Technical Aspects of Bio-Defence

Ajey Lele

Abstract

Most of the time, crucial decisions and strategic predictions are not made in an environment of absolute certainty. The same is true regarding threats from bioterrorism. Preparing against bioterrorism necessitates investments in public health surveillance, timely contributions from the biomedical sciences and the pharmaceutical industry, transnational collaborations and training. All these efforts demand large investments (for a relatively low-priority threat). The current revolution in biotechnology, information technology, sensor technology, and nanotechnology could be effectively used to strengthen biological defence techniques. This paper elucidates cost-benefit trade-offs associated with new scientific approaches in biological defence and argues that it is inappropriate to judge the investments in such technologies purely from a financial perspective.

Introduction

History suggests that when nations do not have an offensive plan for a particular weapon, they undervalue the likelihood that others will use that weapon, and they even dismiss instances of use as accidents or irrelevant events. Biological warfare is meeting the same fate in various countries because of the varying positions (a few call it a major threat and some call it a low-probability threat) taken by many on this subject.[1]

Bio-defence is a contested area. Many analysts have expressed extreme and opposing views. Some are of the opinion that states must invest heavily, in spite of the fact that bioterrorism is a low-probability threat. Such opinions result from studies based on the imaginary scenario buildups needed due to a lack of empirical data. Others are of the view that civilian defense against bioattacks is virtually impossible; preferring a wait-and-watch policy. Risk analysts have long observed a tendency for policy-makers to respond rapidly to visible crises. This tendency encourages reactive policies crafted in the wake of visible or highly publicised events, resulting in ad hoc policy-making with scant attention to competing

Strategic Analysis, Vol. 30, No. 4, Oct-Dec 2006

interests.[2]

A strong opposition to biological defence programmes is based on the fact that research for defensive measures could covertly help the offensive weaponisation programme. And, most importantly, the development of defensive measures will always lag behind offensive measures.[3] However, it must be noted that there is no need of making large investment specifically for biodefence surveillance but introduction of modern technologies in the existing health surveillance itself would serve the purpose to the larger extent.

At present, the existing defences against biological weapons are inadequate. The general population is unaware of the exact nature of the threat, and if biological terror strikes, ignorance may add to the disaster. Also, there is a growing concern about the naturally occurring infectious disease problem in many parts of the world. The severe acute respiratory syndrome (SARS) epidemic has proven the importance of major public health programmes. Conversely, particularly since September 11, 2001, the world has witnessed a growth in "new" scientific approaches to tackling the threat of bioterrorism in the form of disease surveillance and disease control. Based on the ever-evolving knowledge of modern biology, the social sciences, operational research, information technology, epidemiology, and nanotechnology, many states are formulating doctrines with a view to prevention and protection policies.

Today, in the areas of bio-defence, states are forced to make difficult choices because of the scarcity of resources. At the same time, experts on this subject come from different backgrounds, including from microbiology, medicine, physics, and security. Hence, mostly lacking a common framework, these experts promote their preferred approach. And resources are mostly allocated in accordance with bureaucratic positions and power, rather than in response to the actual problem.[4]

Against this background, when the world is facing challenges from threats of bioterrorism, some of which cannot even be predicted today, there is a need to evaluate the costs and benefits of new scientific approaches in bio-defence. Such analysis may help us to formulate a politico-military decision making template and policy initiatives.

Also, in the recent past the world has witnessed significant outbreaks of human and agricultural diseases. Such outbreaks of disease – whether

in humans, animals or plants – present a major risk to countries around the world and preparedness to counter such outbreaks is required worldwide. Such preparedness is also likely to benefit a state in preparing to counter deliberate outbreaks.

In order to prepare for biological attack, the authorities can make maximum use of existing emergency-response resources, and to adopt an approach that is consistent with the principles on which the management of any other type of public health emergency is based. While attacks with biological agents will have some special features, they do not necessarily require the formation of completely new and independent response systems. A well designed public health and emergency response system is quite capable of responding to a limited biological attack and can take the measures necessary to mitigate its effects. A biological agent attack will generally have the characteristics of a disease outbreak, so that city, state and regional public health authorities could be involved in the response, which will have much in common with the infection control strategies used in any outbreak of disease.[5]

The main objective of this paper is to provide an awareness of the leading technologies that are found to be the most instrumental in developing new tools for bio-defence. It further discusses the costs and benefits of such new and emerging scientific approaches in the field of biodefense and argues that it is inappropriate to judge the investment in such technologies from only a monetary perspective. At the same time it is also argued that the investments in novel quick technologies for the purposes of surveillance as a part of health survival mechanism are really cost-effective.

