# 14

# The information revolution and verification

Andrew Rathmell

There is little new about the problematic interplay between technology and verification. Ever since the monitoring of arms control and disarmament agreements became of interest the verification community has had to adapt to technological change. On the one hand, regimes have had to be devised to cope with the latest weapon systems, and, on the other, modern technology has made possible new verification mechanisms.

The current wave of innovation is no different. Developments in information and communication technology (ICT) are driving transformations in the economic, political and military spheres. Powered by the forces of global capital, this trend is unstoppable, although its direction can to some extent be guided. The challenge for the verification community is to exploit the benefits of the information revolution, rather than allow it to create a whole new set of problems.

This chapter provides an overview of the most important effects that the information revolution has had on verification, and explores some of the dividends that progress in ICT could bring. It also considers a number of issues that will have to be addressed if verification is to keep pace with technology.

Advances in information technology (IT) and its convergence with sophisticated communications systems are ushering in what has been labelled an 'information age' or 'knowledge age'. It is argued that contemporary societies, led by the West, are being reshaped into 'knowledge societies'. The concept of the information age demonstrates the evolution from industrial-age manufacturing, through service-based production, to an information economy. The idea of a knowledge society reflects the perception that information is no longer just *a* resource, like capital, labour and land, but that it is increasingly *the* resource.[1]

There is widespread scepticism about the extent, pace and consequences of this information revolution. Some observers argue that the Internet economy has failed

to have a deep impact, even in the US. Others contend that the level of technological change that was achieved in the first half of the twentieth century had more far reaching social, political and economic ramifications than the digital revolution of recent decades.[2]

This chapter remains agnostic about the extent and implications of the information revolution. Nonetheless, it is indisputable that the digital revolution of the 1980s and 1990s, along with associated commercial and political developments, has had a major impact on one aspect of international security that is of particular relevance to verification: intelligence.

Intelligence can be defined as 'refined, analysed and assessed information'. It is important to stress that intelligence is about providing actionable data to decision-makers to help them understand a certain situation. Although covert sources and methods are often emphasised, these should not be at the core of the activity—they are tools that may add value to more openly collected documentation.

Intelligence is at the heart of verification. Confidence- and security-building measures (CSBMs) are about enhancing transparency between potential adversaries, and arms control regimes are reliant on mutually acceptable and reliable compliance mechanisms, which are underpinned by trusted data. In the past, certain organisations, such as the International Atomic Energy Agency (IAEA) and the United Nations (UN), have shied away from the concept. But, today, they are increasingly coming to accept that intelligence is central to their success and credibility.

The information revolution, which is defined to include associated commercial and political changes, has an impact on intelligence in two broad areas. First, the digitisation of data, along with increases in processing power, communication bandwidth, and the production of sophisticated software, has made it possible to filter, collate, store, retrieve, manipulate and disseminate information more effectively and faster than ever before.

These advances were summed up in 1995 by the US Central Intelligence Agency (CIA)'s then Deputy Director for Intelligence, John Gannon:[3]

> . . . in the mid-1980s, the analyst *communicated* within CIA by pneumatic tube; thousands of separate, unrelated *files* were maintained at Headquarters; the mainframe and 'dumb' terminals were the 'latest' in *technology*; a *megabyte* was a lot of information; and most analysts saw *computer expertise* as a speciality in others' hands. In 2006 every analyst will be adept in the use of his/her own

> *interactive terminal* combining telephone, computer, and television; worldnet will provide *instant communications* throughout the . . . [intelligence community] and consumer world; *encryption* will be unbreakable and fast; all information will be *digitized;* and a *terabyte* will be the norm for storage and retrieval of information.

Second, the combination of new technologies (like the Internet), the commercialisation of previously classified technology (including very high-resolution satellite imagery) and political change (such as the proliferation of news outlets in the former Soviet Union) has led to an exponential increase in the amount of data available from 'open sources'. Institutions like the media and academia have always been used by defence and foreign affairs intelligence agencies. However, the division between 'white' (open) and 'black' (closed, proprietary or classified) information was previously seen by the Western intelligence community as approximately an 80:20 split. This ratio may now be 90:6:4 between 'white', 'black', and 'grey' information.[4] There is no doubt that vital added value is provided by 'black' sources, such as the UK–US Signals Intelligence (SIGINT) network, the Secret Intelligence Service, or the Human Intelligence assets of the CIA. Nonetheless, it is remarkable how many of the intelligence requirements of most government departments can be filled in whole, or in part, by open sources.

