

DRAFT Background Paper for Working Group 6:

MISUSE OF SCIENCE

By Michael Atiyah, Ralph Benjamin, Ana María Cetto, Matthew Meselson, and
Joseph Rotblat

SCIENCE is a dominant factor in modern society. The applications of science - whether intentional or incidental - affect us in every walk of life. The outcome of scientific research can strongly influence the norms of our civilization and even determine the fate of the human species. On the whole, the applications of science have been beneficial to human society and have greatly contributed to raising the quality of life, but they have also led to the development of means to destroy human society. While it is unlikely that scientific research itself would be a direct cause of war, it could become such a cause indirectly. In the military area, the build up of weapon arsenals - like that during the Cold War period - carries with it the danger of an accidental, or deliberate, launch, and thus a significant probability of the actual use of the weapons in combat. An attempt by one state to procure a new military capability may be seen by other states as a potential menace, leading to a pre-emptive war. Generally, the acquisition by any state of a weapon technology that gives it military superiority, is bound to create tension and may result in an arms race, with its attendant dangerous consequences. Similar threats may arise from non-military technologies. If some country acquires a new technology - such as biotechnology or information technology - which gives it great economic advantage, this may evoke deep resentment and fear in other countries, creating tension, strife, possibly leading to war.

In many cases the dangerous consequences of scientific research can be foreseen by scientists, and it is incumbent on them to take action to prevent such developments. Some such action is suggested in this Chapter, after a review of the areas of possible misuse of science.

SCIENCE WEAPONS OF THE FUTURE

FROM the dawn of civilization man's ingenuity has fashioned weapons of war. Spears, swords, gunpowder, machine guns were all in their way the application of

science and technology for military purposes. But it is only in the 20th century that the stakes have been raised to potentially catastrophic levels. Chemical, biological and nuclear weapons not only threaten the very existence of life on our planet, they also embody our most sophisticated science. The hope that Francis Bacon held out of science being pursued for the benefit of mankind has been perverted.

Interestingly enough, Bacon himself appears to have recognized the danger, since he said that some scientific discoveries were too dangerous to be divulged to state authorities and should be kept within scientific circles. Unfortunately, his wise words were not heeded, perhaps they were hopelessly naive and unrealistic. As a result, here we are at the end of the 20th century struggling to tame the tiger. Major efforts are devoted to international conventions to proscribe certain types of weapons and to control others. This arena is familiar to Pugwash and represents its *raison d'être*.

Could it have been otherwise? Take the case of nuclear weapons. There are those who argue that, in the very early days, after the principles of fission had been discovered, physicists worldwide could have agreed on the dangers of unleashing the power of the atom and refrained from urging their governments down that path. Certainly governments by themselves did not have the knowledge to make the necessary decisions. Scientists had to inform and prod them into action.

The same story has recurred at subsequent stages. For example, it was Edward Teller who pushed for the hydrogen bomb, after the Soviet test of an atom bomb deprived the USA of its nuclear monopoly.

So it is clear that scientists not only made the scientific discoveries but were actively instrumental in urging their governments to develop the weapons that the science made possible. This is not meant as an indictment but simply as a historical fact. In the circumstances, first of the war against Hitler and subsequently in the Cold War, some scientists thought it was their duty to act as they did.

Of course, science is an international fraternity. Scientists in different countries frequently know each other personally, they collaborate and work together in the pursuit of knowledge. One might hope that they could act collectively at the political level to the extent of not urging their governments to pervert their beautiful scientific discoveries. The fact that this did not happen in the past does not necessarily mean that, in the different circumstances of the future, it could not be brought about. This is the focus of this Chapter.

Predicting the future of science and technology is a hazardous undertaking, but past experience teaches us some general lessons. The rate of progress shows no sign of slowing down, either in fundamental discoveries or in their applications. One revolution succeeds another: computers, molecular biology, electronic communications. It seems safe to predict that there will be many more in the years to come.

Again history teaches us that while most scientific discoveries can benefit mankind some could also be put to evil purposes. Just to look ahead a little, once we have a clearer understanding of how the human mind works the possibility of “intellect warfare,” subverting the brain, might become a horrific possibility. Even closer may be “electronic warfare” whereby the elaborate computer-communications network on which the whole of society will rest could be sabotaged.

Unfortunately the future possibilities are endless. The very ingenuity that drives the scientist can also invent fiendish ways of misusing science. Since we neither want nor can stop scientific research (short of a Luddite reaction of cataclysmic proportions) we must face up to a hazardous future, in which an unending range of possible new weapons and methods of waging war seems inevitable.

In the following sections we review areas of new technologies where the misuse of science and technology may lead to war, but we start off with the nuclear weapons technology, in which continuing research may create new dangers.

Nuclear Weapons

The threat posed by the development of nuclear weapons was the prime reason for scientists setting up the Pugwash Movement; after 43 years, it continues to be the prime focus of concern. The problems have been widely documented in the literature, including several Pugwash monographs. This section deals mainly with one aspect, the role of scientists in the nuclear arms race, a role that continues well after the end of the Cold War.

During the four decades of the Cold War, thousands of scientists, on both sides of the Iron Curtain, used their knowledge and ingenuity to invent “gadgets” that would improve the performance of the weapons on their side or make more vulnerable the weapons on the other side. The role of scientists in maintaining the momentum of the arms race was succinctly expressed by Lord Zuckerman, who served as chief scientific adviser to the British government:

When it comes to nuclear weapons the military chiefs of both sides ... usually serve only as a channel through which the men in the laboratories transmit their views ... For it is the man in the laboratory who at the start proposes that for this or that arcane reason it would be useful to improve an old or to devise a new nuclear warhead ... It is he, the technician, not the commander in the field, who is at the heart of the arms race.

