A NEW KIND OF WAR: BIOWARFARE AND INFO WARFARE

Proper Citation:

“One hundred kilograms of anthrax spores could wipe out an entire city in one go. It is only a matter of time before bioterrorists strike.”

1 A New Kind Of War

The full effects of the horrendous September 11, 2001 attacks on the World Trade Center Towers in New York City are still to be felt. During the two fiscal quarters prior to the incident, the United States had been experiencing economic downturn. The September 11 incident exacerbated the gloomy outlook.

Since the end of the Cold War, the Western world has been experiencing an unaccustomed respite from the fears of large-scale violence. No longer do the two superpowers – United States and the Soviet Union – appear ready to bury civilization under a barrage of nuclear missiles. Military analysts warn that we should now be on our guard against a new type of savagery that kills civilians but spares their homes and offices, strikes without warning, and against which there may be no defense. What is more, this threat requires no radically new technology. The laboratories of academia and the biotechnology industry indirectly contribute to its development. The threat is bioterrorism.

Many experts say that it is no longer a question of whether a major bioterrorist attack will occur, but when. When is now. The United States is currently besieged by bioterrorism. For now, the bioagents is anthrax, spread by the U.S. postal system.

Yet hitherto, people understand natural calamities – earthquakes, hurricanes, tornadoes; people understand man-made destructions – explosions, buildings collapsing, viruses and worms on computers; but very few understand chemical and biological weapons. Not everyone lives or works in tall buildings, not everyone travels on airplanes, not everyone has access to the Internet. But everyone receives mail - important mail, much reviled junk mail, unwelcome bills, and now mail laced with deadly agents.
In the terrifying anthrax maelstrom within weeks after September 11, 2001, the mail system has been swept to the center of the vortex. In the aftermath of the September 11 attacks, the U.S. government has sought to drop bombs on and inserting elite ground troops into Afghanistan. So far the pay off has been little. Instead, the U.S. is not only being forced to play defense, but also to play on its home court, whether by the enemy apparent, or by some other unknown parties. The frontline soldiers in the war on terrorism were supposed to be in protective vests, well armed, well trained and well protected. Instead, the battlefield has turned out to be the postal facilities, where workers are girded in nothing more than blue slacks, short sleeve shirts, and shoes.

The U.S. Postal Service handles more than 200 billion pieces of mail per year or 600 million pieces per day. Its efforts to calm the fear of its 800,000 employees, and the 7 million Americans who visit the post office daily have been far from satisfactory. For a few of the employees, it is postal mortem. For a few of the customers, it is death on arrival. For many, it is mass hysteria.

2 United States Of Anxiety

In a fundamental way, the recent events unfolding in the United States of America have transformed the country into the United States of Anxiety. The anxiety is very different from the risks that we are used to facing – the risk of getting cancer, the risk of dying in an automobile accident, the risk of our kids getting hurt playing in the neighborhood – because in all these cases, we as a nation can fundamentally change the odds.\(^1\)

Daniel Creson, a professor of psychiatry at the University of Texas Medical School and a veteran of many disaster relief efforts, describes response to fear as a two-prong phenomenon. The daylight (understanding of what is previously puzzling), rational part of the brain is full of reassurance, but the deeper, instinctual part is not so sure! Even when we are outwardly calm, we are inwardly anxious. Reasons get set aside. Reinforcers of the emotional response surround the public, and rumors run rampant. The psychological impact of chemical or biological weapon is much greater than the physical impact.

Anthrax is not contagious, but fear is. As America learned of new cases of anthrax within weeks after September 11, 2001, an epidemic of vulnerability and panic spread. It was an epidemic with apparent physical symptoms, some of which even wears striking resemblance to early anthrax. In reality, they may portend an outbreak of mass psychogenic or sociogenic illness, more often known as mass

\(^1\) Katherine Stroup, John Horn, and Adam Rogers, “Facing up to our fears”, *Newsweek*, October 22, 2001, pp. 66-69.
hysteria. Mass hysteria emerges from a largely or completely baseless belief that produces ill effect on the mind or the body.

We are warned to watch out for flu-like symptoms of anthrax just as we head into the flu season, a disease that hits 95 million Americans each year and could still kill about 20,000 annually, more than anthrax might. Combine the current crop of mixed messages, the coming flu season - early anthrax symptoms resemble flu, and continuing terrorist threats, the result may be a truly debilitating epidemic of mass hysteria.

3 High Tech, Low Tech And No Tech

A few hundred kilograms of a properly ‘weaponized’ bacterial preparation, carefully dried and milled to a precise particle size, has the potential to wipe out the inhabitants of an entire city in a single strike. A nuclear bomb in the hands of a deranged person has long been the stuff of nightmares, but the materials needed to make such a device are hard to obtain and exceedingly tricky to assemble. Biological weapons are not nearly so difficult to manufacture, though making them into a form for mass destruction may be quite involved.

Biological weapons have been with us for more than half a century, but military commanders consider them too unpredictable and slow-acting, preferring the touch-of-a-button reliability of explosives. What is more, the international condemnation that the use of biological weapons would provoke gives any rational military strategist pause. Biological weapons were also an unlikely choice for most politically inspired terrorist organizations. Traditionally, political terror groups were trying to get a seat at a negotiation table and to establish the legitimacy of their cause. That goal would not be met by resorting to bioterrorism.

Even so, terrorist experts have feared that the probability of a surprise biological attack on an unprotected city had increased. Many point to a new brand of terrorism - epitomized by Aum Shinrikyo - that lacks the restraints imposed by a political agenda. These are those who do not seem to care about establishing legitimacy, but just want to strike a blow in anger and kill as many people as possible.

3.1 Germ Warfare Agents

In the last century, terrorists used violence to try and get power or approval. Nowadays, those who feel marginalized within the world economy, from religious extremists to the merely unhinged, increasingly just want to kill people or damage industries. So far they have struck mainly with guns and bombs. But the perfect

---

weapon for those who wish only to kill or destroy is germ warfare for which we still have little defense.

Biological warfare (BW) involves the use of living organisms for military purposes. The weapons can be viral, bacterial, fungal, rickettsial, and protozoan. The agents can mutate, reproduce, multiply, and spread over a large geographical terrain by wind, water, and by insect, animal, and human transmission. Once released, biological pathogens are capable of developing viable niches and maintaining themselves in the environment indefinitely. Conventional biological agents include *Yersinia pestis* (plague), tularemia (a plague-like disease), rift valley fever, botulism (caused by a toxin from the common food-poisoning bacterium *Clostridium botulinum*), *Coxiella burnetii* (Q fever), eastern equine encephalitis, anthrax, and smallpox.

### Table 1

A biological lethal weapon inventory and their symptoms. (Table adapted from *New Scientist*, 28, February, 1998).

<table>
<thead>
<tr>
<th>Disease</th>
<th>Agent</th>
<th>Symptoms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aflatoxin</td>
<td><em>Aspergillus Flavus</em></td>
<td>Nausea, vomiting, then acute liver failure or cancer</td>
</tr>
<tr>
<td>Anthrax</td>
<td><em>Bacillus anthracis</em></td>
<td>High fever, labored breathing, rapid heartbeat</td>
</tr>
<tr>
<td>Botulism</td>
<td><em>Clostridium botulinum</em></td>
<td>Nausea, fatigue, cramps, headache, respiratory paralysis</td>
</tr>
<tr>
<td>Plague</td>
<td><em>Yersinia pestis</em></td>
<td>Lung infection, pneumonia, haemorrhage</td>
</tr>
<tr>
<td>Ricin</td>
<td><em>Ricinus communis</em></td>
<td>Convulsions, stupor, vomiting, bloody diarrhea</td>
</tr>
</tbody>
</table>

Biological weapons have never been widely used because of the danger and expense involved in processing and stockpiling large volumes of toxic materials and the difficulty in targeting the dissemination of biological agents. Advances in genetic engineering technologies over the past two and a half decades, however, have made biological warfare viable for the first time.

Breakthroughs in genetic engineering technologies provide a versatile form of weaponry that can be used for a wide variety of military purposes, ranging from terrorism and counterinsurgency operations to a large-scale warfare aimed at an entire population. Unlike nuclear technologies, genetic engineered organisms can be cheaply developed and produced. They also require far less scientific expertise, and can be effectively employed in many diverse settings. These factors rekindle military interest in biological weapons. But at the same time, it also generates grave concern that an accidental or deliberate release of harmful genetically engineered microbes can spread genetic pollution around the world, creating deadly pandemics that destroy plant, animal, and human life on a mass scale.

Recombinant DNA designer weapons can be created in various ways. The new technologies can be used to program genes into infectious microorganisms to increase their antibiotic resistance, virulence, and environmental stability. It is also possible to insert lethal genes into otherwise harmless microorganisms, resulting in
biological agents that the body recognizes as friendly and does not resist. It is even possible to insert genes into organisms that affect regulatory functions that control mood, behavior, and body temperature. It is also possible to clone selective toxins to eliminate selective racial or ethnic groups whose genotypic makeup predisposes them to certain disease patterns. Genetic engineering can also be used to destroy specific strain or species of agricultural plants or domestic animals, if the intents are to cripple the economy of an adversarial country.

Table 2. Not every bacterium or virus can be made into a weapon, and many would be hard to deploy. This table lists the agents most worry scientists as potential bioweapons. (Table adapted from *U.S. News & World Report*, November 5, 2001).

<table>
<thead>
<tr>
<th>Weapon</th>
<th>Availability</th>
<th>Means of spread</th>
<th>Counter measures</th>
<th>Symptoms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Botulism</td>
<td>Easily produced. Iraq and Former Soviet Union reportedly have this weapon.</td>
<td>Through air or food.</td>
<td>Neutralized when heated above 85 degrees. Not contagious. Can be treated with antitoxin.</td>
<td>Severe symptoms include paralysis. Can be fatal.</td>
</tr>
<tr>
<td>Plague</td>
<td>Stored in microbe banks around the world. Weaponized by the Former Soviet Union.</td>
<td>Aerosol could lead to outbreak of pneumonic plague. Also spread by personal contact.</td>
<td>Can be destroyed by heat, sun, and disinfectant. Can be treated with antibiotics.</td>
<td>Could affect thousands. Can be fatal.</td>
</tr>
<tr>
<td>Smallpox</td>
<td>Samples stored in U.S. and Former Soviet Union. Iraq, and North Korea are believed to have it.</td>
<td>Aerosol, personal contact.</td>
<td>Vaccine, given soon after exposure, can prevent deadly illness.</td>
<td>Fatality rate higher than 30% if inhaled.</td>
</tr>
<tr>
<td>Salmonella</td>
<td>Easy to obtain.</td>
<td>Through food.</td>
<td>Not contagious. Some strains can be treated with antibiotics.</td>
<td>Can be fatal.</td>
</tr>
<tr>
<td>Tularemia</td>
<td>The Former Soviet Union produced strains resistant to antibiotics and vaccines in the early 1990s.</td>
<td>By aerosol or through food. Not contagious.</td>
<td>Difficult to stabilize. Killed by heat or disinfectant. Can be cured with antibiotics.</td>
<td>Could affect thousands. Can be fatal.</td>
</tr>
</tbody>
</table>

The widespread use of the basic tools of industrial biology has put the power to create ‘traditional’ biological weapons in the hands of tens of thousands of people. Advanced biological technologies have spread all over the world. There are many
more people who are technically trained, and the methods for culturing large quantities of bacteria are well worked out and commonly employed.