## Implications for verification

The implications of these developments for verification can usefully be discussed in the context of the traditional intelligence process, as used by most defence and national intelligence organisations. This process is based on a model for the development of intelligence or actionable knowledge, which starts with the structured identification of a consumer's needs, recognition of information gaps and the formulation of a collection plan. The documentation is then analysed before it is distributed to the consumer, providing the opportunity for further refinement of the information requirements.

The process is often constructed as a cycle, involving the following steps:

- planning and direction;
- collection;
- processing;
- production and analysis;

- assessment; and
- dissemination.

For now, it is helpful to focus on the effect that the information revolution has had on the second, third, fourth and sixth phases of the cycle. Planning and direction have been less affected by the information revolution so they will not be discussed in this chapter. And assessment remains at root a cognitive activity that is least affected by technological change.

## Collection

The most obvious impact of the information revolution is on the collection of data for verification of arms control and disarmament regimes and export controls, as well as for use as CSBMs. Open sources—available commercially or sometimes at no cost—now provide much of the information that is needed to monitor both the intentions and capabilities of states and sub-state groups that are either party to a regime or are of concern to the international community.[5]

A proliferation of news sources and electronic discussion channels gives access to large amounts of data on the politics, policies and deliberations of all but the most closed regimes and tightly centralised sub-state bodies. The interpretation of information on the intentions and world views of governments and other organisations remains as difficult an analytical task as ever, although the open source revolution has at least provided the mass of documentation for analysts to work on. It is important, of course, not to focus exclusively on the 'new' sources and channels enabled by ICT. A lot of this data will be available from 'traditional' sources, such as scholars, journalists, activists and business travellers. However, the communications revolution, the political opening up of much of the world and economic globalisation have combined to increase the amount and quality of information that 'traditional' human sources can provide.

Meanwhile, very high-resolution commercial satellite imagery (CSI) can be used to monitor physical observables, like troop deployments, border violations and the construction of industrial facilities needed for production of weapons of mass destruction (WMD). The availability of CSI also results from technological change (the miniaturisation of satellites and sensors, improvements and cost reductions in interpretation software, and better dissemination channels) and geopolitical and economic developments (the commercialisation of the Russian military-industrial complex and US government support for the marketing of its surveillance

technologies). The outcome is that anybody with the necessary financial and organisational resources can obtain imagery intelligence which approaches the quality enjoyed by the superpowers in the 1970s.[6]

Information from commercial databases and specialist news services can be used to assess shipping movements and trade flows in regard to export controls or sanctions monitoring. Similar sources can be used to examine the activities of potential front companies and efforts to violate sanction regimes.

At the same time, tracking the movements of individuals is becoming much easier. An increasing number of everyday tasks leave 'digital footprints' that are being exploited by commercial marketers and intelligence organisations. Efforts to 'modernise' government—which most advanced countries are engaged in—will have the effect (notwithstanding data protection legislation) of giving intelligence organisations far more comprehensive pictures of the activities of citizens without recourse to clandestine methods, such as physical or electronic surveillance. This has dramatic ramifications for the monitoring of people and of small groups that are of concern, for instance, in relation to arms proliferation.

## Processing, production and analysis

Analysis is at the root of the intelligence process. It is the activity most vulnerable to human error and least subject to technological 'fixes'. The majority of intelligence 'failures' are due to the foundering either of analysis or of understanding by decision-makers, rather than to a breakdown in collection.[7] For any organisation engaged in processing and analysing data for verification, it is ultimately the quality and mindset of its analysts, combined with the analyst–consumer interface, that determine success or failure.

Nonetheless, the information revolution is having a significant impact on this part of the intelligence process. For the purposes of this chapter, the most important consequence is the convergence of cheap and massive processing power with advanced software, enabling huge volumes of data to be filtered, collated, mined and interpreted. The point is not to replace human analysts, but to assist them with speedily explicating large amounts of information in order to extract patterns of activity that are of interest to decision-makers.

