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 discusses under what circumstances the law of armed conflict will apply to computer network attacks. The remaining chapters examine the themes of participants in conflict, targeting and legitimate military objectives, precautions in attack and defence, measures of special protection, and means and methods of warfare (including the law of weaponry).

The book is not, however, limited to a point-by-point analysis of the current laws of armed conflict. The rise of computer network attacks as both a means and method of warfare is born out of, and in turn has influenced, many different societal and military trends. Therefore any attempt to analyse how the laws of armed conflict should affect this form of warfare must 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, any attempt to limit such work to present capacity and ignore trends would be foolhardy at best.[6] The book 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

[6] 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.

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.

1. Computer network attacks

Computer network attacks 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 networks themselves.[7] The defining feature of this form of 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 disrupt or destroy a network, but instead use electromagnetic energy, usually in hardwired weapons such as electromagnetic pulse (EMP) generators or jammers to achieve their aims.[8] A computer network attack 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 in the past,[9] on the whole it appears that these concerns stem from a narrow interpretation of the concept of 'information' in the context of the definition.[10] 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

[7] US Department of Defense, *Dictionary of Military and Associated Terms, 8 November 2010 (as Amended through 31 January 2011)* (Washington DC, 2010).

[8] 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 counteraction 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', *Framsyn Magazine* April 2005, www.foi.se/FOI/templates/Page____4554.aspx# (last accessed 12 April 2011).

[9] 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.

[10] 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), 141–71, 144.

opinion.[11] Indeed the US military definition of information is 'facts, data or instructions in any medium or form'.[12] 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.

The term computer network attack thus covers a broad range of hostile techniques involving computer code. Such malicious software (malware) can cause extensive disruption, as in the case of the denial of service attacks which hit Estonia, or physical destruction, as with the Stuxnet worm in Iran; both incidents are discussed in detail in Chapter 2. Distributed denial of service (DDoS) attacks, although disruptive, are a fairly unsophisticated method of attack and are usually carried out through the use of a botnet through which a single controller can harness the power of many computers. The attack floods a specific target with requests for service, so that either the target shuts down in the wake of its inability to cope with the incoming messages, or the target is effectively blocked to legitimate requests as the attack exhausts the resources available to the target to handle legitimate requests.

These types of attacks are capable of shutting down websites, servers and backbone nodes; generating massive email and spamming campaigns; and disseminating viruses.[13]

Computer network attacks which cause physical effects, such as the Stuxnet worm, often target the control systems which regulate the 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. These control systems regulate most of the critical infrastructure and have proven particularly vulnerable to attack.[14] Prior to the Stuxnet worm's discovery, there were several incidents to which commentators could point to illustrate the physical threat from computer network attacks, but all required audiences to extrapolate and connect the dots.

[11] For a full definition see 'Information', *A Dictionary of Computing* (Oxford University Press, 2004).
[12] US Department of Defense, *Dictionary of Military and Associated Terms*.
[13] Eneken Tikk, Kadri Kaska and Liis Vihul, *International Cyber Incidents: Legal Considerations*, Cooperative Cyber Defence Centre of Excellence (2010), 112.
[14] Supervisory control and data acquisition (or SCADA) systems and distributed control systems (DCS) are two examples of control systems that are often mentioned in the literature.

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.[15] The attack sent the generator out of control and ultimately caused it 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.[16] One of the earliest reported incidents of this kind of computer attack, the so-called 'Farewell Dossier' incident, took place in 1982 during the Cold War; however, it only came to light once the incident was declassified in 1996. 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:[17]

> [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.

Control systems were again compromised in the 1998 Arizona Roosevelt Dam example cited previously. In another domestic example, in 2000 a disgruntled former employee, Vitek Boden, hacked the control system of the water and sewerage treatment plant in Queensland, Australia. Over a two-month period Boden accessed the system forty-six 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.[18] Incidents such as these have made states increasingly aware of the amount of critical infrastructure that is controlled by computers and their vulnerability to computer network attacks. The result

[15] 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 15 July 2011).

[16] *Ibid*. Footage of the generator is available at www.youtube.com/watch?v=fJyWngDco3g (last accessed 23 June 2010).