The number of trained biologists has been soaring. Life science Ph.D.s awarded in the U.S. increased by 30 per cent between 1975 and 1991 to more than 5,700 a year. By 1994 England alone had 5,700 biology graduate students. American industry now employs around 60,000 life scientists. There are over 1,300 biotechnology companies in the U.S. and about 580 in Europe. Only 25 years ago there were none. Moreover, many less developed countries, including Iraq, have their own biotechnology industries.

A person who is smart, determined, trained in basic microbiological techniques, and willing to take a few short-cuts on safety and go at a few technical problems in mildly unconventional ways, could conceivably do some horrible things.

Two factors have made the threat of a bioterrorist attack greater than ever before:

- First, the unspoken taboo that previously dissuaded terrorists from using chemical or biological weapons against civilians has now been broken. On 20 March 1995, the nihilistic Japanese cult Aum Shinrikyo unleashed nerve gas on the Tokyo subway, killing 12 people and hospitalizing five thousand. Aum was also developing biological weapons.
- Second, with the explosive growth of basic biological research and biotechnology, what was once regarded as esoteric knowledge about how to culture and disperse infectious agents has spread among tens of thousands of people.

Many experts say that it is no longer a question of whether a major bioterrorist attack will occur, but when. Indeed, just days before the start of the air war on January 17, 1991, it is believed that Iraq had moved 157 bombs filled with botulinum, anthrax, and aflatoxin to airfields in western Iraq. In addition, 25 warheads missiles filled with the same biological agents were made ready for use at additional sites.

3.2 Aum Shinrikyo – Japanese Cult

John Sopko and his colleagues on the staff of the U.S. Senate Permanent Committee on Investigations found that despite the Japanese cult’s ineptitude there was plenty of reason to take notice. In a report presented in 1996 at one of a series of Senate hearings on terrorism, they wrote that the cult, which had more than 40,000 members in Japan and Russia and one billion dollars in assets (higher than the $300 million mentioned above), had recruited hundreds of scientists to assist with its

---

avowed purpose of plunging the United States and Japan into a war of Armageddon from which the cult would arise as the supreme power in Japan.\textsuperscript{5}

The cult also had a large biological weapons program, the precise extent of which remains unexplored to this day. There is an Aum laboratory - now sealed - that was devoted to biological agents, which has not yet been fully investigated. As early as 1990 they were trying to aerosolize botulinus toxin. It is believed they had anthrax as well. In 1991, Asahara led an expedition to Zaire to obtain samples of the Ebola virus. It can only be assumed that they had progressed since then, but how far they got no one knows.

The Japanese cult is now pretty much out of action. The concern is that new groups will look at Aum Shinrikyo’s activities, try to copycat and outdo them. Compared with Sarin gas, biological agents might look a lot easier to work with in terms of access to the material, the level of expertise needed, and rather importantly, the higher effectiveness as fatal weapons.

3.3 Anthrax As Bioweapon

Anthrax, a disease of cattle and sheep caused by \textit{Bacillus anthracis}, can also kill humans. \textit{B. anthracis} is a rod-shaped microbe that grows in soil, where it can be ingested by sheep, cows, horses, and goats. That is why anthrax is labeled as a veterinary disease, and why those most likely to contract it work with animals or animal products such as wool. If growing conditions deteriorate, the bacteria form microscopic spores, which can remain dormant but still lethal for decades. In the worst known anthrax outbreak, at least 66 people died when spores were released from a bioweapon plant in Sverdlovsk, Russia, in 1979.

The cutaneous or external form of the disease, which sometimes strikes people who handle infected fleeces, causes unpleasant sores. Animal studies indicate that cutaneous anthrax can be caused by as few as 10 spores. The pneumonic form is far more serious, killing more than 90 per cent of its victims if left untreated. The key to triggering the second form of the disease is to create and disperse spores containing particles of exactly the right size, between 1 and 5 microns, to ensure that they are retained in the lungs. Evidence to date indicates that inhalation anthrax almost never spreads from person to person because infection seems to require thousands of spores. But as few as 8,000 spores per person reliably causes a lethal infection. The spores cross the epithelial lining of the lungs and travel to the lymph nodes, where they germinate, multiply, and then spread to the other tissues, releasing toxins as they go. The first symptoms include vomiting, fever, a choking cough and labored breathing. Antibiotics can cure patients in the earlier stages of the disease.

Without antibiotics, death from haemorrhage, respiratory failure or toxic shock follows within a few days.

A U.S. Office of Technology Assessment (OTA) report emphasizes that, for the most part, transforming *B. anthracis* into a weapon is a low-tech procedure. It also notes that on a clear, calm night, a light plane - similar to the one that crashed into the White House in 1994 - flying over Washington, DC, carrying 100 kilograms of anthrax spores and equipped with a crop sprayer, could deliver a fatal dose to up to three million people.\(^6\)

Making an anthrax weapon capable of murder on this scale is not a trivial undertaking. But while it may be much more difficult than building a fertilizer bomb, the problems are far from insurmountable. The tricky part is not culturing the agent. Indeed, growing *B. anthracis* is hardly more difficult than growing sourdough starter. But processing the crude colony into a form suitable for dispersal is another matter. Turning bacteria into spores, the only form hardy and stable enough to be spread, requires the tricky step of shocking the bacteria with heat or chemicals without killing them.

A project of this complexity would require months of systematic effort, the practical engineering skills of a clever backyard inventor, and luck. These barriers, however, are not impossibly high. Basic microbiology skills - techniques an undergraduate studying the subject would be taught - should be sufficient to isolate *B. anthracis* from cattle pasture in areas where the disease is endemic, such as small areas of the U.S., and larger tracts of land in Russia and South Africa. Using this as the starter culture, a terrorist with a 100-liter culture vessel - about the size of a home fish tank - could in a few days brew up several kilograms of crude slurry containing billions of spores.

Spores tend to clump. Yet the ideal size of particles must be between one and five microns to enter the lungs and trigger inhalation anthrax. It is not easy to get a sprayer to dispense such a fine mist. The particles have to be dried somehow. Drying the slurry would be tricky, though not impossible. Freeze-drying - a procedure in which material is frozen and put under a vacuum to remove water, and which is used on a small scale throughout the biotechnology industry - could be one option.

The slurry then would have to be adjusted to the right size. Grinding the slurry powder into particles of the desired diameter would provide the greatest challenge, mainly because of the risk of contamination. Indeed, the most likely glitch all round is that the terrorists would become the first victims, or that they infect their neighbors and give the game away. A case in point is the best known (or worst known depending on which perspective you take) anthrax outbreak from a bioweapon plant in Sverdlovsk, Russia, in 1979. At least 66 people died from the incident.

To be used as a weapon, the particles would also have to be loaded into a canister for spraying over targets. To be sure the preparation would work, the isolate should be tested for virulence, the particle size measured and perhaps the sprayer field tested with a non-pathogenic bacterium. All the while the whole operation has to stay clandestine and avoid detection.

The current U.S. postal anthrax cases have not changed one crucial reality: turning pathogens into weapons of mass destruction is still a very difficult task. As far as intelligence agencies can tell, the group that has put the most effort into bioterror was Japan’s Aum Shinrikyo cult. They too, went through several futile attempts. In April 1990, members drove an automobile outfitted to disperse botulinum toxin around Japan’s Parliament building. In June, 1993, they tried to disrupt the Royal wedding of Japan’s crown prince by spreading botulinum toxin in a similar way. They also tried, for four successive days the same month to spread anthrax from a rooftop in Tokyo. All they had was nine failures in nine attempts. For Aum Shinrikyo who has a war chest of about $300 million, half a dozen laboratories and experienced biologists to fail so miserably can only attest to the difficulty in deploying biological weapons to cause mass casualties.

But the U.S. postal anthrax cases have shown for the first time in history, some person or group seems to have found an effective way to spread highly toxic anthrax spores efficiently enough to kill and sicken people. And a poorly equipped and poorly informed public health system is now struggling to figure out the basics – how spores do their damage, how many it takes, how they are transmitted?

3.4 Smallpox – Eradicated but Not Gone for Good

Smallpox is a highly contagious, deadly, and disfiguring illness that spreads through populations rapidly and for which there is no treatment. It is not easy to use as a weapon, but it is not impossible. Indeed, the U.S., the Former Soviet Union, and other nations have experimented with smallpox as a bioweapon, until these programs came to a halt in 1972. Officially, the U.S. and Russia still have stockpiles of smallpox virus hidden in vaults in the Center for Disease Control in Atlanta and the Institute for Viral Preparations in Moscow. Iraq, North Korea and possibly other nations and terrorist groups may have the virus as well.

The contagious nature of the virus makes it hard for any terrorist to stay safe while creating an aerosol form.

Even when vaccine is available, to vaccinate or not to vaccinate is a complicated issue. Fatal complications with smallpox vaccine is 1 in 500,000 cases. Now we are also concerned about people who are immune deficient such as people with HIV, or transplant, or older people. The vaccine might produce an illness called progressive vaccinia. Progressive vaccinia is difficult to treat and can be fatal. D.A. Anderson, a key Health and Human Services advisor on bioterrorism and the doctor who led the World Health Organization’s global fight to eradicate
smallpox, advises that it does not make sense to vaccinate everyone when the risk is low. But the balance could change as soon as the first case of smallpox appears.

3.5 Deadly Past in History - Smallpox

Historically, smallpox had proven a particularly vicious killer. It did not, as was typical of most infectious diseases, preferentially attack the most impoverished member of the society. In 45 A.D., it appeared in Asia. A hundred years afterwards in 165 A.D., the Roman Empire was devastated by an epidemic believed to have been smallpox. The pestilence raged for about 15 years, claiming victims in all social strata in such high numbers that some parts of the Roman Empire lost 25% to 35% of their people.

Over subsequent centuries equally devastating pandemics of the viral disease claimed millions of lives in China, Japan, the Roman Empire, Europe, and the Americas. According to an account, Cortez’s capture of Mexico City with just a small army of exhausted Spanish irregulars under his command was possible only because the Europeans had unknowingly spread smallpox throughout the land. When Cortez launched his final assault on the capital, few Aztec soldiers were alive and well. Smallpox, together with measles, tuberculosis, and influenza, claimed an estimated 56 millions Amerindian lives during the initial years of the Spanish conquest.

Table 5. Smallpox is a relatively recent human disease, seeming to have arisen in India less than 2,000 years ago. In ancient times, medical observers could not clearly discriminate between smallpox and other human-to-human epidemic diseases such as measles, bubonic plague, and typhus. As a result, controversy reigns over modern interpretations of ancient medical records. Nevertheless, according to historians familiar with medical records, several major epidemics that claimed a quarter to a third of the affected populations were likely to have been smallpox. (Table Adapted from A. Patrick).