This capability is advancing rapidly in the commercial world. Retail businesses, including supermarkets, have invested heavily in 'data warehouses' that store gigabytes of customer information. This is analysed by data mining technologies, which

identify, for instance, fraudulent credit card use or food purchasing trends. Similar technologies are being developed and applied by law enforcement agencies to profile criminal behaviour. And part of the 'joined-up' system of government in countries like the UK is the effort to combine data sets on citizens—held by government agencies—so that individual behaviour can be tracked and monitored. The objective is to provide better services for people and to prevent criminal actions.

Developments in processing and analytical technologies are at least as important for verification as changes in open sources. Intelligent technologies allow the mass of data provided by the open source revolution to be exploited effectively. Without automated instruments, human analysts would be unable to filter, collate, store, mine and analyse this deluge of information. Furthermore, the production of advanced software tools makes analytical capabilities much more widely available. Whereas in the recent past it was only specialist public sector organisations, such as the US National Security Agency, the UK Government Communications Headquarters and the Australian Defence Signals Directorate that had access to these technologies, they are now routinely employed by small- and medium-sized enterprises and local law enforcement agencies. Given the rate and pace of change in IT, the effectiveness and ease of use of such tools are likely to increase rapidly.

## Dissemination

Presentation and dissemination are an often overlooked part of the intelligence process. However, Western agencies have had to pay more attention to these issues. Intelligence staff at the North Atlantic Treaty Organization (NATO), for instance, often complain that their political decision-makers act on Cable News Network (CNN)'s unanalysed and hastily distributed data, rather than waiting for more considered assessments from the formal intelligence process.

To facilitate the speedy dissemination of well-presented intelligence products, the US intelligence community has responded by taking the lead in exploiting new technologies, such as the Internet Protocol, Hyper Text Mark-up Language (HTML) and video conferencing.[8] The aim is to get analysed work to consumers faster, and to enable consumers to interact with analysts and to arrive jointly at conclusions systematically, supported by an audited reasoning process. In addition, new technologies are being used to display data in a range of formats, text and images, that facilitate understanding and new ways of considering problems.

While these technologies and approaches should make established state intelligence organisations more effective, the point is that they involve commercial off-the-shelf systems. Indeed, many of the tools and techniques now being employed have their origins in the entertainment industry or the financial sector, and, as a result, are available to everyone. Some non-governmental groups, including political and environmental activists, have, in fact, made more effective use of communication and dissemination technologies than have government organisations.[9] This has a significant effect on verification by empowering a range of actors, such as the media, activists, and inter-governmental bodies and non-governmental organisations (NGOs), and by allowing them to construct robust and responsive regional and global information networks.

## Strategic implications

The information revolution is having major ramifications on the sourcing, processing and dissemination of intelligence for those bodies undertaking monitoring and verification. For major governments with established intelligence bureaucracies, one can conclude that these trends will make verification easier.[10] However, the information revolution has some more interesting strategic implications that will affect verification. The most significant of these are the effects on the information power differential and on the role of third parties.

Information power has been broadly described as the sum of a country's resources that it can use to mould the global information environment, just as military power shapes the physical space. Some strategists argue that the information age plays to the strengths of the US and that the country will have a global advantage in terms of 'hard' military and 'soft' information power.[11] Similarly, in specific regions, states that have the appropriate social, educational, political, and technological foundations are likely to be better placed to exploit the information revolution, and thereby strengthen their information dominance over rivals. In the Middle East, for instance, this may apply to Israel, which has the societal infrastructure to exploit IT, and, therefore, to enhance its information edge over its Arab neighbours.

This may well be one trend, but there is a countervailing paradigm of perhaps greater significance. The rise of open sources and the diffusion through globalised commercial channels of ICT for gathering, analysing, and disseminating intelligence have put powerful intelligence capabilities into the hands of even NGOs and technologically backward and impoverished countries. This will go a long way towards

countering the information imbalances between parties to CSBMs or arms control treaties, and make it much easier for all sides to an agreement to gather, analyse and share data equitably.

There could be three specific outcomes to this trend. First, all parties to an accord can have access to the intelligence capabilities that were previously monopolised by the superpowers or regional hegemons. This is likely to have an impact on the willingness of states to enter into agreements and the structure of the verification regime that is put in place.