New Scientific Approaches in Bio-Defence

Defences against any probable bioattack constitute a set of measures designed to maintain the operational effectiveness of armed forces and the well-being of the masses. Conceptually, biological defence structures have two main components: active defence and passive defence.[6]

Active defence comprises measures aimed at preventing biological attacks from reaching their target areas. Such defences include various techniques for intercepting and destroying enemy biological warheads or germ banks mostly at the place of manufacture of bioweapons and/or the place where they are stockpiled. However, destroying bioweapons without

dispersing their deadly contents is a difficult task. To address this issue the Agent Defeat Warhead Demonstration (ADWD) programme was initiated by the US air force in 1999. Today, the Americans are probably in possession of weapons that are specifically designed to destroy hardened or soft biological targets on the ground. These weapons are capable of neutralizing such targets, thus limiting the potential for human casualties resulting from the unintended release of viable biological agents.[7]

Passive defence consists mainly of secondary preventive measures used to minimize the health consequences of the spread of a disease after a bioweapon has been successfully used by an adversary. The key elements of these measures are hazard assessment, detection technologies, physical protection, identification and diagnosis, and medical counter-measures.[8] New scientific approaches have been found that deal specifically with these areas of biodefence. The 21st century is witnessing a shift from the age of physics and chemistry to that of biology, and from the industrial revolution era to a biotech century.[9] Presently, the revolution in biotechnology, information technology, sensor technology, and nanotechnology is being effectively used to strengthen biological defence techniques. Most of these technologies are being used either independently or jointly to design and develop various bio-defence tools.

Biotechnology and Bio-Defence

Biowarfare is closely related to knowledge about diseases. The opportunities for the weaponisation of diseases began with scientific breakthroughs in the early 1970s. In 1973, the first gene was cloned, and three years later the first company to exploit technology based on recombinant DNA was found in the United States.[10] Biotechnology has immense potential to improve biological warfare capabilities. However, the Biological and Toxin Weapons Convention (BTWC) came into being in 1975; as a result, during the last 30 years, even though science has evolved further, no overt attempts have been made to develop new weapons.

Biotechnology is a broad term that applies to all practical uses of living organisms — from micro-organisms used in the fermentation of beer to the most sophisticated application of gene therapy. The technology that is presently the most relevant to bio-defence is closely associated with genetic engineering, a technology based on the artificial manipulation and transfer of genetic material.[11] At the same time, gene therapy could be effectively

used to cure various diseases. Many predict that future bioweapons could be designer bioweapons, and this technology could play a very important role in finding cures for many diseases unknown at present.

Research and development in the field of biotechnology has led to many enabling technologies that in turn have laid the foundation for improvements to products and processes. Of particular importance today are the automation of sequencing in genome projects, bioinformatics, and advances in combinational chemistry and high throughput screening of compounds. Many of these products and processes are being researched and developed for civilian application in medicine, pharmaceuticals, and agriculture, as well as for purposes that are legitimate under the BTWC, such as defence, detection, protection, and prophylaxis.[12]

Biotechnology has been vital to the development of techniques for identifying and diagnosing diseases and for medical counter-measures. And the recent advances in biotechnology offer a real opportunity for the development of effective counter-measures to biological and toxin weapons agents.[13]

To reduce the threat of bioterrorism, rapid progress in vaccine development is of paramount importance. From a biosecurity point of view, vaccine development and production has great strategic value. Recent advances in molecular biology and genetic engineering have led to new vaccine development strategies. Expertise relevant to early-stage vaccine development has become increasingly specialised and more widely distributed.[14] Commercial vaccine developers are also responding to the changed parameters of technological development by making more investments. Newer technologies like the development of 'Orphan Vaccine', which is a vaccine, is likely to be targeted to a limited number of individuals are being introduced in the countries like the US. Orphan vaccines are those vaccines for rare infectious diseases or those of narrow scope—for example, diseases limited to particular regions of the world or intended to combat bioterrorism.[15]

Perceptions about bio-defence are largely rooted in proven medical treatments and prophylactics. Although such strategies are critical to the ways in which immediate bio-threats are addressed, they will be inadequate against futuristic bioweapons.[16] In the future, the science of biotechnology may come in handy to tackle the threats posed by advances in biotechnology.

Information Technology and Bio-Defence

Terrorism is dynamic. Terrorists will always seek new ways of terrorising the public. As our understanding of biotechnology and techniques in genetic manipulation increase so will the terrorists' desire to keep pace with it. Under such circumstances, the post-attack care scenario will remain highly unstable, and this will stimulate a broad range of choices for planning.[17] A robust, well-conceived, state-of-the-art technology based on an information and communication infrastructure is a core component of successful bio-defence response and preparedness. A core element in bio-preparedness is an information technology (IT) infrastructure that enables the collection, analysis, and dissemination of critical information in real time to prevent or mitigate the effects of a bioweapons event on various populations.

The span of bioterrorism, and hence that of bio-defence, is vast. Bioattack brings together three distinctive elements: the state and the terrorist, a biological agent, and a living target. These elements are the responsibility of diverse professional communities with very different areas of expertise. These communities normally operate independently of one another. During a bioattack event, however, they must suddenly find ways to cooperate in mutually beneficial ways. Their IT needs will evolve, as the lifecycle of the bioattack event unfolds. The phases of the cycle may include prevention and preparedness, detection, early response, sustained response, and recovery. The IT infrastructure needs to relate to the entities being supported (for example, communications and resource management); the required capabilities (for example, data management and various procedures); various data needs (for example, information about the number of cases), and users (for example, public health officials and the general public). Since the lifecycle of an attack unfolds over time, this IT infrastructure needs to support all phases of the bioattack event in order to provide continuity.[18] Currently, few software tools are available that cater to such needs.

