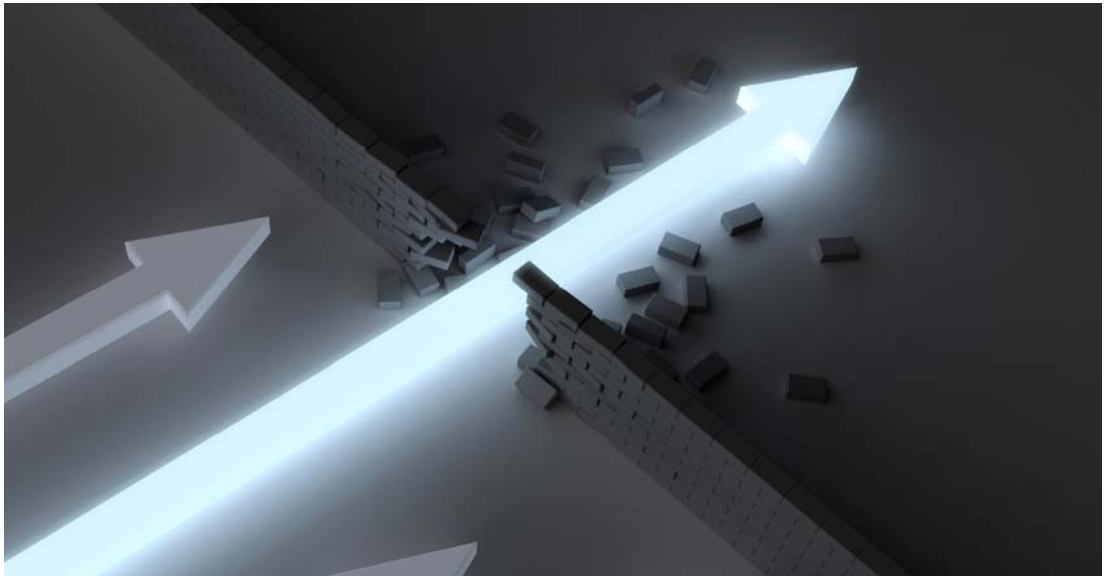


Information Sharing: The New Intelligence Capability



Author: Michael Clayforth-Carr, CEO, VEGA

Introduction

Never has there been a more urgent time to ensure that the UK has a responsive and joined-up approach to its security challenges, than in the early years of the 21st Century. The asymmetric nature of the threats we face, whether they are man-made or environmental, physical or virtual, requires that the security & resilience community acts on intelligence from an increasingly complex network of information proactive and reactive sources with a greater level of speed and accuracy.

UK Security Challenges

1. The need for speed

The enemies we face today are resourceful and, although they implement their plans with varying levels of effectiveness, are able create or change tactics and plans with alarming speed and in apparent unpredictable fashion. This is a pace of change that we are currently unable to match, which means that the best laid plans could be redundant before they are started!

2. Providing analysts with information to act upon

The culture and operations of government departments and agencies charged with the security and resilience have evolved over many years. However, this has tended to be in a partitioned manner which mitigates against seamless co-operation, collaboration and [information sharing](#). The stakeholder community is powerful and

immense. By default though, it's comparatively cumbersome compared with the enemy we face.

Industry must therefore help government introduce [information sharing](#) measures between departments (while still maintaining the integrity of the source information) that enable analysts to make decisions, not manage information.

3. Information system procurement

At the same time, we should also consider how we manage the procurement of complex information systems. If we are assuming that we struggle to respond to security threats, we must ask whether the processes we undertake to define our requirements, build and integrate our information systems lend themselves to implementing new capability quickly.

If current methods hamper the way we respond to security challenges facing us, perhaps we could harness the inherent power and capabilities of the state organs in a way that allows information to be more effectively accessed, assessed and acted upon?

Shift Happens

American lecturer Karl Fisch's globally acclaimed presentation '[Shift happens](#)' demonstrates dramatically just how quickly the information age, and the technology driving it, is changing the world of tomorrow, today!

In light of Fisch's assertions about the pace of technological change, industry cannot be allowed to provide IT solutions that are out of date before the ITT is published.

Similarly, if government finds it challenging to improve the inter-departmental and agency collaboration and co-operation needed to meet this pace of change and the unpredictable nature of the threats faced, it must consider an alternative approach to a solution – something which already helps the way the world rapidly shares information...the Internet.

The Internet has revolutionised our lives in many ways. The one relevant to [information sharing](#) is its ability to enable technology at different levels of evolution to be used to connect individuals and business together. Not having identical computers, applications or indeed levels of security, is not a barrier to accessing the information in the same way.

Therefore if we can all gain access to information using widespread and commonplace NET technologies, our ability to improve the quality of our intelligence should not mean we have to reinvent the wheel to do so.

Adopting best practise from the US

This view of [information sharing](#) / intelligence gathering was first seized upon by the US following the atrocities of 9/11. The US Office of the Director of National

Intelligence (ODNI) reviewed the culture and processes of their Counter Terrorism (CT) machine, and enforced unilateral changes across its homeland security community. The ODNI rewrote policy and changed the culture, recognising that if it proved the appropriate technology, cultural change would happen automatically. They understood the nature of the young analysts now delivering the [information sharing](#); by providing them with common architectural backbone, the analysts were able to use commonplace NET technologies through which to forge new relationships, and through these relationships they could share information.

The architecture provided analysts with the capability to capture, collate, and disseminate intelligence from a variety of proactive and reactive information sources. However, each individual organisation owned its own presence on it while retaining control of their information assets, publishing only what needed publishing.