<table>
<thead>
<tr>
<th>Epidemic Site</th>
<th>Year, A.D. To</th>
</tr>
</thead>
<tbody>
<tr>
<td>China</td>
<td>49</td>
</tr>
<tr>
<td>Rome</td>
<td>165</td>
</tr>
<tr>
<td>Cyprus</td>
<td>251 -266</td>
</tr>
<tr>
<td>Greece</td>
<td>312</td>
</tr>
<tr>
<td>Japan</td>
<td>552</td>
</tr>
<tr>
<td>Mecca</td>
<td>569 -71</td>
</tr>
<tr>
<td>Arabia</td>
<td>683</td>
</tr>
</tbody>
</table>

Among the first to deliberately inflict smallpox on an enemy were the British soldiers during the French and Indian Wars of the mid 1700s. They handed out blankets used by smallpox patients to North American Indians to cause epidemics. And it worked. More than 50% of the affected population succumbed.

It is conceivable that in future bioterror attacks, agents other than non-contagious anthrax, may be used.

3.6 Countermeasures to Combat Bioterrorism

Apart from acting on intelligence, another defense would be to restrict access to the tools of bioterrorism, including starter cultures. In March 1995, Larry Harris, a microbiologist and a member of the Aryan Nations white supremacist group, used a forged letterhead and his professional credentials to order samples of \textit{Yersinia pestis}, the organism that causes bubonic plague, from the American Type Culture Collection, a clearing house for microbiological samples in Rockville, Maryland. The ATCC dutifully mailed the samples, but in the nick of time the staff became suspicious that Harris did not have the expertise to handle plague and the vials were recovered unopened. Harris is being prosecuted for mail fraud—owning plague, it transpires, is not illegal in the U.S. In the U.S., people may keep lethal pathogens at home. But threats to do harm with those pathogens, transporting or storing them improperly, or obtaining them by fraud or theft, are illegal. In Britain, any company that wants to keep lethal pathogens must prove to the government’s Health and Safety Executive that it has adequate containment facilities. But the HSE has no jurisdiction over private citizens.

Not that would-be terrorists need obtain their pathogens through official channels. If they know where to look, many can be isolated from the wild.

But perhaps the most neglected area of planning is the medical response to an attack. The scenario is different with the agent used. Philip Russell, former commander of the US Army Medical Research and Development Command in Fort Detrick, Maryland, believes plague is different from smallpox, which is different from anthrax. Russell is now president of the Sabin Foundation, an organization based in New Canaan, Connecticut, which promotes vaccine use against natural diseases. He proposes the need for a group of folks to go through different scenarios and think about what should be in each scenario. For example, plans are needed to ensure that large amounts of antibiotics, and properly trained and equipped people can be rushed to the scene.

In the U.S., these responsibilities fall on the Federal Emergency Management Agency and the Office of Emergency Preparedness of the Department of Health and Human Services, both in Washington, DC. At the moment, although these agencies have adequate plans to cope with floods, earthquakes, and occasional car bombs,
OEP head Frank Young told a Senate hearing on 1 November 1995 that there was no coordinated public health infrastructure to deal with the medical consequences of terrorism. This is not to say there are no plans at all. In June 1997, President Clinton told government agencies - including the military - to improve their planning for a massive terrorist strike. But at the Senate terrorism hearing, on 27 March 1998, several key witnesses, among them P. Lamont Ewell, president of the International Association of Fire Chiefs, questioned whether the new plans were adequate and whether they had been sufficiently well rehearsed to cope with a real attack. In Britain, the Home Office takes ultimate responsibility for preventing bioterrorism and for preparing to deal with its aftermath. In the aftermath of the postal anthrax incidents, the Bush administration set up a Home Office in the U.S.

4 Anthrax Vaccines

American forces use a vaccine called MDPH, named after the Michigan Department of Public Health vaccine plant that makes it. The British vaccine is similar. Both immunize against a protein in anthrax toxin called protective antigen. The vaccines, however, may not protect against all natural strains of anthrax. In experiments on guinea pigs, for example, MDPH gave 100 per cent protection against only one of the five main natural strains of anthrax. In some studies, anthrax killed between 25 per cent and 96 per cent of guinea pigs that had been immunized with MDPH. Primates may be less susceptible.

So far, MDPH has been tested only with natural strains of anthrax. In December of 1998, Andrey Pomerantsev of the State Scientific Centre of Applied Microbiology at Obolensk near Moscow published details of an anthrax strain that he had genetically engineered to produce bacterial toxins called cereolysins. This Russian strain resists six different antibodies including MDPH.

Experts fear that Iraq may have acquired the Russian strain. The UN Special Commission set up to investigate Iraq’s biological weapons has found records of Russian sales of biological equipment and materials to Iraq as late as 1995. Pomerantsev’s strains were probably developed before 1991, when funding for the Obolensk laboratory dried up.

The search for better anthrax vaccines is hampered by the difficulty of testing them on humans. Hardly anyone in the West is now naturally exposed to anthrax, and it is unacceptable to expose people deliberately. This is why British and American troops are still using the MDPH vaccine that was developed in the 1960s, when workers in wool factories were still exposed to anthrax from sheep.

---

4.1 Ciprofloxacin

Following the anthrax incidents about a month after the September 11, 2001 horrendous attacks on the World Trade Center Towers, the U.S. State Department ordered all U.S. embassies to buy and store three days’ supply of Cipro as a precaution. Bayer, the German pharmaceutical giant, announced that it would increase its production of Cipro by 25% starting November 1 because wholesalers are running low on the drug.

Ciprofloxacin or Cipro is a high potent, high-priced antibiotic used to treat inhaled anthrax.

When ingested or inhaled in large quantities, anthrax is far more deadly as it disseminates more widely within the body. Ingesting is normally not a threat for in the U.S. Farm animals are vaccinated and meat is routinely inspected. But the lethal case in Florida indicates that inhaled anthrax may pose a growing threat. A victim who breathes in the white powder may feel fine for a week, the flu-like symptoms such as fatigue, fever and muscle aches begin to take hold. Chest pains and labored breathing follow within 24 hours, followed by shock and death in the worst scenario.

Inhaled anthrax is highly treatable if detected within the first few days of exposure, before the organism multiplies to a density detrimental to the host. Drugs are usually rather ineffective once the symptoms begin to show.

Cipro is the first drug used to treat any suspected inhaled case of anthrax, but the vast majority of infections can be managed with penicillin or tetracycline once the spores have been evaluated in the laboratory.

The standard treatment regimen involves 60 days of antibiotic therapy, or 30 days of medication and a series of three-vaccine cocktail shots. Intravenous Cipro, along with clindamycin – an antibiotic that works as an antitoxin are first administered. This combination may be effective because even if the bacteria are killed, the toxins they produce continue to circulate through the body. Finally, rifampin – a drug to treat tuberculosis that can penetrate white blood cells – is added to the treatment regimen.\(^{13}\)

Anthrax is a deadly germ with real potential as a weapon, but our fear now poses a greater threat than the bacterium itself. Despite events in Florida, New York, Nevada and District of Columbia, a civilian chance of contracting anthrax is still vanishingly small.\(^{14}\) Taking Cipro may help us feel less vulnerable, but the drug itself has a range of adverse effects. In the face of fear, Valium – a drug to suppress anxiety - may be a healthier choice.

Not that anthrax is a threat to be taken lightly. The infection is rarely fatal when contracted through a skin lesion. In this case, the patient may develop flu-like


symptoms and nasty sores. Most recover even without treatment, though antibiotics are almost always curative.

Experts are adamant in urging people not to stockpile medication. Many of the people buying Cipro simply want to keep them on hand for an emergency, but others are ready to take the medication without any exposure. Cipro is rarely prescribed to pregnant women or anyone under 18 except in known cases of anthrax exposure. When prescriptions are not available from doctors, people turn to opportunists online. A 30-day prevention package costs about $299. The package would not fully protect a person who has actually inhaled anthrax because the spores can take six weeks to germinate.

It would not cause a healthy adult much direct harm unless the “patient” is also taking asthma medications such as theophylline. But taking Cipro as a prophylactic precaution is never a good idea. Abusing any antibiotic is a sure way to breed pathogens that can resist it. By taking the drug as a hedge against anxiety, we will exhaust its power against a range of bacterial menaces.

Cipro is still a potent, broad spectrum antibiotic. Because it was introduced only 14 years ago, it can still eliminate bugs that have developed resistance to older medications. It is still our best cure against gonorrhea, infectious diarrhea, typhoid fever, and hospital acquired pneumonia. By stockpiling Cipro and using them casually, we virtually guarantee that all of those diseases will become less treatable, and the effectiveness of the drug against anthrax diminished. For now, our best defense against anthrax is to leave the drug alone. To squander it is to surrender.

Cipro can also cause a range of bizarre effects from psychological problems and seizures to ruptured Achilles tendon or shooting pains to swollen joints. In animal studies, it can disrupt the formation of cartilage. Cipro can be fatal if taken with the asthma medication theophylline. Most antibiotics can cause nausea, but the user cannot take antacids for they reduce the effectiveness of Cipro.

4.2 Antimicrobial Nanoemulsion

Bayer is not the only company swept up in America’s grim scramble to fend off germ attacks. The $11 million DARPA-funded NanoBio, based in Ann Arbor, Michigan and a spin-off of Michigan University’s Center for Biologic Nanotechnology, has created a nontoxic agent that can destroy most virus, bacterium, and fungus around, from influenza to E. coli to anthrax.\(^{15}\)

The agent, a lotion that looks like sunblock, can help prevent people from contracting anthrax but it cannot cure a victim after infection. The microbe-zapping agent is just soybean oil floating in water with nontoxic detergents. It can be rubbed on the skin, used in hot tub, eaten, or put into beverages like orange juice. What makes the stuff potent is how it is made.

The principle is deceivingly simple. When salad dressing is shaken, bubbles of oil are dispersed in the vinegar. These bubbles contain surface tension potential energy. The potential energy is released when the bubbles coalesce. NanoBio’s proprietary technology – antimicrobial nanoemulsion – forms these bubbles, as the name stipulates, at the supertiny nano level. A nanometer is about 100,000 times narrower than a human hair. The nanodroplets, stabilized by detergents they float in, are small enough to literally bombard lipids or fats found in bacteria and viruses, blowing them up in the process. NanoBio’s formula tricks dormant anthrax spore that ambient surface conditions are ideal for germination into an active bacterium. As the spore germinates, it forms a lipid layer, which the nanoemulsions promptly assault. Within a couple of hours, the anthrax is dead.

NanoBio plans to develop a preventive nasal spray in two years.

There are other promising anthrax zappers. A foam developed by New Mexico’s Sandia National Laboratories supposedly neutralizes pathogens and chemicals. It was used to decontaminate traces of anthrax found in the NBC New York offices on October 12, 2001.

5 Promises But Not Yet A Sure Cure

Traditional terrorists wanted political concessions but now, some groups have as their main aim mass casualties and mayhem. And their weapon of choice is biological weapons. Terrorists would have little trouble getting their hands on the technology. The apartheid government in South Africa produced terrorist weapons containing anthrax, Salmonella and cholera. Former Soviet scientists who have prepared weapons-grade anthrax and smallpox are known to have emigrated, possibly to well-funded terrorist groups.