The initial response to a public health emergency, including an act of bioterrorism, is generally the responsibility of local bodies and could involve many jurisdictions in a region, with states providing additional support when needed. Since local clinicians are most likely to be the first ones to detect an incident, they and local public health officials are expected to report incidents or symptoms of suspicious illness to the state health

department and other designated parties. States can provide support personnel, financial resources, laboratory capacity, and other assistance to local responders.[19] Thus, the involvement of many agencies in the identification and management of bioterrorism and other public health emergencies demands effective communication and collaboration across all levels of government and the private sectors. IT tools play a major role in coordinating the efforts of various agencies.

In recent times, modelling and simulation techniques have been frequently used in various areas of research related to bio-defence. Modelling and simulation are primarily mathematical representations of the real thing. Computer-based modelling and simulation techniques have been available to researchers for several decades, becoming more sophisticated, more powerful, and more comprehensive every year. Life science modeling was referred to as molecular modelling about ten years ago. Today, pharmaceutical and biotech companies rely heavily on a number of modeling and simulation tools for modelling everything from entire biological systems to genomic and proteomic drug discovery compounds and their interactions with cells and diseases.

Combining the modeling capabilities of several software programmes into an integrated system has also been done, although rarely, due to the incompatibility of most interfaces. Modelling and simulation studies in the planning of attacks on Iraqi chemical and biological warfare targets were carried out for three or four years before the start of the 2003 Iraq war.[20] During the past few years, various mathematical models of disease transmission for estimating the infectiousness of diseases by assessing the rate of increase of cases have been developed and used. Such models are able to evaluate the likelihood of an outbreak when a bioweapon is introduced into an unsuspecting population, and through such models we are able to draw preliminary conclusions about the impact of control measures. Also, pollution and disease spread models are available that assess weather and environmental conditions, terrain, and various transport and diffusion processes.

Such IT tools can also be used for training purposes. US scientists have developed synthetic theater-of-war simulators and networks that support multi-entity exercises. Many doctors are trained with these systems, with which virtual patients with realistic symptoms can be treated. Virtual reality

applications are available to training and rescue personnel, allowing them to practice responding to a biological attack and helping them by providing consequence projections.[21] Furthermore, a few terror-tracking tools are available for tracking intelligence inputs based on the information available in cyberspace and for identifying possible adversaries. Also, it could be advisable to develop a country/threat specific synthetic war simulator for training of biodefence personnel.

Sensor Technology and Bio-Defence

For biological threats, detector technology is important for the timely identification of the agents, because such agents are colorless and odorless and may take days to cause symptoms. Cold War detection technology was biased towards military and battlefield requirements – for obvious reasons. However, detection technology was given a major boost after the 1991 Gulf War. Many collaborative research and development ventures between the coalition partners were initiated. In the past decade, rapid improvements in detection technology have occurred. Today, bio-detection has become a priority area for many states, due to the increased probability of a bioattack by terrorists. However, even today there is a gap in the availability of medium- to long-range standoff detection systems.

Bio-detection and identification generally occur in three stages: detection (the recognition that something has changed), recognition (the realization that the change is biological in nature), and identification (the identification of the specific agent, for example, Anthrax).[22] Current systems are normally based on these three stages and are capable of detecting the presence of a bioagent in the atmosphere or in the vicinity. Such systems are capable of giving advance warning to areas of probable bioattack by using weather pattern models. These detection systems can be broadly classified into sensor systems; command, control, communications, and intelligence (C3I) systems; and reconnaissance systems.

Sensors are devices that sense or detect a change in the physical quantity or process variable and convert that change into a useful output or indication. Biosensors are electronic devices that use biological molecules to detect specific compounds.[23] They are compact analytical devices that incorporate a biological or biologically derived sensing element, either integrated into or intimately associated with a physico-chemical transducer.

The usual aim of a biosensor is to produce either discrete or continuous digital electronic signals, which are proportional to a single analyte or to a related group of analytes.[24] Present generation biosensors combine the selectivity of biology with the processing power of modern micro-electronics and opto-electronics to offer powerful new analytical tools with major applications in medicine, environmental diagnostics, and the food and processing industry.

The recent development in sensor technology has mainly been carried out in the United States, Britain, Russia, and Canada. The main detection systems on the military inventory list of the US forces and a few other forces range from simple bio-detectors capable of operating continually for a 14-hour mission to biological aerosol warning systems, which are GPS-based area biological weapons detectors (with a 10-kilometer radius) supported by real-time meteorological inputs. There are also some portable agent-specific detectors like anthrax detectors.[25]

Since September 11, 2001, the detection of bioweapons has become a priority in many countries. The Anthrax letters post- 9/11 is a case in point. In the United States, many laboratories are developing various technologies that have direct homeland security applications, and bio-detection systems have become a top priority. Two distinct but complementary approaches are being pursued in the bioweapons detection arena. In order to identify the physical characteristics of a "germ cloud" present in the atmosphere some distance away from a detector system, air sampling sensors are installed on platforms facing the threat. In particular, micro-air vehicles are sent as probes into the suspect area, providing digital information by data link. In an amphibious scenario, air and water sampling units could be mounted on floating buoys or low velocity missile probes.

