THE INFORMATION REVOLUTION

Commodore (Royal Navy) Patrick Tyrrell
Defence Communication Services Agency, United Kingdom

ABSTRACT

This paper is to examine the nature of information and to look at how it has changed in the "post information revolution" world. Has this changed the way in which we use it, has it altered the way in which we, as human beings, respond to it? I shall also examine some potential threats and look at how information integrity might be better safeguarded. A number of other important questions will be raised but, I fear, not answered: where does the responsibility for information rest; what sovereignty can a nation exercise over information and information flow, how might global networks be controlled and what threats to national information integrity can be identified. These are difficult issues, with no clear answers – but that should not stop us venturing down the information road.

> ***"It is only now that we begin to realise the real scale and profundity of the changes in the conditions of human life that are in progress......The scale of distances has been so altered, the physical power available has become so vast, the separate sovereignty of existing states has become impossible"***[1]
>
> **H. G. Wells**

> ***"The electron, in my judgement, is the ultimate precision guided munition."***
>
> **John Deutch**
> **Director CIA**[2]

INTRODUCTION

In the history of mankind, a phrase often emerges which captures the imagination of the contemporary world. As we approach the end of the twentieth century, journalists, writers, scientists and commentators have vied with each other to achieve some degree of immortality with apposite "sound bites". One such phrase that has lodged itself in the public's consciousness is that of the "information revolution", often with only the vaguest understanding of the concepts involved. Another word that has sprung into our everyday lexicon as a result of this revolution is "cyberspace", initially coined by an American science fiction writer in the early 1980s when observing a number of young boys playing computer games in an arcade and very obviously immersed in some virtual world beyond the monitor screen.

There is a plethora of books, articles, reports and discussion on the implications of the information revolution in every aspect of human endeavour. We cannot envisage modern life without the convenience, speed and universality of modern information systems, from the humble telephone to the ability to be able to join in discussion groups with globally dispersed, but like-minded people, on the Internet. From the cash card to the manipulation of the financial markets on a twenty-four hours, global basis. In these, and many other applications, there is a clear assumption that the information flow is unimpeded, that the information received is clear, unambiguous, correct and uncorrupted. In many cases, there will be an additional assumption that the information flow is private and that the information is confidential between the initiator and the recipient.

The integrity of information has always been a matter of critical interest but the dramatic changes brought about by the information revolution have made it much more difficult to trace the route by which information passes from one point to another. It is this inability to identify, with any ease, the provenance of information, to understand what might be termed *information opacity*, together with the global connectivity of modern systems, that has allowed, for example, the development of extensive global organised crime, described as the world's fastest growing business, with profits (in 1998) estimated at over $1000 billion. Within a military context, these same conditions have given rise to the concept of ***information warfare*** whereby a potential adversary might attempt to exploit vulnerabilities within a nation's information systems.

DATA, INFORMATION AND KNOWLEDGE

It would be instructive at this point to examine the terms that are often used to describe some of the concepts underlying a modern view of information. The Tofflers[3] include in their broad concept of knowledge: information, data, communication and culture. Schwartau[4] considers data to be individual facts or statistics in a raw or uncorrelated state, which, once organised, become information. It is the application of human insight and intuition that can transform this information into knowledge. A French academic, Philippe Baumard[5], goes further and argues that within a society founded upon Greco-Roman philosophy, the basis for knowledge is confined to "objective knowledge" rather than including broader areas such as "conjectural knowledge". He refers to this as "knowing" as opposed to "knowledge". He considers that many organisations, particularly when operating in periods of considerable change, believe that they have to use more and more knowledge and that this in turn forces organisations to process more and more information. He contends that successful organisations and individuals will place a premium on "sense-making" rather than on simply information-collection. Fukuyama[6] examines the role of the information age in the breakdown of hierarchy and authority within society and stresses the role that trust and the shared ethical norms that underlie it in the conduct of society. It is the human understanding, the ability of men and women to reason, that is the hallmark of human society; our ability so to do will be greatly enhanced by appropriate information.

The value of "knowing" has similarities with the philosophy of Sun Tzu who said that the greatest achievement was to destroy the enemy's strategy before it could be implemented. This had to be done in an unexpected manner with the unconventional use of "divine force" or *ch'i*. The opposite of *ch'i* is ordinary force or *cheng*. On the battlefield, *cheng* is a holding force that puts the enemy on the spot and *ch'i* is the flanking manoeuvre that fatally disrupts the enemy's strategy[7]. This is also the basis behind Edward de Bono's concept of "*lateral* or *parallel thinking*: "in parallel thinking there is as much emphasis on concepts as on information"[8]