With bioweapons so readily available, how can governments protect its citizenry from a terrorist armed with anthrax, smallpox or plague? Until now, most biological defense strategies have been geared to protecting soldiers on the battlefield rather than ordinary people in cities. The situations are quite different now, and novel technologies are needed for civilian defense.16

5.1 Hypothetical Bioterrorism

The first simulation has taught officials that biological terrorism poses different problems from a chemical attack, and is potentially much more devastating.

Most doctors have never seen a case of plague or anthrax. So it could be days before they realize what they are dealing with. National governments need to

---

stockpile drugs and vaccines, develop and distribute rapid tests for agents used in bioweapons, and come up with effective ways to isolate infected people.\textsuperscript{17}

Table 4. Estimates of casualties from a hypothetical biological attack. The numbers are based on a 50-kg airborne agent released over a 2-km radius in a city of 500,000 residents. (Table: Adapted from WHO).

<table>
<thead>
<tr>
<th>Agent</th>
<th>Casualties</th>
<th>Deaths</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anthrax</td>
<td>125,000</td>
<td>95,000</td>
</tr>
<tr>
<td>Tularemia</td>
<td>125,000</td>
<td>30,000</td>
</tr>
<tr>
<td>Typhus</td>
<td>85,000</td>
<td>19,000</td>
</tr>
<tr>
<td>Tick-borne encephalitis</td>
<td>35,000</td>
<td>9,500</td>
</tr>
<tr>
<td>Brucellosis</td>
<td>125,000</td>
<td>500</td>
</tr>
<tr>
<td>Rift Valley fever</td>
<td>35,000</td>
<td>400</td>
</tr>
<tr>
<td>Q fever</td>
<td>125,000</td>
<td>150</td>
</tr>
</tbody>
</table>

5.2 Protective Gear

Researchers at Irvin Aerospace in Fort Erie, Ontario, have developed a dome-shaped tent made of ultra tough Mylar that can be filled with a stiff foam - the exact composition of which is a closely guarded proprietary information - that kills germs and also neutralizes chemical weapons. Once covered by the foam-filled tent, a bomb filled with germs can be safely detonated.

But what if germs are already in the air? Geomet Technologies near Washington DC and Irvin Aerospace are about to mark civilian bio-suits. In the meantime, other companies are designing protective gear that actually kills pathogens. Molecular Geodesics in Cambridge, Massachusetts, for example, is developing a suit made of a tough, sponge-like polymer that traps bacteria and viruses, which are then destroyed by disinfectants incorporated into the fabric.

5.3 Surveillance and Monitoring

None of this gear will do any good, however, if the emergency services do not know there has been an attack. And an stealthy assault may not be obvious. A terrorist might not use a weapon that goes off with a dramatic bang, or even produces an obvious cloud of germs. The first hint of a biological attack may be a sudden cluster of sick people.

Even that will be missed unless someone is watching. And few are. In the U.S., financial cutbacks have crippled programs to track disease outbreaks, natural or deliberate. Some could be either, such as food poisoning caused by \textit{Escherichia coli} O157 or \textit{Salmonella}. In Europe, disease surveillance is only beginning to be organized on the continent-wide scale needed to track a biological emergency. But

\textsuperscript{17} Nell Boyce, “Nowhere to hide”, \textit{New Scientist}, 21 March, 1998.
in addition to monitoring infected people, Nicholas Staritsyn of the State Research Centre for Applied Microbiology near Moscow says that more effort should be made to find out which bugs live where. For example, a particular variety of anthrax may occur naturally in South Africa, but not in Canada. Having access to such information could help authorities to distinguish between natural outbreaks and deliberate attacks.

Even when infected people start turning up at local hospitals, early diagnosis of their illness might not be easy. The first symptoms of anthrax, plague and many other potential agents of bioterrorism resemble those of flu: headaches, fevers, aching muscles, and coughing. What is more, some of these symptoms might be brought on by panic attacks or hysteria, which are likely to be widespread among people who have just been told that they are the victims of a biological attack.

One solution would be for hospitals to have the type of high-tech detectors being developed to identify airborne pathogens on the battlefield. With a detector at each bedside, doctors could pick out the volatile molecules released by damaged lung membranes at a very early stage of infection and instantly tell whether a patient was a victim of a biological attack.18

DARPA, Defense Advanced Research Projects Agency of the U.S. Department of Defense, would like to develop reliable (no false positives), lightweight (<2 kilograms), sensitive (can identify as few as two particles of 20 different biological agents in a sample of air), low cost (<$5000) detectors. Such detectors could be deployed around cities to give early warning of airborne disease.

In the meantime, researchers led by Wayne Bryden at Johns Hopkins University in Baltimore are working on revamping the traditional laboratory workhorse, the mass spectrometer, for use in the field or in hospitals. His group has reduced this unwieldy piece of equipment to a suitcase-sized machine that can distinguish between, say, *Shigella*, which causes dysentery, and *Salmonella*.

Tiny electronic chips that contain living nerve cells may someday warn of the presence of bacterial toxins, many of which are nerve poisons. Like a canary in a coal mine, the neurons on the chip will chatter until something kills them.

While the canary-on-a-chip could detect a broad range of toxins, other devices are designed to identify specific pathogens. One prototype, antibody microarray, consists of a fiber-optic tube lined with antibodies coupled to light-emitting molecules. In the presence of plague or anthrax bacteria, or the toxins botulin or ricin, the molecules light up.

---

18 A Strengthened Biological and Toxin Weapons Convention (BTWC): Potential Implications for Biotechnology – An International information and discussion forum on the potential implications for biotechnology R&D and production of the legally binding protocol being negotiated to strengthen the BTWC
Table 3. Pros and cons of various protocols for detecting bioagents. Dog’s nose is solution that turns green on exposure to reagent. (Table: Adapted from Alvin Fox, University of South Carolina, Cepheid, Nomadics, Teracore).

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNA-based detectors</td>
<td>A prototype machine can identify virulent strains of anthrax in about 30 minutes.</td>
<td>Even the newest device cannot continuously monitor the air. It is another 5 or more years to develop a device of this functionality.</td>
</tr>
<tr>
<td>Mass spectrometry</td>
<td>These machines spot anthrax’s molecular profile.</td>
<td>To date no machines adapted for anthrax are available. Development is years away.</td>
</tr>
<tr>
<td>Antibody-based tests</td>
<td>Antibodies interact with spores and change color. It is cheap, fast, and is available now.</td>
<td>This device is rather insensitive. It cannot tell a virulent from a harmless strain.</td>
</tr>
<tr>
<td>Dog’s nose project</td>
<td>This device is portable. Synthetic compounds instantly glow when they detect distinctive particles in the air.</td>
<td>This device has been used to detect traces of TNT. It may take another 5 years to adapt it for anthrax.</td>
</tr>
</tbody>
</table>

Devices based on antibodies are far from foolproof. First, the correct antibodies have to be identified, not easy when one considers the vast number of pathogens that need to be included, and their ever-changing repertoire of surface proteins. Even the right antibodies can identify only what is on the outside of a particle. Bugs can be encapsulated in gels or biological polymers to foil antibodies, or normally harmless bacteria engineered to carry nasty genes.

To overcome this, researchers are developing identification techniques based on RNA analysis. Unlike DNA, which is now used to identify unknown organisms, RNA is plentiful inside cells and need not be amplified before identification begins. And messenger RNA molecules reveal not only what a microorganism is, but what toxins it is making.

Once the biological agent has been identified, what measures should be taken to combat it? Vaccinating people before they are exposed is one answer. This is the strategy the military is betting on. In 1997, the U.S. military launched a program to develop vaccines against potential biological weapons. It will create jabs for diseases for which none exist, such as Ebola, and improve existing vaccines, including the 30-year-old MDPH anthrax vaccine being given to 2.4 million American soldiers.

5.4 Quick Counter Jabs

But vaccines are no panacea. An attacker needs only generate a germ that sports different antigens to those used in a vaccine to render that vaccine ineffective. In
addition, as bioterrorists get more sophisticated, they will develop novel, possibly artificial, pathogens against which conventional vaccines will be useless. To get around these problems, the U.S. military is looking at ways of developing vaccines quickly enough for them to be created, mass-produced and distributed after an attack. The first step, which many researchers including those in the fast-paced field of genomics are now working on, involves speeding up DNA sequencing so that an unknown pathogen’s genes could be detailed within a day. The resulting sequences could then be the basis for developing an instant DNA vaccine.

Making the vaccine is only half the problem, however. Soldiers can be ordered to take shots, but immunizing the rest of the population is another matter. Civilians are unlikely to volunteer for the dozens of vaccinations that would be necessary to protect them against every conceivable biological threat during peacetime. An attack would make many change their minds, but in such circumstances there might not be enough to go around.

Kanatjian Alibekov, now reincarnated as the American resident Ken Alibek and author of *Biohazard*, was a former second-in-command of the Soviet germ warfare program. Alibek, who revealed in 1997 that the Soviets had weaponized tons of smallpox, argues that it is short-sighted to put too much effort into developing vaccines. Instead, Alibek, who is now at the Battelle Institute in Virginia, argues that researchers should concentrate on ways to treat victims of biological weapons. Today’s antibiotics may be useless because germs could be equipped with genes resistant to all of them. For example, Russian scientist Andrey Pomerantsev is believed to have already created such a strain of anthrax.

For any treatment to be effective amid the potential chaos of a bioterrorist attack, speed will be of the essence. Researchers are developing drugs that work against a wide variety of infections and so can be used even before definitive diagnosis. Some are trying to develop broad-spectrum drugs by taking advantage of recently identified similarities in the way many pathogens produce disease. For example, Ebola, anthrax and plague all kill their victims by inducing a widespread inflammatory reaction similar to toxic shock syndrome. A team in Cincinnati is testing an anti-inflammatory drug that could stop all of them. Another gang of bacteria, including plague, *Salmonella*, *Shigella* and *Pseudomonas aeruginosa* (one of the bacteria that can cause pneumonia and meningitis), relies on very similar proteins to latch onto human cells and inject toxins. Drugs that block this system might save people from all these germs.

---

6 BTWC Treaty – Firm But Unfair

One hundred and forty countries, including Iraq, have ratified the 1972 Biological and Toxin Weapons Convention (BTWC), which prohibits the manufacture and acquisition of organisms or their toxins for military use.

However, most governments agree that as it stands the convention is ineffective. Unlike the treaties that ban nuclear and chemical weapons, the BTWC provides no legal means to check if countries are complying. Treaty members are now trying to strengthen the convention to include a system of verification. Europe and many developing countries want UN inspectors to make random visits, at short notice, to any factory or laboratory in any country capable of producing lethal organisms.

But the U.S. government, under pressure from its drug and biotechnology industries, rejects this idea. The companies fear that such visits would expose trade secrets. Supporters of random inspections point out that while the U.S. is willing to go to war to back the UN’s right to inspect any sites it chooses in Iraq, it will not grant the UN the same right to inspect itself or the other members of the BTWC. This is the double standard most countries complain about.