In any mode of attack, bioweapon agent organisms are likely to be widely dispersed in the atmosphere. Apart from those cases in which a terrorist himself or herself is infected, bioweapon delivery methods may include water contamination or aerosol release. Given these new threats, the challenge to the designers of bioweapons detection systems is enormous.[26] Current particle detectors employ lidar (light detection and ranging), a system much like radar that emits a laser beam and then detects the light that bounces back from the objects in its path. In dry conditions, such systems function from a distance of 50 kilometres, but they cannot

distinguish between mists of biological agents and clouds of fine dust or smoke.[27]

In the Gulf War in 2003, no biological or chemical weapons were used by Iraq, and so it is difficult to comment on US preparedness in the areas of battlefield detectors. However, during that war, observers noticed that the Americans were at least not getting false alarms of a biological or chemical weapons attack from diesel fumes or sand particles, as they had in the 1991 Gulf War.[28] From this, it could be inferred that the Americans have reached a reasonable amount of perfection in technologies like UV-lidar bio-detection devices.

Modern detectors can distinguish pathogens from benign micro-organisms or other particles because of their different genetic makeup.[29] Bio-detectors require unique DNA sequences or antibodies to identify and characterise pathogens. Two classes of bio-detectors are especially promising: immuno-fluorescence-based sensors (agent-specific miniature flow cytometers) and DNA-recognition instruments (based on polymerase chain reaction [PCR]). When used together, these are capable of state-of-the-art detection and identification of biological agents.[30]

Concentrated efforts are taking place in many countries to develop multifunction sensors. It may take some time to deploy agent-specific or all-purpose sensors at various probable civilian targets. Some equipment is available that incorporates cutting-edge technologies for various purposes. Environmental sensors are sensors that discriminate between disease-causing agents (pathogens) and the thousands of smaller but harmless micro-organisms that colonise our air, water, and soil. Some sensors use an innovative type of device that detects pathogens based on their unique surface molecules. Such sensors are useful for discerning more than one type of a pathogen.[31]

In addition to such types of systems, which are essentially point detection systems, current research is also aimed at producing standoff detection systems. Such systems could monitor clouds of biological agents from some distance. The aim behind the development of such systems is to observe an area with a 1-to 10-kilometre radius (standoff distance). Also, considerable effort is being made on the development of passive optical and laser technologies to carry out standoff (remote) detection.[32] For such detectors, winged, balloon-based, or rotorcraft platforms could be used.

Today, unmanned aerial vehicles (UAVs) offer a great opportunity to safely deploy such technology to achieve a longer-range warning.

In spite of these developments, scientists are still working overtime to remove the shortcomings. The whole bioweapon detection process itself takes time; current detectors take up to 30 minutes to take a reading. There is a need to reduce the time taken to deliver precise identification and also to reduce the size of the equipment. The goal should be agent identification as close to real time as possible with equipment that is reliable, with a low logistics burden, and which can be operated with the minimum of training. Ideally, it should be hand-held.[33]

Existing and futuristic biosensors are expected to work in ambient environments and to provide early warning or confirmation of a biological attack. Advanced diagnostics are needed to confirm infection in targeted populations before symptoms start showing, and this is where biosensors are going to play a major role.

Nanotechnology and Bio-Defence

Since 9/11, the response to bioterrorism in the form of the invention of new techniques is developing very rapidly. Nanotechnology is fast emerging as a new frontier in biodefense. "Nanotechnology" is used to describe many types of research where the characteristic dimensions are less than about 1,000 nanometers. This technology has diverse applications in various disciplines. Currently, nanotechnology is being used to develop and manufacture various biodefense technologies. It is also becoming increasingly relevant in the field of medicine. However, the technology is still in its infancy, and some of its uses projected today are more prediction than reality. Many believe that nanotechnology will revolutionise the entire field of medicine, from pharmaceuticals to surgery, and naturally this will have a major impact on biodefense.

At present, nanotechnology is primarily used for the development of biosensors. Lately, a sensing device for detecting nerve gas agents in the atmosphere has been developed based on nanotechnology applications.[34] This technology has also been found to be useful in the production of chemical-biological mass spectrometers that are used to detect biological warfare agents.[35]

Technology capable of having a single-cell microchip platform as a toxicity sensor is already available. With this technology, molecular targets can be inserted into the cell, or the cell can simply be exposed to the environment while it monitors continuously for cell death. The readout is direct and virtually instantaneous. This platform will be leveraged in pharmaceutical and biowarfare applications.[36]

Many cells in which numerous life activities and the interaction of protein surfaces take place are measured in nanometers. A few countries are working on extremely small machines and tools that can enter the human body. This is the millionth-of-a-millimetre world of biotechnology today. By using a person's saliva, body fluids, or blood, nano-biosensors can be created to reliably work against pathogens such as viruses. In tissue engineering, a scaffold measuring only 50 nanometers in diametre can be built using nano-fibers. These are the secrets of life, and they are unfolding at the nano-level. The costs of developing drugs and viruses can be reduced by using nano-chips to test various medications or a combination of chemicals and vaccines.[37] Presently, nanotechnology is showing immense potential in the development of various direct and indirect applications useful for biodefense purposes. It is expected that this technology would also be used in future for developing surveillance tools.

