

# Contents

<i>List of Tables</i>	x
<i>Preface</i>	
<i>Gary Chapman, Diego Latella and Professor Carlo Schaerf</i>	xi
<i>Notes on the Contributors</i>	xiii
<i>Glossary</i>	xvii

## **Part I: Cyberwar, Netwar and the Revolution in Military Affairs: Defining the Issues**

<b>1 Defining the Issues</b>	<b>3</b>
<i>Dr Philippa Trevorrow, Dr Steve Wright, Professor David Webb and Dr Edward Halpin</i>	
<b>2 Virtual Violence and Real War: Playing War in Computer Games: The Battle with Reality</b>	<b>12</b>
<i>Martin Bayer</i>	
2.1 Introduction	12
2.2 Gaming platforms	13
2.3 Definition and historical context	15
2.4 Computer game genres	17
2.5 Realism versus reality	21
2.6 Games and professional military simulations	25
2.7 Conclusion	27
<b>3 Strategic Information Warfare: An Introduction</b>	<b>32</b>
<i>Gian Piero Siroli</i>	
3.1 Introduction	32
3.2 Context	33
3.3 Critical infrastructures	35
3.4 Vulnerabilities	37
3.5 Actors: how and who	41
3.6 Open questions and comments	43
3.7 Conclusions	45

## Part II: Implications of the Problem

<b>4</b>	<b>Virtuous Virtual War</b>	<b>51</b>
	<i>Jari Rantapelkonen</i>	
4.1	Introduction	51
4.2	Theory, information technology and accident	52
4.3	War on terrorism – the state of emergency	55
4.4	The necessity and problematics of an enemy	56
4.5	War on Afghanistan – from postmodern moments to information isolation	58
4.6	Battle for the strategic truth	60
4.7	War on Iraq – differences in perceptions	61
4.8	The fog of peace	67
<b>5</b>	<b>Risks of Computer-Related Technology</b>	<b>72</b>
	<i>Dr Peter G. Neumann</i>	
5.1	Introduction	72
5.2	Roles of technology	78
<b>6</b>	<b>Missile Defence – The First Steps Towards War in Space?</b>	<b>82</b>
	<i>Professor David Webb</i>	
6.1	The military use of space	82
6.2	Anti-satellite (ASAT) programmes	84
6.3	Current US developments	87
6.4	Missile defence	89
6.5	The possibility of space weapons control	92
<b>7</b>	<b>Technology as a Source of Global Turbulence?</b>	<b>98</b>
	<i>Dr Stefan Fritsch</i>	
7.1	Introduction	98
7.2	Realistic and neorealist approaches to technology	99
7.3	Interdependent globalism	100
7.4	Technology and IR/IPE from a constructivist point of view	102
7.5	Arguments for a broader perspective on technology	103
7.6	Multidimensional effects of technology	104
7.7	Conclusion	106
<b>8</b>	<b>Nuclear Weapons and the Vision of Command and Control</b>	<b>113</b>
	<i>Dr Bruce D. Larkin</i>	
8.1	The White House and the Department of Defense (DoD)	114
8.2	The White House Communications Agency	115

8.3	Crisis experience: the attempted assassination of President Ronald Reagan	116
8.4	Crisis experience: The September 11 attack	117
8.5	The Global Command and Control System (GCCS) (as defined by the DoD)	119
8.6	GCCS-T: the top secret provision for nuclear operations	120
8.7	Ongoing transformation of command and control systems	121
8.8	War experience: the Iraq War (2003–...)	123
8.9	Is GCCS sufficiently reliable for nuclear operations?	124
8.10	Is SIPRNET sufficiently secure for nuclear operations?	125
8.11	Assessment	130
<b>9</b>	<b>Information Warfare and the Laws of War</b>	<b>139</b>
	<i>Geoffrey Darnton</i>	
9.1	Introduction	139
9.2	Information Warfare (IW)	141
9.3	Laws of war	144
9.4	Key issues	151
 <b>Part III: Country Perspectives</b>		
<b>10</b>	<b>RMA: The Russian Way</b>	<b>157</b>
	<i>Fanourios Pantelogiannis</i>	
10.1	Historical overview	157
10.2	The current Russian RMA and its international consequences	159
10.3	Conclusion and evaluation	166
10.4	Perspectives	167
<b>11</b>	<b>An Overview of the Research and Development of Information Warfare in China</b>	<b>173</b>
	<i>Chris Wu</i>	
11.1	Introduction	173
11.2	Theoretical research on Information Warfare in China	174
11.3	Current IW development in China	182
11.4	IW tactics that could be used by Beijing to attack Taiwan	189
11.5	Combination of US and Taiwanese resistance to IW from Beijing	191

11.6	The possibility of IW between China and the USA	191
11.7	Conclusion	193

## **Part IV: What is Being Done – or Must Be Done?**

<b>12</b>	<b>A Bridge Too Far?</b>	<b>199</b>
	<i>Mike Moore</i>	
12.1	Global engagement	201
12.2	A space Pearl Harbor?	204
12.3	Space cop	206
12.4	The security dilemma	208
12.5	A mind experiment	210
12.6	Velvet glove, steel fist	212
12.7	Unintended consequences	213
12.8	'Last, best hope'	216
<b>13</b>	<b>Threat Assessment and Protective Measures: Extending the Asia–Europe Meeting IV Conclusions on Fighting International Terrorism and Other Instruments to Cyber Terrorism</b>	<b>219</b>
	<i>Massimo Mauro</i>	
13.1	Introduction	219
13.2	The Asia–Europe Meeting (ASEM) framework	219
13.3	Cyber terrorism: an urban legend?	220
13.4	A taxonomy of real cyber threats	222
13.5	Advanced defensive methods and different regional priorities	224
13.6	International and regional cooperation against cyber terrorism	224
13.7	Concluding statement	225
<b>14</b>	<b>Policy Laundering, and Other Policy Dynamics</b>	<b>228</b>
	<i>Dr Gus Hosein</i>	
14.1	Introduction	228
14.2	At the international level: the Council of Europe and the G8	230
14.3	At the national level	232
14.4	The international–national dance: traffic data retention	234
14.5	Democratic challenges and international opportunities	236
14.6	Concluding remarks	239