The motivations for scientists in these laboratories were described by Herbert York, the first director of the Lawrence Livermore National Laboratory:

The various individual promoters of the arms race are stimulated sometimes by patriotic zeal, sometimes by a desire to go along with the gang, sometimes by crass opportunism ... Some have been lured by the siren call of rapid advancement, personal recognition, and unlimited opportunity, and some have sought out and even made up problems to fit the solutions they have spent most of their lives discovering and developing.

The outcome of the scientists' efforts - mainly in the military research establishments in the USA and USSR, and to a much smaller extent in the corresponding establishments in China, France and the UK - was to amass huge nuclear arsenals, at one stage exceeding 70,000 warheads. Had these weapons been detonated in combat, it would have destroyed our civilization and conceivably also the human species, as well as many other living species. On several occasions during the Cold War, we came perilously close to catastrophe. One such occasion was the Cuban Missile Crisis of October 1962; a recent account of the event by Robert McNamara, containing new evidence, has shown that the peril was in fact much greater than was thought at the time.

With the end of the Cold War the arms race came to a halt and a process of dismantlement of nuclear weapons began in the USA and Russia, coupled with negotiations towards comprehensive disarmament, in accordance with Article VI of the Non-Proliferation Treaty.

For a variety of reasons, mainly political, this process has come almost to a complete standstill. At the same time, however, thousands of scientists are still employed in national military research establishments, particularly in the USA, backed by huge budgets. Ostensibly, the Stewardship Operations and Maintenance programme in the USA is aimed at improving the safety and reliability of the weapons in the arsenals. But only a small proportion of the 4.38 billion dollar budget for the FY2000 seems to be directly designated to the reliability of the weapons, and there is suspicion that the real purpose is to develop new types of precision nuclear warheads. Work on the improvement, or enlargement, of nuclear arsenals is also going on in other nuclear weapon states. The worry that this may lead to a new arms race cannot be dismissed lightly.

This worry gains more substance in the light of the move in the United States to abrogate, or substantially amend, the Anti-Ballistic Missile (ABM) Treaty of 1972, and to build up the National Missile Defense and Theater Missile Defense programmes, in which again many scientists will be employed. The arguments that have been put forward to justify the setting up of the new systems at a cost of \$10.5 billion, namely, the threat of a ballistic missile attack from a rogue state, seem so weak that some other reasons are bound to be suspected. In any case, the plans to tinker with the ABM treaty are strongly opposed by Russia and China. The latter may feel compelled to respond with measures that would involve further

expansion of its strategic nuclear forces. All this is likely to become an additional obstacle to the process of nuclear disarmament.

After more than half a century, a huge scientific effort is still being committed to military applications that may threaten the security of the world. This is a serious misuse of science, which the world community should not condone. The whole issue of the nuclear menace needs to be put back on the world agenda, with non-nuclear weapon states and NGOs urging the nuclear weapon states to honour their obligations under the NPT, an obligation specifically reaffirmed in 1995 when the Treaty was extended indefinitely.

At the NPT Review Conference in May 2000, the five nuclear weapon states again reaffirmed their “unequivocal commitment” to fulfilling all of their obligations under the Treaty. The deletion of certain qualifying terms - such as that the abolition of nuclear weapons is an “ultimate” objective or the link with general and complete disarmament - is certainly a significant step forward. However, the absence of a concrete programme for bringing nuclear arsenals down to zero, and no undertaking of no first use of nuclear weapons, imply that the current policies – under which nuclear weapons are seen as necessary for security – will remain in force.

In the scientific community too there are strong calls against the misuse of science and scientists. This was given expression by Hans Bethe, the most senior surviving member of the Manhattan Project. On the occasion of the 50th Anniversary of Hiroshima, he said:

As the Director of the Theoretical Division of Los Alamos, I participated at the most senior level in the World War II Manhattan Project that produced the first atomic weapons.

Now, at age 88, I am one of the few remaining such senior persons alive. Looking back at the half century since that time, I feel the most intense relief that these weapons have not been used since World War II, mixed with the horror that tens of thousands of such weapons have been built since that time - one hundred times more than any of us at Los Alamos could ever have imagined.

Today we are rightly in an era of disarmament and dismantlement of nuclear weapons. But in some countries nuclear weapons development still continues. Whether and when the various Nations of the World can agree to stop this is uncertain. But individual scientists can still influence this process by withholding their skills.

Accordingly, I call on all scientists in all countries to cease and desist from work creating, developing, improving and manufacturing further nuclear weapons - and,

for that matter, other weapons of potential mass destruction such as chemical and biological weapons.

Biotechnology Weapons

As already mentioned, every major technology - metallurgy, explosives, internal combustion, aviation, electronics, nuclear energy - has been intensively exploited, not only for peaceful purposes but also for hostile ones. Must this also happen with biotechnology, certain to be a dominant technology of the 21st century?

Such inevitability is assumed in “The Coming Explosion of Silent Weapons” by Commander Steven Rose, an arresting article that won awards from the US Joint Chiefs of Staff and the Naval War College:

The outlook for biological weapons is grimly interesting. Weaponers have only just begun to explore the potential of the biotechnological revolution. It is sobering to realize that far more development lies ahead than behind.

If this prediction is correct, biotechnology will profoundly alter the nature of weaponry and the context within which it is employed. During World War II and the Cold War, the United States, the United Kingdom, and the Soviet Union developed and field-tested biological weapons designed to attack people and food crops over vast areas. During the new century, as our ability to modify fundamental life processes continues its rapid advance, we will be able not only to devise additional ways to destroy life but will also be able to manipulate it - including the processes of cognition, development, reproduction, and inheritance.

