BIOTECHNOLOGY, BIOTERRORISM + BIOSECURITY

Advances in genetics and biotechnology offer great promise in the fight against infectious diseases. But the same technologies will also increase the threat from bioterrorism. Governments must accord 'biosecurity' a higher priority in defence and foreign policies to reduce the risk of major societal disruptions and international political instabilities caused by infectious diseases, whether of natural or malignant origins. Longer term, technological progress will expand the biothreat spectrum beyond microbial attacks to embrace diverse manipulations of key body functions, including cognition. Meeting these challenges will require profound changes in national security policy, military doctrine, intelligence acquisition and law enforcement, a renewed focus on public health and disease surveillance, the evolution of new private-public partnerships to produce new diagnostics, drugs and vaccines and improved international co-operation to outlaw biological weapons.

By Dr George Poste

Concepts of war and the origins of violent conflict are never constant. The al-Quaeda terrorist attack on America heralds the dawn of asymmetric warfare. America and its allies can no longer rely on massive conventional military power for effective defence against determined enemies who, despite inferior economic and military resources, will seek to bypass military defences and strike directly at civilian targets to provoke terror and erode public confidence in their political leaders. The rise of asymmetric warfare, and the consequences of unpreparedness to fight by new rules, were forewarned by prescient commentators. The 1999 report of the US Commission on National Security concluded with ominous clarity: "America will become increasingly vulnerable to hostile attacks on our homeland and our military superiority will not protect us. Americans will likely die on American soil, possibly in large numbers".

Political timidity in failing to confront the escalation of terrorism over the past four decades has emboldened terrorist tactics. Western national security policies and military doctrine now face a costly duality: sustaining the global strike capabilities of conventional forces while simultaneously implementing the radical changes needed to protect civilian populations and domestic

infrastructure against terrorist attacks by agile, decentralised groups of non-state actors albeit likely aided by rogue nations.

Current defence priorities and governmental organisations are ill-prepared to address these disruptive changes in the threat spectrum.

'Blowback': the technological dependency of industrialised nations increases their vulnerability to terrorism

Defence against asymmetric warfare must accord primacy to the 'blowback' dilemma whereby the advanced technologies that bestow economic and social comfort on the G8 nations also generate a massive range of vulnerabilities, both by offering a diverse array of targets for terrorists and by providing them with new modes of attack. From the bronze age to the nuclear age, technology has been a catalyst in reshaping the pattern of conflict. Many new technologies have 'dual-use' applications, offering simultaneous opportunities for beneficent and malevolent uses. In the 20th century weapons technology was dominated by the principle of 'big bang: big metal' in which advances in physics and engineering were harnessed to devise weapons of increasing explosive destructiveness delivered with increasing precision from air, land, sea and outer space. The economic and technical resources needed to develop these weapons are beyond the capacity of smaller nations and terrorist groups who oppose the current military, economic and cultural dominance of the West. The focus of these protagonists logically shifts to exploring how new technologies could be exploited to disrupt and paralyse the economic and cultural fabric of Western society. As the 21st Century progresses, national security and military strategies will be shaped increasingly by new threats arising from the rapid expansion of research horizons in computing and biotechnology. Cyberterrorism and bioterrorism offer particular appeal to the practitioners of catastrophic terrorism by providing the capacity to inflict devastating damage at very low cost relative to conventional weapons.

The biological arsenal

A dauntingly large number of infectious organisms and biological toxins, each with very different actions and effects, can be used to attack people, animals and plants. The pathogens viewed as the most likely biothreats for humans encompass all branches of the microbial kingdom including: bacteria (anthrax, plague, brucellosis, tularaemia); rickettsia (typhus, Rocky Mountain spotted fever, Q-fever); viruses (smallpox, influenza, dengue fever, various encephalitis viruses and the haemorrhagic fever agents, Ebola, Marburg and Lassa); fungi (coccidiomycosis); and toxins (botulinum, staphylococcus enterotoxin, shigella, ricin, aflatoxin). Biothreat agents are typically ranked accordingly to their lethality, ease of dissemination and ability to spread from person-to-person (contagion). The NATO biowarfare defence handbook lists 31 human pathogens of concern. The Former Soviet Union (FSU) bioweapons programme accorded priority to 11 of these agents, with smallpox, anthrax, plague and botulinum toxin being seen as the most dangerous. Anthrax (non-contagious) and smallpox (highly contagious) are accorded primacy in the bioweaponeers arsenal because of their lethality, facile spread by aerosol, ease of large-scale manufacture and stable storage over long periods without loss of potency.