<b>15 Conclusion</b>	<b>242</b>
<i>Dr Steve Wright, Dr Philippa Trevorrow, Professor David Webb and Dr Edward Halpin</i>	
<i>Index</i>	246

# 1

## Defining the Issues

*Dr Philippa Trevorrow, Dr Steve Wright,  
Professor David Webb and Dr Edward Halpin*

The purpose of this book is to explore key emergent information technology developments for managing conflict, waging war and creating dysfunction within modern societies which are dependent on continuous information flows. It considers how the challenge is being addressed and assesses the longer-term implications and risks of these new approaches to conflict management and control. It is essentially composed of four substantive parts. Part I seeks to define the issues. Part II explores the implications of the problem and Part III presents some different (non-western) country perspectives. Finally, Part IV questions what is being done and must be done if we are to avoid being overwhelmed by competing and contradictory paradigms. The conclusion takes a tentative glimpse at innovations on the horizon and the social and political implications and ramifications.

Cyberwar, Information Warfare (IW), Netwar and the Revolution in Military Affairs (RMA) are terms that have been widely used by military observers for over a decade. In the early 1990s, in the immediate post-Cold War World, researchers such as Ronfeldt and Arquilla<sup>1</sup> who worked for the Rand Corporation, gave an account of what they saw as a new 'high-tech' model of warfare. The theory created by them had already gained credibility within the US military establishment by 1995,<sup>2</sup> though recent writers have claimed that the theoretical arguments are flawed and incomplete.<sup>3</sup> Much of the early discussion was either devoted to the threat to society posed by freelance hackers, or investigated broader theoretical possibilities. Similarly, the debate on the RMA was essentially a speculation in futuristic possibilities which did not yet have a public budget line attached. All that has now changed.

Whilst the attacks of September 11 2001 have been identified as the key events in transforming individual state perspectives on these matters, such a view is largely an exaggeration. A great many other factors have also changed the military paradigms associated with the Cold War. Modern weapons are increasingly being seen as systems where the warheads and

delivery mechanisms are just one component – the muscle deployed by a sophisticated and intelligent cybernetic nervous system. Real-time target acquisition data are handled through complex networks of communication, command and control systems (C3I), and war fighters recognise that it is becoming more effective to attack these information systems directly. The manner in which an efficient and effective attack can be launched on a telecommunications infrastructure may require different strategies and employ different weapons – including ones that fire electrons rather than hot pre-fragmented metal and explosives. The fact that modern societies, and their accompanying militaries, are increasingly dependent on an information infrastructure has inevitably led to a deepening analysis of what is appropriate in exploring future threats, vulnerabilities and opportunities. As a former US Air Force Chief of Staff succinctly put it: ‘dominating the information spectrum is as critical to conflict now as occupying the land or controlling the air has been in the past.’<sup>4</sup>

An additional factor is the extent to which a new military ideology of ‘non-lethal weaponry and tactics’ has begun to permeate military thinking, so that it became a formal North Atlantic Treaty Organization (NATO) commitment in 1998. Such so-called ‘soft kill’ approaches are always backed up with lethal force but the ideology is persuasive: why not take cities intact instead of pulverizing them into expensive rebuilding sites? So, the development of strategies and technologies which can incapacitate other technologies form an integral part of such thinking. Whilst September 11 has accelerated the pace of such logic, ‘homeland security models’ have also increased the pace of dedicating budget lines to specific procurement plans to fulfil what the US is now referring to as ‘full spectrum dominance’.

This paradigm shift has set new levels to US military thinking and budgets on the ‘information battle-space’. IW is no longer seen as an amateur Sunday league adventure in hack activism, but a highly legitimate premier division activity of the world’s most dominant militaries with logistics and new directed energy weapons to match. Indeed, superficially it is hard to distinguish ideas from science fiction from today’s interactive war game entertainment but there are significant differences.

Martin Bayer’s exploration of ‘Virtual Violence and Real War’ finds that, despite the outstanding audio-visual effects of modern computer war games, they are by no means either realistic or authentic. This is contrary to a media propensity to present stories of the effective use of war games for the simulation of, and preparation for, actual battle. Virtual soldiers can carry huge amounts of kit, restocking and recovery is only a button push away and their simulated precision weapons always hit their targets. In reality, soldiers do not have the certainty of ‘bullseye warfare’ and they sit around much of the time or are engaged in repetitive, mundane tasks. These entertaining toys can lead to misconceptions of military activity which do not carry from the play station to the battlefield. New units are not easily

repaired and soldiers are legally obliged to take care of civilians, not blast prisoners of war (PoWs) or refugees at every opportunity. In the future, the key military targets will not be personnel, but the electronic nervous system used to coordinate and control their behaviour – including computer networks and the Internet. Clearly, the international community needs to be prepared to meet more professional threats to the infrastructure of the Internet, individual networks, servers and so on. The question then arises as to who the key players are in the arena of electronic conflict.

Gian Piero Siroli answers this question with a perceptive introduction to IW. The dependency on information infrastructures is emphasized with the targeting of information systems and telecommunication networks becoming an important element in the defence policies of many countries. Siroli sees the exploitation of advanced IT by the military as an important driver in the quest for new warfighting techniques. For Siroli, 'information warfare is the set of activities intended to deny, corrupt or destroy an adversary's information resources including both offensive and defensive operations'.

The second substantive part of the book examines the implications of the problem of the ubiquitous dependency on information technology and the various vulnerabilities and raises many value-laden issues.