Once Iraq had joined the BTWC after its defeat in 1991, the only legal way to find and destroy the biological weapons that its own generals had claimed it had was for the UN Security Council to set up a special commission, UNSCOM. Through its inspections over the past decade, UNSCOM has tested many of the ways in which a verification regime would work for the BTWC. These include the compulsory declaration of all research and development involving biological weapons, and of any facilities that could be used to make them. An inspection team then compares this declaration with other evidence, such as government documents, trade records, interviews with scientists and visits to laboratories and factories.20

All signatories to the BTWC accept this approach in principle. The sticking point is how extensive the inspections should be. Everyone, including the biotechnology industry, agrees to what are known as “challenge” inspections. If there is “substantial and convincing evidence” of a breach, such as an unexplained outbreak of anthrax, a majority of treaty members can demand an inspection. But challenge visits will never be frequent enough to be a sufficient deterrent. They require too much evidence and political risk for the country making the charge.

Europe and most developing countries want random, “non-challenge” inspections. Officials would be able to visit any biological facility at short notice merely to check that everything was in order although this would still not solve the problem of secret facilities. Negotiations on the BTWC have been stuck in a deadlock for four years because the U.S. and the world’s biotechnology and drugs industries will not agree to this. In late January of 1998, as the Iraqi crisis deepened, American President Bill Clinton announced he would support limited non-challenge inspections to clarify unclear declarations. But he explicitly rejected random visits.

The Pharmaceutical Research and Manufacturers of America (PhRMA), which represents American drugs companies, maintains random inspections would expose industry to the loss of its legitimate competitive trade secrets. It is also worried that an inspection for biological weapons would be disastrous for a company’s public relations.

Some wonder if the U.S. is trying to hide more bioweapons research than it cares to admit by refusing random inspections. The only way to prove it is not, in Los Alamos as in Al Hakam (home of Iraq’s anthrax bomb), is to let the inspectors in. The U.S. is ready to go to war to impose inspections on Iraq. It must set a good example and allow the UN to impose them on everyone, including U.S. industry.

Inspection techniques exist that could protect legitimate secrets without hindering verification. DNA probes that screen for specific DNA sequences, possibly coupled with polymerase chain reaction, as well as immunoassays, which use antibodies to reveal specific molecules, are the leading candidates for use in a compliance regime.

These techniques would need to be developed further before the BTWC could use them. But once they were ready, factory managers could supervise the tests at every step, protecting legitimate secrets without hindering the inspectors. For example, instead of taking live microorganisms out of the plant, a company would kill sampled organisms in front of inspectors and scramble the DNA enough to protect proprietary genes without disguising the species. The inspector could then run either PCR or immunoassay tests on the dead organisms with portable kits.

The Chemical Weapons Treaty, which came into force in 1997, already allows random inspections, with “managed access” guidelines to protect the industry. These guidelines could be adapted for biological plants.

7 Forcing Genie Back Into The Bottle?

The example of Iraq has shown how even a relatively undeveloped country can produce an impressive biological arsenal in secret. And it has shown how hard it is to force that genie back into its culture flask. Former President Clinton admitted there is no obvious way to destroy a country’s biological weapons capability with bombs. And it is terrifyingly easy to develop anthrax strains that resist both antibiotics and the West’s only anthrax vaccine, MDPH.

So the way forward must be deterrence, plus inspections that can catch cheats before they get too far.21 It was when UN inspectors in Iraq made routine monitoring visits on short notices to apparently innocent plants that they started noticing things were amiss. That is what the UN should do in every country under the verification regime now being negotiated.

As the nuclear arms race escalated in the early 1950s, the U.S. launched Atoms for Peace, a drive to promote the good things the atom might do. Whatever one thinks of nuclear power, it is hard to deny that nuclear physics and radioisotopes for medicine and research have brought benefits.

Recent alarm about biological weapons may now give us a similar opportunity. We could call it Germs for Peace. Bioweapons have yet to produce a Hiroshima, or Nagasaki. But it is real. It is happening in the U.S. postal services. It may as well be U.S. postal mortem.

Some demented people have tried bioweapons. So countries are now negotiating a long overdue verification agreement to go with the 1972 treaty banning bioweapons. If they succeed, member states will have to declare what they are doing with microbes, and allow investigators in if anyone raises serious suspicions.

But the original treaty was also about the peaceful uses of biology. It called for rich countries to help poor ones combat diseases. This was not merely altruistic. Rich countries wanted poor ones to join the treaty, but most developing countries have more pressing concerns than bioweapons. So the rich nations promised biomedical investment for those that signed.

Little of this ever materialized, but now the poor countries want action as part of the planned verification agreement. This time it may happen, in the form of a plan to help poor countries to monitor diseases.

In Germs for Peace, rich countries stand to benefit as much as poor ones, as emerging infections caused by novel pathogens are one of the 21st century’s more egalitarian menaces. The world is now a global village and physical distances have shrunk thanks to modern transportation system. To face emerging diseases, we need to keep a close watch on infections worldwide. This requires top-quality medical laboratories for diagnosis and epidemiological analysis. These are rare. Even India could not reliably diagnose a suspected pneumonic plague outbreak in 1994. It got foreign help, but fast local action would have been more effective. Africa is especially short of laboratories, yet nearly half the potentially world-threatening, novel infections investigated by the WHO are in Africa or originate from Africa. The peaceful uses part of the bioweapons treaty may yet bring rich and poor together.

The issue is politically sensitive. To assess whether outbreaks are natural or illicit, the epidemiological background has to be ascertained, and this will require international monitors. Developing countries quite rightly want any investment in disease monitoring to be just that, and not a way in for foreign military spotters or reconnaissance.

The investment, if it happens, will have to be purely civilian. Members of the treaty are discussing collaborating on regional epidemiological laboratories, quite separate from any formal effort to watch for biological attack. Ironically, if this comes to pass, the disease monitoring collaboration may become the biological

---

BioWarfare and Cyber Warfare

8 Cyber Warfare – A Keyboard Is Truly Mightier Than A Gun

The end of the Cold War has not really brought about world peace. We have seen the end of one conflict between two superpowers – the U.S. and the U.S.S.R and the beginning of a new one. The new conflict is much more spread, with potentially many more players. This new conflict is a global economic war in which espionage and new technologies will again play an important role in determining the final victors.

Beginning in World War II and continuing throughout the Cold War, the world’s major intelligence agencies - the CIA, KGB’s First Chief Directorate, MI6, etc. - employed the most state-of-the-art technologies available to assemble, communicate and analyze information from friendly and hostile countries. At the same time, counterintelligence agencies - the FBI, KGB’s Second Chief Directorate, MI5, etc. - employed other technologies in efforts to identify and eliminate foreign espionage domestically. The new global economic warfare will see these basic roles continue, but with important changes in four major areas:23

- The primary targets of spies for all intelligence services have shifted.
- The traditional roles of “friends and foes” continue to blur.
- New technologies are changing the traditional methods and techniques, the tradecraft, by which spies operate.
- The traditional tradecraft of spies, if still in use, are applied in new ways.

In other words, the fictional James Bond is obsolete. A computer mouse is truly mightier than a gun.

8.1 The Mighty Electron

In the final days of the Cold War, the crumbling Soviet Union possessed the nuclear weapons to destroy the world but lacked the economic and informational infrastructure to compete as a world power. While the preeminent weapon for most of the latter half of the twentieth century was the hydrogen bomb, it has never been used. It has been displaced and replaced by the awesome capability of a single electron – the electron that surges in a computer to perform all the functions of this mighty device! This is not tantamount to saying hydrogen bombs will never be used. It only says that the electron is now the weapon of choice. Future superpowers will be those nations with the greatest capability to harness the power

---

of the electron for both economic warfare and cyber warfare, or digital warfare, or info warfare, or invisible warfare, however we call the latter.

The desire of foreign spies to uncover and obtain military secrets will continue, but with critical variations. We are witnessing the migration of a national defensive infrastructure that has historically been based on “bullets” for physical destruction into one based upon “information” for economic sabotage. Success by spies targeting an opponent’s information will ultimately prove more valuable, or detrimental, whichever view you choose to take.

8.2 WWW - World Wide Weapon

During World War II, the U.S. Office of Strategic Services (OSS) and British Special Operations Executive (SOE) coordinated resistance activities in German occupied Europe to disrupt communications, transportation and manufacturing. Those daring individuals risked their lives to sabotage telephone poles, derail trains and delay the shipment of raw material to factories producing war materials.

In the new world of digital spies, these same activities can be accomplished from a computer keyboard thousands of miles away. By electronically sabotaging enemy computer networks, cyber spies can accomplish the same result as their OSS and SOE predecessors.

Computer viruses and other computer agents have been developed and deployed that will be activated in time of war. Imagine the consequence of embedding a Trojan horse in the operating system software that runs critical components of computer systems of both friends and foes. A Trojan horse, once activated, can selectively disable the computer infrastructure of a hostile opponent and cripple its economy, communications and defense. It is checkmate even before the chess game has begun.

8.2.1 Computer Plagues

Dark Avenger and a handful of other viruses - Michelangelo, Jerusalem, Pakistani Brain, Frodo, and other newer ones such Love Bug and Sir Camelot – have transformed the way people experience computers. These cyber plagues launch a new lucrative antivirus trade, and leave in the minds of PC users a palpable fear that any file, no matter how innocuous, might carry with it a rapacious, information-destroying agent.24

Though we have experienced many computer viruses, worms, trojans and logic bombs in recent times,25 much of the speculation about cyber terrorism has been dire, and a sober look suggests the nation probably is not at risk for a sweeping

---

cyber calamity. But cunning, targeted efforts launched by terrorists at home or abroad could have devastating effects. The cyberspace, a technological frontier where the outlaws are sophisticated computer renegades and keyboard criminals – hackers, phreakers and virus writers - is borderless.\textsuperscript{26} The U.S. National Academy of Engineering (NAE) is helping the U.S. government to pull together experts to consider countermeasures if there were a concerted attack by a state-sponsored terrorist group or by someone who had really thought deeply about how to attack the U.S. computer systems. According to William Wulf, President of NAE, the U.S. is absolutely, totally unprepared for such an as yet unprecedented cyber attack.

Viruses and break-ins have become a way of life for Internet sites. According to the Cert Coordination Center of Carnegie Mellon University, in 1999, the number of assaults was under 10,000. In 2000, the corresponding number was 22,000.

The key to cyber terror is the same feature that makes the Internet so resilient – the decentralized design. If some trouble develops in one location, the net traffic can quickly be rerouted. This is why we hardly felt any communications problem on and right after September 11, 2001, when communications lines were knocked out in lower Manhattan. That same freeform feature allows anyone from anywhere with a computer connected to a telephone line to get onto the network, without any need to identify oneself, to infiltrate the protected and secured computers at the Pentagon, NATO, or NASA at will if the perpetrator is sophisticated enough.