A world in which these capabilities are widely employed for hostile purposes would be a world in which the very nature of conflict had radically changed. Therein could lie unprecedented opportunities for violence, coercion, repression, or subjugation. Movement towards such a world would distort the accelerating revolution in biotechnology in ways that would vitiate its vast potential for beneficial application and could have inimical consequences for the course of civilization.

Is this what we are in for? Is Commander Rose right? Or will the factors that thus far have prevented the use of biological weapons survive into the coming age of biotechnology? After all, despite the fact that the technology of devastating biological weapons has existed for decades and that such weapons were developed and produced during World War II and the Cold War, their only use in war appears to have been that by the Imperial Japanese Army in Manchuria more than half a century ago.

A similar history of restraint can be traced for chemical weapons. Although massively used in World War I and stockpiled in great quantity during World War II and the Cold War, chemical weapons - despite the hundreds of wars, insurgencies, and terrorist confrontations since their last large-scale employment more than 80 years ago - have seldom been used since. Their use in Ethiopia, China, Yemen, and Vietnam, and against Iranian soldiers and Kurdish towns, are among the very few known exceptions. Indications that trichothecene mycotoxins had been used in Laos and Cambodia in the 1970s and 1980s proved to be illusory.

Instead of the wave of chemical and biological terrorism that some feared would follow the lethal sarin gas attacks perpetrated by the Aum Shinrikyo cult in Japan in 1994 and 1995, and the fear that the arrival of the new millennium would be the occasion for acts of biological and chemical terrorism, there has been only a sudden epidemic of “biohoaxes” and several relatively minor “biocrimes,” confined almost entirely to the United States and undoubtedly stimulated by recent official and media attention to the potential for use of chemical and biological weapons in terrorism. In July 1999, five years after the Aum attack in the Tokyo subway, the US Federal Bureau of Investigation reaffirmed that

our investigations in the United States reveal no intelligence that state sponsors of terrorism, international terrorist groups, or domestic terrorist groups are currently planning to use these deadly weapons in the United States.

Whatever the reasons - and several have been put forward - the use of disease and poison as weapons has been extremely limited, despite the great number of wars and bitter insurgencies that have occurred since the underlying technologies of the weapons became accessible. Human beings have exhibited a propensity for the use, even the veneration, of weapons that bludgeon, cut, or blast, but have generally shunned and reviled weapons that employ disease and poison. We may therefore ask if, contrary to the history of other major technologies, the hostile exploitation of biotechnology can be averted.

The factor that compels our attention to the question is the possibility that any major turn to the use of biotechnology for hostile purposes could have consequences qualitatively very different from those that have followed from the hostile exploitation of earlier technologies. Unlike the technologies of conventional or even nuclear weapons, biotechnology has the potential to place mass-destructive capability in a multitude of hands and, in coming decades, to reach deeply into what we are and how we regard ourselves. It should be evident that any intensive exploitation of biotechnology for hostile purposes could take humanity down a particularly undesirable path.

At present, we appear to be approaching a crossroads - a time that will test whether biotechnology, like all major predecessor technologies, will come to be intensively exploited for hostile purposes, or whether instead our species will find the

collective wisdom to take a different course. An essential requirement is international agreement that biological and chemical weapons are categorically prohibited. With the Biological Weapons Convention (BWC) and the Chemical Weapons Convention (CWC) both in force for a majority of states, including all the major powers - and despite the importance of insuring compliance and expanding the membership of both treaties still further - the international norm is clearly established.

Whether the norm prevails, however, will primarily depend not on the activities of lone misanthropes, hate groups, cults, or even minor states but rather on the policies and practices of the world's major powers and, in particular, on their full compliance with, and active support for, the BWC and CWC.

The CWC prohibits the development, production, acquisition, transfer, and use of chemical weapons and requires the declaration and verified elimination of all chemical weapons and chemical weapons production facilities. The Convention entered into force in 1997 and by April 2000 had 132 States Parties, including all major states - the principal hold-outs being in the Middle East. Its unprecedented verification provisions include requirements: for declaration and internationally verified destruction of all chemical weapons and chemical weapons production facilities; for declaration and routine inspection of facilities that produce certain chemicals that might be diverted for chemical weapons purposes; and for challenge inspection of suspect sites, whether public or private and whether declared or not. During its first three years of operation the Organization for the Prohibition of Chemical Weapons (OPCW), the international operating arm of the CWC, had conducted nearly 700 inspections at declared sites, including 60 chemical weapons production facilities in nine states and 31 chemical weapons storage sites in four states holding some 8,000,000 chemical munitions and containers, most of them in Russia and the USA.

The 1972 Biological Weapons Convention entered into force in 1975. It was the first global treaty to prohibit an entire class of weapons. By April 2000, the BWC had 143 States Parties, the most important hold-outs again being in the Middle East. Unlike the Chemical Weapons Convention of 1993, it has no organization, no budget, no inspection provisions, and no sanctions - only a pledge by its States Parties never to "develop, produce, stockpile or otherwise acquire or retain" biological agents or toxins "of types and in quantities that have no justification for prophylactic, protective or other peaceful purposes," or equipment "designed to use such agents or toxins for hostile purposes or in armed conflict." The significance of the BWC lies in its statement of a clear norm - reinforced by international treaty - prohibiting even the development of biological and toxin weapons.