Jari Rantapelkonen cautions us about the presentation of 'Virtuous Virtual War'. The war against terrorism is not an issue of territory, he argues; rather, it is a media creation in which virtual world technology is bestowed with a virtuous or ethical dimension. It is no coincidence that in 2001 the Rendon group was hired by the Pentagon to create a positive image of new forms of warfare. Virtuous war is equated with virtual war as presented on computer networks – essentially a Military Industrial Media Entertainment (MIME) approach which disarranges reality. 'Information bombs' do not simply destroy capacity; they can also wipe out social memories, relations and international communities. Within the RMA are advanced information networks which can misinform as well as inform, large numbers of people and can facilitate the rapid dissemination of myths and rumours which cannot be verified. The literal 24/7 coverage of the Iraq War blurred the boundaries between reality and fiction. Rather than providing useful information and analysis which can be applied to establish verisimilitude, repetition can be used to reinforce one particular set of perceptions.

Peter G. Neumann in his chapter on the 'Risks of Computer-Related Technology' draws our attention to the fact that almost everything we do nowadays is dependent on computer technology. How should we deal with this? We need reliable, secure, highly available systems. What we have in fact are networks which are highly vulnerable and have many weak links. The Internet, he reasons, is a source of tremendous benefit and yields increasing opportunities for third world development, world wide commerce, education, and information flow. And yet it can offer very little resistance to coordinated

attacks since little effort has been spent on making its architecture robust. Other threats to future availability and integrity include the desire of many governments to control and regulate the Web, corporations to profit from it and a general lack of management to smooth out glitches and thwart spam and the multiplicity of pornographers, swindlers, identity thieves and snoopers who increasingly inhabit cyberspace. For Neumann, the challenge is how to retain the rich opportunities offered by the Internet, whilst restraining its risks, hazards and failures.

Neumann offers us examples of computer-based failures in defence, space, aviation, environment, telecommunications, transportation, medical systems, elections, security, privacy and law enforcement, to name but a few. If we recognise that these risks are an inherent part of new systems then we might be able to build robust systems, deal with our dependencies and prevent system failure. This could become critical when algorithmic and identity recognition systems give us access to many of the goods and services we take for granted. So far, research on robust systems has been ignored in favour of market-driven developments. This lack of vision will become critical as our defence postures are underpinned by their increasing reliance on vulnerable ICT systems.

However, despite failures, and financial and technological setbacks, many US defence programmes are continuing apace.

Dave Webb takes a look at 'Missile Defence' and asks whether this system is merely a by-product of the 'first steps towards war in space?' Webb also takes note of the increasing reliance of the military on space-based systems and examines the vulnerability of these systems to attack. It is this vulnerability that leads to the desire of the US Space Command to control space and position itself so that it can deny access of space to others when it deems necessary. The accelerating US investment in military space technology generally, and anti-satellite systems in particular, are indicators of this aspect of RMA, although, as Webb points out, the increase in traffic may be too demanding on the available bandwidth and it may not be possible to accomplish everything desired to make such plans work. Furthermore, all space-based satellite systems, as well as being costly, remain vulnerable to attack from anti-satellite systems. However, that has not stopped the USA from cultivating cooperation with the UK, Denmark, Greenland and Alaska, Poland, the Czech Republic, Hungary, Romania, Bulgaria, Australia, Russia and Japan. The promise of research and development (R&D) contracts have provided powerful incentives and only Canada has pulled away from involvement.

Stefan Fritsch develops the consequences of this idea further by identifying 'Information and Communication Technologies as a Source of Turbulence'. He uses three theoretical approaches based on IR/IPE (International Relations/International Political Economy) theory, namely: (i) realism/neorealism; (ii) interdependent globalism; and (iii) constructivism, to model the power of modern Information and Communication Technologies (ICTs) to

narrow the sovereign political action of most states. Consequently, many nations have lost powers and shed responsibilities to a range of new actors, including multinational companies, nongovernmental organizations (NGOs) and so on. In many senses, the technology is transforming social reality whilst still being dependent on wider social contexts. Fritsch ends with a series of questions about whether or not such techno-processes are deterministic. These kinds of considerations taxed many of the authors in their examination of what pragmatic measures can be taken to manage some of the more negative consequences of modern security becoming ever dependent on bandwidth.

Bruce D. Larkin further explores the consequences of being reliant on an extremely high-tech Global Command and Control System (GCCS) for the launch of nuclear weapons. Although we are asked to believe that such systems are highly protected, impenetrable and foolproof, Larkin points out that other sophisticated US surveillance and communications systems have failed when tested in battle. He cites US aircraft attacking US units working with the Kurds during the last Iraq war. In exploring the prerequisites of the ideal security arrangements for a GCCS, Larkin concludes that cost will be one of the biggest inhibitors in actually meeting the technological requirements to make any such system failsafe.

Geoffrey Darnton explores the international legal restraints on ambitions to dominate the global information spaces. Darnton finds that although IW is covered by the laws of war in parts, this treatment is comparatively underdeveloped. How can existing international law be applied to situations and practices that were not even envisioned at the time when treaties, conventions and protocol agreements were being drawn up? Darnton identifies specific treaties that lend themselves to reinterpretation in the light of advances in the role and function of ICTs, but he also identifies many of these as second-order consequences. For example, the development of longer, thinner supply chains and communication lines are more vulnerable than the less efficient but more robust systems that they replace. The breaching of these chains of supply would create serious disruption and potential civil disorder. Darnton concludes that clear improvements are required to provide a proper international framework covering IW but asks, 'Who would enforce it?'

Part III examines differing country perspectives. Whilst much of this book is concerned with the increasingly imperial US perspective of dominating the 'information battle space', it is not surprising that other members of the UN Security Council do not share this supremacist approach and are evolving their own plans along similar lines.