8.2.2 Cyber Weapons

Among the possible offensive weapons are:\textsuperscript{27,28,29}

- Computer viruses - a code fragment that copies itself into a larger program, modifying that program in the process. A virus executes only when its host program begins to run. The virus then replicates itself, infecting other programs as it reproduces. It could be fed into an enemy’s computers either remotely or by mercenary technicians.

- Worms - an independent program that reproduces by copying itself in full-blown fashion from one computer to another, usually over a network. Unlike a virus, it usually does not modify other programs. Its purpose is to self-replicate ad infinitum, thus eating up a system’s resources. An example is the infamous worm that crashed the entire Internet network in 1994.

- Trojan horses - a malevolent code fragment that hides inside a program and performs a disguised function. It is a popular mechanism for disguising a virus or a worm. A well written Trojan horse does not leave traces of its

\textsuperscript{27} Yael Shahar, “Information warfare – the perfect terrorist weapon”, \textit{ICT}, February 26, 1997.
\textsuperscript{29} Reto Haeni, “Introduction to information warfare”, August 23, 1996.
www.guest.seas.gwu.edu/~reto/infowar.
presence and because it does not cause detectable damage, it is hard to
detect.

- Logic bombs - a bomb is a type of Trojan horse, used to release a virus, a
  worm or some other system attack. It is either an independent program or a
  piece of code that has been planted by a system developer or programmer.
  It can lie dormant for years. Upon receiving a particular signal, it would
  wake up and begin to attack the host system.

- Back doors and trap doors - a trap door, or a back door, is a mechanism that
  is built into a system by its designer. The function of a trap door is to give
  the designer a way to sneak back into the system, circumventing normal
  system access privileges.

- Chipping - just as software can contain unexpected functions, it is also
  possible to implement similar functions in hardware. Chipping is a plan to
  slip booby-trapped computer chips into critical systems sold by foreign
  contractors to potentially hostile third parties or recalcitrant allies.
  According to some sources, this was originally proposed by the CIA.

- Nano machines and microbes – a nano machine provides the possibility to
  cause serious harm to a system. Unlike viruses, it attacks not the software
  but the hardware of a computer system. A nano machine is a tiny robot that
  could be spread at an information center of the enemy. It crawls through the
  halls and offices until it finds a computer, enters the computer through slots
  and shut down the electronic circuits.
  A special breed of microbes, genetically engineered to eat silicon would
  destroy all integrated circuits in a computer, thus causing the computer
  inoperation.

A few other weapons in the arsenal of information warfare are devices for
disrupting data flow or damaging entire systems, hardware and all. Among these -
High Energy Radio Frequency (HERF) guns, which focus a high power radio signal
on target equipment to put the target out of action; and Electromagnetic Pulse
(EMP) devices, which can be detonated in the vicinity of a target system. Such
devices can destroy electronics and communications equipment over a wide area.

8.2.3 The Bulgarian Virus Factory

In 1989, the first Bulgarian viruses appeared. By the end of that year, one - Dark
Avenger - had spread with enough velocity to attract media attention. Dark Avenger
secretly attached itself to MS-DOS .com and .exe files, adding 1800 bytes of code.
Every sixteenth time the infected program was run, it would randomly overwrite part
of the hard disk. The phrase “Eddie Lives... somewhere in time” would appear,
followed by garbage characters. Embedded in the code was another message: “This
program was written in the city of Sofia © 1988-89 Dark Avenger”. The computer,
now infected and self-destructing, would eventually crash, with some precious part
of its operating system missing, smothered under Dark Avenger’s relentless output.
Viruses spread, most of the time even the affected do not know about them. Programs passed along in schools, offices, and homes - from one disk to the next they carried the infection along, and by 1991, an international epidemic was evident. One-hundred and sixty documented Bulgarian viruses existed in the wild, and an estimated 10 percent of all infections in the United States came from Bulgaria, most commonly from the Dark Avenger. Dataquest polled 600 large North American companies and Federal agencies early in 1991 and reported that 9 percent had experienced computer virus outbreaks. Nine months later, the number had risen to 63 percent. Anecdotal stories of companies losing millions in sales and productivity due to virus attacks became commonplace. The press seized upon the threat and beat the war drums of fear, first in Europe, which was closer to the epicenter. Newspapers carried lurid pieces describing the havoc the Dark Avenger had wreaked.

The origins of the Bulgarian virus factory go back to the 1980s. In the early 1980s, Todor Zhivkov, then president of Bulgaria, decided his country was to become a high-tech power, with computers managing the economy while industry concentrating on hardware manufacturing to match that of the West. Zhivkov envisioned Bulgaria functioning as the hardware manufacturing nerve for Comecon, the now defunct Eastern Europe’s Council for Mutual Economic Assistance. Bulgaria would then trade its computers for cheap raw materials from the Soviet Union and basic imports from the other Eastern Bloc socialist countries.

The prevailing environment in Bulgaria was very promising. Bulgaria had many well-educated young electronics engineers. However, its archaic infrastructure and ill-managed economy were a recipe for failure. Neither were there particularly useful applications for the hardware.

In the second half of the 1980s, clones of IBM and Apple appeared. While factories continued to manufacture PCs, the country did not have any software to make the machines function. In pirating Western programs and operating system, the Bulgarians had to crack copy-protection schemes that stood in the way, and in so doing, they became better and better at hacking.

On record, the first Bulgarian virus arrived in the West in 1989. It started as harmless as Yankee Doodle to the more destructive Eddie to the deadly Nomenklatura, which attacked the House of Commons library, rendering valuable information irrecoverable.

By 1993, Bulgaria was no longer a significant source of new viruses. But the damage was done. At its peak, 1990-1991, both the alarm and the reality of the Bulgarian blight had spread exponentially, from computer to computer, and mind to mind. Today, Bulgaria exists as a kind of cybernetic bogeyman, the birthplace of viruses.
8.2.4 The Computer Plague Threat

As the world population of computer plagues grows exponentially, so does the potential for a real disaster. Computer plagues will affect computer users first, but then, many other innocent people who have never even touched a computer will be affected. For example, a virus let loose in a hospital computer could harm vital patient records and might result in patient receiving the wrong treatment regimen; workers could suffer job losses in virus-ravaged businesses; dangerous radiations could be released from nuclear power plants if the computers were compromised.

On record, there has not been a loss of life or jobs due to a virus. The only loss to date has been financial. But hospitals have already found viruses lurking in their computer systems, the military has been affected, and a Russian nuclear power plant’s central computer has been shut down by a virus.

It is only a matter of time before there is a real catastrophe. Consider

- During the Gulf War of 1991, mercenary Dutch hackers stole information on U.S. troop movements from the U.S. Department of Defense computers and tried to sell it for $1 million to the Iraqis, who thought it was a hoax and spurned the offer.

- During the 1991 Gulf War, Allied forces had to contend with at least two separate virus attacks affecting over 7,000 computers. One of the incidents was caused by the Jerusalem bug, and the other by a “fun” virus, Stoned, from New Zealand, which displayed a message “YOUR PC IS NOW STONED” on the screen. The two assaults caused computer shut downs and loss of data.


- In 1997 and 1998, an Israeli youth calling himself The Analyzer allegedly hacked into Pentagon computers with the help of California teenagers. Ehud Tenebaum, 20, was charged in Jerusalem in February 1999 with conspiracy and harming computer systems.

- In February 1999, unidentified hackers seized control of a British military communication satellite and demanded ransom in return for control of the satellite. The report was vehemently denied by the British military, which said all satellites were “where they should be and doing what they should be doing”.

In a normal day, the U.S. Department of Defense experiences 40 to 60 unauthorized intrusions, or once every 20 minutes or so. Of these, about 60 every week are considered serious attacks. With 2 million computers, 100,000 local area

---

networks, and more than 100 long distance networks, securing information is a formidable task for the agency.

8.2.5 Democratization of Hacking

There are about 30,000 hacker-oriented sites on the Internet. This brings hacking and terrorism within the reach of even the technically challenged, creating a form of democratization of hacking. The tools and programs can be downloaded, and with a click on the keyboard, the virus or bomb can be sent to a network to wreak havoc. According to an estimate, the Internet connects over 110,000,000 computers in 2001. This number is growing at a rapid pace. Consequences of any nefarious attempts to wreak havoc can be considerable.

Another threat is posed not by countries, terrorists, keyboard criminals, nor any odd balls with weird agendas, but by gophers, squirrels and farmers. In 1995, a New Jersey farmer yanked up a cable with his backhoe, knocking out 60 percent of the regional and long distance phone service in New York City and air traffic control functions in Boston, New York and Washington. In 1996, a rodent chewed through a cable in Palo Alto, California, and knocked Silicon Valley off the Internet for hours.

8.2.6 The Nimda Worm – A Case Study

The recent attacks by the Nimda or W32/Nimda worm demonstrate the Internet and Web vulnerability. The first public report of Nimda infections occurred on Tuesday, September 18, 2001, between 8:30 and 9:00 a.m. The worm modified Web documents - files ending with .htm, .html, and .asp - and certain executable files found on the systems it infects. It then created numerous copies of itself under various file names, scanned the network for vulnerable computers and propagates through email, thereby causing some sites to experience denial of service or degraded performance. Computers that had been compromised were at high risk for being used for attacks on other Internet sites. One of Nimda’s features was to attack computers that had been compromised by the Code Red worm and left in a vulnerable state. It also targeted home users’ computers, which were among the most vulnerable. Because of the network traffic generated, Internet Service Providers (ISPs) for home users suffered a negative impact from the worm.

The September 2001 Nimda had several means to infect computers. For example, the worm not only propagated through email attachments and through compromises of vulnerable Internet Information Servers (IIS), but it also spread through shared files on a file server and through Web pages containing JavaScript that had been altered on a compromised server.

The algorithm used to spread the worm concentrated for the most part on local networks. The primary adverse effect of the worm occurred at the “edges” of the Internet. Operators of the backbone of the Internet, though not significantly affected, did experience an increase in customer service calls. Victims could not reach the Internet because of the local scanning and email traffic caused by the worm. They thought that the Internet was down. In other words, they were denied service by the worm!

Nimda is the first significant worm that attacks both computers that act as servers and those that are desktop computers. A server provides services such as a Web site. Code Red exploited the Internet Information Server (IIS), which is a Web server. The Melissa virus spread by means of users’ email on desktop computers. Nimda merges the damaging features of both Code Red and Melissa, and more.

The Nimda worm spread so fast that system administrators, users, and vendors did not have time to prepare. Quick response was a challenge because there was no lead time for advance analysis. In contrast, with Code Red, analysts had a small amount of lead time to examine an early version of the worm before a more aggressive version began causing serious damage. These new no-lead-time attack technologies are causing damage more quickly than those created in the past. The Code Red worm of 2000 spread around the world faster than the Morris worm moved through U.S. computers in 1988, and faster than the Melissa virus in 1999. With the Code Red worm, there were days between first identification and widespread damage. The Nimda worm caused serious damage within an hour of the first report of infection.

Analysis of Nimda was hampered by the lack of the source code for Nimda. The source code is the original form of the program, basic code that reveals how the worm works. Thus, it was not possible to determine quickly what the worm did and what it could potentially do. Analysts quickly obtained the binary code, but it was time consuming to decompile this code and analyze the inner workings of the worm. Analysis through decompiling can take hours, days, or even weeks, depending on the complexity of the program.