Agricultural targets and the food chain are equally vulnerable but have been given less attention by politicians and the media. Natural disease outbreaks affecting livestock and crops illustrate how the introduction of a new pathogen or parasite can cause profound economic and cultural disruptions in agricultural communities and trigger trade barriers to agricultural exports. Foot and mouth disease virus, Rinderpest, anthrax and African Swine Fever loom large as candidates for agricultural bioterrorism. Similarly, the extensive range of infectious agents that affect wheat, corn, rice and other key food crops could inflict major economic disruptions.

Bioagents can be disseminated in multiple ways. Aerosols are the most effective for contaminating large areas and in achieving high rates of infection. Contamination of food supplies and water provide productive avenues for spreading certain diseases and toxins. The deliberate release of infected insects, plants and animals poses an easy way to attack the agricultural sector. Some consider it only a matter of time before deliberately infected human vectors will emerge as the bioterrorism counterpart of the suicide bomber, seeding disease in aircraft, public transport, shopping malls and other public venues where people congregate.

A major obstacle in the development of robust biodefences is that new technological advances will always give the attacker the advantage by enabling them to expand the range of bioagents and distribution methods to circumvent existing defences. Biological agents provide the practitioners of asymmetric warfare with weapons that are cheap,

hard to detect, difficult to attribute and, above all, with the power to terrorise disproportionately to the number of actual casualties.

Recent experiences with the West Nile virus and anthrax incidents in the USA and foot and mouth disease in the UK highlight the challenges in detection, diagnosis, containment and attribution. These incidents each revealed substantial gaps in our preparedness capabilities to confront a major bioterrorism attack.

Assessing the bioterrorism threat: exaggerated fear or ignore at our peril?

Any answer to this question is at immediate risk of succumbing to H.L. Mencken's dictum: "Of course every complex problem has a simple solution and it's invariably wrong!". The only current certainty is uncertainty. We are entering geopolitical and technological landscapes that we do not yet understand. Past precedents offer scant instruction about the future. Politicians and the public want certainty and a clear course for action. The reality, albeit ugly, is that the union of the new realpolitik of catastrophic terrorism with advances in the life sciences will spawn entirely new kinds of terrorist attack that will demand novel defences.

Constructive analysis of the bioterrorism threat is hampered by polarised views and reliance on outdated and uncertain knowledge. One school of opinion holds that the threat is exaggerated. They dismiss the threat on grounds that bioagents are too difficult to produce and use, that terrorists have easier ways of causing havoc than using biological agents and that moral constraints will preclude their use against civilian populations. Until September 2001 similar aphorisms of denial were equally common in dismissing any prospect that hijacked US airliners could be used to destroy the architectural icons of America's economic and military strength until audacious violence showed that those opposed to the West are prepared to play by entirely new rules.

The alternative view holds that it is inevitable that bioweapons will be used against the US and its allies and it is no longer 'a question of if, but when'. Advocates of this pessimistic view argue that there is no instance in history when a new weapon with the potential to radically alter the balance of political and military power has not been deployed.

The middle-ground between the optimists and the doomsayers is that bioterrorism is currently a 'low probability, high consequence' threat. Even if the current risk of bioterrorism is lower than many other kinds of terrorist assault, the more important question is whether the assessment of current risk is a meaningful indicator of future risk. Will predicted trends in global geopolitics and technology make it more or less likely that bioattacks will occur? The available evidence is not reassuring and the prospect that bioterrorism will become increasingly common can no longer be confidently denied.

Those who argue that bioweapons are too difficult to develop or impractical to use must know something that the Former Soviet Union (FSU) overlooked. The FSU Biopreparat programme developed massive quantities of bioagents for use against humans, plants and animals. Even with the crude technologies available three decades ago, the FSU successfully engineered organisms with enhanced virulence and dissemination capabilities and with increased resistance to drugs and vaccines.

The politics of denial must be replaced by a more urgent reality. Denial ignores the implications of the dramatic progress in biotechnology and the accelerating pace of genetic discovery. It ignores the reality of the extent to which biological weapons capabilities, both actual and potential, have spread across the globe. It ignores the historical reality of the impact that each new generation of technologies has had on the evolution of warfare. It ignores the political reality of the strategic leverage that new technologies offer to the protagonists of asymmetric warfare. Finally, it ignores the reality of the intrinsic uncertainty of the future, all the more so in an era characterised by unprecedented technological changes, most of which were not predicted even a decade ago.

and graduate-level courses around the world. Copious volumes of information pertinent to bioterrorism are available in non-classified scientific journals and on the Internet. In addition to the rapid growth in biological knowledge that could be usurped to create bioweapons, the number of facilities and trained personnel capable of undertaking sophisticated genetic manipulations has expanded substantially, including in nations viewed as sponsors of terrorism and with declared hostility towards Western interests.