Fanourios Pantelogiannis further explores the situation from the point of view of the Russian Federation. Whilst Soviet thinkers were the first to postulate and analyse the implications of the ongoing RMA, Russia is now a power in decline and their defeat in Afghanistan led to a reappraisal of the country's military priorities. In this case firepower alone proved to be insufficient,

and it became more important to invest in command, communication computer infrastructure, surveillance, reconnaissance and electronic warfare. With a sense of being left behind, the former Soviet military commanders looked at new weapons technologies and compared these advances with Russian military hardware, which was rapidly becoming outdated.

Russia is under no illusion that refinancing their information infrastructure, satellites, and so on, is vital if they are not to be left behind. Yet much of Russia's current capacity is old fashioned and decreasing – which impacts on every area of strategic intelligence, including real time communications, early warning and so on. Some of Russia's drive towards refinancing their military telecommunications infrastructure has come from missile and nuclear technology exports although this proliferation to other vying powers (such as China, Iran, Indonesia and India) has not met well with the US who sees it as destabilising.

Russia has also recognised the growing importance of IW as a means to not only enhance the political and psychological impact of its operations but also as a way of increasing the effectiveness and precision of all its available weapons systems. Not all Russian military commanders share these new views. Whether the Russian RMA can be sustained will in part depend upon the availability of adequate funding, as well as the extent to which institutional resistance to reform inside the services can be effectively maintained.

Chris Wu considers the historical development and current priorities of China as it prepares for IW. He describes the new methodologies and systems being developed by the Chinese for waging IW – new advances in radar, satellites and computer systems are being augmented by the development of hard weapons such as killer satellites, electric guns and cruise missiles. Wu also points out the difficulties and disadvantages that China faces in the race to keep up with IW techniques. Lack of training, experience, resources and facilities has meant that China has lagged behind the USA. Indeed, China has, in the past, relied heavily on the results of US experience and products to develop their own systems. Wu notes that this reliance has contributed to the vulnerability of Chinese systems which have little in-built protection against hostile attack. Finally, he outlines a possible scenario of IW tactics that could be deployed by Beijing against Taiwan in which he illustrates a severe disparity in the balance of forces between the two. He poses the question 'How can this disparity be reduced in order to safeguard the security of Taiwan?' and makes two suggestions involving the strengthening of the Taiwanese systems and more direct collaboration with US systems (including anti-satellite systems) to enable them to participate fully in IW at all levels.

The final section of this book deals with the practical challenge of 'what is being or must be done' to manage our individual and collective vulnerability to the threats and opportunities of modern information driven state security systems?

Mike Moore also addresses this autonomous, unaccountable drive towards high-tech dominance as 'A Bridge too Far?' He revisits some of the precision 'bullseye' warfare themes introduced by other contributors and the move by the USA to be the only imperial space power. The roots of this thinking were already evident in the 1950s – but not the satellite technology. Now US military superiority is increasingly turning towards a dogged unilateralism and bilateral arm twisting. R&D contract seduction, identified by other authors in relation to missile defence, is being paralleled by policy laundering in the name of the 'war against terror'. Moore poses the question: 'If one state becomes so powerful globally, how do other states retain full national sovereignty?' This is essentially the running theme of this book. In a time of terror, security debates become increasingly polarized into puerile debates – are you for or against us? Such simplifications engender a climate where technology can be presented as offering something concrete to protect us from a growing international turbulence and sense of decreasing security. If this is a 'bridge too far' then the fact that it is happening against an Orwellian backdrop of permanent war should set alarm bells ringing for the fate of every hard-won limit on the excesses of war and state power which protect us from barbarism. What then should happen next?

Massimo Mauro of the European Commission (EC) looks at the informal cooperation taking place between the European member states and ten Asian countries to further clarify and assess future threats arising from cyber terrorism. In 2002 cyber security was seen as a key priority by ASEM (Asia–Europe Meeting) – the process designed to collectively address these issues, including measures to protect critical information infrastructure and to maintain the balance between the needs of national security and law enforcement with those of the business community which depend on privacy and confidentiality. So far, cyber attacks seem to originate from: so-called 'script kiddies', the lowest form of hacker doing mischief with programmes; financial criminals who penetrate economic systems by stealth, hoping for financial benefits (many of whom are insiders); and political opponents who attack a specific country or organization's website to deny access or use. Nevertheless, Mauro argues that the international community needs to be prepared to meet more professional threats to the Internet infrastructure, individual networks, servers and so on. But the question remains as to who the principal enemy is and what mechanisms are being evolved to rank other national spending priorities accordingly?

Gus Hosein identifies a growing trend for such priorities to be heavily influenced by agenda-setting procedures external to most states. What results is 'Policy Laundering and other Policy Dynamics'. By this Hosein means that policy makers use other jurisdictions to further to their goals. The tactics also include modelling – whereby governments shape laws based on laws in other jurisdictions – and forum shifting – where actors pursue inter-governmental organizations (IGO) rules that suit their interests, then

shift to other IGOs when challenges or opposition arises. Hosein sees the emergence of new policy dynamics when national consultative processes either disappear or are severely weakened, with important policy decisions taking place outside traditional democratic institutions. In such contexts, policies are shaped by foreign interests and processes. He provides substantive sections on the CoE convention on cyber crime and the G8 negotiations on high-tech crime. He warns that inter-governmental activities must be paid greater attention since those groups with sway and influence, including external state representatives, are sitting at negotiating tables with unprecedented national powers with the facility to make decisions which are shielded from any parliamentary or democratic process.