In Geneva, an Ad Hoc Group of its States Parties is negotiating a protocol to strengthen the BWC, including measures for verification. It is generally agreed that

provision should be made for challenge investigations of suspected violations, to be conducted by an international organization similar to the OPCW. There is also broad agreement that there should be mandatory declarations of bio-defence programmes, facilities that work with listed agents, and certain other facilities of particular relevance to the Convention. In order to encourage accuracy in declarations and deter prohibited activities from being conducted under the cover provided by apparently legitimate facilities, some states believe that declared facilities should be subject to randomly-selected visits by the international inspectorate, using managed access procedures like those practiced under the CWC to protect legitimate secrets. Other states, supported by pharmaceutical trade associations, particularly in the USA, have so far opposed such measures. Other important issues, including the substantive and procedural requirements for initiating a challenge inspection, assistance in protection against biological weapons, and measures of peaceful scientific and technical cooperation also remain to be resolved and are the subject of intense negotiation.

What can international treaties like the CWC and a strengthened BWC accomplish? First, they define agreed norms, without which arms prohibitions cannot succeed. Second, their procedures for declarations and on-site measures, including challenge inspection, pose the threat of exposing non-compliance and cover-up, creating a disincentive for potential violators. Third, their legal obligations and national implementation measures act to keep compliant states compliant, even when they may be tempted to encroach at the limits, eroding the overall norm. Fourth, treaty-based regimes legitimate and facilitate international action against non-compliance, thereby enhancing deterrence. And fifth, as membership in the treaty approaches universality, and its prohibitions and obligations enter into international customary law, hold-out states become conspicuously isolated and subject to penalty. In sum, a robust arms prohibition regime like that of the CWC, and the kind of BWC protocol that one may hope will emerge from the present negotiation, serve both to insure vigilance and compliance by the majority who are influenced by the norm and to enhance the deterrence of any who may be disposed to flout it.

The prohibitions embodied in the BWC and the CWC are directed to the actions of states, not individuals. Recently, interest has developed in the possibility of enhancing the effectiveness of these conventions by creating international law that would hold individuals - whether they be government officials, commercial suppliers, weapons experts, or terrorists - criminally responsible for acts that are prohibited to states by the biological and chemical weapons conventions. A treaty to create such law has been drafted by an international group of legal authorities. It is patterned on existing international treaties that criminalize aircraft hijacking, theft of nuclear materials, torture, hostage taking, and other crimes that pose a threat to all or are especially heinous. The draft treaty would make it an offence for any person, regardless of official position, to order, direct, or knowingly render substantial assistance in the development, production, acquisition or use of

biological or chemical weapons. A person, regardless of nationality, who commits any of the prohibited acts anywhere in the world would face the risk of prosecution or of extradition should that person be found in a state that supports the proposed convention. Such individuals would be regarded as *hostes humani generis*, enemies of all humanity. International law that would hold individuals criminally responsible would create a new dimension of constraint against biological and chemical weapons. The norm against chemical and biological weapons would be strengthened, deterrence of potential offenders, both official and unofficial, would be enhanced, and international cooperation in suppressing the prohibited activities would be facilitated.

What we see here - the non-use of biological and chemical weapons; the opprobrium in which they are generally held; the international treaties prohibiting their development, production, possession, and use; the mandatory declarations and on-site routine and challenge inspection under the CWC; the negotiations that may lead to strengthening the BWC with similar measures; and the possibility of an international convention to make biological and chemical weapons offences international crimes, subject to universal jurisdiction and applicable even to leaders and heads of state - suggests that it may be possible to reverse the usual course of things and, in the new century, avoid the hostile exploitation of biotechnology. Doing so, however, will require wider understanding that the problem of biological weapons rises above the security interests of individual states and poses an unprecedented challenge to all.

Information Technology Warfare

The orderly functioning of modern society is increasingly becoming dependent on the sound performance of a variety of computer systems. The security of a state could be fatally damaged if another state - or even a group of terrorists or individual hackers - designed methods of putting vital components out of action. For the purpose of this paper we define Information Technology Warfare (ITW) as an attack, undertaken or sponsored by a national or political entity, on the information technology component underpinning the national infrastructure.

Hacking into an allegedly secure Information Technology (IT) system can be as big a challenge as climbing an allegedly unscaleable mountain - but without the discomfort or risk. However, hacking motivated purely by bravado or impish mischief often leads to "passive" stealing of sensitive information, and perhaps selling it, and sometimes it also leads on to "active" falsification or disruptive intrusion, possibly causing quite serious malicious mischief. The dissemination of successful attack techniques, largely via the Internet, encourages others to develop these techniques further, and to exploit them individually, for fraud or blackmail, or on behalf of companies, for industrial espionage or even for sabotage.

It seems reasonable to assume that the same techniques are also being used for military intelligence collection. This may well include collecting information on Information Technology systems vulnerable to disruptive IT attack. In military operations, modern technology may be able to create near-total situation awareness, dissipating the traditional "fog of war." By enabling a military commander to deploy his forces to maximum effect (identifying which units to deploy where, when, how, against which objective) this would act as a very powerful "force multiplier." Conversely, success in disrupting or degrading the opponent's IT system - or other components - required for generating and exploiting this situation awareness would be a very effective "force divider." This aspect of a military conflict might most appropriately be called Military Information Warfare. The word "military" has been included to avoid confusion with the battle for hearts and minds.

Because of the critical importance of Military Information Warfare, military Command-and-Control systems are likely to be far better protected than any civil facilities. However, except in situations of active conflict, they are less important than those civil IT systems critical to the operation of the national communications, utilities, transport, financial and commercial infrastructure. In fact, this civil infrastructure is probably also essential to the logistic support of the national military capability.

Industry, the economy, governance and society as a whole are all increasingly interdependent, and all their elements depend increasingly on information technology. To minimize capital tied up in currently unused stocks, manufacture and wholesale and retail distributors are increasingly organized for an almost direct link from the factory to the point of sale. However, such "just in time" operation increases the IT dependence. Even an apparently insignificant IT function can have a vast impact on the organization served and, well beyond it, on those interdependent with that organization.