8.3 The New Villain

Assassination was once considered as a tool of warfare and tactically applied or attempted by some intelligence services during World War II. During the Cold War, the Soviet Bloc utilized assassination to silence exiles taking refuge abroad. The KGB assassinations of Ukrainian exiles Rebet and Bandera in West Germany, as well as the infamous Bulgarian “umbrella assassination” of Georgy Markov in London, are all cases in point.
8.3.1 CV Please

In the digital world, potential targets of assassination have shifted. Even with the emphasis of advanced computer developments, all nations depend on imbedded computer chips of varying age, some decades old. For example, NASA is still using the VMS operating system, and most state agencies are still using COBOL. Neither VMS nor COBOL are any longer parts of normal computer curriculum. These critically important components control the switching systems in power grids, telephone systems and transportation networks, and commands of space flights. The devastating effect of losing an antiquated but functioning system becomes a reality when the key and indispensable person charged with its upkeep is eliminated. The result of assassinating a political leader pales when compared with the effect in future wars of eliminating key computer programmers and network specialists.

For professional intelligence services, their primary goal is, and will remain, the acquisition of information, not murder. Oleg Tsarev, a retired officer of the KGB’s First Chief Directorate and author, accurately stated that “intelligence stops when you pick up a gun”.

Instead of eliminating key specialists, it can be equally advantageous to lure away the specialists of a nation. Former Soviet scientists are known to have emigrated, possibly to well-funded terrorist groups. In the dilapidated economy after the collapse of the U.S.S.R., government funding fell sharply, and impoverished researchers fled overseas in a massive brain drain. The U.S., being in an economically advantageous position, has been the most fortunate beneficiary, not only from the U.S.S.R., but also from many other countries such as Germany after World War II, Hungary in the 1960s, China after the Tien Anmen incident of 1989.

8.3.2 911, Help Please

A Swedish teenager disabled South Florida’s 911 system in 1997. It is conceivable that the nation’s 911 system could be under attack again. For example, by flooding the service with calls.

Imagine, if 911 is in trouble, who are they going to call for help? 911?

The telephone system is far more complicated than it used to be. It has a lot of nodes that are programmable and databases that can be hacked. Also, the deregulation of the telephone and power industries has created another Achilles heel. To stay competitive and cut costs, companies have reduced spare capacity, leaving them more vulnerable to outages and disruptions in service. Still another flaw is the domination of the telecommunications system by phone companies and Internet service providers (ISPs) that compete fiercely and do not trust each other. As a result, the systems do not mesh seamlessly and are vulnerable to failures and disruptions. There is almost no way to organize systems built on mutual suspicion. Subtly changing the underpinnings of the system and not changing the way these systems are built will keep creating cracks for hacking.
8.3.3 Power Grid

The U.S. has so many different and complex systems of power grids. This would in principle impede a coordinated raid. It is unlikely that an attack on the power grid would trigger an across-the-board collapse. But a concerted assault could be very disruptive. To maintain the vital balance of supply and demand, generators, distributors and traders are constantly in contact, mostly over the Internet.

Though remote, an intruder could use the Internet to leapfrog into the computers that control switches, relays, and breakers. This could lead to slow or freeze operations, destabilizing the grid and causing outages.

There is another concern. With deregulation, there is an increasing interest in energy futures trades at the commodities exchange on Wall Street. Hackers might use social engineering techniques to obtain passwords to computers with access to the networks containing sensitive information from these sources. Social engineering is a technique used to obtain key information, such as passwords, just by talking to employees.

8.3.4 Psychological Warfare

The scenarios described above, other similar tactics and combinations thereof belong to a subset of information war, commonly called “hacker warfare”. However, the term “infowar” includes other ways of manipulating information, among them “psychological warfare”. A psychological warfare is an attempt to warp the opponent’s view of reality, to project a false view of things, or to influence its will to engage in hostile activities. Psychological warfare includes a variety of actions that can be divided up into categories according to their targets. Strategic analyst Martin Libicki proposes four categories:

- operations against troops,
- operations against opposing commanders,
- operations against the national will, and
- operations designed to impose a particular culture upon another nation.

This is usually called “netwar”. Netwar refers to information-related conflict at a grand level between nations or societies. Its intention is to disrupt or damage what a target population knows or thinks it knows about itself and the world around it. A netwar may focus on public or elite opinion, or both. It may involve diplomacy, propaganda and psychological campaigns, political and cultural subversion, deception of or interference with local media, infiltration of computer networks and databases, and efforts to promote dissident or opposition movements across computer networks.

Using the media as a weapon of information warfare is nothing new. The attempt to influence the human element in a conflict is an old tactic. Armies have

34 John Arquilla and David Ronfeldt, “Cyberwar is Coming!”, article for RAND, 1997.
always tried to make their forces seem stronger or weaker than they are, or to convince enemy soldiers that they have no escape but to surrender peacefully. The only difference is the means have changed. Recently, to this component in the military arsenal has been added a relatively new technique of mass information transfer. Now psychological warfare includes the endeavor to manipulate the populace of an enemy country to oppose the war effort, or to depose the reigning government. The means to this end reside in the mass media, and more recently in the Internet. Examples abound.

For example, in the 2001 U.S.-Afghanistan confrontation in the wake of the September 11 incident, the U.S. used the media to sway public opinion and dropped leaflets in Afghanistan to persuade the local population that it was a friendly force to try to depose off an unpopular regime. Under the guise of humanitarian aids, the U.S. delivered food with messages in packages, clearly labeled “The United States of America”. There were even attempts to drop radios so that the local people could tune in. Concurrently, the U.S. counterintelligence services also scan the Internet to rid off any undesirable messages.

Similarly, Osama bin Laden’s videotaped address, aired shortly after the U.S. strikes, aims to incite Muslims in a holy war. As a countermeasure, the U.S. authorities urged and banned the media, very successfully, not to broadcast the videotaped messages.

Psychological warfare through the media has also been used with success by the U.S. in the Gulf War of 1990-91. The Iraqis were led by media reports to believe that the air war was to be a short-term strike, followed by an immediate ground war, in which they felt themselves to have the advantage of numbers and territorial dominance. They were also kept busy along the Kuwaiti coasts, by means of disinformation pointing to an imminent American coastal offensive.

Another example of psychological warfare was the American propaganda war in Haiti. The Pentagon launched a sophisticated psychological operation campaign against Haiti’s military regime to restore depose President Jean-Bertrand Aristide. Using market-research surveys, the Army’s 4th Psychological Operations Group divided Haiti’s population into 20 target groups and bombarded them with hundreds of thousands of pro-Aristide leaflets appealing to their particular affinities. Before U.S. intervention, the CIA made anonymous phone calls to Haitian soldiers, urging them to surrender, and sent ominous email messages to some members of Haiti’s oligarchy who had personal computers.

With CNN and BBC beamed into almost all countries in the world, the U.S. has a great advantage over any other nations in the netwar. But America has not always been on the winning side in psychological warfare. Democracies, by their very nature, are acutely sensitive to public opinion, making them vulnerable to manipulation through the media. American troops left Somalia after the loss of just nineteen American Rangers in a conflict with the forces of Somali leader Mohammed Aideed. That conflict reportedly cost Aideed about fifteen times that
number, roughly a third of his forces. And yet it was the Americans who conceded defeat. Why? Photographs of jeering Somalis dragging corpses of U.S. soldiers through the streets of Mogadishu transmitted by CNN to the United States led to souring of TV audiences at home on staying in Somalia. U.S. forces left, and Aided, in essence, won the information war.\(^{35}\)

It is thus not surprising that the U.S. authorities carefully monitored news media coverage of the recent U.S. air strikes on Afghanistan. There were a number of misfires and casualties. Most of the general populace were not aware of these mishaps because of a lack of news coverage.

There are many other examples. These examples suffice to show mass psychology can be manipulated to one’s end in a war.

8.4 *He who Lives in Glass Houses Should Throw No Stones*

While all this seems to point to an increasing advantage of technologically advanced nations over those less advanced, there is a certain catch to this war game. American strategists are very leery of the prospects of using the more malicious forms of information warfare, for the same reason that American policy forbids the assassination of foreign leaders. We can assassinate a foreign leader, they can easily do what we do upon them. Similarly, the more technologically advanced a nation is, the more vulnerable it is itself to the techniques of information warfare. No nation is more dependent upon the information infrastructure as the U.S. So it is not surprising that American policy makers are quick to point out that infowar scenarios are being studied at present mostly with an eye toward defense rather than offense. The U.S. is living in a glass house of information. It should avoid throwing any stone.

Compounding to the wariness of the American strategists is the fact that it is the civilian sectors that are most vulnerable, with consequences in both the military and the political sphere. Military infrastructure relies for the most part on civilian infrastructure. Nearly every aspect of the military industry, from basic research and development to paying personnel depends on civilian information networks. Indeed, over 95 percent of military communications use the civilian network. Military bases depend on the national electric power grid. Soldiers travel by means of the national bus cooperative. There is no way that the military can protect all of these networks from a focused infowar attack.

Government sites are not better protected. They are riddled with weaknesses, ranging from failure to rotate computer passwords to unauthorized software installation by IT managers. The Department of Defense (DoD) is more secure. Still it has weaknesses. For example, its computers most likely run a standard operating system such as Microsoft operating system. The network has an electronic

\(^{35}\) Martin Libicki, “What is Information Warfare?”, article for the Institute for National Strategic Studies, 1997.
mail link to the outside. While an emailed virus is not likely to bring hijack to the DoD systems, it could bring down the network or corrupt the data.

8.5 Friend or Foe?

The traditional Cold War alignment of the East versus West is gone forever. At the height of Cold War solidarity, the slogan was “the enemy of my enemy is my friend”. Superpowers collected intelligence and attacked the ciphers or codes of friends as well as enemies.

The national interests of former friends and foes are now being redefined in terms of competing economic interests. Cultural and historic friendships between nations will continue to fade as they are replaced by trading partnerships and other interdependent economic relationships. For example, Premier Zhu Rongji of China, together with his counterparts in the Association of Southeast Asia Nations, agreed during the week prior to China and Taipei joining the WTO on November 12, 2001 to establish, within a decade, a 10+1 free trade zone. With 1.7 billion people, this will be the largest free trade zone in the world. It also has sparked the discussion of building a bullet train from Singapore to Kunmin, China.

The new slogan is “the friend of my enemy may also be my friend”, if the price is right. For example, in 1991 Gulf War, George H. Bush forfeited the $7 billion loan to Egypt so that the U.S. could use Egypt as an air base to strike Iraq. A decade later, the son, George W. Bush when he first moved into the White House in early 2001, accused the Russians of exercising atrocities against the Chechens. After the September 11 incident and in an effort to court the Russians into supporting the U.S. attack on Afghanistan, the same president, in the same year, and speaking from the same White House, applauded the Russian’s attack on Chechnya for the latter supposedly harbored Al Qaeda operations.