The fate of trained personnel and pathogens from the FSU bioweapons programme is of particular concern. The FSU civilian Biopreparat bioweapons effort employed at least 70,000 people. The nature and scale of parallel R&D activities undertaken within FSU military laboratories is still unknown. Concern persists that elements of the military programme may not have stopped. There are reports of FSU scientists working in Iraq, Iran and North Korea. Security at FSU bioweapons facilities is lax and economic pressures have increased the risk that both personnel and biological specimens are available to the highest bidder. In spite of these risks, the 'loose bug' problem in the FSU has been given far less emphasis than the 'loose nuke' problem in the weapons threat reduction programmes funded by Western governments. These have focused almost exclusively on the security of the FSU nuclear and chemical arsenals.

New technologies and expansion of the biothreat spectrum

The dramatic pace of research progress in biology and medicine is outstripping the ability of society to assess the full implications of genetics and other powerful biotechnology tools. The intellectual transformation of the life sciences from merely describing biological phenomena, devoid of any insights into the underlying control processes, into a mechanistic discipline in which the genetic networks that choreograph complex biological processes are revealed in exquisite detail holds great promise for improvements in medicine, agriculture and other beneficent uses. But the same knowledge can also be exploited for less altruistic ends.

The rapid expansion of knowledge about the genetic control of microbial virulence epitomises the dual-use dilemma. Modern genetic techniques provide straightforward ways to engineer pathogens to introduce properties that enhance their utility as offensive weapons. These include safer handling during production, longer storage stability, easier dissemination, altered host range, enhanced infectivity and person-to-person spread, increased difficulty of detection, resistance to drugs and vaccines, improved survival in diverse environments and greater resistance to inactivation by decontamination agents. On a longer timescale, the risk of more exotic manipulations must be entertained. These include the use of entirely synthetic genes that enhance microbial virulence or the ability to circumvent available treatment or protective vaccination. Genetic methods also provide routine ways to construct 'hybrid' organisms that combine the injurious properties of multiple organisms and, even more extreme, the perverse construction of organisms whose purpose is not to cause death and injury by infection but to instead disrupt critical body functions such as hormone production or trigger the immune system to destroy the victims' own tissues (autoimmunity). Non-living targets will also likely enter the list of future vulnerabilities. The genesis of micro-organisms able to degrade ubiquitous materials such as petrochemicals, plastics, rubber or computer components could cripple vital military and societal infrastructure with devastating economic and social consequences.

In short, the threat from bioterrorism is credible and is likely to grow courtesy of the accelerating pace of biotechnology research. In contrast to the recent past, when only a few industrialised nations had the technical capabilities to pursue the production of biothreat agents, at least a dozen nations are believed to be engaged in developing bioweapons. Biological terrorism is now within the grasp of small, modestly equipped groups or even lone individuals. A terrorist group can wreck havoc on civilian populations with far smaller quantities of bioagent than would be required to attack large numbers of combat troops on the battlefield. As the power and scope of the life sciences expands it can be anticipated that the potency, diversity and accessibility of biological weapons will increase in parallel. Over time, and the interval involved will be measured in years not decades, advances in biotechnology will facilitate the acquisition of bioweapons by enemies who will not hesitate to use them to neutralise their asymmetric disadvantage against the conventional military power of the West.

The unique complexities of biodefence

Nuclear, chemical and biological threats each pose unique complexities. But the detection, consequence management and control of bioassaults is by far the most complex. These difficulties reflect several unique aspects of the biothreat problem.

The wide range of potential bioterrorism scenarios complicates defence planning and preparedness

The diversity of the biothreat inventory, the ubiquity of diverse targets and the ability of the attacker to use highly different routes of dissemination dictate that it is impossible to provide a uniform picture of the biothreat problem. Bioweapons can cause widely differing levels of carnage, ranging from transient illness and full recovery to extreme scenarios in which millions of people or animals die and/or suffer chronic sequelae. The breadth of the potential attack scenarios greatly complicates response planning and is a major obstacle to efforts to detect and interdict potential bioterrorist attacks before they occur.

The 'stealthiness' of bioattacks accords the attacker the initial advantage and delays mobilisation of defensive responses

In assaults by nuclear and chemical weapons, as with conventional explosives, the scale of the damage is evident immediately. In contrast, the effects of a bioattack are unlikely to be recognised quickly. Depending on the method by which a pathogen is released and dispersed, initial infection of victims can occur within a few hours (for large airborne releases) or extend over weeks or months (for release by contagious vectors). The initial symptoms of many of the more likely human biothreats are indistinguishable from commonly occurring respiratory tract infections such as colds and the 'flu. Early cases are thus easily misdiagnosed. The inevitable delay before an attack is detected gives the attacker the advantage and hinders the rapid mobilisation of containment actions. Delay also allows contagious agents to expand to additional victims and to spread geographically beyond the initial point(s) of release.