In particular, the national infrastructure of utilities: electricity, gas, water, sewage, rail, road and air transport and telecommunications are each dependent on several of the others, and all depend on telecommunication. Banking and financial services are, in effect, further critical national utilities. Local administration and central government, and the health and medical services are all dependent on the aggregate of these utilities, as is manufacture, commerce and civil life. Indeed, even the military services of few, if any, nations' could survive a breakdown of the civil infrastructure for more than a few days.

These complex interdependencies would cause a serious disruption of even a single key IT component, of one of the infrastructure elements, to give rise to very widespread chaos. Restoration of the normal operation of the nation's affairs would then probably lag by many days behind restoration of the relevant IT system itself. Thus, the impact of such an attack would last for at least days, quite likely weeks,

but - except for any consequential physical damage - probably not for months. Hence an attacker is likely to choose his moment for maximum effect.

Protection Against ITW. Having survived the Y2k scare, we must not forget the lesson of the need to create and maintain an awareness of responsibility for IT security and integrity by everyone, from professional designer, maintainer and IT manager to lay user and top management. The most obvious requirements are physical security of access to IT facilities, and redundancy, i.e. separately located spare processor capacity and duplicate records.

Encryption, if properly used, can not only protect the contents of a document, but can also authenticate the identity of its originator, its date and time, the integrity of its contents, and the identity of those able to decrypt and so read it. Finally all inputs and outputs from self-contained IT systems or networks may be routed through a set of “checkpoints Charlie.” The interface-control computers “manning” these checkpoints are known as “firewalls.” If these firewalls are *carefully designed and actively monitored and managed*, they can act as a “quarantine” barrier, keeping out infected, corrupted or unauthorized traffic. It is most important that the various security provisions impose minimal restriction or inconvenience on their users, but are difficult to penetrate, subvert or bypass.

Large organizations may create an internal "attack team", to probe for technical and/or procedural weaknesses in their system, correct those amenable to a hardware or software solution, and keep system managers and users alert to those needing *their* intervention. Smaller organizations could seek an equivalent service from a reputable external IT security consultancy.

All technical or administrative provision for IT security is a compromise, and it entails some financial and operational penalty. The conscious acceptance of that penalty, and acceptance of IT security responsibility, are issues of corporate culture, and require leadership at top level.

No combination of theoretically feasible, let alone financially affordable, countermeasures can guarantee complete immunity to attack. All that can be achieved is:

- to make an attack significantly harder to undertake,
- to make it very much more difficult to conceal,
- to limit its initial impact,
- to speed up recovery to full service,
- to improve the ability to diagnose the nature of the attack, and defend against it in the future,
- to enhance the prospect of tracing and identifying the attacker.

Reasonable capability in all these respects need not be unduly expensive, financially or operationally, *if incorporated in the system design or evolutionary updating concept ab initio*.

A more difficult issue arises from the fact that loss or interruption of service in one organization can have an impact far beyond that organization itself or its customer base, so that the protection of society or of the national interest may demand a level of technical investment and operational penalty, for the sake in IT security, going well beyond that warranted by the financial self-interest of the company or other organization. Hence government action may be required to create legal obligations and/or fiscal incentives for the provision of such IT security measures.

Neither major companies, nor IT and communications systems, nor the community of hackers are restricted by national boundaries. Hence it is also important to establish the widest practicable international co-operation, so that governments introduce similar levels of local IT security, interchange technical information and intelligence on IT crime, and outlaw IT attacks against targets outside as well as within their own boundaries. Hopefully, the self-evident need for international co-operation in this area may also act as a catalyst for good will and co-operation in other spheres.

At the present time, the infrastructure interdependencies are much more critical in the "first world" than in the "third". (This may change in the future, as countries with little prior investment, e.g. in their telecommunications infrastructure, may skip a technological generation.) The present asymmetry could reduce the balance of effective military capability between major and minor powers, with possibly destabilizing effects on world politics. It certainly will make it more tempting for terrorists or even governments in third-world countries to attack IT systems in the first world.

The overwhelming majority of military expenditure, throughout the world, will almost certainly continue to be devoted to lethal weapons. However, we should see a shift in the balance, from lethal weapons towards a higher *proportion* of defence budgets devoted to Military Information Warfare (MIW), in order indirectly to enhance the effectiveness of these lethal weapons. Some of these MIW resources may also create an incidental ITW capability, or indeed might conceivably be explicitly targeted against national infrastructures. These trends could perhaps be judged to reduce the scale of lethal weaponry "required", and hence might result in a welcome reduction in total military budgets.

As a weapon of attack by "the bad guys", ITW has the attraction that, whilst potentially immensely damaging, its use is far less morally abhorrent - or otherwise bad publicity - than other forms of warfare and, in any case, it is probably readily deniable.

Our analysis of the potential of information technology warfare leads us to the following conclusions:

- Modern society forms a network of highly-interdependent activities.
- Virtually all of these activities are directly or indirectly dependent on IT.
- Hence information technology systems critical to the national infrastructure may well become targets for ITW attacks.
- The most technically-sophisticated, and hence potentially most vulnerable societies are therefore likely to mitigate this vulnerability by planned "hardening".
- Such defensive measures have company/organization, national, and international dimensions, and hence may, indirectly, provide a stimulus for wider international co-operation in other spheres.
- The asymmetric nature of ITW vulnerability may have a significant impact on world stability.

Misuse Of Science In Non-Military Research

Even without misuse for military purposes, areas of current research such as biotechnology, or information technology, are likely to lead to profound controversies of economic, political, moral and spiritual nature, and may result in a polarization of society with its concomitant threat of tension, strife and war.