Scientific Solutions and Cost-Benefit Analysis

Scientific solutions in the field of biodefense have two types of costs. First, these solutions themselves could help the proliferation of biological weapons or make a terrorist aware of the benefits that the modern technology can provide for successfully launching a biological attack. Second, huge financial investments are required for research, development, and production of bio-defence technologies. Hence, any hasty and ad hoc investment in the field of biodefense could prove damaging. For a low-probability threat like bioterrorism, there is a need to invest in scientific solutions that are based on realistic risk and threat assessments. Such assessments are essential, because no nation-state wishes to invest in resources that are based on solely on perceived threats; states always like to invest in resources that are relevant and necessary. But at the same time, they always have to remain prepared to fight a worst-case scenario. Any cost-benefit analysis of investments in scientific solutions for bio-defence should be done with this in mind.

Cost-benefit analysis (CBA) entails rational decision-making. People use CBA every day, and it is older than written history. Yet although our natural grasp of costs and benefits is sometimes inadequate, when the various options under discussion are complex or the data are uncertain, we need formal techniques to keep our thinking clear, systematic, and rational.[38] Normally, CBA is used as a narrow financial tool, and this interface between physical and social sciences is mostly shaped by the prevailing economists' views about how a problem should be framed.

CBA of bio-defence solutions necessitates an assessment that attempts to integrate the physical and economic aspects, not one that merely judges things by their monetary value. Rather, potential investors need to thoroughly and consistently evaluate the pros and cons of new scientific approaches. Mostly, CBAs are expressed in monetary terms, but in the case of biodefense, the issues go well beyond simple financial considerations.

Effective policy-making that can handle the challenges of bioterrorism requires an assessment of the countervailing dangers introduced by remedies initially intended to decrease a specific risk (the risk that the policy aims to reduce), even when that risk is partially dreaded, and when both the potential target and the countervailing risks are difficult to quantify. Therefore, standard theories for evaluating risk are not generally found useful for assessing risks of virtually unlimited cost and finite probability.[39] Moreover, even if an attack were carried out successfully, the range of consequences runs from a minor annoyance to a catastrophe that could change society fundamentally. Under these circumstances, CBA becomes extremely tricky.

But the process of CBA is even more complex, because the choice of variables assessed changes substantially when fear is factored into a technical assessment. A key question for decision makers is whether policy responses should be based in part on the perception of peril, including feelings of fear, or on a calculation that considers every potential casualty to be equal — whatever the emotional and symbolic content of a threat might be. Certain hazards evoke particular dread, which can lead to an overestimation of the risk or to reactive policies whose costs may exceed their benefits.[40]

Furthermore, with bio-defence and bioterrorism, the uncertainty is tremendous. The risk, the extent of an attack, and the diagnosis, treatment,

and prophylaxis of disease is highly uncertain, leaving decision-makers with little solid ground on which to base their decisions.[41] The basic problem with such threats is that the elusiveness of a potential bioterrorism event precludes clear-cut solutions, and the right reaction to a real attack may change during the development of an attack.[42]

Sometimes, cost-benefit or cost-effectiveness balancing approaches include little or no consideration of the individual,[43] and in the case of biodefense, such approaches are based on the argument that individual interests are to be subordinated to not only a cost benefit in the traditional sense of public health, but also to a national security interest. Further, because biological agents can be used randomly across many communities, or even more extensively, in the case of aerosol dispersion, predictions of the rates of infection are most uncertain, leading to a need for counter-measures that have very broad safety margins. Another problem unique to bioterrorism is the fact that biological agents that pose no natural public health risk could be weapons of choice for bioterrorists, and this creates a high cost with benefits accruing only in the event of a biological attack with that agent, which scenario is widely known to pose only a small risk. The consequences of an attack, however, could be catastrophic.[44]

Risks of Bio-Defence

Technological progress inevitably has its victims. It is difficult to think of a single invention in history, no matter how beneficial to society that has not made somebody worse off.[45] The technological advancements in the field of biodefense are no exception. Most of the new scientific developments are helping immensely towards the design and development of new biodefense techniques, while at the same time the same technological revolution is simplifying the procedures for making and modifying bioweapons. In general, all modern and emerging technologies should be viewed in context of their significance to the development of biodefense technologies and also in context of the likely implications for the development of bioweapons.

