LONDON FIRST BREAKFAST BRIEFING – 9 MAY

ADDRESS BY SIR IAN ANDREWS CBE TD

CHAIRMAN, SERIOUS & ORGANISED CRIME AGENCY

Information Sharing and national security: why is it more difficult than it should be?

- Information is the life-blood of any organisation, and no more so than for those charged with countering threats to national security. The ability to collect, store, analyse and interpret information effectively is a prerequisite to taking decisive action to prevent threats from materialising and to pursue those who pose them.

- Effective intelligence sharing <u>across</u> organisations is just as vital. Almost all operational meetings between partners in the NS space conclude that there should be more of it: and I doubt that anyone would take issue with either of these propositions, whether in the context of espionage, cyber attack or organised crime. But why then do issues of information and intelligence sharing continue to trip us up? And at least as many chief executives and private sector Boards seem to get into hot water over information security failures as over more general operational issues.

- There is no shortage of senior level recognition, ambition or will power around the need to share information. The need to break down silos and replace the old "<u>need to know</u>" culture with an adventurous "<u>dare to share</u>" approach has echoed around Whitehall and the law enforcement and intelligence communities for at least 20 years. And it increases in volume with each failure where information issues – and the apparent failure of intelligence to "join the dots" of which 9/11 and Soham have been particularly high profile examples – are believed to be at the root of the problem.

- We always seem to fall short of this information sharing nirvana, and the high expectations of leaders are often not met. Why? Perhaps we need to acknowledge more than we sometimes do that information sharing is inherently difficult – not so much as a concept but at the level of detail and practicality – and it is the detail that gets in the way when organisations try to share data.

- So what are the problems? There are many, both noble and ignoble.

    - First, there is a perceived inconsistency of message from governments. On the one hand the need for open data, transparency and "dare to share"; on the other, the need to respect privacy of the individual with ever more stringent action and penalties threatened against those who mishandle personal data. While these two objectives need not be in conflict it can lead to confusion and caution at working level.

    - Then there is respect (or fear) of the law. No one – from the most senior to the most junior - wants to be held to account for a confidentiality or data breach. The danger of an inadvertent breach is often perceived to outweigh the benefits of sharing the data - especially as risks are to the individual while the benefits accrue to the organisation. Let's be clear, current legislation does not prevent sensible data sharing – especially when national security is involved. Indeed, I have heard it from the Information Commissioner himself that, as long as there is good reason to share data and the appropriate safeguards are in place, no-one will fall foul of him.

    - Trust is also fundamental to effective information sharing - and its absence is often the largest barrier. How can we be confident that those we released it to will use it correctly? This is especially important in the national security arena where much information will originate from covert and sensitive sources and real damage can result if it is mishandled. But trust between organisations cannot be just switched on - it requires deep understanding and mutual respect for each others culture and ways of operating.

    - Data may, of course, include information collected through organisations' own operations which needs to be managed alongside that from third parties supplied in confidence on the understanding that it will not be used further. The breach of such third party obligations is a significant sin in the intelligence world and its presence can make bulk data sharing difficult in process terms.

- Related to trust can be a lack of mutual understanding. Intelligence practitioners know that most intelligence is ambiguous and incomplete: indeed some elements may be misleading or even simply wrong. While intelligence can be a guide for action and strategy it may not offer the certainty that its customers seek. Effective intelligence sharing therefore needs appreciation of the strengths and limitations of intelligence on both sides. It may be possible to answer the question "Is it safe to do business overseas with company x or individual y?" with intelligence to inform a risk based judgement, but rarely to provide certainty.

- Process and technology: the application of protective marking schemes, accreditation of systems to different levels and different approaches to security vetting of staff also creates barriers. In the UK, the marked differences in approach and technical capabilities between the police and intelligence services, Whitehall and the private sector can and do frustrate the ready sharing of information. If your systems aren't as well protected as ours, can we be sure that our information will be safe on them? And if your staff are not as carefully vetted, how do we know that our information won't fall into the wrong hands? While such concerns can easily be exaggerated, they exist and need to be confronted if effective information sharing is to take place.

- As a recent report by Thompson Reuters and the Atlantic Council has recognised, regulation also imposes cost both in terms of both administration and business opportunities forgone. There is a need for a clear dialogue between government and the wider public and private sectors to determine what works best to ensure that prosperity and security are not incompatible – and that regulation is understood, proportionate and fit for purpose.

- There are, of course, many ways in which private organisations are encouraged, and sometimes obliged, to submit data to central authorities including those in law enforcement: and bad experiences of these regimes can cause mistrust. A common complaint is that no feedback is ever

received on the information provided. This can be particularly problematic for organisations which run high volume information operations interfacing with the public - but must do so with limited and in austere times reducing numbers of staff. One such example is the Suspicious Activity Reporting regime which SOCA runs under Proceeds of Crime legislation. But with more than 0.25M reports received annually, individual customer attention and feedback is all but impossible: nor is it alone.