The Conclusion by the editors addresses some of the issues for civil society of planned military procurement of information-targeting weapons and systems in the immediate future. The capacity for global telecommunications interception, achieved by the US-dominated Echelon network of worldwide listening posts capable of listening in to all phone, fax and e-mail correspondence, has already caused widespread fears for the future of democracy as we understand it. Already, the national guarantees embodied with various EC member states, in regard to privacy for example, are transcended by Echelon's ability to absorb all entries on the telecommunications highway without as much as a warrant or a 'by your leave'. The European Parliament and Commission has already recognised that such a facility has tremendous implications for the fairness of international economic negotiations, not to mention the manipulation of political discourse which might pre-date any future war and how it is fought.

Because the 'war against terror' is being fought on the basis of intelligence by individuals which can not be checked, the line between information and intelligence is blurred and we begin to experience the start of unaccountable policing. Statewatch in London has been pre-eminent in addressing the extent to which this is already happening. We have seen how IW is still based on the quality of 'information extraction'. Events in Abu Ghraib, Guantanamo and elsewhere have revealed a new willingness to trawl a wider mass of people for potential associates and to torture those incarcerated in the hope of generating further information sources. Some of the commercial telecommunications monitoring systems already on the market such as 'Watson and Holmes' (a telecommunications monitoring system) automatically generate arrest lists from telephone contact chains. It is not hard to see how spurious justifications of association could be generated by telephone tree records to implement extremely repressive actions against specific communities or activists who dissent from the status quo.

Now that both outsourcing of torture and extrajudicial killings are being justified by the war on terror, it is only a stitch away for high-tech digital

weapons to become personally targeted onto other digital media held by future suspects, including computers and mobile phones.

The RMA encompasses capabilities yielded by advances in nanotechnology. The book ends with some consideration of how such technology could potentially master us unless adequate checks and balances are put in place to avoid any prejudiced future targeting decisions being made by advanced weaponry on autonomous, algorithmic, self-deciding modes.

Acknowledgements to a Leeds Met student, Professor David Webb and Dr Philippa Trevorrow for the translation of Chris Wu's chapter.

## Notes

1. J. Arquilla and D. Ronfeldt, 'Cyberwar is Coming!', *Comparative Strategy*, 12(2) (Spring 1993), 141–65.
2. Colonel R. Szafranski, USAF, *A Theory of Information Warfare: Preparing for 2020* (15 July 2005). Available at <http://www.iwar.org/iwar/resources/airchronicles/szfran.htm>.
3. For example, C.H. Gray, *War and Computers* (New York: Routledge, 2005).
4. See [http://www.dtic.mil/doctrine/jel/service\\_pubs/afd2\\_5.pdf](http://www.dtic.mil/doctrine/jel/service_pubs/afd2_5.pdf) (accessed 15 July 2005).

# Index

- Aces of the Deep* 18  
address resolution protocol (ARP) 222  
Aegis system 76  
Afghanistan 58–60, 82  
*Age of Empires* 16  
Agreement Governing the Activities of States on the Moon and Other Celestial Bodies 93  
air-borne laser 90  
air-launched miniature vehicle 85  
Allen, Richard V 116  
*America's Army* 23  
*America's Army: Operations* 20, 25, 27  
*America's Army: Soldiers* 17, 18  
anti-ballistic missile systems 84–5  
anti-satellite weapons 84–7, 205  
    China 86–7, 185  
    Soviet Union and Russia 84–5  
    USA 85–6  
arcade games 14  
*Armoured Fist* 18  
Arnett, Peter 64, 69  
Arnold, Henry 'Hap' 207  
artificial intelligence 14  
ASAT *see* anti-satellite weapons  
Ash, Timothy Garton 208–9  
Asia–Europe Meeting framework 219–20  
autosynchronous transfer mode (ATM) 40  
axis of evil 57  
  
*Back to Baghdad* 17  
ballistic missile early warning system 90  
ballistic missile submarines 161  
banking and finance 36  
    vulnerabilities 38  
Barinov, Vladimir 160  
*Battlefield 1942* 16, 20, 29  
Bayer, Martin 4  
*Bin Laden Liquors* 17  
bin Laden, Osama 56, 57, 61  
Blair, Tony 62  
  
*Blitzkrieg* 16  
*Blue Max* 13  
Bradbury, Ray, *Fahrenheit 451* 115  
brilliant pebbles system 86  
Brooks, Vincent K. 65  
Brown, Rear Admiral Nancy 133  
Buzan, B. 109  
  
C3I 4, 119  
    Taiwan 189  
C4ISR 158  
*Castle Wolfenstein 3D* 14, 20  
Center for Defense Information 88  
Center for Nonproliferation Studies and the Monterey Institute of International Studies 88  
Cheney, Vice-President Richard (Dick) 123  
China  
    anti-satellite programmes 86–7, 185  
    information security threats 188  
    information warfare 173–95  
    attack on Taiwan 189–91  
    attack on US 191–3  
    definition of 180–1  
    difficulties in development 187–8  
    network troops 186–7  
    strategy 187  
    system and system building 182–4  
    theoretical research 174–82  
    weapons development 184–6  
People's Liberation Army 173, 174  
People's War 178, 179, 192–3  
research and development  
    Cheng-Do University of Electronic Science and Technology 174  
    Military Strategy Research Centre 174  
    National Intelligence Property and Computer System Research Centre 174  
    PLA Institute of Electronic Technology 174

