



The Future of “Fused Intelligence” in the Fight Against Terrorism

Peter Ship, Intelligence Specialist at crime and intelligence software provider Memex, discusses the benefits of Data Fusion Centres in the ongoing fight against terrorism

Memex

www.memex.com

In the wake of the recent Mumbai bombings and previous national disasters in the UK, there is a greater need for analytical-driven policing and an improvement in the way information is shared among police and law enforcement agencies in the battle against crime and terrorism. In any terror emergency, there are three simple objectives – prevention, detection and managing the aftermath – and the key to reaching all of these is relevant and timely information.

Police and law enforcement agencies in the UK have come to realise they need to access more than just their own data. The very nature of current terrorism activity from fundamentalists has highlighted the need to gather information from new sources and specifically those within local communities and the private sector. Before 9/11 occurred terrorism in the UK was usually linked to organisations such as the IRA, and was primarily dealt with by top level Government agencies and specialist police units. The comparatively small pool of information required meant that sharing of information was much tighter and therefore easier to manage. But now, the unpredictable and volatile nature of modern terrorism means information is required from sources rarely used in the past to identify the link in an investigation and to identify developing threats. This has created an imperative need for both improved collection and an information sharing network in the UK. When investigating or identifying terrorism plots it is often the tiny but vital piece of information that completes the jigsaw so partnership information – the data that is shared between police forces

and local authorities for example – becomes extremely important.

A more consistent structure of police and law enforcement agencies across the UK should mean the goal of sharing information nationally is achievable but the US, despite their organisational inconsistencies, is beating the UK's agencies in the information race. Data Fusion Centres are a fresh concept in the US in gathering and analysing information, integrating a variety of Government agency and private sector information and intelligence to provide a more accurate picture of potential risks. The US's approach of identifying the best analytical tools on the market and utilising these systems has allowed them to form an information sharing network which is ahead of the UK. Whilst the same tools are used in the UK, they are as yet to be used across fused data and therefore have yet to provide the benefits seen in the US.

In the UK, the demise of CRISP (Cross Regional Information Sharing Project) in 2007, the interim solution until the PND (Police National Database) is completed, due to existing data problems means the UK will not have a fully functioning information sharing network until at least 2010, despite increased terror threats. Although the current measure INI (IMPACT Nominal Index) is proving itself to be an invaluable tool in the UK police's armoury, by improving their ability to manage and share information, there is still some way to go to realising the ultimate goal of the PND.

In contrast, the US is flourishing with fusion centres stretching from Arizona to New York and there are many more planned. The Georgia Bureau of Investigation (GBI) is one of the most recently established centres embracing information sharing technology. Seven law enforcement agencies, serving 2.5 million residents, use the system which allows for the submission of tips and leads, intelligence and case management functions thus providing a robust platform for information sharing.

However, operating in an atmosphere of trust and security while managing intelligence, incident reports, public records and other types of secure information from numerous agencies is a daunting challenge. The technology can allow law enforcement agencies to gather and analyse intelligence at the highest level but it is the political concerns of obtaining, holding and using information that makes it more difficult to share information. Both the UK and the US have a raft of legislation dealing with retention of data and privacy which all intelligence sharing networks must take into consideration when an agreement is made to fuse data across different agencies and private organisations. However, many private sector organisations have a wealth of experience in managing information and their knowledge and expertise in this area can offer many benefits to the law enforcement industry.

As well as the support of expert knowledge, the technology also needs to meet the legal requirements of data retention. Intelligence gathering software offers many security processes to ensure agencies remain in line with

legislation and guidelines, including allowing system administrators to set security levels for both the users and the records. At user level permissions can be granted for access to different levels of information depending on what is required. This can be segregated by teams or departments depending on the investigation and gives each of them different levels of access. Every action by a user is recorded and audited such as editing and creating records, which allows organisations to understand the information they have and analyse it more efficiently.

The software also allows every record to be given a security level depending on the sensitivity of the information. The ability to assign covert or overt security to records ensures that each agency can manage their own information more securely and prevent data misuse. However, although users are unable to find covert records in a search, the notification of the search which is sent to the owner of the record can often be the first sign of a link between investigations highlighting the benefits of a shared information system.

Data Fusion Centres create an environment of trust by encouraging the use of agreed protocols of non disclosure contracts between law enforcement agencies and also between any private sector organisation which may be involved. Risk assessments are also carried out so organisations can assess how much risk is involved in sharing their information helping them to decide what data to share. These actions ensure that everybody involved understands what information is to be shared, why it is shared and who owns the information.

www.memex.com

North America

Memex, Inc.
1595 Spring Hill Road
Suite 200
Vienna, VA 22182 USA

T: +1 703 556 4031
Toll Free: +1 866 MEMEXUS
F: +1 703 556 4282

UK & International

Memex Technology Ltd
2 Redwood Court
Peel Park
East Kilbride G74 5PF
Scotland

T: +44 (0)1355 233804
F: +44 (0)1355 239676

Registered in:
Scotland

Company number:
SC108095

Registered Office:
2 Redwood Court, Peel Park,
East Kilbride, G74 5PF

VAT No:
481 0520 74

However, the major benefit of Data Fusion Centres is that one overarching memorandum of understanding is created between all agencies involved encouraging trust and providing more information for analysis. This is an attraction for private sector organisations who can often be put off sharing sensitive information if they are apprehensive about data being leaked to competitors. Current procedure in the UK requires the creation of a memorandum of understanding each time an information sharing partnership is agreed, which is a significant barrier in the willingness of law enforcement agencies and private sector organisations to share data.

The increased need to manage vast amounts of information across the country due to the added requirement of community information means that unlike Data Fusion Centres, the PND in the UK can never be the whole solution as it has limitations on the kind of information available to search over. A more flexible system is required to allow each force in the UK to access and share data and I would prefer to see a phased approach through regional hubs akin to the fusion centres in the US to accommodate each area of the UK and improve analysis. Currently, strategic analysis only takes place within individual agencies before the information is shared making it harder to identify any gaps in the data. A modern information sharing network also requires to take data from other sources, both regularly and as required for specific investigations. The importance of regular feeds from the likes of London Transport is evident but there is also a need to access data from other sources. The NHS link in the

Glasgow Airport attack is an excellent example of why these other sources are required for specific investigations and why fused data between all sectors is important.

Encouragingly, police in the UK are improving their current systems and processes to gather and use data more effectively thus improving the sharing process. However, this also highlights the need for efficient, structured business processes within police and law enforcement agencies to enhance the use of intelligence gathering IT. Good technology with properly trained investigators and analysts behind it can begin to bridge the information-sharing gap. However, users also need to understand what the software is for and how it works in order to maximise the benefits of having the access to the data. Otherwise it will be a wasted instrument in the fight against terrorism and other crime.

Data fusion is growing as an advanced tool for law enforcement and the success of fusion environments rests on careful consideration of legislation and how the technology is used. Intelligence sharing has moved on vastly over the last few years but it will always evolve and the attitude to the IT required and its benefits in gathering information need to evolve too to ensure police in the UK have a 21st century tool for combating 21st century crime.

Memex