5-1998

Technology and Terrorism: The New Threat for the Millennium

Stephen R. Bowers
Liberty University, srbowers2@liberty.edu

Kimberley R. Keys
Liberty University

Recommended Citation

Bowers, Stephen R. and Keys, Kimberley R., "Technology and Terrorism: The New Threat for the Millennium" (1998). *Faculty Publications and Presentations.* Paper 65.
http://digitalcommons.liberty.edu/gov_fac_pubs/65

The main aims of the **Research Institute for the Study of Conflict and Terrorism** are:

- to research into the causes, manifestations and trends of political instability and conflict throughout the world

- to study the activities of extremist organisations and their international links and support

- to publish balanced assessments of issues vital to international security based on the results of this research and analysis.

To promote these aims the Institute is developing graduate education and training in appropriate specialist fields through links with universities and other institutions of higher education. It is creating contacts with industry and business to encourage greater understanding of the commercial implications of political conflict. It also commissions and co-ordinates research and reports on special projects.

Conflict Studies are published by the **Research Institute for the Study of Conflict and Terrorism**. The views of the authors are their own and do not necessarily reflect those of the Institute.

The Institute is a non-profit-making company, limited by guarantee and registered as a charity in the United Kingdom. Apart from subscriptions the Institute is supported by donations from trusts, foundations and corporations. Reg. Charity No. 261152

Technology and Terrorism:

The New Threat for the Millennium

Stephen R. Bowers and Kimberly R. Keys

Stephen R. Bowers is an Associate Professor of Political Science at James Madison University in Harrisonburg, Virginia. Prior to coming to JMU, Dr. Bowers was with the First Special Operations Command at Fort Bragg, North Carolina. Some of his other military assignments have included the US Special Operations Command at MacDill Air Force Base in Tampa, Florida, Special Operations Command (Europe) at Patch Barracks in Stuttgart, and the Special Warfare Center at Fort Bragg. He is the author of Conflict Study 248, *Ethnic Politics in Eastern Europe* (February 1992) and the co-author of *Tibet: Endurance of the National Idea* (1994).

Kimberly R. Keys is a Senior Analyst with Orion Scientific Systems in McLean, Virginia, specialising in developing information technology solutions for international security problems. Prior to her work at ORION, Kimberly Keys served as an international relations analyst with General Research Corporation in McLean, Virginia and focused on developing information solutions to support security problems of the Ballistic Missile Defense Organization (BMDO).

May 1998

Technology and Terrorism:
The New Threat for the Millennium

Stephen R. Bowers and Kimberly R. Keys

INTRODUCTION

In the post-Second World War era, terrorism emerged as one of the more significant aspects of low intensity conflict. While historians can trace terrorism back to the efforts of the 'Zealots' to break Roman rule over Palestine in the year AD 66, most analysts regard it as a relatively new phenomenon. As such, it has posed special problems not only for the security of nations but has also threatened the very foundations of democratic society by disrupting popular confidence in institutions. Terrorism has emerged as a standard tactic to be used in low intensity conflict. M. L. R. Smith contends that terrorism is becoming the norm in societies that are not technologically advanced and are still struggling with democratisation.[1] Unfortunately, many contemporary examples of the use of terrorism, especially in the case of Bosnia, seem to prove his point.

Complacency is one of the more consistent human traits and, by the latter part of the decade, some scholars have begun to speculate that terrorism, as a critical international factor, is on the wane. This assumption can be bolstered by statistics indicating a decade-long decline in the number of terrorist incidents; yet those statistics mask a more significant fact. The most important point about any analysis of terrorism at the end of the century is that while the number of incidents are down the *lethality* of the terrorist potential has risen to a frightening degree. The key to this ominous development is found in the overwhelming technological progress of late 20th century society.[2]

Technology, defined as the application of scientific knowledge to human problems, has contributed greatly to our ability to deal with situations in such a way as dramatically to alter the course of our existence and has challenged traditional state centric views of reality. It is modern technology to which we give credit for almost every improvement in medicine, nutrition, education, and our general standard of living. Technology has changed the nature of relations among nations and within them. Yet it is this same technology which has affected the nature of the life-threatening hostilities of the past century. As the most primitive weapons have been replaced with sophisticated, silent, and deadlier ones, technology clearly receives the credit. Technological innovations force us to consider the role that non-traditional, namely non-state and transnational actors play in threatening our security. As will be demonstrated in the following examination, the emergence and active proliferation of computer, biological, and chemical terrorism is a consequence of technological innovations. In all three of these, technology is an intervening variable that has made each threat more significant. The emergence of the computer as a technological device associated with terrorism is a very new phenomenon while chemical and biological munitions, though of recent origin, have been recognised as weapons of mass destruction for much longer. It is recent technological innovations which have made them more viable as weapons. The sheer volume of such activities and their destructive potential makes terrorism more problematic, harder to monitor, and more difficult to deter.

New terrorist tools

Technology has had a great impact on the development of the terrorist threats emerging since the end of the Second World War. Access to new terrorist tools, the broadening of the terrorist market, and the advent of sophisticated and readily available computer technologies are all significant factors in this evolving threat. With the passage of time and the advancement of numerous technological innovations, such as the miniaturisation, portability and increased precision of weapons, and the spin off of technology into a variety of other domains, the tools of the terrorist became less expensive, more destructive, and widely available through less secure non-governmental outlets. In the early 1970s, public awareness of this development was heightened by news that a college undergraduate, using open source materials, had designed a nuclear explosive device. In fact, with the exception of the necessary small quantity of uranium, the student had produced a fully workable nuclear bomb. Subsequent reports about the ease with which this substance could be acquired further stimulated fears about a changing terrorist threat.

These important technological tools have been augmented by significant motivational factors. Among the most important of these, according to Bruce Hoffman, are the resurgence of terrorism motivated by religion, the increasing amateurisation of terrorism, and the enhanced professionalism of terrorists. Today's terrorists, Hoffman writes, are more 'adept in their tradecraft of death and destruction; more formidable in terms of their abilities of tactical modification'.[3] Thus, access to new tools, a broadened supply of available terrorist goods, and the advent of computer technologies are not the only critical developments to increase the nature of the terrorist threat. In fact, it may well be that the 'soft' motivational factors make the technological factor more deadly.[4]

In the past, general attitudes towards terrorist behaviour were based on the belief that terrorist groups were operating on assumptions which were similar to those of conventional political actors. The terrorists presumably understood, therefore, that there was an accepted threshold for violence and proceeding beyond that was to invite massive official retaliation. The appearance of non-state terrorist actors motivated by ethnic or racist hatred, religious zeal and apocalyptic visions of mass destruction has resulted in a rejection of those unspoken 'rules of the game'. For many of these groups, excessive violence performs a redemptive purpose and, because they are non-state actors, their apprehension by law enforcement agencies cannot be taken for granted. Unlike the more traditional terrorists, the activities of these groups are much less likely to be media-driven.