[17] Thomas C. Reed, *At the Abyss: An Insider's History of the Cold War* (Presidio, New York, 2004), 269; for a first-hand account see Gus W. Weiss, '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 12 April 2011).

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

has been the increasing emphasis on cyber attacks as one of the major threats to both the US and UK critical infrastructure in recent reports.[19]

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.[20] That attack combined electronic attack techniques in the form of brute-force jamming, precision missiles to eliminate the facility itself and, most interestingly, computer network attack techniques. The ability of non-stealthy Israeli aircraft to penetrate Syrian airspace without interference rests in part on technology, carried on board modified aircraft, which allowed specialists to hack into Syria's networked air defence system.[21] As one commentator noted, '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'.[22] Israel is not the only state to have developed this technology. The US 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.[23] The US version of the system has at the very least been tested operationally in Iraq and Afghanistan, most likely against insurgent communication networks.[24]

[19] US Department of Homeland Security, *National Infrastructure Protection Plan*, US Department of Homeland Security (2009), www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf (last accessed 4 July 2011); UK Cabinet Office, *The National Security Strategy of the United Kingdom: Security in an Interdependent World*, UK Cabinet Office, Cm 7291 (2008).

[20] David A. Fulghum, Robert Wall and Amy Butler, 'Cyber-Combat's First Shot: Attack on Syria Shows Israel Is Master of the High-Tech Battle' (2007) 167(21) *Aviation Week & Space Technology* 28.

[21] David A. Fulghum, Robert Wall and Amy Butler, 'Israel Shows Electronic Prowess', *Aviation Week & Space Technology* 25 November 2007, www.aviationweek.com/aw/generic/story_channel.jsp?channel=defense&id=news/aw112607p2.xml&headline=Israel%20Shows%20Electronic%20Prowess (last accessed 12 April 2011).

[22] *Ibid*. [23] *Ibid*.

[24] David A. Fulghum and Douglas Barrie, 'Israel Used Electronic Attack in Air Strike against Syrian Mystery Target', *Aviation Week & Space Technology*, 8 October 2007,

The computer network attacks launched against Georgia in 2008, although not attributed to the Russian authorities, also demonstrate the utility of attacks launched in support of conventional strikes. In those attacks a high degree of coordination was observed between computer network attacks against targets in specific locations and their conventional bombardment. This approach prevented the Georgian authorities from keeping information flowing during a critical period both to the international media and to its own residents.[25] Other hypothetical examples include the use of computer network attacks 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. Alternatively, 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 front line. These examples are a few of the more commonly cited; many more are possible.

2. Law and war in the internet age

Raymond Ku has noted that with each controversy involving the internet, the law is forced to confront cyberspace on two levels.[26] 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.[27] 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.[28] 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

www.aviationweek.com/aw/generic/story_channel.jsp?channel=defense&id=news/aw100807p2.xml (last accessed 12 April 2011).

[25] See generally Tikk, Kaska and Vihul, *Cyber Incidents*, 66–89.

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

[27] *Ibid.* [28] *Ibid.*, 129.

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 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, both as participants and 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.[29] However, while that may be an ideal solution for application to domestic law issues, such an argument cannot work at the international level. 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; in respect of the use of force it is the balancing of rights and obligations of states, and, most obviously in the case of the laws of armed conflict, the balance between humanitarian principles and military necessity.[30] 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 book

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

[30] The classic statement of this latter balance is found in the Preamble of the St Petersberg Declaration, *Declaration Renouncing the Use, in Time of War, of Explosive Projectiles under 400 Grammes Weight (St Petersburg Declaration)*, 29 November/11 December 1868.

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, nevertheless, just one facet of the larger civilisational shift, and it needs to be understood in that context.'[31] This view is shared by British military historian Jeremy Black:[32]

> … 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, the context of warfare defines it more than the military technology it utilises.

The 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.[33] As Dinstein points out, these humanitarian concerns are shaped by the global *zeitgeist*, and affect the law though influencing the practice of states and the drafters of treaties.[34] The information revolution, and

[31] 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.

[32] 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.

[33] 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, Geneva, The Hague, 1984), 265–80, 265.

[34] Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict* (2nd edn, Cambridge University Press, 2010), 4.