The current National Security and Resilience (NSR) situation is complex in that it covers resilience both in response to terrorist action and civil disaster or contingency. The recent publication of the National Security Strategy (NSS) provides a useful opportunity for taking stock.

The UK has had a counter-terrorist strategy (known as CONTEST) for some years. It is based on a framework of four Ps:

- Preventing things happening by dealing with the underlying causes
- Pursuing those intending violence to reduce the threat
- Protecting the UK by reducing physical and electronic vulnerability
- Preparing for attacks should they nevertheless happen.

The CONTEST strategy was made public in 2006 - in itself a sign of changing times and a recognition of how much information is now in the public domain about the activities and capabilities of the police as well as, intelligence and security agencies.

The latest advance was the publication by the government in March 2008 of the National Security Strategy for the UK. It is important because it acknowledges and captures the nature of the changes that are occurring. It also sets out the government’s aspirations for the way things should develop further.

The NSS, for the first time, puts terrorism formally in the wider context of other threats to the nation and its people. It carries forward the logic of the resilience agenda in recognising that responses to threats and catastrophes may have common features independent of their origins. It broadens the scope of national security to look at the risks to the UK from terrorist, criminal, man-made and natural disasters.

The Strategy also notes the pervasiveness of the internet and mobile communications. Such familiarity and accessibility to those active in crime and terrorism, means that a great deal of the recruiting, planning, preparing and organisation of criminal and terrorist activity now takes place in the electronic space. Increasingly, this is the battlespace within which government needs to be effective if it is to detect and prevent malicious activity.
At the same time, our electronic dependency also provides opportunities for criminals and, potentially, for terrorists.

“Terrorists also aspire to attack our critical national infrastructure; and to use new methods, including electronic attack... organised crime including fraud, the trade in illegal drugs and illegal weapons, illegal immigration and human trafficking... is increasing... these phenomena are not new; but they are taking new forms and exploiting new opportunities, including revolutionary changes in technology and communications...”


In summary, the government’s intention is to encourage a broader and more connected view of National Security that links more closely the integrity of the state and the safety of the individual. It seeks a more effective coalition of central and local government, security and intelligence agencies, law enforcement, business and commerce, as well as non-profit organisations and individuals.

In effect, both a globalisation process and a multi-agency approach is required if a coherent and effective response to NSR is to be achieved, and if Critical National Infrastructure (CNI) is to be protected.

The government has a leadership role to play and to date they have made some major changes to address the multi-agency approach with:

- The creation of the National Security, International Relations and Development Committee (NSID), formed from the Cabinet, chaired nominally by the Prime Minister
- The reorganisation of the Home Office. This includes the creation of the Office for Security and Counter-Terrorism (OSCT), a unified Borders Agency and extensions to e-Borders, continued (for the moment) commitment to the National Identity Scheme (NIS) and new Police Counter-Terrorism structures
- The last spending round that favoured security, intelligence and counter-terrorism (and constraints on defence spending)
- Reviews of intercept as evidence and data security, new asset freezing proposals, new court rooms and judicial arrangements for terrorist trials, and proposals for detention beyond 28 days.
In the future, consideration is being given to:

- Consultation on ideas for a joint Parliamentary National Security Committee
- Strengthening of horizon-scanning and forward planning capability
- Creation of an (advisory) National Security Forum with representation from government, the wider political scene, voluntary sector, academia and others to discuss strategy and exchange ideas.

The NSS also seeks to balance terrorism against other threats to civil society, with for instance ‘flood ing and flu’ seen as a greater immediate threat to our way of life than terrorist incidents. In any such cases, the response level will be the same with the focus on operating within a complex multi-agency environment.

PROBLEMS AND ISSUES

There is a definite distinction between responding to a large scale crisis, which so far the UK has not suffered, and a point attack, such as 7/7. In a large scale crisis, there will almost certainly be features that distinguish it from a more straightforward situation. Specifically, in a complex multi-agency environment, which involves significant military engagement and a requirement for interoperability between all agencies - particularly the first responders (police, fire service, paramedics, NHS, etc), local and central government, the security services and military.