Why should we be interested in these differences and how can they help us understand the issues surrounding information integrity? There is a seemingly natural tendency, in the field of information technology as well as in other technical arena, to allow the technology to drive the development of systems, regardless of the requirements of the society or organisation. Understanding of the human aspects of decision-making is important if we are to be able to focus upon those areas where integrity might be vital and identify other areas where such assurance of integrity is of less importance. The military doctrine of command and control warfare (C2W) focuses on the requirement to influence human behaviour and the definition includes the integrated use of physical destruction, electronic warfare, deception, psychological operations and operations security. It is the use of such techniques as deception and psychological operations that can affect the way that a commander will interpret information, almost certainly by building upon his natural tendency to think inductively rather than laterally. Such *ruses de guerre* have a long and distinguished history from the Trojan Horse to the “Man who never Was”. It is instructive to look at work done on expert systems[9] where an essential attribute is the heuristic nature of these systems compared with more conventional programs. It is a knowledge revolution with increasing emphasis being placed upon information flow and knowledge accessibility. The concept of “*intellectual capital*” is now increasingly accepted within the commercial world as one of the most important assets within a company. Developing and enhancing this asset is the key to success as the phenomenal growth of some Internet companies like *Amazon.com* can testify. In attempting to bring these different strands of thought together, it is instructive to look at the *knowledge spectrum* (figure 1). This examines the linkages between a number of concepts and links the processes controlling the translation of data into information with those traditionally human virtues by which information becomes knowledge.

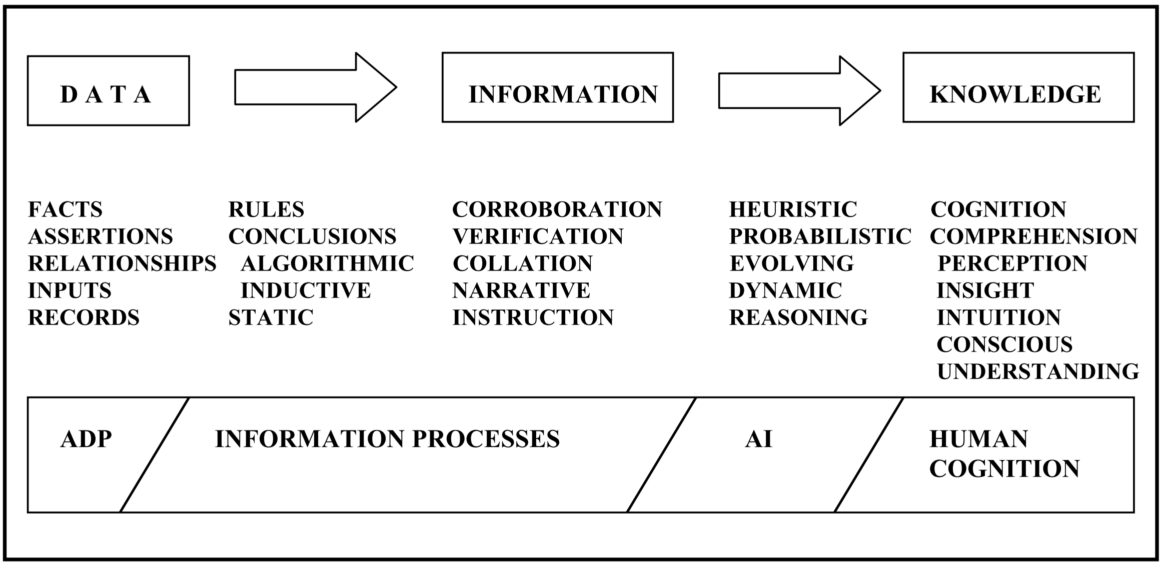

Figure 1: The Knowledge Spectrum

There are also four key stages in the life-cycle of information, its creation, its harvesting, its dissemination and its use:

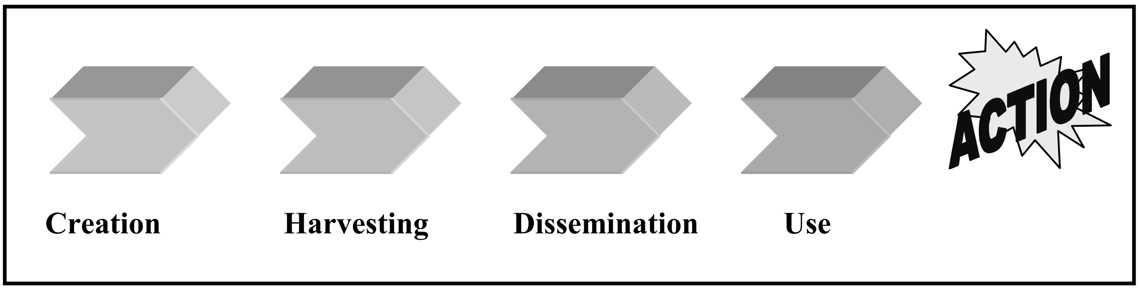

Figure 2: Stages in the life-cycle of Information

These four stages are distinct although share many similar characteristics. The technological developments of the past few years have affected primarily the speed and volume of harvesting and dissemination of information. To be effective, we must be better at the use of information and the ability to lead to better actions.