This can be likened to corporate websites, where users locate specific information and sites through search engines. Corporations allow staff to access the web through gateways and use services provided by others, such as internet banking or social networking sites, which demonstrates controlled access.

Once individuals have found other 'like minded' people, they communicate by e-mail, collaborative tools, virtual environments, video conferencing etc. It is not a single system but a federation of systems working to the same standards.

The US solution has therefore shown us all what can be achieved by adopting NET technology and utilised the intuitive tools that we all already use. The only, but significant, difference is that the network is secured and interconnection policies are strictly controlled. By utilising 'Commercial Off The Shelf' (COTS) technologies, (many developed for the finance industry), it is possible to build Secure Managed Interfaces (SMIs) that can control the boundary between an organisation and the 'network'. Each organisation owns its own presence on the network and dictates the level of access its own users have by the security threat mitigation level required to gain accreditation or, put more simply, they control their own destiny. The content's management and usage is controlled by the organisation and achieved through COTS technology.

With the US approach mandated, culture change was a natural evolution. The younger generation of analysts used the system as a social networking tool, posting minimal information to 'go fishing' for like-minded individuals who found them using the search engines. As a result, [information sharing](#) had been enhanced significantly.

Could this work in the UK?

The UK already connects and contributes to the US CT sharing network as described above. Some of our national intelligence systems connect directly,

through a UK accredited and secure gateway, to our US, Canadian and Australian allies – proving that the technology works already. The real question therefore is not whether this can be achieved technologically (it already has been), but can we make it work without a decree within current UK policy?

This paper suggests that it is possible, and, furthermore, without dismantling established departmental infrastructures or currently operational information systems managed by incumbent industrial partners. In fact, some companies have already connected existing infrastructure to this type of [information sharing](#) network.

The Office for Security and Counter Terrorism (OSCT) is currently working alongside the pan industry alliance [RISC](#) (UK Security and Resilience Industry Suppliers' Community) to understand how to provide a clear method of connecting existing national systems using the US approach rather than having to replace them all simultaneously.

Currently, many suppliers provide the 'back office' capability to the various organisations. But if they all work together, it could create a 'classified internet' that allows information that needs sharing to be shared in a timely way that allows action to be taken on it.

A solution such as this will not compromise the raw information; only that which needs publishing to the wider community will get published. As in the US (and in compliance with the new Cabinet Office government framework for information management), each department would own its own information. However, what it also provides is the capability to share information at such a speed that it will enable the security and resilience community to respond appropriately to combat the asymmetric tactics and networks of our enemies.

Such a network would also enable non-traditional security players to have a presence on this 'classified internet', including those worried about non-malicious threats such as flooding, pandemics etc. This relates directly to the aspirations of the [National Security Strategy](#) to provide a joined up approach to meet the diversity of the identified issues. These issues may require non-obvious solutions; indeed non-obvious players may pick up the threat before traditional security sources.

The NET technologies would make it possible to create connections using very 'limited' information release; it would only take a key word, posted on a website with contact details, to make a connection between two analysts. One-to-one they can then pass information in a more controlled manner.

And there is no reason why it should stop at merely sharing information – perhaps usage could be made of [virtual world technology](#), so that the 'players' within an interest group can meet and train, developing a community of useful contacts – it is not necessarily *what* you know, but *who* you know.

The UK's adaptation of such an approach does not therefore need a single mammoth procurement where individual requirements get 'compromised' to meet varying organisation-specific requirements. Instead, a central 'core' and 'network' are required to link the network together. Individual procurements can move at each department's pace.

As for the definition of the interconnection requirements, industry in the main, understands these because they connect to the 'web' already. It is just the way the security enforcing elements – all of which are off the shelf – have to be configured to meet the 'code of connection', that slightly complicates the issue. This again refers to configuring commonly-used net capability, not bespoke code.

Conclusion

It seems that the US approach to intelligence gathering, based on web-enabled [information sharing](#) offers a viable approach to meeting the UK intelligence requirements of the early 21st Century. It helps:

- Improve our response time to match that of our enemies and the security threats they pose, by releasing the power of the information hold across government
- Enhance the investment in current infrastructure and technology by circumventing the need for organisational change, updates to procurement policy or the sensitivities of where information is stored
- Empower analysts to do the job with which they are charged, make decisions that help protect the UK and its citizens against current threats, and provide them with ability to meet the challenges of future and, as of yet undefined, threats

So what of these undefined threats in the coming years? Can the UK have such a system (sharing multiple information streams and enhancing intelligence) in time for a UK security landmark such as 2012, and provide a capability to develop, practise, and perfect the capability well ahead of 2012?

This paper suggests that as an industry, we can – at least in an embryonic but functional way. The truth is, this must be in place by April 2010 anyway.

To have a cohesive and complete intelligence platform in place, that answers immediate security questions and addresses future requirements, we must ensure a sound architectural foundation is implemented in the coming months.

[RISC](#) aims to achieve industry agreement on the way forward in the coming months, with the objective of working towards this common goal for an architectural backbone to be in place to meet the current intelligence challenge and that which we all face for 2012 and beyond.

As Karl Fisch reminds us, shift happens and we need to shift now.

VEGA Group PLC, 2 Falcon Way, Shire Park,
Welwyn Garden City, Herts, AL7 1TW, UK
Tel: +44 (0)1707 391999 **Fax:** +44 (0)1707 393909
www.vega-group.com pr@vega.co.uk

VEGA