Prevention of bioattacks before they occur is obviously the most desirable situation. Unfortunately, there are substantial shortcomings in current intelligence gathering capabilities for the reliable identification of illicit production of bioagents. This is reflected in the failure to detect the offensive bioweapons programme in the FSU, conducted on a colossal scale for more than two decades. Substantial R&D investment has been made by the US since the Gulf War to develop sensors to detect biothreat agents in the external environment before they infect people. However, this is a difficult technical challenge and progress to date has been slow. The routine use of environmental sensors to detect illicit production of bioagents or to warn large populations of a pending bioattack is viewed as unlikely for at least a decade, and possibly longer. For the foreseeable future biodefence will depend primarily on strengthening measures to achieve faster clinical diagnosis of a bioincident once it has begun and thereby accelerate deployment of containment actions to limit casualties and minimise the economic, social and political consequences.

The fragility of current public health and medical biodefence capabilities

The first indication that a bioattack has occurred will likely come only after astute GPs or medical centres report that they are seeing unusual numbers of ill people seeking care or from similar reports from agricultural surveillance systems for attacks on livestock or crops. It may also be difficult in the early stages of an incident to determine whether disease is due to a bioterrorist attack or to natural causes. Equally distressing is the lack of comprehensive electronic surveillance systems in both the medical and agricultural sectors to provide accurate real-time reporting of abnormal patterns on a national basis. Public health officials would be hard pressed today to provide decision-makers with reliable and up-to-the minute estimates of the location or scope of any bioattack, to maintain accurate counts of the number of exposed individuals and affected victims, and to assess the effectiveness of interventions in containing the incident.

Rapid recognition that a bioattack has occurred is hindered by the lack of diagnostic tests for rapid identification of bioagents. Existing tests are slow and add to the delay before a definitive declaration of a bioincident can be made. In addition, diagnostic laboratory tests for many of the anticipated biothreat agents are either not yet developed or available only in a few highly specialised academic and military laboratories. The majority of hospital and commercial medical diagnostic laboratories in the US and Europe are not equipped for the routine testing and isolation of biothreat pathogens. In addition, the ability of the few specialised microbiology testing laboratories that perform such tests to cope in the face of the dramatic escalation of testing demands once a confirmed incident has occurred is a further cause for concern. Similar deficits in diagnostic testing capacity also apply to surveillance against agricultural terrorism.

A mere few hundred casualties requiring intensive care would overwhelm the entire hospital network in any major city in America or Europe, irrespective of whether the cases were caused by a bioattack or any form of disaster. Most hospitals

are woefully under-resourced. Economic pressures have eliminated any vestige of excess (reserve) capacity in beds, staff and equipment, rendering hospitals unable to accommodate any large infusion of new patients. Public fear and panic will be prominent features of a bioterrorism attack. Health facilities will not only have to diagnose and treat legitimate victims of the attack while still providing care for those ill from natural disease but they will also be confronted with a potential tidal wave of hypochrondical individuals who believe that they are 'victims' of the attack. The 'worried well' may constitute the majority seeking health care in the aftermath of a biological attack. Public fear of contagion, and alarm over the possibility of additional attacks, will spur large numbers of people to flood into health facilities to seek testing and quickly overwhelm medical services.

Limitations in the availability of drugs and vaccines

Medical management of a bioincident will be hindered substantially if insufficient drugs and vaccines are available. Current stockpiles of the few drugs/vaccines which are currently approved for use against biothreat agents are insufficient to manage any bioincident that requires drug treatment of thousands of individuals or protective vaccination of millions of people. Second, little investment has been made to develop new drugs and vaccines against those biothreat agents for which no meaningful medical interventions exists. This situation reflects the longstanding neglect of the 'bio' problem as a national security threat and the lack of financial incentives for the private sector to develop products for biothreat pathogens absent government guarantees to purchase sufficient product to allow companies to recoup their R&D costs and to achieve a reasonable profit.

Recent decisions by the US and several European governments to expand antibiotic reserves and vaccine stocks for anthrax and smallpox are welcomed. In the short term, however, significant shortfalls in drugs and vaccines will exist. For biothreats for which drugs or vaccines do not exist, biodefence will depend solely on aggressive public health actions to implement a cordon sanitaire via quarantine and other traditional infection control measures to limit disease spread.