HISTORICAL PERSPECTIVE OF INFORMATION

Information has always been an important aspect of human society; after all, the ability to communicate and to transfer ideas and concepts is considered to be one of the defining parameters of *homo sapiens*. Until relatively recently in human development, communications were either by word of mouth or, if to be transmitted beyond a small group, written down. The development of printing in Europe by Gutenburg and Caxton in the 15th century had a profound influence on education and the broadening of the intellectual base by providing a relatively cheap, consistent, accurate and available source of knowledge to a wider audience than hitherto. It was not until the latter half of the nineteenth century that further major improvements could be made in the way human beings transferred knowledge. The advent of the telephone and wireless technology removed, for the first time, the requirement for a human intermediary in the transfer of data and permitted the instantaneous transmission of information over large distances. The transfer of information though remained essentially a *linear* and a *transparent* process by which data was assessed, the analysed information was then available to be transferred to the user who could then act upon it as required. The recipient could, if required, follow a clear audit trail to assess the validity of the information. So, for example, if Wellington at the Battle of Waterloo, wished to amend his tactics he would write his new orders and despatch them to the appropriate commander for action. If the body of the messenger was later discovered with his pouch missing there would be a strong presumption that the information contained in the message was now in the hands of the French.

While the first half of the twentieth century saw a number of qualitative improvements to the way in which data might be moved around the world, it was the technological imperatives of the Second World War that provided the impetus for the fulfilment of Babbage's great vision: the computer and the consequential information revolution. As with many technological developments throughout history, the driving forces behind the early innovations in this revolution were almost exclusively military, reflecting the priorities of World War II and the

Cold War. The major change as we approach the twenty-first century is that the factors driving these technologies forward, rely far less upon national defence budgets or other government expenditure than upon commercial priorities, applications and pressures. The reasons for this shift from military to civilian are complex but have much to do with the relative stability and affluence enjoyed by the West within the interstices of the Cold War as well as with the ability of the commercial world to develop a global and competitive market place.

THE INFORMATION REVOLUTION

The term "revolution" has been used extensively to characterise the exponential development of information technology over the past decade. Whereas fifteen years ago, computers tended to automate human activities to achieve speed and accuracy and, in the event of failure, whose functions could be replicated by the manual process, modern systems are extensively interlinked and interdependent and can no longer be considered to be automated manual systems. Science and technology promises us that, in the near future, artificial intelligence (AI) systems will perform many of those actions now done by the human operator; only limited human 'control' will be required and most operators will be content merely to respond to that which the sophisticated software demands of them. There are already a number of disturbing implications arising from this "key-and-forget" dependence on systems, particularly amongst children where, for example, they display a loss of an instinctive comprehension and appreciation of mathematical problems when keying them into a calculator. They accept the displayed result with no urge to mentally check its veracity. Indeed, many of them may not have the ability to understand the mathematical process behind even the simplest calculation. These young children will be the managers of the future. In a report examining the shooting down of the Iranian Airbus Flight 655 by the *USS VINCENNES* on 3 July 1988, Rochlin[10] draws out some of the perils of increasingly sophisticated, increasingly centralised command and control (C2) systems, becoming larger, more rigid and more saturated with information and responsibility each year but without a concomitant improvement in the capability of the human brain to deal with such demanding concepts.

INFORMATION INTEGRITY

Information as a Strategic Asset

It would be wrong, however, to concentrate exclusively upon the technological advances inherent in the *"information revolution"*; the technology, although highly sophisticated, is merely a tool to manipulate information, to collate, store, sort, refine, and assemble as the user demands. Modern computers and communications can store information, process it and make it accessible in ways never before achieved but that, while conferring great added benefits to a business or organisation, they also enhance the scale and opportunities for mismanagement, theft, loss and abuse, as well as the indiscriminate dissemination of information in a manner inimical to the broad objectives of any organisation. Information as a military strategic asset has long been recognised by commanders with particular emphasis on the requirement for good intelligence on an enemy's intentions and, at the same time, protecting information as to their own plans and operational status. Making this information readily available throughout the military environment, from the strategic levels of command down to commanders at the front line raises a number of complex problems if commanders at all levels are to be confident of the integrity, relevance and validity of the information presented to them. A latter-day Wellington, therefore, would no longer discover the physical body of his messenger, his digital messenger would have delivered the message, but how do we know that no one else also received it or that the message received by Wellington's commander was the same as that originally sent? The recent destruction of the Chinese Embassy in Belgrade by NATO warplanes is a clear example of the dangers inherent in accepting information without checking its provenance.

