



Discussion Papers

Asymmetric Risks and War with Iraq:

How serious are the economic risks from digital attack?

By DK Matai

Chairman and CEO, mi2g

March 11, 2003

Introduction	The long-tail phenomena	Command and control attacks
Economic Costs	Technology-led asymmetric warfare	Addressing the threat of digital warfare
The asymmetric threats	Blended threats and digital reconnaissance	Future digital attacks

Introduction

Any future war with Iraq will have important economic, as well as political and security-related, consequences. First-order consequences might include increased oil prices and higher defence expenditure, at a time when it appears that tax revenues will be rising much slower than government spending. There will also be second-order consequences such as the fallout from asymmetric risks. These will depend on the war's outcome and on whether it brings peace and stability to the region or has the opposite effect.

This paper addresses some of the potential unintended consequences of conflict with Iraq. It is based on a speech delivered to 25 senior executives from the insurance, reinsurance and banking industry at a closed discussion at the VISA HQ in London on 20 February.

Economic Costs

Despite recent events that include the NATO rift and the European show of disunity with the US, it seems that a war with Iraq is likely to take place in March or early April. Weather conditions will hamper a long campaign in the summer months, and could force a delay to the Autumn if it does not break out over the next few weeks. By then concerns in other parts of the world, such as Pakistan or North Korea, may impact upon plans to engage in military action.

Any prevailing uncertainty in regard to the war with Iraq is likely to depress further the capital markets and hinder growth. So, in the end, economic factors may persuade the US and others to embark on the conflict in hope of reducing the negative economic outcomes from the crisis. Most wars in US history have tended to stimulate economic growth partly because of higher defence spending. In contrast, the Gulf war in 1991 was followed by a recession. Even if the war with Iraq is won quickly, there remains some doubt as to how easy it will be to capitalise effectively on the world's second largest oil reserves. Two scenarios are worth noting (figures arising from the US Congressional Budget Office and within discussions within the House Budget Committee):

1. It may be a short and neat war as it is hoped. A short war over a month or two would cost between \$44bn and \$60 bn, with an additional £12bn to \$48bn a year for occupation. The costs of stabilization and clean-up, and the construction of bases, bridges and roads would be additional to this.

2. If the war is protracted, with street-to-street fighting, the use of chemical or biological weapons (CBW), and the firing of oil wells there would be severe economic consequences in terms of loss of confidence in the West and a longer capital markets downturn, which would tend to undermine support for and satisfaction with Government foreign policy; the immediate costs of war to the US alone would likely well exceed \$100bn. Add to that the escalated costs of clean-up, maintaining a presence to ensure an effective rebuild of the country and over ten years the total bill could rise to well over \$1.6 trillion.

Most importantly, the war with Iraq may be won on the ground but lost in terms of the battle for the hearts and minds of the 1.1 billion Muslims around the globe. So far the “War on Terror” has largely avoided being perceived as a war on Muslims. However, the war in Iraq will be different. Unlike the Gulf war where coverage of the conflict was predominantly controlled by the BBC and CNN, Al-Jazeera and other 24-hour Arab new channels, the global Internet and eMail access, will offer an alternative media platform direct to populations, and will influence mainstream journalism (see previous February 19 Discussion Paper by Jake Lynch).

The asymmetric threats

In recent weeks we have seen the UK’s Prime Minister, Tony Blair, authorise the use of the military to guard Heathrow Airport and the Home Office has reminded us of the potential threat from terrorists, including the use of unconventional weapons. Large-scale exercises preparing for such attacks are being planned. Any war with Iraq is likely to exacerbate such threats, at least in the near future.

There has been an open threat from a range of radical organisations that they will embark on a campaign of terror and economic disruption should the war with Iraq materialise. No doubt, some of this rhetoric is empty and pulls a veil over the real threat from those who may have been planted as sleepers in the past. Some radicals may take negative inspiration from what they perceive as a hopeless situation. This could result in small disaffected groups waging asymmetric warfare on the West through Chemical, Biological, Radiological, Nuclear, Digital or Suicide (CBRN-DS) means blended with conventional physical attacks.

