

UK National Security Strategy 2008 – the Devil is in the detail

Author: Steve Coles, Secure Systems Director, VEGA

Introduction

It is often said that 'the Devil is in the detail'. This was again proven to be true with the publication of the UK's first National Security Strategy earlier this month.

Critics of the strategy have labelled it as more of a list than a strategy, suggesting that without any detailed implementation plan, there is a real risk of it becoming nothing more than the basis for "some sort of talking shop".

However, security minister, Lord West, denied that drawing up a list of threats was a pointless exercise, saying: "There are some areas which we have got very well under control; there are other areas where a lot of work is needed and what this is doing is identifying that and giving us a focus as a way to move forward."

"If there was an easy answer to all of this we would not have had to go down this route. It is highly complicated and it is very difficult, but we are leading the world on this," added Lord West.

And it is in this complication that the devil really lies. The process of joining up a plethora of intelligence sources and a network of incompatible, legacy information systems, compartmentalised within government departments, in order to provide a detailed overview of the potential threats facing the UK, is overwhelming in its complexity.

The National Security Strategy is correct therefore to outline the variety of threats facing the UK. How else can we fully understand the requirements to counter these threats if we do not know what they are, how they are inter-related, and, most importantly, how we can ensure that all UK security and resilience assets work coherently to provide the best capability response?

A quick review of some of the key points outlined in the National Security Strategy highlights the increasing complexity that will be facing a co-ordinated UK security response:

1. The creation of four regional counter-terrorism centres and four regional intelligence centres
2. Call upon public vigilance to support the (local) intelligence communities
3. Greater requirement on military/security and intelligence services/police to work alongside each other (with JTAC bringing together 16 different departments)

4. Protection against the threat of new technology attacks (cyber terrorism) include against CNI
5. Increased number of surveillance targets (the report states that the UK is currently facing 30 known plots, and monitoring 200 networks and 2000 individuals)
6. Enhancing protection against terrorism of national borders with new technology and new UK Border Agency
7. Build on the Civil Contingencies Act 2004 and the contingency plans of first line responders and role of local emergency planners
8. Implement national and local planning and co-ordination bodies to deal with the threat of pandemics outbreaks

All these initiatives contribute to the following truisms:

1. There is a major requirement to have a detailed understanding of an increasingly complex joined-up security environment. The need is not only to understand the interactions and interdependencies of the various information systems, but also the people and infrastructures on which they rely. This demands a serious level of trust across the security communities and with industry players, which is challenging but necessary.
2. The increased speed and accuracy demanded of this intelligence infrastructure, against the backdrop of an evermore effective, pernicious and sophisticated cyber threat, requires information systems to be highly secure (and remain secure) to ensure the intelligence's integrity so that it is delivered when and where it is needed most: 'right information, right place, right time'. Also a system that can not be altered to defeat threats as they appear will be redundant very quickly. This demands collaboration of the very best that the UK has to offer, not a turf war over market share.
3. Finally, there is an increased requirement to identify, qualify and track an increasing number of individuals and cells who have the potential to harm UK citizens or infrastructure.

These three points are even more pertinent as the Government acknowledges the fact that any National Security Strategy must be viewed from a truly global perspective. There is a greater need for the rapid and secure exchange of information – locally, national, and internationally. The activities of terrorist suspects, organised crime and the spread of pandemic disease are not bound by geographic borders and the UK security community has to be compatible to call upon and work with information sources from across the globe. In this respect, the UK is in line with many of our allies in developing the 'need to share' policies associated with Counter Terrorism.

Additionally, the role specified in the National Security Strategy for UK citizens to support intelligence networks will not only add to the complexity when designing the architecture of these information systems, but will also mean that the intelligence community will have to consider how it can continue to ensure the integrity of the information when it now has a requirement to be accessed by those working at different levels of security clearance. As Carl Fisch once commented, “shift happens” (opens in new window).

So how do we propose we address these challenges?

- **The Complexity Challenge** – The ability to understand the complexity inherent in successfully transforming legacy, standalone information systems into a cohesive joined-up network that improves capability is an issue already being faced by the UK military and its pursuit of a Network Enabled Capability. Here the issue is being addressed through the application of enterprise architecture and the creation of the MoD Architectural Framework (MODAF) repository. This approach is providing the UK MoD with a visualisation and understanding of full capability of each of its systems and their interdependencies, and identifying how this capability can be enhanced or alternatively where gaps in capability or interoperability appear.
- **Custom Built Secure Portals** – Secure communication and information portals already exist across the Government’s defence and security community, but the increasing need for information sharing with a variety of different infrastructures means that purpose-built system architectures do not have the flexibility to deliver the levels of security demanded of the information they are meant to protect. Robust, secure portals comprising COTS equipment that is configured to the individual requirements of an organisation provide a cost-effective solution that allows information to be exchanged in a timely manner and with its integrity intact. We only need to look to the US to see the benefits of this type of architecture.
- **Knowing who you are dealing with** – National security depends on having accurate and timely information regarding the movements and activities of people who are of concern whilst ruling out those who are innocent. This requires the application of identity management technology and secure, integrated, cross-Government data management. Government has already started down this road with the roll-out of biometric visas, the National Identity Scheme and eBorders in tandem with a number of other secure systems. There is a risk is that without an end-to-end “customer” journey-related understanding across these initiatives of the lifecycle costs and benefits, they may fail to produce the benefits envisaged. Application of identity specific enterprise and performance architecture modelling tools and techniques, and through life cost

and benefits modelling, will be essential to understanding the root causes and effects in such complex systems.

The consideration of these three approaches can go some way to taking the proverbial Devil out of the detail demanded by the critics of the National Security Strategy. What is required now is a commitment from government to work together with industry to help make this happen.

Providing government with the ability to understand this inherent complexity, as well as enabling its departments to exchange key information securely and successfully track those who would intentionally or inadvertently cause harm to our nation, are three of the key ways in which industry can help government ensure that the appropriate security capability is developed to protect the UK in the 21st Century.