The application of the information revolution to organisations, whether civilian or military, has not been uniformly beneficial. Strassmann[11] reports that there appears to be no direct relationship between shareholder returns and the amount a firm spends upon information technology. This view is supported by an Economist study[12] looking at the introduction of electricity into US industry in the early years of the twentieth century where financial benefits only emerged once senior management came to terms with the new technology. In a survey[13] of 70 firms from the Times Top 1000 database, there was a clear discrepancy between CEO's and their IT directors' perceptions. Two interesting facts emerged: first there was a degree of complacency as to the business benefit of IT and, secondly, there was a clear cultural difference between the CEO and his IT-director and CEO's were reluctant to give their IT-director too great a say in the running of the business. These divergent perspectives arise from a lack of understanding, on the part of the CEO, who fails to comprehend the underpinning technologies and, on the part of the IT director, who does not recognise the strategic imperatives of the business. Despite these factors, there is, however, a clear relationship between the catastrophic loss of information systems and the success of a business: in a study on small to medium sized firms, it was reported that some 75% of those firms which suffer a major computer failure, mostly through fire or theft, go out of business within twelve months[14]. It is the unwillingness of an organisation to be able to safeguard strategic information effectively in such eventualities that can lead to their catastrophic collapse. Often, senior management takes little or no interest in the provision, protection and utilisation of this strategic information, frequently to their cost. The role of senior management is obviously key to the success of the above approach: all too often, however, senior management tends to abrogate responsibility to the technical management side of the organisation, leaving them to determine how, why and when modern technology should be employed within the organisation. IT directors, for their part, tend to suffer from a lack of strategic view for information management and an emphasis on what they perceive as their primary role of supporting operations. As a result, the tactical issues tend to take priority over the strategic. Many senior managers, both in the civilian and defence environments are, still afraid of the computer and even more of the cyberworld to which it gives them access.

Military Information Requirements

The very nature of military operations and their exposure to intensive media scrutiny, however, will inevitably place greater demands on the military leadership, with dramatic consequences for failure. In looking at the information needs of military commanders, it is useful to examine the types of military activity in which they are involved. There is considerable difference between the information skills required in a peacekeeping operation, for example, than in that required during a major conflict. This *"spectrum of conflict"* provides a useful analytical tool and can allow us to distinguish a number of common threads.

Recent operations in Kosovo, for example, have highlighted the requirement for an ability to move from one part of this spectrum to another. The present "peacekeeping" operation could quickly degenerate into a more serious conflict as the ethnic Albanians flex their muscle towards the Serb population.

Military Information Systems in a Civilian World

Even a cursory examination of modern information systems will reveal that the military establishment is no longer at the technological cutting edge; the commercial world is driving research and development in an unprecedented manner. Commercial firms are increasingly considering their information systems to be revenue expenditure, purchased over a short period and replaced at regular intervals. The military and government requirements for long design phases, followed by in-service periods measured in decades rather than four or five years, are inimical to the use of the latest technology. Military systems, at the same time, are becoming increasingly interconnected with those of the civilian world and there is an increasing drive for interoperability between military and civilian systems. As the pressure on the military grows for initiatives such as private finance, creation of agencies and the growing need to rely on civilian firms for much of their deployment and support, there must be an awareness of the increasing interdependence of risk.

Threats to Information Integrity

There are a number of threats that we can identify to the integrity of information. There are three key parameters in assessing the nature of a threat: the first is the identity of the perpetrator, the second is the *modus operandi* and the third is that of motive. One of the distinctive features of threats to digital information is the difficulty associated with the identification of a perpetrator. There are a number of potential sources from which an attack might be launched:

a) The serendipitous hacker (sometimes referred to as a "computer intruder") who considers computer systems to be a challenge waiting to be unlocked and may stumble across opportunities to penetrate information systems fortuitously;
b) A disgruntled employee pursuing a personal grudge;
c) The professional criminal seeking to penetrate the security of a system for his own financial gain;
d) A national, or multi-national, company intent on achieving commercial advantage over its overseas competitors;
e) An international non-governmental organisation wishing to pursue its own agenda;
f) Hostile intelligence services intent on identifying and exploiting points of vulnerability of another nation-state and its military and commercial infrastructure;
g) Terrorist organisations keen to destroy or degrade a target nation's social, commercial or military information infrastructure.

The *modus operandi* adopted by such perpetrators varies widely but one frequently used tool is that of the virus, a piece of software, written in such a way that it can make copies of itself and able to corrupt particular parts of the system at predetermined times. Originally developed at the University of Sofia, Bulgaria, by a disgruntled Professor of Mathematics, they are now a familiar part of the computing landscape. The skill base developed in Eastern Europe was well recognised by the KGB who made considerable use of these and other computing hacking talents[15]. Viruses continue to plague the information world as was seen with *Melissa* and *Chernobyl* during the early part of 1999. It has been estimated that some 200 new viruses are being developed each month[16]and there is evidence to suggest that hackers will try to make the most of the Millennium period to cause mayhem or wreak havoc.