The main issue is the need to effect a more ‘joined-up’ approach to any response in the face of this multi-agency environment. This involves not only technology but also doctrine and process. This ‘joined-up’ approach needs to be implemented in harmony across all organisations involved so that they may be exercised to a high standard of delivery ahead of any crisis. If not the danger exists that in a crisis, organisations and individuals will revert to what they know best and ignore newer technologies. The widespread use of commercial mobile phones by the emergency services in 7/7 is a case in point.

There is, therefore, a growing ‘cross-over’ area in which many of the approaches, disciplines, capabilities and skills developed to meet the needs of traditional defence and security clients are equally needed in the UK civil government sector. This ‘cross-over’ area does not have the degree of coherence, predictability or the procurement doctrine familiar in individual departments such as the MOD. The government aspires to something more coherent and ‘joined-up’ There are some good examples of effective partnership but there is no clear plan to achieve it. Substantial obstacles exist in the range and nature of accountabilities of different parts of the sector, their enabling legislation, and the way budgets are allocated.

There are plans for a ‘single budget’ for counter-terrorism and security, but this is likely to be, at best, the sum of the parts rather than an accountability mechanism. There is a real risk that the nation will remain compartmentalised. This will make it impossible to identify and procure the systems that would enable it to ‘join-up’ across organisational boundaries when faced with a multi-agency crisis. In these circumstances first responders and the security services would be unable to react to crises efficiently and comprehensively.

“Terrorists also aspire to attack our critical national infrastructure; and to use new methods, including electronic attack... organised crime including fraud, the trade in illegal drugs and illegal weapons, illegal immigration and human trafficking... is increasing... these phenomena are not new; but they are taking new forms and exploiting new opportunities, including revolutionary changes in technology and communications...”

The consequences of agencies not being informed results in confusion and delay when losing time is likely to cost lives. If the situational awareness of different agencies during a complex emergency is not the same, responses are likely to be both slow and uncoordinated. Relatively simple solutions, adapting legacy systems or using Commercial off the Shelf (COTS) solutions, can plug these holes quickly and efficiently.

**THE FUJITSU APPROACH**

Information and Communications Technology (ICT) has a major role to play in enabling this more ‘joined-up’ approach and delivering interoperability. Fujitsu is one of the largest suppliers of IT systems to both government and the private sector; with installations in the Home Office, Cabinet Office, MOD, HMRC and Security Agencies. We are in a pre-eminent position to assist government departments to work more effectively both singly and also with other organisations. Fujitsu Defence and Security, as one of the UK’s leading IT Systems Integrators, is well placed to manage this process.

There are two distinct areas where Fujitsu can bring its defence and government expertise in ICT systems to bear:

- At one level, it is a matter of integrating, across a secure government infrastructure, information which is already available in silo systems. This will provide the authorities with the right information to enable them to manage the crisis at a strategic level.
- At another, as a key systems integrator, it is bringing new advanced capabilities together to generate interoperability at the operational level. This would include capabilities such as Crisis Communications Service, integrating incompatible communications networks, and our openJOP system, providing situational awareness for operational commanders at Gold or Silver level.

Fujitsu has demonstrated its ability to develop and deliver such systems in the Defence and Security markets. For these markets we take COTS products and integrate them, building in all the necessary security and encryption controls. While not seeking to transfer such products unchanged into the civil NSR market, the combination of Fujitsu Defence and Civil Government capabilities, and an understanding of client needs, would provide rapid effect solutions without unnecessary delay.

Fujitsu has strong credentials for the broadly defined NSR market. It has both knowledge and experience in working with central government, government departments and the MOD. This experience, combined with defence and security credentials in classified, secure, resilient and sensitive information and communications technology means that we are familiar with the language and working methods of all the organisations involved in UK NSR.

Fujitsu is also experienced and well-regarded as a partner in coalitions with other suppliers. We have been a trusted partner with government, including the MOD and The Home Office, for 40 years. We have worked and are working in consortia with partners in industry. The specific capability areas include:

- Secure communications and networks
- Integration and management of information and data from multiple sources and in multiple forms
- Command and control
- Identity management
- Information and data assurance, integrity and security
- Secure data storage

In conclusion, Fujitsu is well placed to provide the required level of secure integration and management of existing silo based information systems across a multi-agency operating environment at the strategic level. At the same time, we are capable of delivering integrated and proven technologies that provide the operational commander with secure interoperability from COBR to the policeman on the street - and indeed the informed citizen.