The U.S. benefited greatly from Jordan in its efforts against Al Qaeda operations. Close intelligence cooperation between the United States and Jordan dates back to 1990 when the late King Hussein warned U.S. leaders about the emergence of a network in Afghanistan headed by bin Laden. This close ties have continued under the reign of King Hussein’s son, King Abdullah, who ascended to the throne after King Hussein died in 1999. “The unsung heroes in intelligence terms are the Jordanians,” said terrorism expert professor Magnus Ransdorp of St. Andrews University. “The Jordanian track record, given the size of the country, is mammoth, in terms of the contribution to our understanding of the al Qaeda network.”

The U.S. carefully coordinated its attacks on Afghanistan in 2001. Goaded by sentiment to punish the perpetrators who had attacked the World Trade Center Towers, the U.S. exercised diplomacy to court supports to form a coalition,

---

performed intelligence gathering such as working with King Abdullah of Jordan\textsuperscript{37} and consulting President Eduard Shevardnاردزه of Republic of Georgia who was involved in the Soviet-Afghan conflict of the 1980s, and worked with news media on psychology to avoid possible anti-war sentiment domestically. The Soviet-Afghan conflict of two decades earlier, on the other hand, was a stark different brawny arms-and-tank all-out attack. The December 1979 New Year eve Soviet invasion of Afghanistan was the most violent of power move by the Kremlin to ward off the developing urge of change and to alienate the generation of the 1980s.\textsuperscript{38} As we know now, the conflict leads to an unpopular long drawn-out war that eventually resulted in the Soviet withdrawal in 1991.

9 What Is In Store?

Former CIA Director James Woolsey stated that with the end of the Cold War, the great Soviet dragon was slain. He wryly noted, however, that in its place the intelligence services of the United States are facing a “bewildering variety of poisonous snakes that have been let loose in a dark jungle; it may have been easier to watch the dragon”.

The single greatest threat to world peace in the early part of this new century is the utilization of weapons of mass destruction - nuclear, chemical, biological and digital - by fundamentalist terrorist organizations. These groups are already using the Internet to:

- Recruit and communicate members with similar fundamentalist beliefs.
- Coordinate terrorist activities with other aligned groups that share interests in a common outcome.
- Raise money through computer based keyboard crimes.
- Attack the national information infrastructures of hostile countries from thousands of miles away.

The CIA and other intelligence services must operate with shrinking budgets and manpower - the CIA will shrink 25 percent from its peak - but confront an array of new threats to national interests in different parts of the globe. To meet these challenges, all intelligence services will be forced to rely on digital solutions, massive computers and artificial intelligence in linked computer networks and databases to compensate for the reduction of people and resources.

The traditional world of spies such as James Bond exists now only in fiction. New intelligence services that most effectively identify, develop and implement the tools and techniques of the “cyber spy” will provide their citizens with an incalculable advantage in the new century.


Terrorism is an excellent example of how the focus of war has shifted toward civilian populations. For example, the September 11, 2001 horrendous attacks on the World Trade Center Towers. The aim of terrorism is not to destroy the enemy’s armed might, but to undermine its will to fight. Terrorists seek to disrupt the daily life of their target nation by striking at the most vulnerable points in the society. Such vulnerable areas included transportation networks and public events, which insure good media coverage. By hitting the citizen just where the nation thinks is safest, the terrorists cause the greatest confusion and loss of morale.

Today, almost every aspect of our lives is dependent on information networks, terrorists have a whole new field of action. And while the technology to operate and protect these networks is quite costly, the means required to attack them are relatively cheap. In the simplest case, one needs only a computer, a modem, and a willing hacker. According to Alvin Toffler, “It’s the great equalizer. You don’t have to be big and rich to apply the kind of judo you need in information warfare, That’s why poor countries are going to go for this faster than technologically advanced countries.”

According to Time Magazine, the Defense Science Board at the Pentagon warned that annoying hackers trying to crack the Pentagon’s computers were not the only things the defense strategists have to worry about. This threat arises from terrorist groups or nation-states, and is far more subtle and difficult to counter than the more unstructured but growing problem caused by hackers. A large, structured attack with strategic intent against the U.S. could be prepared and exercised under the guise of unstructured ‘hacker’ activities. There is no nationally coordinated capability to counter or even detect a structured threat.

10 Ongoing And Future Business Practice

We have gone into length to talk about cyber warfare in military scenarios. Very similar scenarios can be played on business grounds and between competing companies.

10.1 Business Warfare

Since World War II, business has been customer-oriented, and King Customer has reigned supreme. In the plan of today and the future, a company has to be or will have to be competitor-oriented. The plan will carefully dissect each participant in the marketplace. There might even be a day when the plan will contain a dossier on each of the competitors’ key people, their favorite tactics and style of operation.

---

39 Alvin Toffler and Heidi Toffler, War and Anti War, making sense of today's global chaos, (Warner books 1993).
More and more, successful business campaigns will have to be planned like military campaigns. Companies will have to learn how to attack, to flank competition, to defend positions, and how and when to wage guerrilla warfare.

For these, we may learn from two great works on war: \[41\]
- Sun-tzu ping-fa or Sun Tzu the Art of War is one of those rare texts that transcends time. Though it was written 6th century B.C., it is arguably still one of the most important works on the subject of strategy today. Written by Sun Wu, Chinese general of the state of Wu, The Art of War was intended only for the military elite of his time period. However, this treatise would later be absorbed by others of influence, from the fearless samurai in feudal Japan to the shrewd business leaders of the 21st century.
- General Karl von Clausewitz (1780-1831) was one of the greatest writers on war. His magnum opus, On War, is carefully studied in military schools to this day, for its principles are as valid for nuclear as for conventional and guerrilla warfare. Weapons may have changed, but warfare itself is based on two immutable characteristics: strategy and tactics.

These great works have been applied to business: in trading, \[42\] in strategic planning, \[43\] in marketing, \[44\], and others.

10.2 Business Cyber War

The business sector has become increasingly dependent on information for decision making and the Internet for dissemination. Internet users - business, consumers and home users inclusive - now use the Internet for many critical applications as well as online business transactions. A relatively short interruptions in service can cause significant economic loss and can jeopardize critical services.

It is not inconceivable that viruses, worms, Trojan horses, logic bombs, and back doors can be incorporated in software for use by clients so that a vendor can have a handle over the users. Hardware can also be designed with chipping feature for the same purposes. Indeed, in this new world of cut-throat business competition, it is not always economically feasible to develop all critical technologies and supporting software in-house. It is prudent to find a compromise between farming out projects and developing in-house. For example, in the biotechnology sector, it is very common for companies to license software from bioinformatics companies. In an effort for the licensee to avoid possible financial losses resulting from viruses, worms, Trojan horses, logic bombs and back doors, in the licensing agreement

---

between licensor (bioinformatics company) and licensee (biotechnology company), a clause may be included. A sample is provided below:

Viruses; Disabling Codes. Licensor represents and warrants that any Software and computer media furnished to Company pursuant to the License Agreement shall be free from computer viruses and any undocumented or unauthorized methods for terminating or disrupting the operation of, or gaining access to, software, computer systems or other computing resources or data, or other code or features which result in or cause damage, loss or disruption to all or any part of computer systems or other computing resources. Licensor shall not incorporate into Software any termination logic or any means to electronically repossess any Software licensed under the licensing agreement. “Termination logic” shall mean computer code that uses the internal clock of the computer to test for the date and/or time (e.g., Friday the 13th), use count, execution key, or any related techniques, as a trigger to render inoperable or otherwise disable the Software or any related computer system.

“Assassination” in the business sector can also be strategically exercised by hiring away key employees from chief competitors. This has happened. On January 24, 1997, Informix Software Inc., a Menlo Park database software firm, filed a lawsuit against its largest competitor, Oracle Corp. of Redwood Shores, claiming theft of trade secrets. The suit was filed in Oregon’s Circuit Court for Multnomah County in Portland, Oregon, USA. The action stems from Oracle’s recruitment and hiring of 11 employees from the Informix product-development laboratory in Portland. The suit charges Oracle and a former Informix employee with misappropriation of trade secrets and unfair competition. It was seeking injunctive relief and punitive damages.45

Just prior to the incident, Wall Street Journal had predicted Informix to be the database company of the new century. After the incident, and with a legerdemain trick from Oracle by turning news media coverage of the incident into a promotion campaign, Oracle came out the victor in the “assassination” and psychological campaign. During the heydays of dotcoms hype, Larry Ellison, the CEO of Oracle, was briefly the richest man on Earth. The stock of Informix plummeted after the incident and it never recovers to its luster.

“Assassinations” of employees have spurred a lucrative business. Head hunter and executive search agencies spring up to fill the gap. Head hunter agencies are for more routine and project level jobs. Executive search agencies are for management level positions. Essentially, these agencies move the work force from one sector, such as the academic sector, to another, such as the private sector. Or they move the work force from one company to another. At low unemployment, such as during the dotcom heydays, jobs and positions are bountiful and these agencies enjoy their best business. At a time of economic downturn, such as during the demise.com period of 2001, these agencies have a harder time to find vacancies to relocate those out of jobs.

Despite the faltering economy and a flurry of layoff across most industries in 2001, demand for high skilled workers with expertise in biotechnology remains strong. Most companies seem reluctant to relinquish any talent simply to shave costs, and the few employees that have been let go quickly find employment in competing companies.

“Friends and foes” can also be played in the business sector. This comes in the forms of strategic alliances, partnerships, and consortia to pool resources to achieve a goal that would otherwise be impossible or much harder to achieve alone. The International Human Genome Sequencing Consortium of the public sector and Celera Genomics of the private sector are excellent examples.

“Social engineering” is also common in the business sector. Workshops and conferences are fora for social engineering. End-of-the-meeting-day gatherings at pubs are the best places to tune into company secrets or new breakthroughs. It seems, after a few beers and drinks, experts, researchers and scientists talk more freely.

“Psychological wars” are usually waged by companies to their target audiences. For example, pharmaceutical companies use television advertisements to stretch their advertising dollars to the point of misleading viewers by instilling fear such as showing golden age inconveniences and ailments, or else by derogating viewers’ ego such as promoting life-style drugs whose primary functions are to restore social faculties or attributes that tend to diminish with age.

After the September 11 blitz that turned civilian airliners into missiles, killing some 4,000 people, the United States must plan for new and different foes who will rely on surprise, deception and asymmetric weapons, or those meant to overcome the lopsided U.S. edge in conventional arms. “Asymmetric wars” may also be waged in the business sector by smaller, more savvy companies against monopolistic competitors. For example, in the 1980s, while others were losing money in the computer business, Digital Equipment Corporation was making a lot of profit by exploiting IBM’s weakness in small computers.

It is thus not inconceivable that all the information warfare scenarios described above can be nefarious attempts by one company against the other to gain competitive advantage.

11 Ending Note

We hope this chapter will not make uncomfortable reading. Our intent is to bring to the readers increased and ongoing awareness and understanding of biowarfare and cyber-security issues, vulnerabilities, and threats to all stakeholders in physical and cyber spaces. We also hope to bring awareness that the business sector is also a war field.

We just cannot deny the deniability.