The motive for attack may well determine the level of threat to an organisation and identify some of the necessary actions to be taken to neutralise that threat. In examining motive, we need to look at the types of "*attack*" that might occur and how to counter them. The use of a pejorative term such as "*attack*" is useful in that it conveys the sense of violation of the integrity of the information and, therefore, of the company itself. It also reflects the military pedigree of these particular issues and the initial thinking behind much of the overall philosophy. In addition to intentional attacks, any information infrastructure will be vulnerable to a number of events, protection from many of which could be built into the systems. These events will include natural disasters such as fire or flood, technical breakdown in the system itself or the failure of a supporting system (which may or may not be under the control of the organisation). Supporting systems would include power supplies or the telecommunication service as well as the technical failure of components of the system itself. Once intentional and *force majeure* have been taken into account, there is always human error as employees can, and do, make mistakes, some of which can have major implications to the operation. On 21 November 1985, the Bank of New York suffered a multi-million dollar loss[17] simply as a result of a simple typing error in one line of code, a similar error, in 1991, led to the failure of a major portion of the US telecommunications infrastructure when an AT&T telephone switch in Manhatten failed. The failure of Ariane-5 rocket in 1996 was caused by a similar, simple computer code error. All of these events only serve to highlight the lack of proper checks as well as the failure, over a wide range of business and government, to give serious consideration to potential threats. Such eventualities, however remote, can be factored into the operational doctrine of the organisation and suitable contingency plans made.

A more difficult issue, however, is the response to deliberate and malicious acts: these can range from the unauthorised access into part of the system, the theft of information contained therein, the destruction of data, the insertion of misleading information into a database or the "take-over" of a system by someone for their own ends. An example of this occurred between March and May 1994 when the USAF facility at the Rome Air Development Center, was attacked[18]. Some thirty systems had been compromised, with 'sniffer' technology inserted in order to acquire user IDs and passwords. The hacker used multiple sites and multiple countries as a conduit for his attack in order to frustrate attempts to trace him. The countries were in Europe, South America and Mexico. When finally arrested by Scotland Yard, the hacker was found to be a 16 year-old youth living in London. This ability to obfuscate the source of an attack is one of the distinctive attributes of modern technology, a form of the *information opacity* mentioned earlier, and has a number of implications. If a state or organisation wished to launch an attack upon another state or organisation, this could be conducted through an innocent third party, giving rise to a perception by the target that the third party was the real perpetrator. We have already considered the intertwining and interconnectivity of systems and a deliberate attack on the supporting infrastructure, including, for example, power or telecommunication bearers, or on information systems external to the organisation, Reuters news reports, stock reports from global based traders or status reports for military logistics from commercial suppliers could have serious implications for the organisation itself. The boundary of any organisation is no longer integral and is permeable to digital information. This is discussed below with particular respect to national sovereignty. Any strategy designed to safeguard an organisation's strategic information must, perforce, examine the external information linkages to the organisation's own systems.

Response to the Threat

Although the evidence for serious attack is limited, it is clear, however, is that few attacks are recognised as such by the users of a system. In the USA, the President set up a study into the "Critical National Infrastructure" and the UK Home Secretary has taken responsibility for the protection of electronic commerce within the UK[19]. How do we attempt to safeguard systems, whether military or civilian, if they are to be interconnected with other systems? To be able to assess the nature of protection required, formal *risk management* techniques will have to be developed to undertake the following:

a) Identify the vulnerabilities to information integrity both within and between systems (the modern tendency to increased networking has raised the potential for vulnerability exponentially);
b) Identify potential threats;
c) Quantify the threats; and,
d) Develop appropriate recovery strategies.

The development of suitable strategies for recovery is particularly important. Evidence from the US Department of Defense shows that there are a large number of attempts to penetrate systems, both military and commercial, and there is an increase in the frequency of attacks in the UK partly as a result of a greater degree of interconnectivity and also from the increasing sophistication of hacker tools. The US defensive IW programme has identified a three-phase approach: *protect, detect* and *react*. This approach allows systems to be protected, as far as is practicable, while appropriate systems are in place to detect intruders into the systems, with a suitable organisational framework designed to report intrusions and to be able to react rapidly to any intrusion, prevent further attack, ameliorate damage sustained and restore service as fast as possible. This process concentrates on the systems within an organisation and does not address the vulnerability of those systems outside the organisational boundary. Inevitably, it is not only very costly to protect all systems but also impractical and, in consequence, when looking at those systems which do not demand the highest integrity, the policy is to concentrate upon the "detect" and "react" elements. The determination of the appropriate information integrity is, therefore, of fundamental importance and will, in future, demand routine and rigorous ***"information audits"***. These will be similar to those already conducted within organisations for monitoring such strategic assets as finance and personnel. The audit will examine what information is required by the user, where the information comes from and how is it to be processed. It must address the information imported to an organisation from external systems and how the integrity can be assured. This must, perforce, be a dynamic process particularly where information requirements change rapidly in the light of operational requirements as, for example, within military structures. Much has been done over the last few years to understand the extent and influence of information systems as a part of the preparations for the Millennium. It will be important to use this data to maintain an understanding of the systems and their dependencies once the Millennium period is past.