Genetic engineering, a rapidly expanding area of research, is one of the disciplines to give rise to serious concern about its likely impact on society. Most of the research in genetic engineering has beneficial applications, primarily in medicine. An outstanding example is the International Genome Project, which will be completed in the near future. It will provide knowledge of the DNA make-up of the three billion base pairs of the human genome, and their location on the 23 pairs of chromosomes in the normal human cell. This knowledge will be of immense value for improving human health, by enabling better diagnosis of disease and the early detection of genetic pre-disposition to disorders, such as certain types of cancer. It will also lead to improved methods of treating diseases, e.g. by providing personalized drugs, tailor-made for the individual patient, or by therapeutic cloning, in which stem cells are used to repair organs damaged by degenerative diseases or in accidents.

Apart from the medical applications, there are also likely to be very important beneficial applications of genetic research to nutrition: improving the quantity and quality of agricultural yield and/or the frequency of crops, diminishing dependence on rainfall, etc.

However, other outcomes of research in genetic engineering may be highly contentious and create serious difference of opinion on fundamental issues. Human cloning is such a divisive issue; at present there is a general feeling of abhorrence towards it, but many people may change their stand if the technology of animal cloning becomes more reliable. Another divisive issue is designer babies, achieved by adding (or deleting) specific genes to embryos to endow the born child with desired characteristics, such as greater physical strength, intellectual prowess, or artistic talent. There is already conjecture about new types of human species being developed by genetic engineering, significantly different from the species that has developed by the process of natural evolution.

Another incursion into the process of natural evolution might come from attempts to procure immortality, or at least a great extension to the human lifespan. At present this is biologically limited to about 120 years, largely by the number of divisions a given type of cell can undergo. But research on ageing has indicated ways to overcome this limitation, thus raising the spectacle of people living much longer, to 200 years, perhaps forever.

Apart from raising highly sensitive questions of a fundamental nature, all this is also likely to lead to a fateful polarization of human society, mainly resulting from the unequal access to the benefits of genetic engineering research. The technology required to achieve the advantages is very costly and thus available only to the very rich. The rich classes will not only indulge in luxuries; they will also live longer, enjoy better health, and produce offspring - either clones of themselves or purpose designed - with the qualities of Superman. Are we heading towards a new structure of society with two classes of citizen: the patricians and the plebs, in their modern equivalent?

This is not idle speculation or scare-mongering. Although some of the prognostications of the experts in the field sound like science fiction, they are not. They are within the foreseeable capabilities of the technology. The threats of conflict and war, inherent in a polarized society, have to be tackled, primarily by taking steps to ensure a more equitable access to the beneficial outcome of scientific research.

The threat resulting from the uneven distribution of the benefits of technology looms large also in another of its branches, the information technology, but in an aspect different from that described above under Information Technology Warfare.

The Internet is no doubt the fastest growing area of technological development. In the industrialized countries, it has already established itself as a new mass medium, overtaking radio and television. E-mail has changed the mode of communication between people; more letters are sent every day by electronic mail than by conventional letters and fax together. Business conducted via the Internet is growing at a fantastic rate. Information technology is producing dramatic changes

in all aspects of life. It changes market patterns and the rules of competition. It accelerates globalization in all its aspects. Technologically, distance and time are becoming almost irrelevant; the world is becoming a global village.

All this sounds very benign, but actually it contains a serious threat, a threat of similar nature to that discussed above under genetic engineering, i.e. unequal distribution of benefits. As with all new technologies, information technology is initially very expensive and thus accessible at the beginning only to those who can afford to pay for it. This is the case with computer technology. Ninety per cent of all computers are at present in the industrial world; mostly in the United States. The language of the Internet is almost entirely English, although this language is spoken by only ten per cent of the world population. The benefits of the information technology are therefore almost exclusively available to the English-speaking industrialized nations, resulting in the less developed countries falling back very rapidly in technological attainment.

In the area of information technology - with the many benefits likely to accrue from it - there is a widening gap between the rich and the poor countries, and some analysts see this as a portent of a catastrophe to civilization. As stated earlier, a widening gap between nations is a source of aggravation in international relations, a likely cause of tension, strife, and even war. Hence - it is alleged - the rapid growth of the Internet might itself become a cause of war: a war that has been described as between "the West and the Rest."

If we are to avert such a catastrophe, steps should be taken urgently to remove its source, the uneven access to the Internet. A worldwide campaign is necessary in the industrialized countries, to provide computers to the poorer countries. The entrepreneurs in the information technology, who have become very rich and are now spending some of the riches on philanthropic causes, should be persuaded to make their products more easily available to the poor countries, though this task should really be undertaken by international agencies, such as the World Bank or the IMF. It is also important for the computer scientists and technologists to put in a greater effort into development of techniques of automatic translation of Internet texts; this would help to overcome one of the biggest obstacles in the Internet, the language barrier.

Such measures will not only remove the threat of conflict arising from the uneven accessibility to the computer technology, but will also lead to the improvement of the economic situation of the poor countries. In addition, it will reduce ignorance, prejudice, and xenophobia in the world, thus contributing to the elimination of other causes of war, as discussed in other chapters of this volume.

Looking ahead to the more distant future, another misuse of science may result from advances in related subjects: robotics and nanosecond technologies. Attention to this danger was recently drawn in a paper by Bill Joy, a senior scientist in a top

computer technology company and a pioneer in the development of software technologies.