Unfamiliar political challenges

Actions to limit the consequences of a bioattack are extremely complex. They require swift action by public health, medical, military and law enforcement authorities in concert with multiple private sector entities. These groups may have little or no prior experience of working together. Key decision-makers will be confronted with unfamiliar and complex technical issues that have the potential for catastrophic outcomes if the wrong judgements are made. To date, none of the Western democracies have established coherent strategies to mount robust biodefence responses on any significant scale.

A major bioincident will confront politicians and key decision-makers with unfamiliar and controversial challenges, ranging from international co-ordination between governments to definitive actions to contain infection at the local level. Difficult and complex legal and ethical issues will abound. National leaders will face complex constitutional decisions about whether to impose martial law, suspend civil rights, ban commercial trade and travel or to authorise emergency seizure and diversion of private assets for national security purposes. Those involved in the direct containment of infection will be forced to make difficult decisions regarding the triage of patients, the denial of care when rationing scarce drugs and vaccines and the prospect of mandatory testing and treatment of individuals without their consent. The imposition of quarantine and other constraints on public freedoms will inevitably be controversial. A bioincident of any scale will also demand proficient actions to maintain law and order, to ensure the availability and safety of food and water and management of vexing problems associated with the decontamination and disposal of infectious waste and the unwelcome prospect of mass disposal of corpses.

Recent US experiences from field exercises involving the simulated release of plague and smallpox in American cities demonstrated that even when disaster plans and management structures were theoretically in place, they collapsed quickly due to ill-defined roles and responsibilities that led to misplaced territorial battles over claimed authority for decision making and a stark revelation of shortcomings in the training of emergency staff and the poor co-ordination between local, regional and national authorities.

Any attack that overwhelms local or regional capacities for dealing with severely ill patients or fatalities will increase public unrest and erode trust in government. Sustained, high rates of serious illness will generate widespread psychological trauma and panic well beyond the geographic location(s) of the incident(s). Mass disruption does not require mass casualties. Merely the suspicion or threat of a bioattack can pro-

voke widespread public alarm and fuel overt panic and civil disorder. Adverse public reactions will be aggravated by any perception, real or imagined, that a bioincident is being mismanaged or is out of control. The almost guaranteed certainty of irresponsible actions by the media will be an additional catalyst for public panic and civil disorder. Perceptions of governmental incompetence and mismanagement of the crisis, augmented by pervasive public feelings of vulnerability, helplessness and uncertainty, will place enormous pressure on law enforcement authorities and the potential for anarchic collapse will be all too real.

The agenda for strengthening biodefence

Based on the preceding assessment of the dismal state of current biodefence preparedness, how can these shortcomings be redressed? Critics who claim that the diversity of the 'bio'-threat precludes the development of meaningful defence capabilities overlook that current doctrine for nuclear defence did not spring to life fully formed. It reflects five decades of assessment, refinement and technical progress. History shows that in the period immediately following the emergence of any radically different threat, security doctrine is ill formed and ambiguities abound. During the cold war era legions of military personnel on both sides were deployed to 'game' different threat scenarios and responses, ranging from limited police actions to catastrophic nuclear exchange. The idea that a perceived threat was either too complex, or too unpredictable, to address would have been met with scorn and charges of defeatism. We must be no less demanding in our pursuit of robust defences against bioterrorism.

The multi-dimensional nature of the biodefence challenge demands that a systems-level 'holistic' approach must be adopted based on an overarching strategy that addresses all aspects of the problem. Tragically, the historical neglect of the 'bio' problem in the national security calculus dictates that current biodefence initiatives, albeit minimal, have proliferated an ad hoc fashion absent in any strategy for integration of diverse activities, the coordination of different branches of government and limited planning for international co-operation. We can no longer afford the luxury of funding fragmented efforts, many of which have dubious technical validity.

Biodefence is not a zero-sum game. The need to build new intelligence capabilities to detect and pre-emptively excise biothreats before they are deployed should not be bartered against funds to develop new sensors, diagnostic tests and computerised epidemiological networks for faster incident detection and containment. In turn, these investments should not come at the expense of new R&D initiatives to discover new drugs and vaccines or investments to strengthen medical and public health infrastructure. New approaches are also needed for improved decontamination of affected areas or the application of new architectural and engineering standards to protect buildings from bioassault. However, the timelines required to make these different elements a practical reality varies enormously.