The 'silent terrorist'

One of the most consistent actions immediately following terrorist events of past decades was the predictable demand for credit by the group responsible for that event. More recently, however, major terrorist actions have been followed by silence as no group announced its responsibility or a shadowy, previously unknown group claimed to have committed the act. Several incidents have fallen into this category: the destruction of Pan Am Flight 103 over Lockerbie in 1988, the downing of Air India Flight 182 over the Atlantic in 1985, the Atlanta Olympics bombing in 1996, and the Khobar Tower bombing in Saudi Arabia are some of the most notable. The emergence of a new 'silent terrorist' creates an even greater climate of fear because of the uncertainty over motivations. Not knowing the identity or motivations of the terrorist group means greater difficulty in predicting the next target. The immediate uncertainty surrounding the identity of the perpetrator of the Khobar Tower bombing resulted in considerable tension between the US, and its allies and also exacerbated tensions between the US and Islamic nations suspected of complicity in the event. Such post-incident confusion and uncertainty about the actual perpetrator make cases like this even more troubling.[5]

An additional factor complicating the terrorist threat has been the proliferation of 'markets' at which individuals and organisations can purchase sophisticated weaponry previously either available only through limited official channels or completely unavailable. The deterioration and collapse of the former Soviet Union has resulted in a dramatic broadening of the range of available weapons. Throughout the region, vendors at open-air bazaars have begun to offer attractive and expensive western products for civilian use as well as deadly but inexpensive military weapons. Everything from hand grenades to rocket launchers can be purchased by customers with hard currency. More importantly, senior military commanders with access to advanced nuclear weapons, facing the prospect of lost income following the economic collapse of their employers, have been increasingly inclined to sell the instruments of mass destruction for which there is a ready and eager market.

It is not the weapons and the actions of the former Soviet Union alone which have heightened fears of an enlarged threat. There is a veritable flood of materials which support chemical and biological capabilities from which would-be terrorists can draw. Countries like Iraq and Iran routinely receive the precursor materials which support the development of these terrorist technologies. While we decry the availability of deadly Soviet technologies, western nations like the United States have also contributed to this situation. For example, a biological agent repository in Bethesda, Maryland actually allowed the transfer of anthrax to the Iraqi authorities in 1986.

While new weapons technologies and a flood of sophisticated Soviet weapons enhanced the destructive potential of the terrorist, other technological innovations have made society more vulnerable. The 1980s saw a phenomenal expansion of computer technologies and the introduction of the computer into almost every aspect of our lives. By the present decade, computer networks have effectively linked banks, businesses, government, universities and almost every national institution into an elaborate and, in many ways, delicate network. Such devices have done much to bring about the globalisation of societies which are intimately linked into an electronic superstructure that reduces cultural divisions. Consequently, terrorists attempting to attack targets in this global community cannot limit the impact of their actions to one particular group or facet of society. In this larger social entity everyone becomes at least part of the terrorist target.

The operational nature of computer technology has greatly enhanced the power of actors who would use this innovation to threaten society. As a result of the organisation of sophisticated 'client-server' technologies, a great amount of processing power can be transferred to the client and away from the provider's central controls and security regulations. Consequently, terrorists now have a ready target whose capabilities can be transformed into weapons against the very society which created the technology being used to disrupt its orderly functioning.

A new type of terrorist

As a result of these developments, there are countless new possibilities for a completely different kind of terrorist. In the traditional view, the terrorist is an extremist motivated by some political, ethnic, or sociological grievance and working with others who share this outlook. We understand the terrorist, we believe, by examining group motivations. By learning to identify the signatures of terrorist behaviour, we can make realistic projections about future terrorist actions. We can also understand the relationship between events such as, for example, the expansion of Israeli settlements and possible terrorist strikes against targets in Israel. In general, analysts have placed terrorism within the framework of studies of nationalism, the activities of certain dictatorial regimes, or radical ideologies such as Islamic fundamentalism.

This analytical approach has been supported by academic research on terrorism which was averse to operational demands of agencies charged with combating the terrorist threat. Academics have been interested in explaining broad trends in terrorist violence and have focused on incident-based research as the basis for generating knowledge about such trends. Consequently, they have examined terrorism primarily within the broader field of general theories of violence. Specific terrorist actions were viewed largely as the subject matter for case studies for examining theories of violence. In doing this, academic specialists drew from the fields of sociology and other disciplines which focused on group behaviour.[6]

There has been an apparent reluctance within the academic community to approach terrorism within a context that would be useful to the government officials dealing with this problem. These counter-terrorist (CT) analysts and operational planners were faced with the problem of identifying and forecasting future terrorist threats. In an effort to interdict these, CT planners needed to look beyond the theoretical analysis of an incident and treat the group as an organisational entity. To understand the behaviour, both present and future, of a terrorist organisation is to understand its ideology, formation, recruitment and training patterns and to identify its likely targets.

TERRORISM AND THE COMPUTER

The benefits of technology are being realised by a new breed of terrorist, the cyber-terrorist, who uses lawlessness to achieve aims through the exploitation of computerised systems deployed by the target.[7] The terrorists of the immediate Second World War era faced numerous challenges in their efforts to communicate. All too often, they had to resort to cut-outs, dead drops, hidden messages and other relatively slow and primitive devices, each of which carried with it risks of detection, delay, or misunderstanding. Modern, computer driven telephone systems offer both the average citizen and the terrorist a quick and effective means of communication. Cellular phones have been especially valuable in easing the burdens of communication for individuals on the move.

Terrorist recruitment and training

The computer has been particularly useful to terrorist groups for recruitment and has made possible the careful investigation of volunteers. It is among them that infiltrators are most likely to be found and, with the aid of computerised records, individual backgrounds can be checked before the admission of new members to sensitive positions. Groups wanting to infiltrate their own agents into different organisations can also rely upon the computer to create more effective and verifiable cover stories to deceive agencies conducting background investigations. For the genuinely sophisticated terrorist, the computer is a tool for training and planning. By creating computer models of targets, it is possible to have an advance 'virtual walk-through' of facilities selected for terrorist operations.[8]

In what we now think of as the 'computer age', it is not only groups but also lone individuals who can pose a great threat to the security of institutions and even nations. While not arousing the fears of mass destruction associated with biological and chemical weapons, cyber-terrorism is joining conventional terrorism as a significant threat to the security of our institutions and the computer hacker stands alongside the terrorist cell as a phenomenon whose actions and motivations must be understood. However, unlike the more traditional terrorist who was vulnerable because of the demands of fund-raising, recruitment, and security, the cyber-terrorist operates in a much more risk-free environment and never has to come into the open to engage in such activities as arson, assassinations, hostage-taking, or kidnappings. Cyber-terrorism has thus emerged as an attractive terrorist option for several reasons. First, danger to the terrorist himself is limited. The acquisition, training, and staging of weapons deployed against a target does not exist in cyber-terrorism as in traditional terrorism. Additionally, computers have no physical protection, such as mylan sheathing or large barricades, a convenient omission which facilitates the success of an attack. Third, risk of capture and arrest are limited. In fact, a cyber-terrorist has the opportunity to learn from past mistakes, thus improving his skills. Equally troubling is the fact that we have fewer tools and much less experience for dealing with this terrorist threat and analysts have few tested, refined models which might guide responses.

National security

For cyber-terrorists, the inherent vulnerability of information systems creates an opportunity which can be exploited with surprising ease. This opportunity is the result of a market in which 'information brokers' now play an essential role in almost every aspect of business, politics, and science. For such operations, data is a commodity whose value is based on the traditional assumption that knowledge is power. In this environment, the skilled hacker can destroy the power base of an advanced society by sabotaging the data stored on its computers. Furthermore, recognising knowledge as power, information warfare may become another important category of low intensity conflict which must be considered as an important national security factor.