The terrorist attacks of September 11, 2001 as well as the 2002 incidents in Mombasa, Bali, Karachi and Moscow have introduced the public to the risk of asymmetric warfare.

The long-tail phenomena

Modelling the fallout from asymmetric attacks, be they manifest in cyberspace or in the physical world from chemical, biological, radiological or nuclear (CBRN) threats is of significance to emergency response planners, operational managers as well as the insurance and reinsurance industry. Many of the CBRN threats have long-term complex clean-up requirements beyond the initial decontamination and sectioning procedures, affecting entire postal code zones rather than just one room or building.

After the Oklahoma bombing, the US authorities carried out a simulation to study the effects of a biological weapons attack involving the release of the smallpox virus. By the end of the simulation the disease had spread to 25 states and 15 other countries. It was unclear what would be the most effective global and local responses and how the antidotes would be mobilised. The authorities concluded that they were not prepared for such attacks. Since then preparations have been rolled out in the US and in Europe for mass vaccinations of the public in the event of outbreaks.

More recently, Anthrax laced envelopes, which arrived at US Government offices after the September 11 attacks caused severe disruption within Capitol Hill as certain buildings – including majority leader Senator Tom Daschle’s offices – had to be closed so that they could be decontaminated. Although very few lives were directly lost due to Anthrax exposure, the disruption caused to mail handling procedures worldwide was significant, the psychological impact was profound and the recovery time was measured not in days but months.

Technology-led asymmetric warfare

The big fault line visible in the world today lies at the junction of radicalism and technology. Terrorists have organized themselves to penetrate open societies and turn the power of modern technologies, upon which we

depend, against us. **mi2g** started collecting data on overt digital attacks on computer systems across the globe in 1995. From only a handful in the first three years, the number of attacks taking place exceeded 85,000 in 2002. Some years have seen a 10-fold increase.

The most significant finding from our intelligence database is that trends in digital attacks over the Internet act as a barometer of political tensions worldwide. It is interesting to note that in recent months the trend of attacks against online systems based in the United Kingdom has escalated – 211 overt digital attacks in August grew to 479 in September followed by a sudden explosion of activity in October, where a total of 2,253 successful attacks were recorded. And that is not all. We have seen that there has been a tendency for hackers to choose the 'low hanging fruit' such as ill-prepared small to medium size business enterprises.

This is the age of automated attack tools that are freely available on the Internet. As soon as any software vulnerability associated with a particular operating system or application becomes public knowledge, the release and use of tools exploiting that vulnerability takes place within a few hours. As a result, economic damage is incurred and confidence suffers.

The large and well-protected government or corporate networks are often much harder to penetrate, requiring greater time, skill and experience together with extensive penetration of personnel and physical security measures.

Blended threats and digital reconnaissance

The biggest threat could still be a blended one: digital attacks that cripple emergency response, transport or telecommunications with some insider help, could be employed by terrorists in conjunction with conventional or CBRN-DS attacks to magnify the effects of their intended disruption and damage.

In recent months, information about critical infrastructure has been ferreted via the Internet and scanning of critical infrastructure components has become more frequent; this has been traced back to IP addresses in Saudi Arabia, Kuwait, Pakistan and Indonesia.

Sophisticated computer programmes used by engineers to find stress points and weaknesses in buildings, bridges and dams had also been found at the tail end of 2001 and early 2002 in computers belonging to suspected Al-Qaeda members in Kabul, Afghanistan. So even if the ability of a terrorist organisation to conduct direct attacks against critical infrastructure is limited, cyber attacks can be used as a highly effective reconnaissance tool to enable more effective physical attacks.

Command and control attacks

There is growing concern about "Command and Control" digital attacks, which would impact the critical national infrastructure such as: telecommunications, electricity production and distribution, water storage and distribution, nuclear power plants and gas facilities. This would probably require extensive insider help to achieve a significant attack that lead to breakdown. Former or present employees, however, who may have specialist knowledge of critical infrastructure and the operation of the SCADA, PLC and DCS systems can execute an attack from the outside. Vitek Boden was convicted in Australia in late 2001 of hacking into a computerised waste management system and causing raw sewage to be pumped into public waterways.