The most immediate gains can be made by improving the training of healthcare professionals to recognise and manage bioattacks and in strengthening public health and medical resources to improve the speed of bioincident detection and containment. Aggressive actions could achieve these goals in two years. The importance of new diagnostic tests in accelerating incident detection also offers a fertile area for improved biodefence. A focused research programme to create a repertoire of new diagnostic tests based on the genetic profiles of biothreat pathogens could solve this major gap in biodefence capabilities within five years. In contrast, the discovery of new broad-spectrum drugs and the genesis new technologies for rapid production of vaccines are more complex and will likely require at least a decade.

Promulgation of clear regulatory guidelines for the approval of diagnostics and drugs for biothreats based solely on animal experiments will also be needed. Adoption of 'fast track' approval for biodefence agents in comparable fashion to anti-HIV products has obvious appeal in providing commercial incentives to create broad-spectrum drugs and vaccines against human and veterinary biothreats.

Building new intelligence gathering capabilities to detect the illicit production of bioagents and their pre-emptive removal is perhaps the most formidable and lengthy task in the biodefence agenda. In monitoring clandestine production of nuclear weapons, the intelligence services enjoy the luxury of telltale 'signatures' that enable them to detect and track these illicit activities and to intercede to circumvent their deployment. Equivalent 'signatures' do not exist to allow the remote monitoring of biopathogens. Illicit biological activities can be hidden easily in institutions that have legitimate interests in microbiology, genetics and fermentation. Remote monitoring of biothreat production is all but impossible. It still

depends primarily on direct 'on site' acquisition of samples as in the case of the discovery of Iraq's bioweapons programme. Technical solutions to devise signatures for improved remote monitoring of bioagent production and the emergence of novel methods for covert sampling can be anticipated, but these will take time. Equally important, the historical focus of the intelligence and defence communities on non-biological threats dictates that these organisations currently lack the technical expertise in biotechnology needed to analyse and respond to this critical challenge. Remedy of this deficiency must be an urgent priority.

Political desires notwithstanding, there are no easy or quick solutions to the bioterrorism problem. Unfortunately, the political response in Washington since the events of September 2001 has been to adopt an expedient 'knee-jerk' reflex of throwing money at the problem without any critical assessment of strategic needs or in-depth technical evaluation of the likelihood of success. Billions of dollars have been allocated for biodefence without clear priorities or performance objectives and devoid of any assessment of whether the technical competencies of the government agencies charged with the task of building biodefence capabilities are up to the task since most have little or no experience in biodefence or, worse still, showed overt disdain for involvement in activities that they either viewed as irrelevant or alien to this mission. The European situation, with the potential exception of the UK, is characterised by the virtual absence of declared biodefence policies.

Creation of robust biodefence capabilities demands a coherent strategy that fulfils the following requirements. The first is the urgent need for a reality check, no matter how unsettling. Current vulnerabilities and gaps in biodefence must be quantified, together with a stringent technical analysis of how these could be best addressed and the time frames in which solutions might reasonably be expected. Second is the need for sophisticated technological leadership to distinguish technically realistic solutions from hyperbolic fiction. Imposition of a stringent filter to separate worthwhile R&D efforts from expedient opportunism and financial greed has become an urgent priority in the light of the feeding frenzy now under way in Washington as government laboratories, universities and private companies and their highly paid lobbyists seek to capitalise on Washington's fiscal largesse in allocating billions to new bioterrorism defence activities. The deluge of exaggerated, and unsubstantiated, technical solutions now being proffered to various government departments will likely seduce technologically unsophisticated administrators to fund flawed initiatives and, worse still, create the political illusion that something meaningful is being done!

A major problem facing Western governments in marshalling the technological expertise needed to address these criticisms is that the relevant skills in biotechnology reside largely outside of government. This contrasts with the evolution of nuclear defence policies and other key military R&D programmes in which the leading edge science was conducted in government laboratories or could be accessed via well established links with the defence industry. Hitherto, biology has had little impact on natural security planning, military doctrine or foreign policy. The life sciences are now emerging as relevant not only to the bioterrorism threat but biotechnology can also be expected to produce radical changes in the global geopolitics and economics that will have broad implications for national defence, foreign policy and international commerce. The current defence industry evolved in response to the military demands of the cold war. This situation is now likely to be mirrored by the parallel emergence of a life sciences defence industry as governments are forced to build new public: private partnerships to meet their biodefence needs.

Full engagement of the private sector in this important mission will not occur, however, unless governments recognise the need to eliminate current bureaucratic, commercial and legal disincentives for commercial companies. Foremost will be the need for governments to guarantee that a sustainable market for biodefence will exist in terms of both sales and profitability. Legal protections and indemnification for companies producing drugs and vaccines that are approved solely on the basis of animal efficacy trials and if used in emergency settings at government request either as investigational agents prior to regulatory approval or if used in settings of government mandated testing and treatment in which informed consent provisions have been suspended.