- PLA Joint Staff-3 174
- Shanghai Institute of Technical Physics 185
- satellite navigation 185
- China Institute of Science 174
- China Internet Network Information Centre 184
- Chinese Academy of Sciences 195
- civilians 24
- Cold War 3, 16–17
- collateral damage 25
- Comanche* 18
- Combat Flight Simulator* 18
- Combat Mission* 16
- Commando Libya* 18
- Commandos II* 19
- commercial aviation problems 76
- commercial off-the-shelf (COTS) war games 12, 16, 38
- Committee on the Peaceful Uses of Outer Space (COPUOS) 93
- Commodore 64 13
- Commodore Amiga 13
- Common Aero Vehicle 87
- Common Operating Environment 119
- Communication Intelligence (COMINT) 34
- communications servers 126
- compliance 237–8
- computer-aided virtual environments (CAVE) 15
- computer-communication technology 73
- Computer Emergency Response Team (CERT) 223–4
- computer game genres 17–20
- computerized control systems 77
- computer-related risks 72–81
  - commercial aviation 76
  - computer-communication technology 73
  - election process 75–6
  - Internet 73–4
  - medical applications 77
  - military problems 76–7
  - openness 74
  - privacy, secrecy, surveillance and monitoring 75
  - roles of technology 78–81
  - vulnerability 74
- Y2K 37, 77–8
  - see also* threat assessment
- computer viruses 74
- Conflict: Desert Storm* 25
- Conflict Zone* 17, 20, 25
- constructivism 102–3
- Convention on Cybercrime 230–2, 233, 234
- co-orbital ASAT 85
- Cossacks* 16
- cost factors 142
- Council of Europe 230–2
- Counterspace Operations, Air Force Doctrine Document 2–2.1* 87
- Counterstrike* 23, 28
- Counter Surveillance Reconnaissance System 87
- crisis experience 116–18
  - attempted assassination of President Reagan 116–17
  - World Trade Center attack 117–18
- Critical Foundations Report 35, 36
- Critical Infrastructure Assurance Office 33
- critical infrastructures 222
- critical systems 77
- cruise missiles 186
- cyber culture 140
- Cyber Defense Exercises 130
- cyber security 220, 221
- cyber terrorism 220–1
  - international and regional cooperation 224–5
- cyber threats 222–4
- Cyberwar 3, 130, 177
- Da Cheng system 189–90
- data retention 234–6
- Dawn of Aces* 16
- DDoS *see* Distributed Denial of Service
- Defence Advanced Research Projects Agency (DARPA) 242
- Defence Meteorological Support Program 82
- Defense Information System Agency 120
- Defense Information System Network (DISN) 126
- Defense Message System (DMS) 126
- Defense Special Weapons Agency 121–2

- de Martens clause 145–6, 147  
 Denning, Dorothy 220  
 Department of Disarmament Affairs 35  
 Der Derian, James 52  
 Diehl Microsystems 244  
 discrimination 148, 150  
 distributed control systems 40  
 distributed denial of service (DDoS)  
 40, 221  
 Dolman, Everett C. 212–13  
 domain name server (DNS) 42,  
 128, 222  
*Dreamgun* 14
- Earth surveillance 205  
*Eastern Front* 19  
 Echelon global telecommunications  
 surveillance 244  
 economic ideology 142  
*EF2000* 18  
 Einstein, Albert 73  
 Eisenhower, President Dwight D. 207  
 election processes 75–6  
 electromagnetic pulse (EMP) 223  
 electronic intelligence satellites 83  
 Ellul, Jacques 103  
 enemy, necessity for 56–8  
 energy 36  
 vulnerabilities 38  
 European Aeronautic Defence and  
 Space Company 91  
 European Court of Human Rights  
 239  
 European Network and Information  
 Security Agency 224–5  
 European Space Agency 84  
 External Terminal Access Control Access  
 Control System (XTACACS) 126
- Fatal Judgement* 14  
 Federal Computer Incident Response  
 Capability 34  
 Federal Intrusion Detection Network 34  
 Felgengauer, Pavel 162, 166  
 file transfer protocol (FTP) 126  
 financial criminals 221  
 first-person shooter games 20  
 First World War 16  
*Flight Simulator* 19  
 force application 210  
 Force Application and Launch from the  
 Continent (FALCON) system 87  
 forum shifting 228  
 Franks, General Tommy 51, 66  
 Friedman, Thomas 243  
 Fukuyama, Francis 101  
 full spectral dominance 209  
*Full Spectrum Warrior* 26, 27
- G8 230–2  
 Galileo GPS system 84  
 Game Boy Advance 13  
 gaming platforms 13–15  
 Garwin, Richard L. 215  
 GCCS 119–20, 122, 126, 131, 133  
 reliability 124–5  
 GCCS-T 120–1  
 GCSS 126  
 Geneva Convention 145  
 George, Laura 89  
 Gilpin, Robert 108–9  
 Global Combat Support System *see* GCSS  
 Global Command and Control System  
*see* GCCS  
 global engagement 201–4  
 Global Information Grid 122  
 globalism, interdependent 100–2  
 globalization 140  
 Global National Satellite System *see*  
 Glonass  
 global positioning systems (GPS) 83,  
 185, 199  
 Glonass 83, 164  
 Goltz, Alexander 158  
 GPS *see* global positioning systems  
 Graham, Stephen 243  
 Grey, Robert T. 214  
 Grotius, Hugh 139, 142, 151–2  
*Gunship!* 18
- hacking 41–2  
 Hague Convention 145  
*Half Life* 20, 26  
*Half Life: Counterstrike* 20  
 Harrigan, Steve 58  
 Harris, Sir Arthur 201  
 Heng Shan system 189–90  
*Hidden & Dangerous II* 16  
 high-power microwave (HPM) 223  
 Holbrooke, Richard 57