The many linkages between military and the less secure civilian information systems gives this development a special relevance for national security. Initially conceived as an instrument to facilitate military command and control functions, what we now know as the Internet was created as the result of an initiative by the US Department of Defense. Given the expense of computers and the geographical dispersion of individuals involved in defence related research, the DOD set out to create linkages between distant computers. Eventually, an unclassified network was created and, as a result of the early success of interactive computing, there was great pressure from universities, non-military research scientists, and private groups involved in work with computers. By the mid-1980s, the National Science Foundation had effectively linked five major computers and what eventually became known as the Internet was in operation. Within a few years, thousands of other networks were connected and interactive computing had become as common as the morning commute to the office and, in an increasing number of cases, was actually replacing it.

Since computers serve as more than repositories for data, but also play a vital role in the performance of an infinite variety of functions, the orderly operation of this electronically connected society is very much at stake. According to Arnaud DeBorchgrave of the Center for Strategic and International Studies, during recent tests, computer specialists have demonstrated an ability to crash the computer systems of both the New York Stock Exchange and the social security system. Moreover, according to Arnaud DeBorchgrave, 80 per cent of the Fortune 500 companies have been electronically penetrated by hackers.[9]

THE CYBER-TERRORIST POTENTIAL

In 1993, terrorists created a great panic in New York City with an attack on the World Trade Center. As the most visible instance of foreign terrorism on US soil, this event heightened American fears of the terrorist potential. Yet the incident had a direct impact on only a small number of people and the actual damage was minimal. The cyber-terrorist potential extends far beyond what was seen in the attack on the World Trade Center and even the more destructive and deadly strike in Oklahoma City two years later. With a cyber-terrorist attack, the damage is devastating on a totally different dimension. The World Trade Center attack was conducted by individuals utilising traditional terrorist technology and, in their efforts to gain entry to the Center, they exposed themselves to detection and, eventually, arrest. The cyber-terrorist, however, has no need to drive into underground parking garages or disable conventional alarm systems in order to disrupt powerful institutions. All major financial transactions, banks, stock exchanges, and economic structures are driven or linked by computer networks. The networks can be penetrated by physically remote terrorists who can destroy popular confidence in a nation's economic system and thereby inflict a different kind of damage and affect more people than conventional terrorists who cause disruptions with poison gas, bombs, or bullets. The key point is not that one kind of damage is more significant than another. The loss of life is disastrous in a manner that brings about great personal grief. The damage to national security data stored within compartmentalised information systems or to citizens' financial data stored in an electronically accessed bank account is also disastrous but on a different level. Given the transition of post-industrial societies into a new type of revolution – the information revolution – the nature of damage to critical knowledge and information systems is exceptionally destructive to societies which have become dependent on these new technologies. All types of damage are costly and present problems for each afflicted population. The most important concern at this juncture in the development of terrorism is to recognise that terrorist activities can result in a much greater variety of types of damage to individuals and to society.

Targeting human systems

The ability of the cyber-terrorist to disrupt the normal economic functions of a modern state is matched by his ability to destroy popular confidence in infrastructures which are essential to human life and our technologically advanced life style. Because computers control the processing systems of numerous factories throughout the post-industrialised nations of North America and Western Europe, the cyber-terrorist can gain access to computers that determine sensitive and precise levels of nutrients in many food products. Consequently, millions of consumers could easily be sickened because of minuscule alterations in familiar and trusted products. Cyber-terrorists have the potential to target the health industry, the infrastructures of our civil society, the financial systems, our transportation networks, systems of public safety, our communications infrastructure, the environment, and national military organisations. In the United States, emergency 911 systems have been effectively shut down by individuals. In short, no service, system, or institution is beyond the reach of skilled criminals determined to bring about havoc.

'Information warfare'

The actions of the cyber-terrorist may have many impacts. One of the most significant is that the computer is now recognised as an instrument of war and can be used to fulfil important military objectives for both conventional and terrorist forces. The term which embodies this general concept is 'information warfare'. Lessons learned from cyber-terrorist actions are being incorporated into contemporary information warfare strategies. There is a general acceptance of the argument that an important aim of warfare is to affect an adversary's information systems. Controlling inputs into his decision-making process is one way in which the enemy's perceptions and actions can be influenced.[10] Since almost all vital information is now retrieved, processed, and stored with the aid of the computer, intrusion into the computer system gives any aggressor the capability of directing his adversary's behaviour in such a way as to ensure his defeat.

An additional impact is the flood of terrorist group sites on the world wide web. This has transformed the computer into a terrorist instrument for advertising and recruiting. Many groups now routinely maintain a computer home page. Through this site they can advance their beliefs as part of a propaganda effort and attempt to attract converts. The home page also provides clues as to their interests and, because other groups read this page, the computer thus aids the group in communicating with others who share their interests. It has become apparent that via the computer, groups are now able to share technologies that are employed in terrorist actions.

BIOLOGICAL TERRORISM

Another demonstration of the degree to which technology has transformed the terrorist threat is the emergence of biological terrorism. Few weapons inspire greater fear than those biological warfare (BW) agents which have appeared not only on the modern battlefield but also in discussions about current terrorist activities. As one of the weapons of mass destruction associated with the newest and most threatening of terrorist groups, biological weapons challenge conventional modes of thinking about the contemporary terrorist threat. Previously, there was a major psychological barrier to the use of such weapons of mass destruction against civilian populations. The idea of such an action was regarded as so distasteful that no group seemed seriously to consider it. In March, 1995, however, this barrier was broken when a Japanese group employed a deadly chemical nerve agent against civilians riding the Tokyo subway. After that incident, traditional assumptions about an aversion to the use of weapons of mass destruction against civilians were abandoned.

A deadlier agent

Although military planners often use the term 'bio-chemical' to designate a single class of weapons, biological and chemical devices are significantly different instruments. First, biological agents are much deadlier than their chemical counterparts and their utilisation is likely have long-lasting effects and to result in a much greater death toll.[11] The lethality of biological weapons is such that 10g of anthrax spores could produce the same death toll as a ton of a chemical nerve agent like sarin. The US Congress' Office of Technology Assessment estimates that, if it were dispersed by an efficient aerosol generator, 100kg of anthrax could produce over 1m deaths in a city the size of Washington, DC.[12] Second, while the physiological and medical effects of chemical weapons are well defined, those of biological agents are very broad and more difficult to treat. Third, modern military organisations have developed some skill in detecting the use of chemical weapons, but it is much more difficult to determine if biological weapons have been deployed in a battlefield environment. US troops in the Gulf War, while trained for dealing with chemical threats, had no operational capability to detect the presence of biological agents. The first biological detection instruments were not introduced in this theatre of operations until February 1998, when the threat of renewed fighting prompted new concerns about this danger. The fact that the US has achieved only limited success in the development of such instruments means that little has been accomplished in terms of providing protection against this special danger. The main problem is that there are numerous potential biological agents – approximately 60 – which may be introduced, each of which requires special detection measures. Consequently, the most effective method of preparation for a biological threat is to maintain a stockpile with a wide range of medical products which could mitigate the effectiveness of biological agents.[13] While it would seem prudent to develop an indications and warning system to prepare for and respond to a biological threat before its implementation, little has been done to undertake such a measure.