Current research in biotechnology parallels earlier research of the 1940s and 1950s in the nuclear field. The knowledge base developed for nuclear technology was applicable to both military and industrial purposes.[46] Similarly, the knowledge base being developed for commercial genetic engineering and used to create bio-defence technologies could potentially

be misused for the development of a wide range of conventional and designer bioweapons.[47]

There is a need for better oversight of genetic engineering, because certain experiments involving the cutting and splicing of genetic material could have dramatic and unexpected consequences and relevance for biological weapons. However, it is not genetic manipulation in isolation that creates potential and unexpected risks; rather, the combination of a better understanding of life at the molecular level with other scientific advances, including nanotechnology, materials science, and bioinformatics, poses an even greater risk.[48]

Biotechnology has the potential to improve biological warfare and biodefense capabilities through improvements to products and processes. Product improvements may involve the genetic modification of pathogens and the creation of new agents, as well as the development of new equipment for analysis and production. Process improvements influence the ways in which agents are manufactured. Many of these products and processes are being researched and developed for civilian applications in medicine, pharmaceuticals, and agriculture, as well as for purposes that are legitimate under the BTWC, such as defence, detection, protection and prophylaxis. However, the investigation of these products and processes also generates considerable knowledge about the potential offensive use of certain substances, which could interfere with the biological processes in humans, animals, and plants. In certain cases, the offensive properties of known or potential biological warfare agents are being actively investigated in order to develop adequate defensive technologies and procedures.[49]

Technological advancements used directly or indirectly for developing bio-defence expertise also permit the production of new agents capable of use as bioweapons. Recombinant DNA and other genetic engineering technologies are making biological warfare an effective military option.[50] As the tools of biotechnology develop, so does the potential good and the potential evil they may bring about.[51] Biotechnology in the guise of bio-defence technology presents a more dangerous and complex non-proliferation problem than any other technology.

A further dimension to the advancement of life sciences and technology that will have important implications for the evolution of the biological

weapons threat is the growing global dissemination of such advancements. Indeed, the way in which science and technology is developed, produced, and disseminated on a global basis has changed significantly in the years since the BTWC entered into force in 1975. Much of the material being produced is for dual use; the private sector is responsible for most of the advances; and knowledge and capability will become increasingly dispersed around the world, as biology and biotechnology are applied to more and more aspects of life.[52]

Information technology and sensor technology used for bio-defence purposes could, in a way, be called clean technologies, because they do not contribute much towards the production of new agents. However, these technologies contribute indirectly by enhancing the possibility of the manufacture of bioweapons by state or non-state actors. A state actor may create a few specific bioweapons for testing its sensors. Such weapons and knowledge increase the danger of further proliferation. Also, the technological know-how for designing a bioweapon is easily available on the internet, and non-state actors can easily make use of it.

Detection technologies like sensor technologies have their own limitations. Research into the development of technologies for detecting biological material in the natural environment is ongoing. While several technologies show promise as broadband detectors, there is no magic gadget that detects all biological materials at the requisite levels of sensitivity and specificity.[53] Agent-based detection technologies are normally very costly. Also, the process of developing agent-specific sensors is seriously limited. Terrorists can always hoodwink the sensors by designing new germs, and, therefore, the defensive measures will always lag behind the offensive measures.

Nanotechnology raises many ethical questions about the medical advances that it will spur.[54] There is a possibility that research into new vaccines against various diseases could inadvertently – or on purpose – create lethal human viruses. Defense experts are worried that even scientific papers published in medical journals may cause important technical information to fall into the wrong hands.

Apart from these major technologies, a few other technologies used for biodefense purposes can be applied to the field of biowarfare. UAVs, which are used for bioagent reconnaissance, could also be used in bio-

offensive ways by terrorists. These aircraft could be used by terrorists to drop biological bombs or spray biological agents like Anthrax.[55] Also, air-conditioning systems of offices or shopping complexes could be used to spread bioagents.

India and Bio-Defence

In India, the Defence Research and Development Establishment (DRDE) at Gwalior is the primary establishment for studies in toxicology and biochemical pharmacology and development of antibodies against several bacterial and viral agents. In a way, India is capable of responding effectively to threats like anthrax, brucellosis, cholera and plague, viral threats like smallpox and fever and biotoxic threats like botulism. Also biological protective gear like masks, suits, etc. are available. The national institute of communicable diseases advises the Government of India on issues related to prevention and control of communicable diseases in the country.[56]

India has made significant progress in bio-technology but needs to integrate its entire apparatus of biodefence by using specially designed information technology tools. Also in the arena of sensor technology there is a need to invest more. As explained above currently this technology is available with few Western countries. India needs to collaborate with them. There is a necessity to modify this technology based on country-specific requirements. The research and development in the area of nano-technology is currently at very nascent stage in India. Further developments in this field need to have an additional focus on bio-defence technologies.

Conclusion

Bioattacks do not create conventional disaster scenarios. Disaster management under such circumstances is extremely complicated. Many government and non-government organizations need to work in sync in such a situation. Such attacks require multiple levels of intervention. Modern technology opens up a vast array of options for tackling these attacks effectively.

However, modern technology also opens the gates to the easy creation of bioweapons. It is not possible to stop the growth and reach of modern technologies that are capable of creating a revolution in both the offensive and defensive fields of bioweapons. Therefore, states will have to act

shrewdly and need to evaluate their investments in this area carefully. The new scientific approaches also bring about many risks to a world that is already deeply troubled. Will these new approaches to biodefense reduce the threats or increase them further? Unfortunately, there is no clear answer. Bio-defence technology is here to stay, in spite of the fact that it is a double-edged sword. The technology has the potential to produce both astonishing medical advances and dreadful bioweapons.