Responsibility for Information Integrity

Who then, should take responsibility for ensuring the integrity of information? Should it be a matter of technical competence only, or should it be a senior management function? The implications of either a systems failure or information compromise could be so severe as to affect all members of staff within the organisation and, consequently, it is they, collectively, who should assume responsibility for their own informational integrity. Senior managers should determine the organisation's policy for information assets and identify how compliance with that policy will be measured and reviewed. The list of items to be considered includes the identification of those assets, the quality and quantity of information required and the protection of information from, *inter alia*, unauthorised access, abuse and misuse. Companies will need to examine the question of the increasing inter-twining of systems and the potential for the increasing dependence of one organisation upon the systems of another. A simple example would be the use of commercial telephone capacity to support an organisation's own network. Although the use of service level agreements should ensure the delivery of an acceptable service, there will be increasing scope for the use of such interconnectivity for nefarious purposes. This is already the case where organisations have connected up to, and extensively use, the Internet.

Information Warfare, Sovereignty and the Nation State

It is clear from the preceding discussion that the issue of information integrity is one that affects individual companies, multi-national corporations, governments and, ultimately, the relationships between nations. It is, therefore, instructive to consider the genesis of the concept of *information warfare*, the relationship between military information ethos and its civilian counterpart and to examine the implications for the sovereignty of the nation-state as questioned by H G Wells in the quotation at the head of this paper.

The Concept of Warfare

In any conventional attack upon a nation-state, it is clear as to what constitutes an *"act of war"*. Such an act would be followed by the outbreak of hostilities, as happened, for example, after the Argentinean forces invaded the Falkland Islands in April 1982. A broad definition of warfare was given by Malinowski (1968) as an *"armed contest between two independent political units, by means of organised military force, in pursuit of a tribal or national policy."*[20] Clearly, included in this definition would be the attacks on London by German bombers in World War II. These attacks, designed to destroy London's ability to function as a financial and commercial centre, were conducted by "*organised military force*"; as we have seen above, the capability to achieve that same end now exists without recourse to such force; would such an *electronic blitzkrieg* be considered to be an act of war and would the answer to this be different if the perpetrators were not a nation-state but a corporate body such as a multinational institution? This is more than an interesting, esoteric intellectual point: if a nation-state cannot determine whether or not it is at war or, indeed, determine who might be conducting a concerted action to damage, destroy or degrade important national assets like, for example, the City of London, the future stability of the nation-state could well be in doubt.

In such circumstances, which part of the nation-state should be charged with ensuring an appropriate defence and, if necessary taking appropriate action to recover the situation? Even within conventional operations, the co-ordination and liaison between those national and international bodies at the forefront of law enforcement has not always been comfortable, with extensive inter-organisation rivalry, lack of consistent communication and incompetent management of joint operations. Over recent years, considerable effort has been made to improve this situation. Within commercial organisations, they, themselves, must assume responsibility for safeguarding commercial secrets and taking any necessary legal action against other firms who infringe their intellectual property rights. Attacks within electronic systems, however, are not as clear-cut as those outlined above and, at present, there is no coherent view as to how both government and commerce should approach the problem.

The Concept of "Information Warfare"

Within the phrase "information warfare", the term *"warfare"* is pejorative and is reminiscent of John Fowles comment[21]:

> ***"Men love war because it allows them to look serious. Because it is the one thing that stops women laughing at them"***

Considerable play has been made over recent years about the idea of information warfare as a new and novel manner of attacking society. I do not believe that it is a new issue, but rather one that has been made more insidious by the ability to harvest large quantities of information and to disseminate it globally. The talk about *cyber-warfare* or *information warfare* centres upon the ability of an attacker to use an attack on a nation's information systems as an alternative to more conventional attacks. These can include those activities which do not normally fall within the purview of the military but reflect the increasing dependency of military systems on commercial and governmental information activities which are essential to the effective functioning of modern military operations. Modern technology is such that a deliberate, unauthorised and systematic attack could be launched against a nation state by another nation, by a commercial organisation or by a group of individuals. This could mean that the identity of the attacker could be unknown, or incorrectly identified (if the attacker is able to deceive the victim as to the true origin of the attack), at least in the early phases of a sustained attack. Such an attack might be launched from a wide variety of dispersed locations, all of which could be easily concealed within civilian society. The extent of the damage could be considerable where, for instance, there was serious degradation of the UK or US financial markets, it is possible that such actions could have unpredictable consequences in a world increasingly connected through global markets and trans-national corporations. This implies that an unknown computer assailant could cause considerable damage to the social, industrial and financial fabric of society, relatively secure in his own anonymity.