Historical antecedents

Despite the fact that we often discuss BW as a modern phenomenon, this concept can draw upon several historical antecedents. Historians note that in the 14th century, the Tatars catapulted plague-infested corpses over the city walls of Kaffa, a besieged city in the south-west Ukraine, as a way of spreading disease among the defenders. The tactic was both effective and economical. During the French and Indian Wars of the 17th century, English soldiers gave Indians blankets which had been exposed to the smallpox virus. The resultant smallpox epidemic enabled the English to win an important military victory. Water supplies were polluted with dead bodies by Roman troops 2,000 years ago as well as by Confederate troops during the American Civil War. The early 20th century saw more ambitious applications of BW tactics. The Japanese tested biological weapons on prisoners of war and sparked an epidemic of bubonic plague in China and Manchuria by spreading flea infested debris over major cities in the region. Alerted by the Japanese programmes, the British selected an island off the Scottish coast to conduct biological experiments with anthrax. They evidently had considerable success in creating lethal substances but much less in developing decontamination measures. As a result, over 60 years later the island is still completely off limits. These lessons seem to have had a cautionary impact on the conduct of operations during the Second World War and, with a few notable exceptions, biological weapons did not play a significant role.[14] The most significant exception relates to activities of the Japanese during their occupation of China. According to numerous accounts, Japanese medical personnel stationed in Harbin, China subjected American, Chinese, Korean, British, and Soviet prisoners of war to experiments involving the bubonic plague and other illnesses. Over the course of several years, an estimated 4,000 prisoners died as a result of these experiments and, at the end of the war, Japanese military officials attempted to destroy all traces of their operations. Similar experiments took place at Japanese POW camps in Manchuria.[15]

Modern biological warfare

In the post-Second World War era, technology began to have a significant impact on the utilisation of what is, in fact, an ancient method of coercion. No longer a casually employed or spontaneous tactic left to the discretion of battlefield commanders, biological warfare was studied at national level and factories were established for the purpose of either creating new biological weapons or determining how to counter an adversary's biological arsenal. Our infatuation with these weapons was such that, in at least one instance, a biological weapon was designed for the explicit purpose of killing Fidel Castro.

Over the years the former Soviet Union devoted a great portion of its scientific energies to the production of an enormous arsenal of biological warfare instruments for use in possible military confrontations with its adversaries. Despite denials of involvement in any such programme, the Soviet effort to produce militarily usable biological instruments was intense. Even though the former USSR signed the Biological Weapons Convention, which called for a rejection of these weapons, President Boris Yeltsin eventually acknowledged that this agreement was routinely violated. The largest production facility was located in Stepnagorsk, Kazakhstan, but, during the 1970s and 1980s, approximately 20 others were situated elsewhere in the former USSR. Soviet surrogates such as East Germany were also actively involved in BW research. The Stepnagorsk factory existed for the sole purpose of producing bombs and missiles loaded with anthrax. Biological warheads were even installed on one version of the SS-11 intercontinental ballistic missiles that were targeted against the United States. Although Stepnagorsk is now closed, there are reports that three or four similar plants are still in operation in Russia.[16] In 1998, when Kanatjan Alibekov, a Russian scientist who once served as Deputy Chief of the Main Biopreparat in Vector, Russia, made such an assertion, the Russian Foreign Ministry was quick to deny that Russia has continued to develop biological weapons under the cover of defensive research. Alibekov maintained that as late as 1992, he was involved in directing decisions to strike American cities first with biological weapons.[17]

In 1978, Georgi Markov, a Bulgarian defector working for the BBC, was the victim of a biological weapon designed in Soviet laboratories. This incident called attention to the former USSR's use of such devices as tools for assassination. Accounts of fighting in Afghanistan and, more recently, Chechnya, provide evidence of the Soviets' technological advances and apparent willingness to use those deadly devices as instruments of mass destruction. As the former Soviet arsenal is now being dispersed to the world's highest bidders during Russia's new struggle not for world conquest but simply for survival, security planners have been required to devote greater attention to the possible emergence of a wider biological terrorist threat. In late 1997, the Russian government apparently entered into secret agreements with Iran to sell a portion of their biological arsenal, thus contributing to the further destabilisation of the Middle East.[18]

Warfare becomes terror

Eventually, most world leaders recognised the risks of biological warfare and the commitment to avoid its use became almost universal. With this development, biological weaponry came to be regarded as the exclusive tool of regimes outside the community of civilised nations. Biological warfare, as a concept, had been transformed into biological terror. The collapse of the former Soviet Union and the sudden availability of its many weapons represented an early warning that biological terrorism had emerged as a new and more sinister threat to the security of those institutions upon which we depend for our security and well-being.

In February 1998, security specialists and the general public alike were alarmed by reports that two US citizens had been arrested while in possession of what was initially thought to be a deadly portion of anthrax. These reports heightened awareness of the pervasive nature of technologically advanced weaponry now in the hands not only of various governments but also of terrorists of every ideological or political persuasion. This chilling incident occurred at a time of growing concern about the possibility that Iraq might use BW as a way to fulfil its national aspirations, thus elevating biological terrorism to the level of a national policy.

The international biological threat is heightened by the fact that such weapons are remarkably cheap and easy to produce. The most significant danger of the Cold War was the result of confrontations between the rich and/or powerful nations. However, in the world of biological terror, possible combatants can be found among the ranks of the impoverished and less powerful who aspire to force political and economic change with these relatively new and inexpensive weapons. While the United States and other western nations terminated offensive BW programmes after 1969, many nations have found these to be affordable, devastatingly effective, and, therefore, irresistible instruments for their national arsenals. The fact that biological weapons may be directed against a wide range of targets further enhances their attractiveness. Convenient targets may include military organisations, military dependants, unsuspecting civilians, livestock, or even crops. Equally appealing is the stealth with which biological agents can be deployed. A nation may be under attack for weeks or months without realising it. After all, disease is a routine part of the human condition, so the first suspect is nature rather than a political adversary.

The ease of production of biological agents is such that not only nations but also non-state actors can produce them effectively. The required technology is commonly available, relatively unsophisticated, and rarely falls into the category of highly classified data to which general access is denied. As a result, any consideration of BW threats must take into account the possible actions of both nation states and terrorist groups which may not be affiliated to state agencies. Biological terror need not be state sponsored in the contemporary technological environment.

The potential for biological terrorism

Modern technology's most important contribution to the development of biological weaponry has been the improvement of weaponisation. In past centuries, BW was often conducted but its instruments were crude and, in terms of logistics, rather limited. Tossing a plague-infested body over the ramparts may have been extremely intimidating and very effective but biological warriors could not always count on having a ready supply of appropriately infected corpses. By the late 20th century, because of technological applications, deadly biological substances can be produced in a concentrated form and are easily transported. Neither availability nor delivery represents a logistical challenge today.

The assumption of traditional terrorism was that a small number of casualties would have a dramatic impact on the much larger general audience. The real targets of terrorism were those who witnessed the horrors rather than those whose deaths may have resulted from a terrorist incident. The terrorists' primary objective, we assumed, was to undermine popular confidence in the system rather than to kill large numbers of people. The development of modern technology, especially in the area of biological weapons, has changed this and contemporary terrorists can think in terms of killing very large numbers of people in a single action.