Many modern bio-defence techniques demand huge investments. States find it difficult to decide on the level of their investments in such technologies, because the nature of the threat itself is unclear. Also, technological advancements are making preventive measures more dangerous. This could force states to think differently. Even if states decide to invest less in bio-defence technologies, the problem of germ weaponisation will remain. Currently, the field of biotechnology is growing very rapidly and has immense business potential. This gives rogue states or non-state actors more opportunities to buy or produce bioweapons easily. Access to dangerous pathogens is going to become much easier in the near future. Interested parties may be in a position to use dual-use research facilities. Hence, curbing new scientific approaches in biological defence may not help to stop the proliferation of bioweapons. In fact, halting scientific development is likely to have an adverse impact, as it would lead to the non-availability of deterrents.

It would be prudent if states were to carry out balanced threat assessments for deciding on cost-effective investments in the field bio-defence. Also, the relevance of bio-defence techniques should not be looked at only from the point of view of biowarfare and bioterrorism. Presently, the global community is facing a daunting task to tackle emerging and re-emerging diseases. The SARS epidemic is a good case to illustrate the efficacy of dual-use technology and its benefits to public health programmes. Bio-defence techniques have a much bigger role to play in society than merely that related to bioterrorism.

The BTWC signatory countries should identify ways to ensure that the global diffusion of science and technology does not result in a more serious biological weapons threat. Also, as science and technology continue to advance, and as global technology diffusion proceeds, export controls will become increasingly difficult to manage (export controls continue to make a contribution to halting the spread of bioweapons and related technology).

But the fact that such controls only buy time so that other tools of policy can work raises the question of how much time and effort should be put into preserving these controls.[57] Devising more appropriate tools of disarmament is a good starting point to tackle these issues.

References/End Notes

1 Richard Danzig, "Catastrophic Bioterrorism: What Needs to be Done?" Center for Technology and National Security Policy, US Government Printing Office, Washington, DC, 2003, at http://www.biotech.law.lsu.edu/blaw/general/danzig01.pdf (Accessed on September 10, 2004).

2 Jessica Stern, "Dreaded Risks and Control of Biological Weapons," *International Security* 27 (3), Winter 2002-03, p.90.

3 Susan Wright, *Biological Warfare and Disarmament*, (Rowman and Littlefield, Maryland, 2002, pp. 80-86.

4 Richard Danzig, no.1

5 "Public health response to biological and chemical weapons: WHO guidance" (2004) at http://www.who.int/csr/delibepidemics/chapter4.pdf (Accessed on October 15, 2006).

6 Graham Pearson and Brad Roberts, "Defending against Biological Attack: Importance of Biotechnology in Preparedness," *Defence Science Journal* 51, (4), October 2001, p. 380.

7 "Agent Defeat Weapon: Agent Defeat Warhead (ADW)", at www.globalsecurity.org/military/systems/munitions/adw.htm (Accessed on April 12, 2005).

8 Graham Pearson and Brad Roberts, no.6, p. 383.

9 Jeremy Rifkin, *The Biotech Century*, Phoenix, London, 1999, p. 1.

10 M. Wheelis and M. Dando, "New Technology and Future Developments in Biological Warfare," *Disarmament Forum*, (4),2000, p. 44.

11 "What is Biotechnology?" http://www.ucsusa.org/food_and_environment/biotechnology/page.cfm?pageID=340 (Accessed on February 21, 2006).

12 *Bio Weapons Report 2004,* BioWeapons Prevention Project [BWPP], Geneva, 2004, pp. 6-7.

13 Graham Pearson and Brad Roberts, no.8.

14 Gregory Koblentz, "Pathogens as Weapons," *International Security* 28, (3),Winter 2003-04, pp.126-135.

15 http://www.immunizationinfo.org/immunization_policy_detail.cfv?id=40 (Accessed on October 16, 2006)

16 James B. Petro *et al.*, "Biotechnology: Impact on Biological Warfare and

Biodefense," Biosecurity and Bioterrorism, *Biodefense Strategy, Practice and Science* 1 (3), 2003.

17 Richard Danzig, no.1, p. 23.

18 Helga Rippen, "A Framework for the Information Technology Infrastructure for Bioterrorism," at www.rand.org/scitech/stpi/Publications/public.html (Accessed on April 15, 2004).

19 Ibid.

20 Tim Studt, "Modeling and Simulation: Recreating the Real World," *R & D Magazine* March 2003, at www.lanl.gov/orgs/t/t3/docs/RDX0303Modeling.pdf (Accessed April 15, 2005).

21 David Siegrist, "Advanced Information Technology to Counter Biological Terrorism," at http://www.potomacinstitute.org/publications/studies/advtech.pdf (Accessed on January 5, 2005); "Jane's NBC Manual 2000-01," Jane's Information Group, London, 2002.

22 Tim Otter, "Biological Warfare: A UK Perspective," *Military Technology,* May 2003, p.57.

23 "The Vermont Health Alert Network: Definition of Terms," at http://www.vdh.state.vt.us/common/define.htm (Accessed September 12, 2004).