Addressing the threat of digital warfare

It has been our experience that certain organisations have suffered incredible losses through digital attacks that exploited software vulnerabilities exacerbated by the lack of a proper data back-up regime. One would assume that such regimes were relatively easy to implement, but frequently such regimes, dependent upon human implementation, fail. It is often the case that where really heavy damage has occurred - be it from hacking, viruses or worms - it has been with local insider help from within the victim organisation.

It is crucial therefore to apply security precautions in the area of personnel vetting and monitoring, ensuring that an individual can be completely trusted before they are in any position to cause harm to an organization.

Instituting policies to prevent successful penetration by groups using subterfuge is necessary along with a requirement to have the correct legal contracts with personnel, customers and suppliers.

The US \$50bn that was reserved by insurance and reinsurance companies post September 11 has led to a significant increase in premiums and a raft of exclusions in most policies. Yet, risk cannot be managed effectively without invoking some insurance measures. The growth of risk exclusions by insurance companies in the area of cyber-crime and terrorism has necessitated the deployment by vulnerable corporations of alternative methods of risk transfer. The US Congress has responded to this by passing the Terrorism Risk Insurance Act last November, effectively banning most of these insurance policy exclusions on commercial lines, and facilitating government assistance. The United Kingdom has the Pool Re system for terrorism cover which is not comprehensive. The UK government is currently hoping to extend this system without having to implement new legislation.

Future digital attacks

It is unlikely that governments will choose to remain oblivious to the challenge of daily digital attacks on their citizens and their livelihoods given the economic damage being caused.

Successful overt digital attacks – as opposed to scans, attempts or covert attacks – are predicted to follow the trend, albeit more slowly, established over the last seven years and could number between 120,000 and 140,000 worldwide in 2003. Blended attacks – physical attacks synchronised with digital attacks – could materialize in the coming two years. Although new viruses and worms released in 2003 may reduce, the damage caused by a few killer viruses or worms – some politically motivated - will run to billions of dollars.

A US war with Iraq is likely to further increase the number of digital attacks, with a corresponding cost to business and government. Successful and verifiable attacks against the United States are likely to be between 80,000 and 100,000 in 2003. We can expect that there will be increasing consolidation and unity in 2003 between fundamentalist and anti-capitalist hacker groups with a united agenda against Western interests. The Israel-Palestine conflict, the Allies' War on Terrorism as well as the India-Pakistan conflict over Kashmir will continue to bring fundamentalist hackers closer to each other. Eastern European, Central Asian, Indonesian and Malaysian hacking groups will continue to assist the fundamentalist agenda.

There could be a backlash against Arab and other Islamic countries' online presence from Western vigilante hacker groups in 2003 if pro-Islamic hacking and consequent online damage of Western economic interests continues apace.

If there is a destabilizing impact from the war with Iraq on certain Islamic countries such as Saudi Arabia or Pakistan, and they are subsequently engaged in internal conflict, the digital attacks within those countries and across their neighbours could rise sharply. Proliferation of broadband (24/7 always on) internet services will result in small to medium size entities as well as individual users (micro entities) coming under more frequent hacker and virus attack. Identity theft, credit-card theft as well as customer/personnel data and software piracy will increase as digital crime proliferates in 2003. Unsuspecting individuals and small to medium size businesses with broadband access could also become surrogates for increasingly targeted Distributed Denial of Service (DDoS) attacks as well as providing cover for terrorists.

***DK Matai** founded mi2g in 1995. He has formerly worked in the R&D labs of IBM, Inmos, ST Microelectronics and Helvar Electrosonic on Massive Parallel Processing (MPP) and supercomputing applications. He is widely quoted in the international media on the risks and reward of digitisation.*

***mi2g** advises on eBusiness systems, the management of Digital Risk and Bespoke Security Architecture for financial institutions and multinationals in Europe, America and Asia. mi2g has been collecting data on overt digital attacks since 1995. For more information contact: intelligence.unit@mi2g.com.*