- Finally there is Culture. Organisations (and individuals) often view information as a significant source of power, something over which they should assert exclusive rights of exploitation and interpretation. But the world of "big data" is undermining that notion - too much information and no time to understand it can lead to paralysis rather than power. Some organisations – not least in government – are recognising that sharing with others helps to develop a common appreciation of the threat: and of how they can help each other. Banks, for example, have recognised that an attack on one today, is an attack on another tomorrow and that sharing experience does not need to put their proprietary information at risk: indeed, it helps to protect it. But this can still be a cultural anathema in the intelligence and security worlds – for both good and less good reasons.

So there are many reasons why information sharing is difficult: but it is not all bad. And there is best practice in the national security space.

- Perhaps the most striking exemplar is the UK's approach to CT. The CONTEST strategy has ensured very effective cooperation between law enforcement, intelligence agencies, local authorities and other domestic and international partners. The hugely successful collaborative intelligence effort underpinning the Olympics (of which SOCA was proud to be a part) shows what can be done given the will and resources.

- CONTEST has also managed to engage the private sector through the work of the Centre for Protection of the National Infrastructure which has greatly improved awareness of the vital role private sector security management and operations have

to play in protecting society against terrorism. Information sharing and the development of ways to use intelligence securely and with confidence, to cultivate a strategic appreciation of the threats and to alert recipients to specific threats has been vital to its success

- The Serious Organised Crime and Police Act 2005 provided explicitly for legal information exchange between SOCA and almost any partner, institution or individual and its subsequent exploitation for the investigation or prevention of organised crime. We have used this freedom extensively, not only with partners in law enforcement and public sector, but also with the private sector.

- For example, we have "washed" data from partners against our own intelligence on organised crime to help inform understanding of criminal threats and identify potential for operations and intervention; this assists financial institutions to identify accounts associated with fiscal fraud and HMRC and DWP to develop investigations into fraudulent claims;

- We share assessed intelligence with partners about key trends in criminal activity and methodology that may impact on business operations and security, enabling them to take longer term preventative measures; an example of this was the action we took a couple of years ago to persuade the wholesale banks to stop issuing E500 notes in the UK as their almost sole utility was for money laundering;

- And we share tactical intelligence –names of specific known criminals who may be a threat to a particular business or reputation; this can involve informing wire transfer companies of those subject to Serious Crime Prevention Orders and Financial Reporting Orders or alerting financial institutions to compromised credit card information: almost a million last year alone.

So far so good: but what of the future? What are the lessons we need to apply to the development of the new National Crime Agency?

- Thanks to last month's Crime and Courts Act, we are now on the glide path to the establishment of the NCA which will "go live" on 7 October. The NCA will build on

the capabilities SOCA has developed and take the response to serious, organised and complex crime to a new level. I am immensely proud of what SOCA has achieved since it was established in 2006, but I am convinced that the NCA is an important and necessary evolution. All of SOCA's infrastructure and staff will move into the new agency. For the first time, under this government, organised, immigration and cyber crime are recognised as threats to our national security, and the NCA is acknowledged to be a key part of the response. It will have broader coverage than SOCA and DG NCA will have the statutory authority to direct priorities across law enforcement agencies in England and Wales. No more will he have to rely on a coalition of the willing!

- The year until 31 March – its last – saw stunningly successful operational results for SOCA. Staff morale is high and – as the Home Secretary saw for herself on a visit only yesterday – there is great excitement about the new challenges and opportunities the NCA will bring. I thought I would conclude with a view on some of the issues the new Agency will face as it gets off the ground especially with regard to its relations with the private and commercial world.

- We are in the middle of an historic paradigm shift for organised crime. In the early C20th, it took the form of protection racketeering and black market activity. In the 1970s, the explosion of the international trade in narcotics, coinciding with increased ease of global travel, fuelled corruption, money-laundering and in some states, national instability and terrorism. Now, almost in the blink of an historic eye, the internet has opened up a whole new global digital landscape for organised crime. It is one in which national, international, and even jurisdictional borders are increasingly irrelevant and which demands a sophisticated technical response. But it is rapidly evolving and woefully under-policed: it is a world the NCA must configure itself to tackle.

- The key words are <u>economic</u> and <u>cyber</u> crime. Just as instances of technical cybercrime - hacking, malware and phishing, for example, will increase, so too will the use of the internet and cyber technologies to facilitate more 'traditional' crime. As life in general becomes ever more digital, criminals will become increasingly reliant on digital technology and the internet. But we should not lose sight of the

fact that this is still: fraud, theft and extortion. No-one ever described BC and the SD Kid as train criminals!