Second, the increased role of open sources of information and commercially available processing tools should make it easier for countries to share data. National intelligence agencies that are reliant on their own sources and methods will always be reluctant to share documentation and intelligence. But CSBMs and arms control regimes rely on transparency and information sharing; squaring this circle has been a vital but tricky part of past CSBM and arms control processes. The information revolution eases this problem. For instance, an increasingly popular concept is that of regional conflict prevention, involving crisis monitoring centres. In the mid-1990s, the Association of South-East Asian Nations (ASEAN) Regional Forum mooted the concept and it also emerged during the Middle East arms control and regional security talks.[12]

But this concept has been hindered by credibility problems. Quite simply, states that do not yet trust one another are loath to allow such a facility to have access to sensitive sources and methods. Increasingly, however, centres could rely exclusively on open sources, assisted by advanced processing and knowledge management techniques. They would be able to produce unclassified intelligence on military deployments, doctrines and budgets, for example, that would underpin global or regional CSBMs and arms control regimes. As important, staff seconded to such centres would have the opportunity both to work with erstwhile enemies in a relatively open atmosphere and to achieve a common understanding of their operational environment.

Third, and perhaps most significantly, the information revolution could transform the role of outside parties in verifying the implementation of peace accords, and, in some respects, arms control regimes. Generally, peace agreements have been verified by states parties, often with the help of a small number of outside countries, notably the US. This was the case, for instance, with the Israel–Egypt Separation of Forces Agreement of January 1974. With global arms control measures,

such as the 1968 Nuclear Non-Proliferation Treaty(NPT), it has also been certain leading states that have sometimes supported verification with national intelligence. Overwhelmingly, the international community has relied on the US—the only country with the global monitoring resources needed for the job.

The information revolution changes this situation. While the American intelligence community will continue to have capabilities unmatched by other states or by the commercial sector, an increasing number of verification tasks can be carried out using open sources and methods. Consequently, the capability to assess agreements is proliferating along with the technology. Since 1995, the Western European Union (EU) has operated a satellite centre that primarily uses CSI to assist with monitoring the 1990 Conventional Armed Forces in Europe (CFE) Treaty. The IAEA is beginning to fuse a range of open sources to enable it to detect proactively violations of the NPT. Research centres are showing an increasing capability to track weapons of mass destruction (WMD) developments across the world, and NGOs, such as the transnational Forum on Early Warning and Response, are exploiting open sources and communication networks to help predict humanitarian crises. And companies like the US-based Open Source Solutions and Stratfor offer a routine political and military monitoring service.

The result is that future arms control and CSBM regimes will be able to call on a much wider range of outside parties to assist with verification. The US will still have a role to play, but agencies like the IAEA and the Organization for the Prohibition of Chemical Weapons (OPCW) will be able to do much more themselves. In addition, other state actors (such as the EU), non-state actors (like research institutes and activist networks), companies and media outlets will be able to contribute to verification.

## Challenges

The information revolution not only makes verification easier, but, in certain respects, it poses new problems. Three of the most significant are:

- encryption;
- technology diffusion; and
- electronic attack capabilities.

The debate over encryption policy is a well-worn one in Western societies. Towards the end of 1999 the US government seemed to have acknowledged that it was

fighting a losing battle in seeking to control the export of encryption software. Its more liberal approach parallels that of other states.[13] Nonetheless Western intelligence agencies are still grappling with the likely loss of one of their most useful sources: signals intelligence from intercepted communications.

Encryption poses a similar problem for CSBMs and arms control verification. Western intelligence agencies that help to monitor such regimes rely heavily on SIGINT, tapping into global civilian, military and government voice and data links. Although they have the computing power to crack most encryption codes in time, the widespread availability of encryption to governments, citizens and sub-state groups will make their job much harder, more time consuming and more resource intensive. The proliferation of strong encryption thus makes it harder for national signals intelligence agencies to assist with verification.

The problem presented by encryption is a subset of a wider issue raised by the diffusion of ICT in the global market. Through the so-called Revolution in Military Affairs, developments in ICT are enabling the US and some of its allies to become more powerful in conventional military terms. No other state will be able to match the mobile and lethal force that the US will deploy under its Joint Vision 2010 blueprint for network-centric warfare.[14] But states and sub-state groups will be able to exploit niche technologies like WMD, allowing them to pack a powerful punch. Another concern is that small states and sub-state groups may exploit freely available commercial information and communication technologies in order to utilise limited resources against their larger opponents.