Controlling the proliferation of biothreats: international actions, research constraints and codes of conduct

In November 1969 President Richard Nixon issued National Security Memorandum 35 stating that "mankind already carries in its hands too many seeds of its own destruction", declaring that the US would renounce all methods of biological

warfare and limit its R&D activities to defensive purposes. US biological and toxin stockpiles were destroyed and production facilities dismantled. Nixon also endorsed a treaty proposed by the United Kingdom to prohibit the development, production and possession of biological weapons that led to the 1972 Biological Weapons Convention (BWC) which sought to establish an international norm in preventing the spread of bioagents and to facilitate international action against violators. In contrast to the Chemical Weapons Convention (CWC) which established formal verification mechanisms for inspections to ensure compliance, the BWC failed to set legally binding requirement for declaration of compliance and made no provision for inspections. In 1994 efforts were launched to redress these deficiencies. In late 2001 the proposed revisions were rejected by the US administration on the grounds that they would do little to ensure compliance and that protections for the legitimate commercial interests of companies subject to inspection were inadequate. The debacle of the UN inspection effort in Iraq was cited as an illustration of the ineffectiveness of enforcement measures.

The future viability of the BWC is uncertain. Yet the time has never been more urgent to develop international political consensus to establish mechanisms to deter the production and use of biothreats to investigate suspected violations and impose meaningful penalties and sanctions against violators. Both the BWC and CWC are directed to the actions of states, not individuals. This has led to recent proposals that the legal focus should shift to make the actions of individuals who produce or use biothreats as propagating a crime against humanity.

Biology is poised to lose its innocence: the impact of bioterrorism on policies for the conduct and publication of research

In rejecting the draft BWC Protocol the Bush Administration emphasised that inadequate attention had been given to new risks posed by progress in biotechnology. The US counter proposals included the need for signatory countries to "sensitise scientists to the risk of genetic engineering", to establish "national oversight of high-risk experiments" and for scientists to adopt a "code of ethical conduct that would have universal recognition". Even if the unspecified nature of the latter begs many issues, the intent is nonetheless clear. Life sciences researchers can no longer ignore the national security implications of their work and must participate in limiting the proliferation of new modes of bioterror. The traditional academic career requirement of "publish or perish" cannot be allowed to become a vehicle whereby "publish, and we all perish!".

The growing importance of biological knowledge in national defence is also likely to portend a change in the cultural environment for research in the life-sciences. The USA Patriots Act passed in November 2001 will require security background checks for scientists working with "select agents", the euphemism for those pathogens deemed most likely to be used by bioterrorists. The US Congress is mulling additional legislative bills that will impose stringent controls on the access, use, distribution and transport of pathogens, the registration of research laboratories and the genetic fingerprinting of microbial collections to serve as forensic markers that can contribute to identification of unauthorised transfer or criminal use of biomaterials.

The open scientific literature and the Internet are becoming a rich source of valuable information to the bioterrorist. A few examples of academic research placed in the public domain serve to illustrate the dilemma: the genetic codes of devastating pathogens such as bubonic plague, anthrax, smallpox and the 1918 pandemic strain of influenza; the use of gene shuffling to generate antibiotic resistant organisms; new methods to create viruses with altered modes of spread; and the construction of viruses containing genes that facilitate their escape from detection by the body's immune defences or, worse still, paralyse the immune system completely. As the volume of similar 'dual use' biological knowledge expands, greater consideration must be accorded to the security implications of how publication might benefit those intent on devising new forms of bioterror.

The issue is not whether areas of 'forbidden knowledge' should be defined in which research is completely prohibited. Rather, the issue is how can we best demarcate boundaries for 'constrained knowledge' whereby freedom of research enquiry is not impeded but unconstrained public access to certain forms of research data would be limited to researchers with bona fide scientific credentials seeking to use the information for beneficent purposes. This does not offer an ironclad guarantee against abuse but it would provide both a deterrent obstacle and also enable tracking of who had access to any information or materials that become the subject of security investigations. Freedom of intellectual enquiry has been the bedrock of progress, reason, tolerance and personal autonomy and it

must be protected. The research communities in physics, chemistry and engineering have been successful in managing the conflicts raised by dual use technologies and to accept constraints on public domain knowledge based on national security considerations. Biology and medicine cannot escape the same debate. The scientific and medical communities must be in the vanguard of the debate or suffer the consequences of potentially draconian constraints imposed by well-intentioned, but ill-informed, legislative actions.

