The Economic Impact of War with Iraq – Asymmetric Risks

11th December 2002, Institute of Economic Affairs (iea)

DK Matai, Chairman and CEO, mi2g

***iea** Introduction - Concern about war between some Western countries and Iraq has mounted in recent weeks. War with Iraq may have important economic consequences as well as political and security-related consequences. First-order consequences might include increased oil prices and also higher defence expenditure at a time when it appears that tax revenues will be rising much more slowly than government spending. There will also be second order consequences. These will depend on the outcome of war and on whether war achieves its objective of bringing peace and stability to the region or, in fact, makes the region less stable.*

My Lords, Mr Chairman, Ladies and Gentlemen

It is a great pleasure to address such a distinguished audience at the Institute of Economic Affairs with strong reinforcement from two noted experts. I am going to speak about the unintended consequences of the possible conflict with Iraq.

Economic Costs

At present there is an uncertainty as to when the war with Iraq is likely to take place although there is a consensus that it is most likely in the early part of 2003. Any ongoing uncertainty in this area is likely to depress the capital markets and hinder growth. So, in the end, there may be no choice left other than to embark on the conflict in hope of the most benign economic outcome. Most wars in America's 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, it is extremely doubtful as to how easy it would be to capitalise on the world's second largest oil reserves. Two broad-brush scenarios are worth noting:

1. It may be a short and neat war as it is hoped. Various independent studies have calculated that a short war would cost over $50 Billion.

2. If the war is a protracted one, there may be severe economic consequences in terms of loss of confidence in the West and a longer capital markets downturn, which would impact on support for and satisfaction with Government foreign policy; the costs would also double and cross $100 Billion.

The cost of rebuilding Iraq post the war would also be significant and depend on the damage caused. If Weapons of mass destruction are used by either side, the clean up and recovery costs would be immense.

Over a ten year period, the medium to long term cost of a war that went well would still be in excess of $100 Billion whilst a war that went horribly wrong could end up out by a factor of ten and cost in excess of one Trillion Dollars.

Also, 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 avoided being perceived as a war on Muslims. In the war with Iraq, we may not be so lucky. In the Gulf war, there was the BBC and CNN, now there is Al-Jazeera and the global Internet and eMail access to contend with as well.

The asymmetric threats

In recent weeks our Prime Minister, Tony Blair, and the Home Office have reminded us of the potential threat from terrorists, including the use of unconventional weapons. I should imagine that any war with Iraq will exacerbate the threat in this area.

There has been an open threat from a range of radical organisations that they will embark on causing terror and economic disruption should this materialise. No doubt, some of this rhetoric is empty and it pulls a veil over the real threat from the few 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 disaffected small groups waging asymmetric warfare on the West through Chemical, Biological, Radiological, Nuclear or Digital (CBRN-D) means blended with conventional physical attacks.

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

Long tail phenomena

Modelling the threats 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 the emergency response planners, operational managers as well as the insurance and reinsurance industry. Many of the CBRN threats have long term clean up requirements beyond the initial decontamination and sectioning procedures. Also, entire postal code zones can be affected as opposed to just one room or a building.

Post the Oklahoma bombing, US authorities carried out a simulation to study the effects of a biological weapons attack that unleashed 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.

More recently, Anthrax laced envelopes, which arrived at US Government offices post 11th September last year caused severe disruption within Capitol Hill as certain buildings – including Senator 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 devastating and the recovery time was measured not in days but several 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, on which we depend, against us.

We 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 has now crossed 77,000 in 2002. Some years have seen a 10-fold increase!

The most significant findings from our intelligence database are that trends in digital attacks 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 on the UK 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 of tools exploiting that vulnerability takes place within a few hours.

The large and well-protected government or corporate networks which will often require relatively greater time, skill and experience together with extensive "social engineering" are as a consequence much harder to penetrate.

As a result, economic damage is incurred and confidence suffers.

Blended threats and digital reconnaissance

Equating hacker groups with terrorist organisations that kill people with powerful explosives may not be justified. Having said that, the biggest threat could still be a blended threat: digital attacks that cripple emergency response, transport or telecommunications with some insider help, could be employed by terrorists in conjunction with conventional or CBRN 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 programs 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 require extensive insider help.

Former or present employees, 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, as in the case of Vitek Boden in Australia, who was convicted last year 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 a digital attack exploiting software vulnerabilities that were exacerbated by the lack of a proper data back-up regime. One would assume that this was an easy to implement process.

It is usually 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 organisation and instituting policies to prevent the success of common social engineering tactics. Also, there is a requirement to have the correct legal contracts with personnel, customers and suppliers.

The USD 50 Billion that was reserved by insurance and reinsurance companies post 11th September 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 in the past for many areas has necessitated the deployment by vulnerable corporations of alternative methods of risk transfer, but the passing of the Terrorism Risk Insurance Act in the US by both houses of Congress in November will effectively void most of these exclusions on commercial lines insurance policies and allow much needed government backing to be implemented. In the UK we have 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.

Some thoughts for the future

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 remain in Billions of Dollars.

If the war with Iraq in early 2003 materialises, USA will remain one of the most attacked countries digitally followed by other NATO member countries and allies. Successful overt attacks against the US are likely to be between 40,000 and 50,000 in 2003.

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 US/UK War on Terrorism as well as the India-Pakistan issue on 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 on Arab world 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 of 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.

Conclusions

The war with Iraq may have unintended economic consequences:

1. If blended threats of CBRN-D terrorism coupled with conventional attacks from fundamentalist groups materialize in the West it would be difficult to predict the impact of such an attack on health care, financial services, local government, transport, distribution etc just as it was difficult to envisage the economic consequences of 9/11 precisely such as the bankruptcy of large airlines in the US: United Airlines and US Airways as well as in Europe: Swiss Air and Sabena.

2. The vacuum left behind post the removal of Saddam Hussein's power base in Iraq could trigger political power fluctuations around Gulf countries such as Saudi Arabia, Kuwait and Bahrain as well as Iran and Central Asia. This would affect energy prices, business and consumer confidence.

3. There may be a period of instability where Saudi Arabia and Pakistan may have internal conflict. Any adverse situation within Saudi would influence events throughout the Islamic world. A power struggle within Pakistan would create an Indian sub-continent crisis followed by a global one if her nuclear weapons were to fall into fundamentalist hands.

4. In order to win the next election, it would be mandatory for any participating government to be seen to have won or to have dealt with the Iraq situation successfully.