The emergence of biological terror as a threat signals the arrival of a new kind of terrorist who, unlike the traditional one, does not feel the need for public recognition and is not driven by the media. This new terrorist, according to Dr. Jerold Post, a prominent profiler of terrorists, is more likely to be motivated by a desire to cleanse society as an expression of either religious zeal or ethnic hatred. Such an individual is less concerned about simply calling attention to a political or social demand and is more inclined to undertake mass killings in order to bring about the destruction rather than the reform of society. He is unlikely to espouse the standard political agenda common to terrorists of past decades.[19]

Equally significant is the fact that biological weapons, in contrast to the highly touted 'smart bombs' of the 1990s, lack the precision valued by military planners. They depend upon environmental conditions and if these are not ideal, dispersion is difficult if not impossible to predict. The value of such instruments lies in their ability to bring about a death toll numbered in the tens or hundreds of thousands rather than the smaller numbers associated with conventional weapons. Consequently, lacking dual utility, they can be employed only under specific strategic circumstances when the primary objective is mass terror.

However, while lacking in precision, these weapons do enjoy flexibility. With reasonably skilful biological engineering, it is possible to devise and deliver biological substances which are less than lethal. Consequently, while we usually speak of biological terror, *biological sabotage* is also a possibility. Not wishing to inflict devastating losses on a target population, BW planners may simply incapacitate an adversary to the extent necessary to accomplish specific military objectives. Perhaps an epidemic of mild flu will satisfy their strategic needs better than a full scale attack of the plague. Thus, it is important to note that 'doomsday' scenarios are not the only ones utilised in planning for BW.

The proliferation of biological weapons has quickly assumed proportions to rival the spread of nuclear weapons. It is, perhaps, this factor which makes the BW threat most significant. According to recent reports, the list of nations possessing biological weapons now includes, in addition to Russia, Iraq, Iran, China, North Korea, Egypt, Syria, Taiwan, Israel, and Pakistan.[20] The threat lies not in the length of this list but in the fact that many of these nations reject the political and territorial status quo and are more likely to use such weapons to advance an aggressive agenda.

Biological agents do, however, have important limitations. Among the most feared is anthrax. While it is extremely lethal and has an 80 per cent mortality rate, it is not contagious. Victims, therefore, must be directly exposed to it. It is also important to recognise that while many people have expressed fears that anthrax or other biological agents might be introduced into a community's water supply, such a tactic generally results in a significant dilution of their effectiveness. Therefore, we can conclude that the vulnerability of modern society is somewhat over-estimated. In fact, some analysts suggest that biological weapons have never been employed by terrorists or, perhaps, even by states. There have been threats regarding the use of biological agents but most of these have turned out to be hoaxes.[21] Finally, while there are 'anti-status quo' states which possess such munitions, there are important arguments which deter them from their use. Most compelling is that biological weapons are indiscriminate and difficult to direct, contain, or control. Biological agents, with their capacity to reproduce themselves, may well bring about unpredictable and devastating results. Consequently, the 'terrorist states' realise that their own troops might well be devastated by these weapons because of something so mundane as a shift in the direction of the wind. In a similar fashion, non-state terrorists are aware of the frightening personal risks they face in handling biological weapons and are likely to choose another less risky option.

Moreover, terrorists have found themselves increasingly successful in achieving their goals without resorting to the actual use of these terrible weapons.

CHEMICAL WEAPONS

Closely related to biological weapons and equally impacted by the development of technology, chemical weapons first attracted attention on the battlefields of the 20th century. While the production process for chemical weapons is much longer than that of biological weapons, they can be designed to kill much faster. Our first experiences with chemical weapons were during the First World War when mustard gas acquired its reputation as one of the most brutal and inhumane of modern weapons. In spite of the widespread horror with which most people responded to reports of the effects of mustard gas, by the Second World War most nations had considerable experience in studying and developing a variety of chemical agents.

Binary weapons

One of the most significant events in the evolution of terrorism has been the development of binary weapons. Such a device is a chemical weapon for which individual precursor components may be stored separately. When the elements are combined there is a qualitative change in which essentially harmless substances are transformed into an agent of great lethality. The binary weapon eases the storage risks for terrorists and, with proper engineering, enables the terrorist to remove himself from the scene of an imminent chemical terrorist incident.

The development of the binary weapon has taken place just as counter terrorist activity has become more effective in dealing with the traditional terrorist methods. Hi-jacking, bombing, and kidnapping, those routine tactics employed by terrorists since the advent of terrorism as a phenomenon, are no longer as effective as in the past. Groups relying on them face an increasing risk of detection and apprehension. It is, therefore, ironic that the success of counter terrorist forces in suppressing the use of conventional weapons now forces terrorists to give renewed consideration to chemical weapons.

Chemical agents

Numerous chemical agents, perhaps thousands of them, are of potential value to terrorists. Insecticides and herbicides are prominent in this category as are broad groups of substances which may be categorised as **choking agents** such as chlorine, **blistering agents, nerve agents**, and **blood agents** such as hydrogen cyanide. Blood agents are poorly suited for use against large groups of people and their use is generally confined to assassinations. There are three specific chemical weapons of special interest to contemporary terrorists. One of the deadliest is VX gas, a colourless, odourless liquid that is virtually undetectable and can spread through either air or water causing convulsions, paralysis, and death. A second is one of the best known blistering agents, mustard gas, a colourless, odourless liquid that, when inhaled, causes long-lasting blisters. Like other blister agents, mustard gas is designed to incapacitate rather than to kill. The third is sarin, one of the most notorious nerve agents and a highly toxic gas which attacks the central nervous system. Sarin was developed by German scientists in the years before the Second World War. It is absorbed through the respiratory tract and may result in death by suffocation. Its use in the Japanese subway attack led to worldwide fears about the utilisation of chemical weapons by terrorists.[22] Nerve agents are now the most commonly stockpiled chemical weapons and are preferred because of their greater lethality in comparison with blister, choking, and blood agents.

Discussions of weapons of mass destruction inevitably produce an effort to weigh the relative merits of nuclear, biological, and chemical weapons, the three major components of this deadly category. There is a great deal of disagreement about this question because of the difficulty of determining when a particular characteristic actually becomes an advantage. Target characteristics in particular will have an impact on the utility of such devices. Nevertheless, there are some general assumptions that indicate the relative merits of chemical weapons.

Chemical weapon characteristics

First, chemical weapons, like their biological counterparts, are relatively inexpensive in comparison with nuclear weapons. They are easy to obtain or to manufacture with your own resources and, since they can be tested prior to employment, they are fairly reliable. Moreover, it is possible to establish a convincing cover operation for the production of such weapons. Numerous businesses can claim legitimate uses for the elements used in their production. Where terrorists lack the modest level of intellectual sophistication required for development of their own chemical agents, the lower levels of security employed in the storage of such devices – in contrast to the security measures employed for biological and nuclear weapons – makes outright theft a realistic option. Since chemical weapons are utilised by the police and security agencies of a number of states, some of which are notoriously lacking in a concern for physical security, would-be terrorists have numerous arsenals to choose from in planning for procurement by theft.

The fact that there are several states willing to supply chemical weapons to terrorists makes availability even greater. The list of nations either known or suspected as suppliers is long and includes Libya, Iraq, Russia, Syria, North Korea, and Cuba. Apparently, before the collapse of the former USSR, Soviet-supplied chemical weapons were used in numerous Third World conflicts and, according to several reports, nations which had Soviet chemical weapons allowed terrorist organisations such as the PLO to draw from their arsenals for attacks against civilian targets.