These technologies range from mobile, secure, satellite communications, through intelligence gathering and mission planning tools, to precision-guided munitions. If networked, media-savvy groups or state organisations take advantage of this combination of technologies they could pose serious military threats to status quo powers.[15] Russia has faced a precursor to this problem with the Chechen rebels, and the US with Osama bin Laden. In verification terms, this raises difficult questions about the nature of dual-use technologies and the convergence of military and civilian technologies and applications.

These difficulties are brought into sharp focus in the emerging debate over information warfare (IW). This is a broad concept, but a particularly problematic aspect is that of electronic attack or, more specifically, Computer Network Attack (CNA). The latter involves the use of computers to launch a logical strike on terminals via digital networks and telecommunication links. Assaults may result in the

denial of services or the compromising of data integrity and confidentiality. Although long used as a tool of espionage and to some extent integrated into battlefield electronic warfare, CNA is becoming of greater concern to countries and businesses that are ever more reliant on networked information systems and the Internet. A number of states have followed the US lead in identifying logical threats to their increasingly interconnected and interdependent Critical National Infrastructure (CNI) as major security concerns.[16]

These fears have led to a debate over how best to characterise and deal with the danger. The approach currently favoured by the US and its allies, which are investing in offensive IW techniques, is to treat it as a criminal or terrorist problem. They are pushing for enhanced international co-operation in order to put in place the legal, technical and policing measures necessary to ensure that all countries work together to protect their CNI and the global information infrastructure.

An opposite perspective has emerged from states that feel threatened by the possibility of offensive IW by the West. Russia has championed this approach and has proposed that the UN treats IW as a military issue in the General Assembly's First Committee and discusses outlawing it. This involves viewing CNA as military technology, and thus devising laws of armed conflict and, possibly, arms control measures to restrict its proliferation and use.

There is growing pressure from within Western militaries to exploit their advantages in this field.[17] This is likely to energise other members of the international community to push for controls and to consider ways of limiting this new capability. Paradoxically, the problem is that any conceivable regime to restrict the use or possession of IW poses tremendous challenges for verification. The tools and skills needed to conduct CNA are not only inherently dual-use, but they are also virtually impossible to monitor in a globalised, digital economy.

## Conclusion

The information revolution should be a boon to verification. At heart, verification is about transparency and information sharing, which are both facilitated by progress in ICT. The latter gives advanced governments far greater capabilities to track and assess national and international developments. Meanwhile, the proliferation of these technologies diffuses monitoring capabilities widely across the international system. The environment in which today's arms control and CSBM agreements were forged was characterised by the uneven distribution and concentration of

data in key states. In the information age, data resources will be much more broadly dispersed. Instead of relying on a handful of great powers, arms control and disarmament regimes can be checked by a network of official and unofficial actors with extensive collection, analytical and distribution capabilities.

This will have a significant impact on the identity and role of third parties, and on proposals for regional or global monitoring and information-sharing mechanisms. If the capability to check agreements is widespread and can largely rely on open sources and methods, then the dynamics of arms control regimes will change. International agencies, such as the IAEA and the OPCW, will gain in power and autonomy. As multinational organisations gradually lose their fear of 'intelligence' and develop in-house intelligence structures, they will be able to exploit the information revolution to collect, process and analyse vast amounts of open source data on potential non-compliance. This will allow these institutions to verify compliance much more effectively, and will make them less reliant on intelligence from national technical means, which can be politically difficult to use. At the same time, private interests, like media organisations, research centres and NGOs, will play a greater role. Even small and technologically backward states will be able to contribute to verification, rather than relying exclusively on allies, such as the US.

But technological developments will also pose challenges for existing and future verification regimes. Encryption will make the work of intelligence agencies harder, and the diffusion of niche dual-use technologies that can be exploited asymmetrically by small groups and weak states raises complex monitoring issues. The latter is particularly evident in relation to IW, which presents both a conceptual and an implementation problem for the verification community. Conceptually, decisions need to be made about whether to treat this new military capability as an arms control or criminal matter. In terms of implementation, if it is seen as a question of military technology, then there will be tremendous problems in devising a monitoring regime to check development or the use of illicit capabilities.