- Horner, General Charles 65  
 humanity 148, 150  
 Hussein, Saddam 63, 66, 199  
 hypertext transfer protocol (HTTP) 126
- Il-2 Shturmovik* 16  
 Illustrative Risks 76–7  
*Indizierung* 18  
 information battle space 4  
 information bombs 5  
 information and communication  
   technologies (ICT) 32, 36, 98  
   vulnerabilities 37–8  
 information infrastructure 32  
 information society 99  
 Information Society Directorate-  
   General 34  
 Information Society Technologies  
   Programme 34  
 information war 180  
 information warfare 3, 54, 141–4, 165  
   China 173–95  
   Chinese definition 180–1  
   key issues 151  
   US definition 175–8  
 Institute for Disarmament Research 35  
 interaction 106  
 intercontinental ballistic missiles  
   161, 163  
 interdependent globalism 100–2  
 inter-governmental organizations 100,  
   228, 236  
 International Court of Justice 145–6  
 international governmental  
   institutions 106  
 international law, principles of 148–51  
 International Peace Bureau 145  
 international political economy 98  
 international relations 98  
 Internet 73–4, 221  
 Internet Protocol (IP) 126  
   version 4 222  
   version 6 222  
 Internet Service Providers (ISPs) 223  
 Infrastructure Protection  
   Task Force 33  
 Iraq war 61–7, 123–4, 199  
*Iron Storm* 15  
*Istrebitel Sputnikov* 85  
 Ivanov, Sergei 168
- Jagged Alliance* 18  
 joint direct attack munitions 199–200  
 Jumper, General John P 87
- Keller, Bill 68  
 Kellner, Douglas 54, 56  
 kill chain 82  
 killer satellites 185  
 killer trainers 26, 27, 28  
 Kuan, Shen Wei 173, 174  
 Kurtz, Howard 58
- Land Warrior III* 17  
 Lara Croft 12  
 lawfulness 148, 150  
 laws of war 144–51  
   dimensions of meaning 144  
 LeMay, General Curtis 201  
 Little, R. 109  
 logistics 25  
 Lu Zi system 189–90  
 Lyotard, Jean-François 69
- Macedonia, Michael 26  
 McGeary, Johanna 62  
*Medal of Honour* 16, 21, 29  
*Medal of Honour: Allied Assault*  
   21, 24–5  
*Medal of Honour: Frontline* 13, 21, 22  
 Medetsky, Anatoly 158  
 medical system failures 77  
 Medium Extended Air Defense System  
   (MEADS) 91  
 Mid-Infrared Advanced Chemical Laser  
   (MIRACL) 86  
 MiG-29 fighters 161  
 military communications satellites  
   (MILSTAR) 83  
 military industrial media entertainment  
   (MIME) 5, 53  
 military problems 76–7  
 military use of space 822–4  
 Milosevic, Slobodan 57  
 missile defence 89–92  
   current US developments 87–9  
   international response 91–2  
 modelling 228  
 monitoring 75  
 Morgenthau, Hans 108  
 MSEWDDS 136

- multinational corporations 100, 105
- Multi-Service Electronic Warfare Data Distribution System *see* MSEWDDS
- Mumford, Lewis 103
- mutually assured destruction 89
- Myers, General Richard B. 65, 211
  
- nano-technologies 242
- National Airspace System 244
- National Command Authority 113
- National Infrastructure Assurance Council 34
- National Infrastructure Protection Centre 33
- National Military Command Center 118
- National Plan for Information Systems Protection 43–4
- Near Field InfraRed Experiment (NFIRE) 88
- neorealism 99–100
- Netwar 3
- Network-Centric Warfare 176–7
- Network Operations Centre (NOC) 128–9
- Neumann, Peter 78
- neutrality 148–9, 150
- Nikolayev, Andrea 159
- Nimda worm 223–4
- NIPRNET 126, 127
- nongovernmental organizations 7, 88, 100, 236–7
- non-lethal weaponry 4
- North American Free Trade Area 104
- North Atlantic Treaty Organization (NATO) 4, 17
- nuclear weapons 113–38
  - assessment 130–2
  - crisis experience 116–18
  - GCCS 119–20
  - GCCS-T 120–1
  - Iraq War 123–4
  - ongoing transformation of command and control systems 121–2
  - reliability of GCCS 124–5
  - White House Communications Agency 115–16
  - White House and Department of Defense 114–15
- Nuremberg Principles 143
  
- Office of Strategic Influence 61
- Omar, Mullah Mohammed 51
- Omohundro, Captain Read 135
- ongoing adaptability 131
- openness 74
- Operation Allied Force 82
- Operation Desert Storm 82, 173, 178
- Operation Enduring Freedom 59, 82
- Operation Flashpoint* 22, 23, 24, 27
- Operation Flashpoint: Cold War Crisis* 15, 17, 20
- Operation Iraqi Freedom 63, 82
- Outer Space Treaty (1967) 93, 213
  
- Panzer General* 19
- Patriot missile defence system 76
- PCs 14
- physical distribution 36
  - vulnerabilities 38–9
- Pioneer Project 115
- platform centric warfare 177
- policy laundering 228–41
  - centralized policy counter-moves 239
  - international level 230–2
  - national level 232–4
  - traffic data retention 234–6
- Powell, Colin 62, 64, 117, 118
- precision bombing 199–200
- precision-guided munitions 163
- Presidential Decision Directive 39 33
- President's Commission on Critical Infrastructure Protection 33, 43
- Prevention of Arms Race in Outer Space (PAROS) 93–4
- Prisoner of War* 17
- prisoners of war 5, 24, 57
- privacy 75
- professional military simulations 25–7
- proportionality 148, 150
- Putin, Vladimir 162, 163
  
- Qiang Wang system 189–90
- Qualcomm 111
  
- Reagan, President Ronald, attempted assassination 116–17
- realism 21–5
- real-time strategy games 19
- Real War* 17, 20

- reconnaissance, surveillance and target acquisition systems 163  
 Rendon Group 51  
 Rendon, John W. Jr 51  
*Return to Castle Wolfenstein* 14, 15  
 Revolution in Military Affairs 3, 46, 82  
   Russia 157–72  
 Rice, Condoleezza 61  
 RMA *see* Revolution in Military Affairs  
*Rogue Spear* 17  
*Rogue Spear II* 22  
 role-playing games 18  
 Rumsfeld, Donald 61, 84, 113, 204  
 Russia  
   anti-satellite programmes 84–5  
   ballistic missile submarines 161  
   Draft Military Doctrine 159  
   information warfare 165  
   Military Industrial Complex 162  
   Military-Technical Revolution 159  
   RMA 157–72  
   sea-launched ballistic missiles 161  
  