For groups unable to locate a state sponsor, the availability of chemical weapons is increased by the fact that so much of this material has been left over from previous conflicts and is not subject to very secure storage regimes. In recent years, governments which have developed these weapons have disposed of millions of tons of chemical agents and, all too often, have stored them at sites which are not secure. Since many of these agents retain their potency, by locating the storage sites terrorist groups can equip themselves with working chemical weapons at virtually no cost. Chemical weapons developed for use but not employed during the Second World War are stored by many nations. The largest number of these weapons are in North Africa and the Middle East where they can be easily obtained by casual searches in the desert. When the US Army disposed of surplus chemical agents in 1977, it even announced the locations of the storage facilities, two of which are widely regarded as being less secure than 'a local supermarket'.[23]

Second, in their employment such weapons can be directed against selected targets, generally humans or other living organisms, while not disturbing the physical structures that might be of eventual use to the forces of a state terrorist. In addition, these weapons offer considerable threat or demonstration potential that can be used to persuade a target to yield to demands rather than face the consequences of a full and unrestrained strike utilising chemical weapons.

Third, most chemical agents will rapidly disperse following their employment. This feature constitutes an important tactical advantage. They can be used in an attack when the terrorist force intends to enter a facility after staging a chemical strike. Thus, the terrorist is able to effect that most fundamental of military objectives, physical occupation, and is not limited to the simple destruction of a target site. This characteristic represents an important contrast with both nuclear weapons and conventional explosives.

Fourth, the presence of chemical weapons, with current technological limitations, is difficult to detect. While conventional weapons are vulnerable to numerous detection methods, chemical agents, so often odourless and colourless, are almost impossible to detect, even while in use. Detection during storage is even more difficult. In situations where stealth is an essential terrorist tactic, the chemical weapons have qualities which make their use ideal.

Finally, it is possible to engineer the effects of chemical weapons in such a way as to produce relatively mild effects or some of the most horrible consequences imaginable. A chemical attack can lead not only to death, but to death under incredibly odious and painful circumstances. Chemical weapons, in contrast with others, are extremely weight effective. A small package of chemical agents is estimated to be 40 times more effective as a weapon than a comparable package of conventional explosives. The flexibility of chemical weapons also means that they can be used either as weapons of mass destruction or as weapons directed against individuals.[24] The Soviet Union's assassination of the Ukrainian émigré leader Stefan Bandera, undertaken with a weapon that simulated the conditions of a heart attack, is one example of how this can be done. Such a tactic, if successfully employed, will allow the assassin to escape with the greatest of ease because authorities do not immediately realise that death was by other than natural causes.

The use of chemical weapons in terrorist attacks

While it appears that biological weapons have been employed rarely or not at all as terrorist tools, there are several incidents in which chemical agents have been used. The most important of these took place in Tokyo on 20 March 1995 when members of a Japanese terrorist group placed small containers on five trains on three lines of the city's subway system. As a result of this incident, 12 people died and another 5,500 people were injured when the gas spread through various trains. With this attack, people who had never heard of the chemical weapon sarin learned that this substance was in the possession of the Aum Shinri Kyo, a group determined to cause not only as many deaths as possible but also inflict terror on the city's entire population.[25] As an apocalyptic group advocating the end of the world at the millennium, Aum viewed its chemical attack as a means of advancing its apocalyptic vision.

Because of the peculiar qualities of many chemical weapons, it may be impossible to determine if there has actually been a chemical strike. The subway incident sparked official attention to this threat and revealed incidents, previously either ignored or simply not understood, which apparently fell into this category. One of these took place on 27 June 1994 in a mountain resort northwest of Tokyo when seven people died and 264 were injured by a substance that drifted into a residential area. After the subway incident, investigators determined that the unidentified substance was sarin. On 5 March 1995, railway passengers were overcome by a colourless gas released on the train between Yokohama and Tokyo. A few days later, three attache cases containing a vaporiser device and glasses of a poisonous gas were discovered in a Tokyo subway station. Evidently, the contraption was designed to force the gas into the subway ventilation system. While authorities have yet to determine who engineered these attacks, they concluded that they were probably efforts by the Aum to perfect their technology and tactics.[26]

There may well be other examples of chemically oriented terrorist attacks which were simply not recognised as such. We do know, however, that the threat of chemical attacks has been employed on numerous occasions. During the final days of the Nixon Administration, the so-called 'Alphabet Bomber' announced his intention to come to Washington armed with nerve gas he intended to use to kill the President. Taking the threat very seriously, authorities launched a massive manhunt and arrested the would-be assassin as he prepared to pick up the final ingredient for the nerve gas. In 1992, a German neo-Nazi group undertook a plan to pump hydrogen cyanide gas into a synagogue but was prevented from implementing the attack because of intervention by the police. While the 'Alphabet Bomber' and the German terrorists were evidently serious and may well have had the required technical skills, numerous other terrorist threats have been exposed as hoaxes. In an effort to force the Russian 14th Army out of Moldova in 1994, a Moldovan general who was the Deputy Minister of the Interior declared his intention to contaminate the Russians' water supply with mercury. After his removal from office, a search revealed that he apparently possessed none of the 32kg of mercury that he claimed.

Great Britain's Animal Liberation Front (ALF) has on several occasions threatened the chemical contamination of products whose manufacturers were accused of funding research using animals. Although countless items have been withdrawn from stores, no contaminated products have been found. Canadian animal rights groups have used the same tactic and likewise failed to follow through on any of the threats.

It is tempting to dismiss the threats as being of no consequence because products were never actually subjected to the chemical poisons. Yet, we must keep in mind that the removal of goods from circulation and their subsequent inspections were a costly process. In every case, the companies lost a great deal of money. Evidently that was the actual objective of the terrorists, meaning that the chemical threat was effective. It is important to remember what the overall aim of terrorism is: the creation of an environment in which people lose confidence in political, economic, and social objectives. Chemical terrorism can be a very effective instrument even when no person suffers from physical contact with a chemical agent. This is especially true where economic interests are at stake.

GENERAL CONCLUSION: INDICATIONS AND WARNINGS SYSTEMS

A simple categorisation of the various types of terrorist threats and analyses of the sources of those threats, by themselves serve little purpose beyond advancing our knowledge and understanding. What is necessary is to apply our research in order to deal with new terrorist threats. Accordingly, as noted above, a system of 'indications and warnings' must be developed if we are to make use of our accumulated knowledge.