Starting from the plausible assumption that the present rate of advance in computer capacity - a hundred-fold increase every decade - will continue, he foresees that the million-fold increase in 30 years will result in the development of "thinking" computers, robots endowed with artificial intelligence and which can also replicate themselves. The uncontrolled self-replication is one of the dangers in the new technologies, with the risk of substantial damage being caused either accidentally or deliberately. Unlike the known weapons of mass destruction - nuclear, chemical, and biological - whose design and manufacture requires large-scale activities or rare raw materials, in the new danger "knowledge alone enables the use of them," according to Bill Joy. In this sense, the threat from the development of self-replicating robots is greater than mankind has experienced before. Although the threat is still in the distant future, scientists should already now start a serious discussion of ways to deal with it. In seeking such ways Bill Joy concludes:

The only realistic alternative I see is relinquishment: to limit development of the technologies that are too dangerous, by limiting our pursuit of certain kinds of knowledge.

Voluntary constraints on certain areas of scientific research, by an ethical code of conduct for scientists, rather than by legislation, are among the various ways to prevent the misuse of science. This will now be discussed.

THE POLITICAL SCENARIO

IN the face of the many dangers arising from the misuse of science, what can, and should, scientists do?

Since we are considering not science *per se*, but science in a political and military context, much will depend on the political scene in the world. Any predictions must take account of the political realities.

There are two extreme scenarios. The optimistic one is that, in the near future, we shall achieve an effective world government where war has finally disappeared and all conflicts are settled peacefully within the law. This should be our long-term objective and in course of time we might have something approaching this utopia. When this happens our worries about the misuse of science will evaporate. There will be no wars in which to misuse science. However, we must make sure human civilization survives, without catastrophe, until then.

The other extreme scenario, which is regrettably more likely, is the pessimistic one in which we revert to a world rent by major divisions, a world of Hitlers and Stalins and constant confrontations. In this scenario, a repeat of 20th century history with science being misused seems highly probable. The international fraternity of science would have great difficulty surmounting such barriers.

The most likely scenario for the 21st century is somewhere in the middle. Conflicts of various sorts will continue, war will not disappear overnight and politicians, the world over, will continue to act much as they do at present with narrow national interests predominating. World government is not yet on the horizon, but the worst forms of dictatorships may be over. In other words we are doing as the best weather forecasters do and predicting “the same tomorrow.”

In these circumstances, where international politics is not totally polarized the prospects of the world scientific community getting together with a view of preventing further misuse of science becomes possibly realistic. In the untidy but not totally hostile world that we now have, the scientific community has a chance of saving its soul. We could try to avert the 21st century equivalent of the nuclear bomb, whatever that might be. If this is indeed a feasible project, we should try to find appropriate mechanisms, in fulfilment of our social responsibility.

STIRRING THE ETHOS OF SCIENTISTS

AS stated earlier, a large part of the investment of human efforts and financial resources in science during the whole of the 20th century has been geared towards war. The consequences of this aberration are immense piles of weapons of mass destruction, some of which have been deployed, and many others that are still menacing our precarious existence.

This in itself would be a reason powerful enough in favour of promoting a serious ethical commitment from scientists. There are however other motivations to do so, such as:

- the widespread public mistrust in science, and the need for the public to be informed of the potentialities of science and its applications;
- the present trends of privatization, patenting and secrecy of the knowledge that has been created by science;
- the old and new challenging problems faced by humanity (environmental problems, health problems, etc.), which require for their solution a dedicated scientific effort;

- the need for scientists to be alert to possible dangerous uses and applications of their work, especially those that threaten human health and the environment;
- the need to increase the scientific effort towards the benefit of human beings and nature.

Except for industrial and military research science was until recently predominantly academic, following its own internal rules and norms. The search for truth, objectivity, testability, the advancement of knowledge, freedom of thought, those are the kind of values that scientists have cherished most within academic circles. There has been little space for explicit ethical debate in academia; in fact, ethics has been traditionally considered to be a polluting element - along with political, philosophical, ideological or simply humanitarian considerations. Scientists have been supposed to *do* science, not to *reflect on* science and its consequences outside the scientific domain. Academic freedom has meant freedom to move within well-established scientific borders. For a long time, only few scientists ventured to openly trespass these boundaries for reasons of ethics.

Industrial scientists did not have this academic freedom; rather than to search for truth or to understand the world, their mission was to produce useful knowledge and apply it with a specific objective. These scientists would be much more likely to encounter ethical dilemmas, especially when considering issues external to their work, such as public safety, human welfare, etc. When it came to producing useful results and effective applications, however, such ethical dilemmas represented an obstacle to efficient performance. Their priority was the welfare of their enterprise, not human welfare.

However, as mentioned earlier, some consequences of the applications of science have been too serious to be ignored by the scientists themselves. In addition, society has become much more concerned about science, and demands responsiveness, transparency and accountancy from the scientists. Scientists are more and more forced to justify their work in terms of its social and economic impact, in order to get it funded, or even to get paid for their work.

The above does not apply just to industrial scientists; it is clear today that any scientific research, however remote from everyday reality - even if apparently irrelevant - is prone to lead to some application of human or environmental consequence. Ethical considerations cannot any more be left to a handful of bold or eccentric scientists with their “personal” problems of conscience. Ethics is, indeed, not just a personal issue; it is a collective one, implicating all scientists in their individual capacity as well as the scientific institutions.

This means, then, that an integral approach to the issue needs to be developed, simultaneously addressing it at various levels and with specific tasks. Some of the following suggestions are controversial, but all need to be considered seriously.

Scientific academies and societies should:

- include ethical considerations in their terms of reference, to be followed by their members and applied to all their activities;
- establish independent ethics committees, with members who are competent both in science and in ethics, to examine potentially harmful implications of proposed projects, give advice to governments and other institutions on ethical matters, etc;
- promote studies and organize open debates on ethical issues.