24 Anthony P.F. Turner, "Biosensors: Past, Present and Future," at http://www.cranfield.ac.uk/biotech/chinap.htm (Accessed on September 12, 2004).

25 *Jane's Nuclear, Biological and Chemical Defence,* 2000-01, pp. 75-77.

26 John Eldridge, "Patrolling a Biological Frontier," *Jane's International Defence Review,* February 2003, p.38.

27 Rocco Casagrande, "Technology Against Terror," *Scientific American*, October 2002, p. 60.

28 K. Chang, "Refining Sensors for Bio-terror Attacks," *International Herald Tribune*, April 3, 2003.

29 Rocco Casagrande, no. 27.

30 "Chemistry of Counterterrorism," at http://www.chemengineer.about.com/library/weekly/aabyb101501.htm (Accessed December 10, 2005).

31 Rocco Casagrande, no. 27, p. 55.

32 Office of Technology Assessment, "Technology Against Terrorism: The Federal Effort," Ch. 4, Government Printing Office, Washington DC, 1991, p. 53.

33 John Eldridge, no. 26.

34 "Engineers Develop Biowarfare Sensing Device," at www.nanotech-now.com/news.cgi?story_id=07929 (Accessed on November 23, 2005).

35 "Investors Focus on Biowarfare," at news.nanoapex.com/modules.php?name=News&file=article&sid=846 (Accessed on November 21, 2004).

[36] "Nanotechnology Business Directory", at www.nanovip.com/directory/Detailed/677.php (Accessed on January 26, 2005).

[37] Manuel Cereijo, "Cuba's Killer Virus and New Nanotechnology," at www.amigospais-guaracabuya.org/oagmc087.php (Accessed on August 15, 2004).

[38] "Benefit Cost Analysis Guide," at www.tbs-sct.gc.ca/fin/sigs/ revolving_funds/bcag/bca2_e.asp (Accessed on December 26, 2004).

[39] Jessica Stern, no.2, pp. 81, 101.

[40] Ibid., p. 102.

[41] Victoria Sutton, "A Multidisciplinary Approach to an Ethic of Biodefence and Bioterrorism ," *The Journal of Law, Medicine and Ethics,* Summer 2005, p. 311.

[42] E. Brenitz, "The New Jersey Anthrax Crisis," panel discussion at the Bioethics and Bioterrorism Conference, Washington, DC, February 28, 2002, summarized by B. Garland in *The Journal of Philosophy, Science & Law,* 2, March 2002, at http://www.psljournal.com/archives/newsedit/bioethics_bioterrorism2.cmf (Accessed on April 12, 2005).

[43] D.R. Buchanan, *An Ethic for Health Promotion: Rethinking the Sources of Human Well-Being,* Oxford University Press, New York, 2000, p. 168.

[44] Victoria Sutton, no. 41, pp. 315-316.

[45] Joel Mokyr, "Man vs. Machine," at http://reason.com/9601/MOKYRbk.shtml (Accessed August 28, 2004).

[46] Jeremy Rifkin, no.9, p. 1.

[47] "Emerging Technologies: Genetic Engineering and Biological Weapons", The Sunshine Project, Background Paper no. 12, November 2003, at http://www.sunshine-project.org/publications/bk/bk12.html (Accessed on September 28, 2005).

[48] Michael Moodie, "Reducing the Chemical and Biological Weapons Threat: What Contribution from Arms Control?" Testimony prepared for the Senate Foreign Relations Committee, March 19, 2002.

[49] BioWeapons Prevention Project (BWPP), *Bio Weapons Report 2004,* Geneva, 2004, pp. 6-7.

[50] US Department of Defense, "Biological Defence Program," Report on the Committee on Appropriations, House of Representatives, May 1996, p. 4.

[51] Mark A. Prelas, "The Classification and Manufacture of Biological Agents," in Tushar K. Ghosh (ed.), *Science and Technology of Terrorism and Counterterrorism,* Marcel Dekker Inc, New York, 2002, pp. 110-116.

[52] Michael Moodie, no. 48.

[53] Janusz Kocik *et al*., (eds.), *Preparedness Against Bioterrorism and Re-Emerging Infectious Diseases,* IOS, NATO Science Series, Amsterdam, 2004, p. 191.

[54] "Nanotech: The New Frontier in Biomed," School of Biomedical Engineering and Health Systems, at http://www.biomed.drexel.edu/new04/Content/news_events/display_news.cfm?NEWS_ID=77 (Accessed on August 13, 2005).

[55] "Full Text of Colin Powell's Speech," at http://travel.guardianunlimited.co.uk/print/0,3858,4599533-103550,00.html (Accessed on August 15, 2005)

[56] Inputs are based on author's field trip (in the year 2003) to DRDE, Gwalior and www.nicd.org (Accessed on November 1, 2006).

[57] Developed by the High Security Animal Disease Laboratory (HSADL), Bhopal. Also, author's discussions with Dr. H.K. Pradhan (on September 14, 2006 at New Delhi) who led a special team of scientists for this purpose and developed it in less than six months on September 14, 2006 at New Delhi.

[58] Michael Moodie, no. 48.

Ajey Lele is Research Fellow at IDSA.