In 1975, at the dawn of the modern biotechnology era, scientists were concerned that new gene splicing methods and cross-species transfer of genes might convert harmless microbes within the body into virulent pathogens or produce long term genetic damage to body tissues. These concerns stimulated the Asilomar Conference which resulted in a voluntary moratorium on certain forms of genetic manipulations until the risks were evaluated and assuaged. Asilomar stands a landmark whereby science independently questioned and regulated its own enquiries. The same ethos must be reawakened to address the dual use challenge of biotechnology and bioterrorism.

'Biosecurity' is more than defence against bioterrorism

Biodefence is transitioning from a topic of historical neglect in national security matters to a growing recognition that political and technical trends are likely to escalate the bioterrorism threat. Nonetheless, it is crucial in shaping future national policies that the concept of 'biosecurity' be embraced and interpreted as representing issues that are far broader than defence against deliberately induced disease caused by micro-organisms.

A comprehensive political approach to biosecurity must address the prospect that serious political instabilities, notably in Africa and Asia, are likely to be triggered by the unchecked spread of natural diseases such as malaria, TB and AIDS. Similarly, the emergence of new pathogens and the depletion of natural resources as a result of uncontrolled population growth and environmental deterioration each pose the prospect of triggering political instabilities and in so doing increase the likelihood of Western military actions. In addition to the substantial direct risks posed to developing nations themselves by infectious and parasitic diseases, these long standing problems, together with inadequacies in international public health responses and the increased international traffic in people, animals and disease transmission vectors increases the risk that epidemic disease will spread to Western nations.

In a large measure these issues are but incremental extensions of the ongoing debate about global-

lengthy list of potential abuses and dangerous uses of the same knowledge.

Those who seek to usurp the burgeoning knowledge about the molecular foundations of biological systems to devise new ways to attack people, plants or animals will have no shortage of molecular targets against which to direct their repugnant skills. Of particular concern is the prospect of novel biothreats that affect human brain function. Targeted manipulations could range from subtle, reversible changes to devastating and irrevocable alterations. These could include 'on-demand' induction of phobias, depression, violence, lethargy, seizures, catatonic withdrawal as well as the manipulation of intellectual capabilities and memory processing. Whether used selectively to target political leaders, or to attack larger populations, 'neuro-behavioural modulation' weapons represent a novel biothreat that could emerge in the next 20 years.

Paradoxically, although biotechnology will be the driving force in revealing how specific gene networks can be altered for either beneficent or malevolent outcomes, the means by which these manipulations will be achieved will probably involve the use of chemicals that selectively target biological circuit control nodes such as transcription factors. Longer term, the most sinister 'bio-threats' may thus form chemical assaults and our surveillance and defence capabilities will again need to shift to address the altered threat spectrum.

History reveals repeatedly how comfort and complacency insidiously undermine the vigilance of nations, companies, communities and individuals in sensing emerging threats which, once manifest, can be seen in retrospect to have had obvious origins and predictable evolution. The fruits of three centuries of industrial harnessing of science and technology has granted the West military, economic and technological strengths that immunise it against myriad security threats and natural disasters. However, the public is now fed a diet of populist political sound bites designed to reassure that all is well and thereby blunt any critical public debate about risk, unresolved ambiguities and, above all, any examination of the merits of alternative approaches. The progressive purging of complexity and ambiguity from the political agenda and public debate means that contrarian views are too easily dismissed as extremist or alarmist. Ironically, in dismissing concerns about technology-driven risks, politicians are increasingly prone to invoke faith in technological determinism as the solution.

The debate about the nature and scope of biosecurity and the adequacy of current institutions and policies to analyse and respond bioterrorism to address the new public health issues posed, emerging infectious diseases of natural origins and the overall challenge posed by biotechnology has barely been enjoined. Biosecurity is destined, however, to move to centre stage in the political agenda as a consequence of the remarkable pace of research discoveries in the life sciences and their profound implications for global society. As the debate intensifies the participants might do well to reflect on the 19th century exchange between the Prince Otto Von Bismark and the pre-eminent German scientist Rudolph Virchow, the founding father of modern pathology and cellular theory. Bismark remarked: "Politics is the art of the possible, the calculated science of survival." In reply Professor Rudolph Virchow stated: "Survival owes little to the art of politics, but everything to the calculated application of science." May history judge us as having been equal to the task. **DDW**

Dr George Poste CBE, FRS is Chief Executive Officer of Health Technology Networks, Scottsdale, Arizona. He is a member of the US Department of Defence Science Board and in this capacity Chairs the Task Force on Bioterrorism. He is a member of the bioweapons working parties of the Royal Society and the US National Academy of Sciences. The views expressed in this article are personal and do not reflect any official opinions of the US Department of Defence, The National Academy of Sciences or the Royal Society.