Technology poses the same dilemma it always has for verification: how to harness the benefits while minimising the downsides. A particular problem with the contemporary 'technology rush' is that societal concepts and institutions tend to fall behind the emergence of new technology. This lag is likely to be especially large in the context of the international community, which rarely acts quickly in any case. As technology moves further ahead of international policy-makers, it will probably

take some time for the dividends to be harnessed. Meanwhile the downsides will be left to worsen.

**Dr Andrew Rathmell is Executive Director of the International Centre for Security Analysis and Senior Lecturer in the Department of War Studies, King's College London, UK. He is editor of the *Gulf States Newsletter,* a specialist correspondent for *Jane's Intelligence Review,* and a regular contributor to the media.**

# Endnotes

[1] Alvin and Heidi Toffler, *War and Anti-War*, Little, Brown and Co., New York, 1993, and Daniel Bell, *The Coming of Post-Industrial Society*, Basic Books, New York, 1999.
[2] Rob Kitchin, *Cyberspace*, John Wiley and Sons, Chichester, 1998.
[3] CIA Directorate of Intelligence, *Analysis: Strategic Plan*, Central Intelligence Agency, 1996, pp. 1–2.
[4] Grey information is open source data that is not freely available to the general public.
[5] Robert Steele, 'Virtual Intelligence: Conflict Avoidance and Resolution Through Information Peacekeeping', *Proceedings of Conference on Virtual Diplomacy*, US Institute of Peace, Washington, DC. 1–2 April 1997.
[6] Karen Plumb, Robert Harris and David Needham, *Commercial Activities in High Resolution Imaging from Space*, reference paper for British National Space Centre seminar entitled 'From Space to Database', London, 19 February 1997; *The Potential Uses of Commercial Satellite Imagery in the Middle East*, UNIDIR, Geneva and Albuquerque, New Mexico, 1999.
[7] Richard K. Betts, *Surprise Attack: Lessons for Defense Planning*, Brookings Institution, Washington, DC, 1982, and Roberta Wohlstetter, *Pearl Harbor: Warning and Decision*, Stanford University Press, Stanford, CA, 1962.
[8] Fredrick Thomas Martin, *Top Secret Intranet: The Story of Intelink—How US Intelligence Built the World's Largest, Most Secure Network*, Prentice Hall, Upper Saddle River, New Jersey, 1998.
[9] Kevin Soo Hoo, Seymour Goodman and Lawrence Greenberg, 'Information Technology and the Terrorist Threat', *Survival*, vol. 39, no. 3, autumn 1997, pp. 135–155; John Arquilla and David Ronfeldt (eds.), *In Athena's Camp: Preparing for Conflict in the Information Age*, RAND, Santa Monica, California, 1997.
[10] Quite apart from the fact that they will be able to exploit technological changes to enhance their own national technical means. Note, for instance, the US investment in military surveillance technologies that can also be used for verification.
[11] Joseph S. Nye, Jr, and William A. Owens, 'America's Information Edge', *Foreign Affairs*, vol. 75, no. 2, March–April 1996, pp. 20–36.
[12] Desmond Ball and Amitav Acharya (eds.), *The Next Stage: Preventive Diplomacy and Security Cooperation in the Asia-Pacific Region*, Strategic and Defence Studies Centre, Canberra, 1999, pp. 30–31; Ariel E. Levite and Emily B. Landau, 'Confidence and Security Building Measures in the Middle East', *Journal of Strategic Studies*, vol. 20, no. 1, April 1997, pp. 143–171.
[13] Cabinet Office, *Encryption and Law Enforcement: A Performance and Innovation Unit Report*, May 1999; William Cohen, Janet Reno, Jacob Lew and William Daley, *Preserving America's Privacy and Security for Americans In the Next Century: A Strategy for America in Cyberspace: A Report to the President of the United States*, Washington, DC, 16 September 1999.
[14] Eliot A. Cohen, 'A Revolution in Warfare', *Foreign Affairs*, vol. 75, no. 2, March–April 1996, pp. 37–54.
[15] Lloyd J. Matthews (ed.), *Challenging the United States Symmetrically and Asymmetrically*, US Army War College, Carlisle, Pennsylvania, 1998.
[16] Andrew Rathmell, 'International CIP Policy: Problems and Prospects', *Elsevier Information Security Technical Report*, vol. 4, no. 3, 1999, pp. 28–42.
[17] Julian Borger, 'General heralds age of cyberwar', *The Guardian*, 5 November 1999.