National science and technology authorities should:

- promote and respect the establishment of the independent ethics committees with the participation of representatives from the academic community, industry and other research environments;
- formulate general policies to be adopted nationwide and, when pertinent, be subject to legislation.

Research institutions should:

- establish codes of conduct that set ethical norms for themselves and for the work carried out by their scientists;
- promote, respect and defend scientists' compliance with ethical codes of conduct;
- promote and advance ethics of science as a field of study.

Universities should:

- include relevant aspects of ethics in the curricula of the various scientific disciplines;
- establish pledges to be taken individually by students at their graduation, along the lines of the Hippocratic Oath taken by medical graduates.

Funding institutions and agencies should:

- submit research projects to pertinent revision by ethical committees, before funding them;
- not fund projects that can have an outcome detrimental to human beings or the environment. *[N.B. The practicality of this recommendation has been questioned by some of us; this is clearly an issue that calls for more detailed discussion.]*

Scientists should:

- make an effort to understand and properly explain the scientific facts underlying specific situations, as well as warn about the potential harmful consequences of new discoveries or developments;
- contribute to the establishment of codes of conduct and commit themselves to their compliance;
- show solidarity with those colleagues who take a firm ethical (and validated) position by whistleblowing, thereby putting their work or their freedom at risk.

International organizations should:

- organize fora for discussion of issues of science ethics among experts and representatives from different countries;
- work out and adopt international guidelines and norms of conduct to orient scientific research to the benefit of humankind.

This list could be made much longer. There are of course many conflicting issues that arise in practical reality, such as: management of pertinent scientific information, autonomy of scientists, levels of decision-taking and sharing of responsibility, dealing with uncertainties and unforeseen events, varying sets of morals between different cultures, disciplines or professions, etc. This is why it is so important to maintain the ethical debate alive and to take ethics in science as a serious matter for analysis.

In recent times there have been some interesting developments that indicate a rising interest in science ethics, probably to a large extent due to the growing concern about increasing damage to the biosphere, and to as yet unknown consequences and implications of scientific and technological progress in domains of genetics, informatics, and other new branches of science. Among these developments, the following need to be mentioned:

- The creation in 1996 by the International Council for Science (ICSU) of a Standing Committee on responsibility and Ethics in Science, SCRES
- The adoption in 1997 by the General Conference of UNESCO of two principal documents: the *Declaration on the Responsibilities of the Present Generations Towards Future Generations* and the *Universal Declaration on the Human Genome and Human Rights*
- The establishment in 1998 by UNESCO of a World Commission on the Ethics of Scientific Knowledge and Technology.
- The World Conference on Science in 1999 in Budapest organized by UNESCO and ICSU, which provided an important framework for various related events.

A proposal that aroused much interest and debate at this Conference, was to work on a pledge for young scientists to be taken at graduation. It has received many individual responses, and important scientific associations are giving a collective response, such as the European Physical Society (by preparing a position paper on the subject) and the AAAS Committee on Scientific Freedom and Responsibility (by planning a seminar for the US scientific community). In fact, a number of bodies have already adopted different forms of pledges or codes of conduct, which can be used as a basis for a serious effort to extend the idea of the pledge to universities and institutions worldwide. Whether it is possible to arrive at a universal pledge that is meaningful, or rather the pledge will have to find a plurality of local expressions, is not clear at this stage.

An Early Warning Committee

In addition to the general programme outlined above (and partly overlapping it), we are interested in considering specifically how scientists collectively could forestall dangerous future misapplications of science. Roughly we have in mind a high level international "Early Warning Committee" whose brief would be to look ahead and identify dangerous trends, areas where science was offering new military possibilities. Once clearly identified there would then have to be political action, an appropriate convention with safeguards as necessary, to prevent their possibilities being realized. It might sound a difficult process but it is surely easier to prevent things starting than, as now, to try to stop things after they have happened. The difficulty is not primarily technical, it is more a matter of political will and scientific organization.

It may be that such a project is unrealizable because "looking ahead" is so difficult, but the idea seems worth pursuing and even partial success may be better than inaction.

On the negative side, and this merits serious discussion, is whether drawing attention to a dangerous possibility is itself dangerous. "Letting sleeping dogs lie" might be safer. Much would depend on the precise procedure followed, including the publicity given. A low-key process, one which did not make widely alarmist predictions, would obviously not raise the same risks as a high-profile campaign.

The nature of our putative "Early Warning Committee" and of its relation to the international political process also needs careful thought. There are a number of obvious possibilities. It could be:

1. a committee set up by the United Nations and responsible to the Secretary-General (and the Security Council);
2. a committee of ICSU, more clearly under scientific control;

3. a committee formed collectively by leading scientific Academics of the world;
4. sponsored by a number of leading universities.

These different possibilities indicate possible positions on a political-scientific spectrum. There may be clear advantages in having a committee under control of the international scientific community. There would be less bureaucracy, it would be easier to set up and there would be less political interference. On the other hand, if the committee is to have a real effect it needs to be able to operate through the political system. “A gentleman’s agreement” is not as good as a binding international convention.

So there are important questions of balance that need to be addressed. It is possible to envisage a two-step process in which the international community, perhaps through a few institutions (as in (3) or (4)), takes the initiative in setting up a committee. Later, once the committee has identified some hazards, the United Nations might be brought in.

Considerable thought has to be given to the precise terms of reference of the committee. Clearly, at the present, it could not attempt to ban all scientific-military research. It should focus on new and potentially devastating possibilities, a decade or so down the line, where work has not seriously started and where a stop can be realistically called.

Even without a formal “Early Warning Committee” it is open to scientists to identify dangerous trends and to try to take appropriate actions by voluntary means. This may work, but it may not be adequate in the long term and a more formal mechanism of the kind outlined should be examined.