 Sandburg, Carl 12  
 satellite navigation systems 83, 185, 199  
*Saving Private Ryan* 21, 29  
 SCADA 38  
 Schriever, General Bernard 207  
 Scientific and Technological Options Assessment (STOA) 34  
 script kiddies 221  
 sea-launched ballistic missiles 161  
 Second World War 16, 200  
 secrecy 75  
 Secret Internet Protocol Router Network *see* SIPRNET  
 security 41, 188, 208–10  
   *see also* cyber security 140  
*Serious Games Summit* 26  
 Sharavin, Alexander 161  
 Shen, Weiguang 179  
 ‘shock and awe’ 67  
*Shogun* 16  
 ‘shoot ‘em ups’ 18  
 short-range attack missile 85  
*SimCity* 19  
 simple mail transfer protocol (SMTP) 126  
 simulations 18–19  
  
 Sinclair Spectrum 13  
 Single Integrated Operational Plan 121  
 SIPRNET 120, 124, 127, 135  
   security of 125–30  
 Siroti, Gian Piero 5  
 Smith, Shepard 58  
 soft kill 4  
*Soldier of Fortune II: Double Helix* 17, 23  
 SONET 40  
 Sony Playstation 13  
 Sorenson, Erik 64  
 Soviet Union  
   anti-satellite programmes 84–5  
   *see also* Russia  
   space  
     control of 212–16  
     military use of 82–4  
     non-weaponization of 215  
   space-based infra red system 90  
   space-based radar 87  
   Space Commission 205  
   space cop, US as 206–8  
   space Pearl Harbor 204–5  
   space race 211–12  
   Space Tracking and Surveillance Systems 90  
   space weapons control 92–5  
     treaties 93–5  
   *Special Force* 17  
   spheres of authority 106  
   *Splinter Cell* 17  
   SS7 39  
   SS-19 (Stiletto) missiles 160–1  
   SS-24 (Scalpel) missiles 161  
   SS-25 (Sickle) missiles 161  
   SS-28 (Topol-M) missiles 161  
   *Star Wars* 202–3  
   state of emergency 55–6  
   Strategic Command 204  
   Strategic Defense Initiative 86  
   strategic information warfare 32–48  
     actors 41–2  
     context 33–5  
     critical infrastructures 35–7  
     vulnerabilities 37–41  
   strategy games 19  
   *Stronghold* 16  
   Su-24 aircraft 161  
   super computers 186

- Supervisory Control and Data
  - Acquisition *see* SCADA
- surface-to-air missiles (SAMs) 157
- Surowiecki, James 80
- surveillance 75
- survivability 224
- Synchronous Optical Networks *see* SONET
- synthetic aperture radar 184–5
  
- Taiwan, information warfare
  - against 189–91
- Taliban 59, 60
- technological determinism 103
- technology 98–112
  - arguments for broader perspective 103–4
  - constructivism 102–3
  - interdependent globalism 100–2
  - multidimensional effects 104–6
  - new modes of interaction 106
  - realistic/neorealistic approaches 99–100
  - roles of 78–81
- Teets, Peter B. 216
- Telnet 126
- The Age of Kings* 16
- Theatre Missile Defence 92
- Thompson, Hunter S. 51
- threat assessment 219–27
  - advanced defensive methods 224
  - Asia–Europe Meeting framework 219–20
  - cyber terrorism 220–1
  - cyber threats 222–4
    - see also* computer-related risks
- Topol-M missile 163
- traffic data retention 234–6, 237
- transformational SATCOM 87
- transmission control protocol (TCP) 126
- Trojan horses 42, 74
- turbulence 98–112
- Typhoon* 18
  
- ultra fast electric big gun 185–6
- Unclassified but insensitive Internet protocol network *see* NIPRNET
- Underash* 17
- United Nations 17, 35
  
- unlawful combatants 57
- unmanned aerial vehicles 26, 83, 175
- USA
  - anti-satellite programmes 85–6
  - definition of information warfare 175–8
  - Department of Defense 114–15
  - information warfare against 191–3
  - military superiority 210
  - missile defence 87–9
  - National Security Strategy 213
  - security dilemma 208–10
  - US Space Command 202–4, 242
  
- Vietcong* 16, 22
- Vietnam War 216
- Virilio, Paul 53, 67–8
- virtual private network 121
- virtual soldiers 22–3
- virtual weapons 21–2
- virtuous virtual war 5, 51–71
  - Afghanistan 58–60
  - battle for strategic truth 60–1
  - necessity for an enemy 56–8
  - ‘peace’ 67–9
  - war on Iraq 61–7
  - war on terrorism 55–6
- vital human services 36
- vulnerabilities 39–40
- von Braun, Wernher 206–7
- vulnerabilities 74
  
- Walker, John A. 128
- Waltz, Kenneth 100
- Wang, Baocun 179–80
- Wang, Pu Feng 179, 180
- warfare 142
- war games 12–31
  - definitions and historical context 15–17
  - gaming platforms 13–15
  - professional military simulations 25–7
  - realism versus reality 21–5
- War on Iraq 63, 66
- war on terror 55–6
- White House 114–15
  - Communications Agency 115–16
- White, Thomas D. 207
- Wibben, Annick 55

- wide area network (WAN) 126, 222
- Williams, Brian 58
- Winner, Langdon 103
- wired equivalent privacy (WEP) 222
- world politics 104–6
- World Trade Center 55, 115, 117–18
- World Trade Organization 105
- World War II – Black Gold* 17
- Worldwide Military Command and Control System 121
- worms 74, 223–4
- Wright, David 89
- Xu, Guang Di 183
- Y2K 37, 77–8
- Yorktown* missile cruiser, immobilization of 76