- The NCA will need to have the capabilities to disrupt criminal activity and pursue those who perpetrate it. It will take the lead in some areas of activity, coordinate in others and support partners in their operations. Improving effective sharing of intelligence between law enforcement and the private sector across all crime types has never been so vital.

- So what do we need to do? There are actions for government, the law enforcement community, the NCA and the private sector.

- Government needs to provide the right strategy and institutional framework to ensure that the scope and direction of activity across all parties, public and private is coordinated. The NSC focus on organised crime and recognition of the need to mobilise a whole of government response to it is it seems to me a potential game changer. The lessons from CONTEST are important here too. Plans to refresh and enhance the organised crime strategy *Local to Global,* the establishment of OSCT within the Home Office (and the policy lead on CONTEST) as the departmental anchor for the NCA, and of course the construction of powerful economic crime and cyber crime capabilities in the NCA itself are key steps.

- Government also needs to ensure that legislation and codes of practice governing exchange of information are clear and widely understood in the context of public protection and fighting crime. The Cabinet Office initiative to simplify the protective marking system may help here.

- It needs to build on the processes and infrastructure already in place to promote the flow of relevant information to the central authorities and between participants where appropriate. Those vehicles include the National Fraud Intelligence Bureau in the CoLP; the Central Police E-Crime Unit's Virtual Task Force with industry; the SARs regime; and the SOCA/NCA International Crime Bureau, which manages the interface with Interpol, Europol and international law enforcement.

- It will also need secure communications networks enabling cross agency and sector connectivity.

- But the real key to success will be the extent to which the law enforcement community, and especially the NCA, can foster effective and productive information sharing arrangements with the private sector. As well as ambition and leadership this will need the commitment on both sides to address the issues and barriers I described earlier. It will not be easy. It will require senior time, effort, and attention to detail and dedication of resources which will be hard to find in the face of what may appear to be more pressing operational and business imperatives. But success will depend on it and failure is inevitable if it is not done.

- Work is already in hand and there are examples we can draw on to give us encouragement that this will happen.

    - The Crime and Courts Act has embraced the information sharing powers that applied to SOCA, and even enhanced them in some areas. This has enabled the design of the NCA intelligence hub to place information sharing – including with the private sector – at the centre of its operating model.

    - Significant cross-departmental and private sector participation in the Economic Crime Coordination board (under NCA chairmanship) is already in progress, promoting information sharing on fraud in particular. And the Head of the Economic Crime Command will be Jeremy Outen formerly of KPMG.

    - There has been significant investment in data handling technologies across law enforcement and national security agencies, especially in advanced analytics which enables multiple datasets to be compared, researched, analysed and interpreted with a high degree of sophistication.

    - The establishment of the Cyber Security Information Sharing Partnership – Government and industry working together to build a comprehensive picture of the cyber threat and develop the best defences. This Partnership

has the potential to generate the same information sharing arrangements we have seen from the Pittsburgh based National Cyber Forensics and Training Alliance.

- And the National Cyber Crime Unit of the NCA provides the opportunity to take the partnership with industry to new levels by building on the relationships developed by its precursors.

- We need to "operationalise" flows in both directions. With information about suspicious activities (whether related to financial transactions, actual or potential frauds, cyber attacks or other indicators of criminal attack) gathered centrally and shared, placed alongside intelligence derived from investigations and covert sources of suspected and known criminal activity, and applying data analytics to interpret the significance of all this data. We would then be much better placed to design and prioritise our response.

So to conclude: the transformation of technology is both a threat and an opportunity. Much is going on across government and law enforcement, but much remains to be done. Frankly, we are hugely under prepared!

We may be very good at tracking international drugs and money laundering conspiracies, intercepting illegal commodities and dismantling organised crime groups. SOCA has had great success in putting criminals enjoying multi-millionaire lifestyles from luxury properties around the world behind bars: and taking their assets. I like to think that once we have got onto the trail of such a group – like the RCMP – we always get our man (and occasionally woman). But that is not going to be enough.

We need now to recruit, train and equip our staff to fight crime involving transnational flows of data rather than just drugs. This is not something that law enforcement can do alone. The range and depth of the NCA's partnership working with the private sector – but also with others such as academia – will need to grow beyond that of SOCA. Both parties will benefit: the NCA by enhancing its capacity to fight crime and protect the public; and the private sector will be better equipped to understand, identify and counter criminal threats to business.

Mutual trust will be the key. Better data sharing will be the result, information sharing will be the glue that binds us together, and a more effective attack against the criminal threats that plague us the outcome.

If the NCA and law enforcement generally is perceived as a black hole for information – it will have failed. But it is not only data that we need to share better to banish the black holes from our universe - ideas, capabilities and people are equally important. To return to my first message - this is very easy to say and has been said many times before. This time we need to make it so. The protection of the public – including all of you – depends on it.