Information Infrastructure and the Nation-State

The terms *National Information Infrastructure (NII)* and *Global Information Infrastructure (GII)* have gained considerable currency in the past two or three years and reflect the organic and dynamic nature of the information and communication networks that have developed to support required levels of interconnectivity, integration and dependency. Despite the name, however, neither the NII nor GII exist as coherent or integrated systems. They are not owned by one company or agency, the government has little influence on their overall development and they are driven by consumer demand. They consist of a plethora of different systems, communication bearers, switches and facilities. There is a continual flow of information across international and organisational boundaries, the magnitude of which is increasing exponentially as the "global infrastructure" continues to evolve. The vulnerabilities of such systems are an unknown quantity and are unable to be properly assessed because of the dynamic pace of change and the inability to define the overall system.

Within the western world, London retains its role as one of the major foci for financial and commercial activity. Information flows are key to its success in retaining its primacy: financial markets are now controlled through 'real-time' global operations rooms electronically handling £ trillions per year; the damage to The Baltic Exchange, following the IRA bomb, caused considerable disruption to the UK's trade, shipping and commercial business. The activities of a single trader based in Singapore led to the demise of one of England's most prestigious banking houses and its ultimate take-over by a Dutch bank. The benefits accruing to the UK from the presence of these activities in London are considerable and reflected in our national balance of payments. It is clear that a number of nations, institutions and corporate bodies would like to see this status change and for other cities and nations to assume London's current mantle. It is possible that in the future some may be prepared to attempt to precipitate change by damaging the City's information infrastructure.

Sovereignty

Blackstone defined sovereignty as "*a rule of action prescribed or dictated by some superior, which an inferior was bound to obey."* Sovereignty is a concept central to the definition of a nation-state and its ability to define and control the way in which the state interacts with other nation-states. Historically, it was considered to be a secularising concept that reflected the decline of universal religious authority and actively encouraged belief in the territorial supremacy of the state[22]. Because there is no state beyond the state, no super state, as it were, each state is "sovereign" in international society, a law unto itself. In the aftermath of the First World War, US President Woodrow Wilson's fourteen points proposed a degree of circumscription on a state's degree of sovereignty[23], a process continued in the UN Charter which, although the UN was an association of sovereign states, reserved the right to intervene in the implementation of measures to enforce peace[24]. This was clearly evident in the actions taken against Iraq after the Gulf War and, more particularly, in the actions against Yugoslavia where the UN and NATO intervened in an internal matter. Elsewhere in Europe, the development of the European Union has, of necessity, required a transfer of sovereignty over certain issues to be transferred from nation-states to Brussels. It appears that what is often termed "national sovereignty" can, in reality, be considered to be made up of a number of overlapping layers which might include *ethnic sovereignty*, where political power only resides in citizens of a particular ethnic background; *linguistic sovereignty*, where the power resides in those who possess particular linguistic skills and *cultural sovereignty* where the characteristics of a nation-state are defined in terms of its cultural heritage and an assault on that heritage is considered to be an attack on the sovereignty of the state itself. This can be seen, for example, in the case of France were the government has been making considerable efforts to staunch the import of US culture, films, fast-food outlets, etc. Another area of traditional sovereignty has been that of *information sovereignty*, where a nation-state attempts to control the flow of information both within the state itself and across national boundaries. One consequence of the information revolution has been the increasing inability of governments to control the flow of images and ideas that shape human tastes and values. As the concept of *cyberspace* matures, it is clear that the notion of national boundaries will become increasingly irrelevant. How then can nations ensure the integrity of their systems, can governments insist upon minimum standards of ethical behaviour or taste in relation to material freely available to their citizens or will it be a free-for-all? The increasing globalisation of the information infrastructure also calls into question the concept of the nation-state where, for example, a company operating in one country, may well have a political affiliation with another nation or, indeed, increasingly may have no particular national affiliations but seek to fulfil corporate goals, whatever the cost might be to individual states. Paul Kennedy believes that "*the real "logic" of the borderless world is that nobody is in control - except, perhaps, the managers of multinational corporations, whose responsibility is to their shareholders, who, one might argue, have become the new sovereigns, investing in whatever company gives the highest returns*."[25] The concept of sovereignty, therefore, is under increasing pressure and is unsuited to the developing global information infrastructures. It will, however, continue to be used for the foreseeable future in the public discourse of international relations, offering diplomats a hallowed concept by which to carry on political debate, and representing, in a variety of situations, the ongoing struggles of a given people for self-determination and independence.