Developing such an indications and warning system entails providing an infrastructure to forecast potential terrorist incidents and prevent them from happening. The larger question remains of what can we do at a practical level to help policy makers and forces responsible for responding and interdicting to the activity of a terrorist group. Although there have been many responses to understanding and forecasting terrorism in the past, the behavioural or organisational approaches still remain the most effective. Here, the terrorist entity is treated as a group, and the group is studied as an organisational phenomenon with both short and long term goals, an ideology or worldview which drives its activity, specific patterns of training, recruitment, logistics preparation and operational preparation, to include target analysis.[27]

Although this methodology is very successful when assessing organised groups, it is less adequate in the face of the more loosely organised which leave fewer 'footprints' of their activity. For example, it is more difficult to monitor a previously unknown group that appears seemingly from nowhere and leaves the operational planner and analyst little time to observe its activity. Given the prospect of the new threats of biological, chemical, and computer terrorism and the potential for less organised and formalised groups of individuals to acquire these destructive capabilities, it becomes increasingly difficult to study and forecast future terrorist related activities. For example, is it possible to monitor the activities of a cyber-terrorist who performs a file transfer protocol (ftp) to an anonymous server as an anonymous user in order to load a virus which will destroy the sensitive databases maintained by a national security agency? Although it is increasingly difficult to see signatures of such group or individual activity, it is not impossible to develop methods and tools for monitoring such activities and such measures should not be ignored. As the Defense Science Board Study notes, the 'too hard problems of chemical, biological, nuclear and even information terrorism can no longer be ignored because they are "too hard" ';[28] It is especially important to curb these activities now because the technologies which serve the forces of chaos and disorder can be made equally subservient to the agencies charged with maintaining order.

Identifying the indicators

The first step in developing an indications and warning plan for technology-enabled threats like chemical, biological and nuclear is to identify indicators of activity for such threats. What signatures or footprints can the trained analyst or operator monitor for a group or individual, whether organised or not, planning to use chemical or biological agents? What footprints does the seasoned cyber-terrorist leave behind? Selecting the types of activity to monitor and ensuring that these activities are subject to monitoring (the traditional behaviouralist approach) is very important. Instead of focusing time and money on decomposing the threat presented by these weapons and their potential for destruction, policy makers should develop analytical frameworks which chart the observable activities that can be monitored. Those activities include such things as production capabilities, the theft or acquisition of precursor materials, and the existence of factories and processing facilities, to name just a few potential indicators. In this regard, one is reminded of how Iraq acquired a preliminary capability to build biological weapons. Iraq actually acquired the biological agent anthrax from a biological processing firm in Bethesda, Maryland. In 1988, US Customs allowed the export of a significant amount of anthrax to be exported to the Iraqi Atomic Energy Commission. If the counter-terrorist expert develops and implements frameworks for monitoring such indicators, perhaps such activity could be prevented. While it is important to develop acceptable frameworks, it is also essential to devise analytical tools which will allow CT planners to collate diverse sources of information and to understand complex relationships and data.

Co-ordination and information-sharing

Although we can better interdict chemical, biological and information terrorism through the development and implementation of comprehensive analytical frameworks and tool-kits, rectifying problems in co-ordination and information-sharing among agencies responsible for the problem continues to be essential. Co-ordination and information-sharing is even more important with this threat, as critical data is often derived from diverse sources across the globe at the local, state, national, and international level. Indeed, the 'correlation of diverse data sources would likely enhance our ability to identify key indicators and provide warning'. (Defense Science Board, 37). This task is not so easy, but fortunately, advances in information technology and data sharing techniques allow this goal to be accomplished. High level policy advisors and government officials are recommending the development of an 'active, two way global information system, which exploits international information sources and facilitates the two-way sharing of data at the local, state, and national level' (Defense Science Board, 37). Use of such an information-sharing infrastructure would have been key in interdicting or even preventing the disaster Americans faced at the World Trade Center in February 1993. In this respect, integrating agency level information bases, such as those of the Department of Energy, the Federal Bureau of Information, the Department of Defense, the Immigration and Naturalization Service and the National Guard, with real-time data at international borders, such as cargo manifests, global financial transactions, global airline ticket manifests (DSB, 37-38) would be critical in piecing together kernels of data that then paint a more complete picture of chemical, biological, or cyber-terrorist activity. The US Government has recommended that a Secure Transnational Threat Infrastructure (STTI) should be established in order to integrate data from diverse sources. Indeed, such an infrastructure needs to be fielded now if we are effectively to interdict activity from these technologically driven threats. Since the signatures of chemical, biological, and information terrorism are very small, we need to focus our time and energy on the development of comprehensive frameworks which allow us to warn of such activity and share any data which would contribute to signalling the existence of such activity.

An 'indications and warning' office

Co-ordination does not just entail developing indications frameworks for understanding the threat and information technologies for sharing data. Formal co-ordination also needs to be in place. Such co-ordination could include the development of an 'indications and warning' office at some level of the US federal system to alert both government and private users about the emergence or presence of new terrorist threats. Its activities should also be co-ordinated with those of international agencies sharing responsibilities for dealing with terrorist threats. This endeavour has a particular value in that it recognises the extent to which the public and private sectors are linked via computer networks. It is also based on a recognition of the fact that civilian and military threats are not distinct entities but rather part of a social network facing a common threat. An 'indications and warning' office could play an essential role in the development of vulnerability assessments and the dissemination of such assessments to user networks.

An additional responsibility of such an office should be to provide warnings about certain types of potential terrorist activities. Information about how to identify the signs of chemical attacks would be especially valuable in saving lives in the event of such an attack. The type of public information campaign undertaken during the Cold War era would be effective in creating an awareness that would promote public safety. It is also possible to identify many of the facilities that are likely to become targets of terrorist attacks and post information about how to respond to incidents. Education should become a managerial responsibility and the designation of institutional response teams should ensure adherence to guidelines on terrorism.

Identification of terrorist groups

Co-ordination also entails pooling intelligence collection resources and methodologies to include a consistent effort to identify terrorist groups as well as radical groups which might evolve into terrorist groups. This can be undertaken using both classified and open source materials. The proliferation of radical and extremist groups is so enormous that no single government agency can hope to maintain an adequate record of their activities and orientations. Only by pooling resources can such an undertaking prove adequate to our counter-terrorist needs.

Government agencies have, however, made only modest efforts in addressing these concerns. Ten years after Walter Laqueur's 1987 observation that far too little was being spent for CT efforts, agencies of the US Government were spending a modest $250m annually for the development of equipment and techniques for computer security.[29] If cyber-terrorists gain the prominence that seems likely, the threat generated will affect far more institutions and individuals than were ever intimidated by the bomb-wielding fanatics envisioned in the early terrorism scenarios. Electronic crime alone is already costing American businesses billions of dollars each year. In terms of monetary losses, cyber-terrorism could result in an even more devastating cost. Defence against cyber-terrorism will exact a monetary price far in excess of anti-terrorism spending of recent years because every organisation now connected to the world wide web – banks, corporations, universities, and others – will require some sort of security assistance. The cost of information security technology will be borne by management executives as well as consumers and may well become one of the most significant expenses associated with computer operations.

What can be done to counter this booming menace to a modern society that has grown both dependent upon and accustomed to the benefits of modern technologies? Interest in one important protective measure was shown by proposals to create a new directorate within the US National Security Council to co-ordinate the efforts of various agencies concerned with the cyber-terrorist threat. Such an undertaking, at a minimum, would give greater visibility to counter-terrorist measures and, perhaps, enhance the effectiveness of those efforts.

Detection systems

Research on the development of more effective intrusion detection devices is essential if valuable data and services are to remain secure. One of the greatest cyber-terrorist threats is that of the silent invader who alters computer procedures in such a way as to threaten public or institutional welfare. The threat to food production and medical operations cannot be removed without the introduction of detection systems to warn managers that sabotage may have occurred.

Designers of computer systems can contribute to anti-terrorism efforts by developing 'firewall techniques' which will limit or minimise damage in the event of a system's security being breached. Such innovations would play a crucial role in preventing the destructive consequences of an intrusion from spreading throughout the system and further undermining popular confidence in national institutions.