We have grown used to change, especially over the last decade, and yet, as human beings, we are continually unsettled by it. On whatever criteria one measures revolutionary change, it is clear that it summarises, most effectively, the world of today. The role of information in today's world is not qualitatively different from that of our forebears; we need information to be able to make decisions, to interact socially and to live. What has changed, however, is the quantitative nature of the information and the words of Stanislaw Lem, a Polish philosopher, who remarked that *"the era of great politicians has passed because the flood of information makes it impossible, too complicated, to make decisions."*[26] The issue of information integrity, when faced with such a flood of information, becomes critical and decision makers have to know what information is valid, what is corrupt, what is relevant and what should be ignored. Modern information processes, as we have seen, are vulnerable to an extent and information can be corrupted, degraded, destroyed or otherwise damaged. Although evidence is hard to collect, there have been a number of occasions when systems have been violated and financial or other damage occurred as a result.

The technological pace of change shows no sign of slowing and many of the problems highlighted will need to be addressed in the near future if we are to develop appropriate skills, models and methodologies to be able to quantify the threat to the systems of the future. The implications of doing nothing are so severe that this must be a problem for society in general, rather than restricted to a relatively narrow and focused group of information technologists. The knowledge spectrum, ranging from data, through information to knowledge, could be useful. We have concentrated upon information, information flows, information integrity and information management, but what we will need to focus our attention on will be the process by which this information is used by the human brain. We may well be assisted in this by the development of artificial intelligence and whatever might follow AI but the human aspect will remain. We must attempt to answer the difficult question as to how we can return to the decision makers, in whatever field they might be, the ability to take decisions with a degree of confidence as to the integrity and relevance of the supporting information.

NOTES

[1] H.G.Wells: *A Short History of the World,* London Penguin 1936.

[2] Deutch, John: ‘Oral evidence to US Senate Committee of Government Affairs’ - 26 June 1996 - reported in *The Times*, 27 Jun 96.

[3] Toffler Alvin and Heidi: *War and Anti-War - Survival at the Dawn of the 21st Century,* Little, Brown & Co. 1993

[4] Schwartau Winn: *Information Warfare - Chaos on the Electronic Superhighway,* Thunder’s Mouth Press, New York 1994

[5] Baumard: *From InfoWar to Knowledge Warfare: Preparing for the Paradigm Shift,* InfoWar Con, Brussels, May 1996.

[6] Fukuyama, Francis: *TRUST: The Social Virtues and the Creation of Prosperity,* London, Hamish Hamilton - 1995 pp 25-26

[7] *The Economist,* Survey of Defence Technology 10 Jun 95 p10.

[8] De Bono, Edward: *Parallel Thinking - From Socratic to de Bono Thinking,* Viking 1994 pp 215-25

[9] Peppard: *IT Strategy for Business,* Pitman Publishing 1993

[10] Rochlin, Gene ‘Iran Air Flight 655 and the USS VINCENNES’, article in: *Social Responses to Large Technical System*s, Amsterdam Kluwer Academic Publishers 1991

[11] Strassmann Paul: *The Politics of Information Management - Policy Guidelines*, The Information Economics Press 1995

[12] *Economist* article: ‘What Computers are for’, 22 January 1994 p 68.

[13] MORI poll conducted for Computer Associates reported in *Management Today* - June 1996 p78.

[14] *Business World*, 20 March 1994

[15] See for example Stoll, Clifford: *The Cuckoo's Egg,* London: Bodley Head 1990 for details of a KGB run hacker activity.

[16] Government Computing - April 1996. p 10

[17] Schwartau, Winn: *Information Warfare ,* op.cit. pp 96-98

[18] Reported in several places. See, for example, CSIS Report on Global Organised Crime pp50-52 op cit.

[19] Statement by Home Secretary to Parliament: Monday, 25 Jan. 1999.

[20] The Oxford Companion to Politics of the World Oxford University Press 1993 pp 962-965

[21] Fowles, John: *The Magus*, London Jonathan Cape 1977

[22] See: *Oxford Companion to Politics of the World* op.cit. pp 851-853

[23] Brogan, Hugh: *History of the United States of America,* Longman London 1985 pp495-495.

[24] Calvocoressi, Peter: *World Politics since 1945,* Longman, London 1991. pp122-124.

[25] Kennedy, Paul: *Preparing for the Twenty-First Century*, New York, Vintage Books 1994.

[26] Lem, Stanislaw: reported in *The Times Magazine* 11 May 1996.