If our efforts to anticipate the full impact of cyber-terrorism are inadequate, official endeavours with regard to the threats of chemical and biological terrorism are not much better. As the Chemical Weapons Convention went into effect in 1997, there were fears that the many nations believed to be secretly producing such munitions would be able to elude detection. Most of the detection devices used during the Gulf War were cumbersome and regarded as ineffective. Just as this threat is, in large measure, the result of technological innovations, technology can also be utilised in combating it. With regard to chemical terrorism, an improvement in detection capabilities would have a positive impact on spreading counter terrorist efforts more effectively into this area. New, smaller, and more reliable devices, however, are being developed and, with concerted efforts, should be available for those nations concerned about chemical threats. Researchers at the Los Alamos National Laboratory in New Mexico have recently created a lightweight acoustic resonance device that is able to recognise the signature of specific chemical munitions.[30]

Restrictions on chemicals will also have some impact on the ability of groups to enter into the arena of chemical terrorism but, for the most part, restrictions simply make the weapons more expensive. This added expense, however, does have the effect of denying chemical weapons to the more poorly funded groups which are often the most reckless. Special restrictions should be placed on the precursor chemicals that are essential to the development of some of the deadlier chemical weapons. Simple monitoring of purchases would assist law enforcement personnel in their prevention and detection efforts.

At each stage in the evolution of terrorism, counter-terrorist officials have faced special challenges. In general, CT planners have been successful when they were able to match or exceed the technological skills of their terrorist adversaries. The contemporary technological revolution has had an unprecedented impact on society. It has, in effect, 'democratised' knowledge, making it equally available to the rich and to the poor or to the mighty and to the powerless. Consequently, the forces of order no longer enjoy an inherent advantage in the competition with those who would prevent the orderly functioning of society. Therefore, their success will not be a function of privilege or position but rather the reward for their greater ingenuity and resourcefulness.

NOTES

[1] M. L. R. Smith, 'Low Scale Warfare', *www.globalterrorism. com.*

[2] Bruce Hoffman, 'The Confluence of Domestic and International Terrorism'. Paper presented at the Defense Intelligence Agency Conference on Counterterrorism Analytical Methodologies, 17–18 November 1997, p. 3.

[3] *Ibid.*

[4] Bruce Hoffman, 'Responding to Terrorism Across the Technological Spectrum', in *Athena's Camp: Preparing for Conflict in the Information Age* (Rand/National Defense University, 1997), p. 31.

[5] James K. Campbell, 'Weapons of Mass Destruction in Terrorism: The Emerging Threat Posed by Non-State Proliferation', *www.emergency.comlwmd-terr.htm,* 1996, pp. 1–3.

[6] Martha Crenshaw, 'Current Research on Terrorism: The Academic Perspective', *Studies in Conflict and Terrorism,* Vol. 15, Number One, 1992, pp. 1–11.

[7] Barry Collins, 'From Virtual Darkness: New Weapons in a Timeless Manner'. Paper presented at the Defense Intelligence Agency Counterterrorism Analytic Methodology Course, 17–18 November 1997, p. 2.

[8] Michael Wilson, 'Terrorism in a New World – Evolution in Revolution, The Nemesis Group, 1994, pp. 1–2. Defense Intelligence Agency Counterterrorism Analytic Methodology Course, 17–18 November 1997, p. 2.

[9] Ken Lormond, CBN News, Washington, DC, 15 March 1996.

[10] Richard Szafranski, Colonel, USAF, 'A Theory of Information Warfare', *www.cdsarcaf* millapjlszfram-html,* pp. 1–3.

[11] US Congress Office of Technology Assessment, *Proliferation of Weapons of Mass Destruction: Assessing the Risks* (Washington, DC: Government Printing Office, 1993), pp. 3–4.

[12] John G. Roos, 'The Ultimate Nightmare: Sooner Than Most People Think, the U.S. Might Face the Specter of Nuclear, Biological, or Chemical Terrorism', *Armed Forces Journal International,* March 1997.

[13] Lt.-Col. Robert P. Kadlec, 'Twenty-First Century Germ Warfare', *The Battlefield of the Future,* 1997, pp. 2–3.

[14] Lt.-Col. Terry N. Mayer, USAF, 'The Biological Weapon: A Poor Nation's Weapon of Mass Destruction', *Ibid.*, pp. 2–5.

[15] Lee Wha Rang, 'Japan's Germ Warfare and the Korean War', *www.kimsoft.comlkorealjp-germ-htm,* 27 July 1996.

[16] NBC Evening News, 25 February 1998.

[17] 'Moscow Denies Bio Weapons Claim', Associated Press, 26 February 1998.

[18] Mayer, pp. 4–6.

[19] David Phinney, 'The New Terrorists', *ABCNEWS.com*, 1 March 1998.

[20] NBC Evening News, 25, February 1998.

[21] 'CB Terrorism', Canadian Security Intelligence Service, *www.infowar.com*, 1997, p. 11.

[22] 'Chemical Terrorism', Canadian Security Intelligence Service, *www.infowar.com*, 1997, pp. 9–10.

[23] *Ibid.*, pp. 10–13.

[24] 'CB Terrorism', Canadian Security Intelligence Service, *www.infowar.com*, 1997, pp. 3–4.

[25] 'Postscript: Chemical Terrorism in Japan', Canadian Security Intelligence Service, *www.infowar.com,*1997, pp. 1–2.

[26] *Ibid.*, pp. 3–4.

[27] Wayman C. Mullins, *A Sourcebook on Domestic and International Terrorism* (Charles C. Thomas Publishers Ltd: Springfield 1997) pp. 127–167.

[28] Office of the Under Secretary of Defense for Acquisition and Technology, *Department of Defense Responses to Transnational Threats*, October 1997, p. 40.

[29] John F. Harris, 'Panel Urges Federal Government to Step Up Fight Against Computer Terrorism', *The Washington Post,* 21 October 1997.

[30] Chemical Weapons Detection Devices Get Smaller', CNN, 1 January 1997.

FURTHER READING

Barrett, Neil, 'Hacking Down the Highway', *Traffic Technology International,* Oct./Nov. 1997.

W. Seth Carus, *The Threat of Bioterrorism* (Washington, DC: National Defense University, 1997).

Cole, Leonard, *The Eleventh Plague: The Politics of Biological and Chemical Warfare* (New York: W. H. Freeman, 1997).

Douglas, Joseph D., *America the Vulnerable: The Threat of Chemical and Biological Warfare* (Lexington Books: Lexington, Mass, 1987).

Laqueur, Walter, 'Looking to the Future', *Current,* Number 386, 1 October 1996.

Leitenber, Milton, *Biological Arms Control* (Project on Rethinking Arms Control, Center for International and Security Studies at Maryland School of Public Affairs, University of MD, College Park, 1996).

Norris, John, *NBC: Nuclear, Biological, and Chemical Warfare on the Modern Battlefield* (London: Brassey's, 1997).

Winn Schwartz, *Information Warfare: Cyber-terrorism – Protecting Your Personal Security in the Electronic Age* (New York: Thunder's Mouth Press, 1996).

Zulaika, Joseba and Douglass, William A., *Terror and Taboo: The Follies, Fables, and Faces of Terrorism* (New York: Routledge, 1996).