JOHN HARRIS MEMORIAL LECTURE

25 JUNE 2003

Tonight I was only going to talk about technology and forensic science, but on the way in Peter and Sir John and I were talking and we recollected that we are still using sniffer dogs, and we are using fish, and we are using all sorts of animal technology, in order to help us catch criminals and we ought to acknowledge them. Mine is under the table, so if there is any bother tonight I shall make sure she turns – as she did yesterday when I had the privilege of being with the Prime Minister and the Foreign Secretary to welcome President Putin, with the Queen and the Duke of Edinburgh – when a sword was withdrawn at the end as they dismissed the guard. I don't know whether it was the sword or the bearskin, but the dog took deep offence and barked at it, so at least I know I am well protected.

I want to say a word or two tonight about the overview of the way the world has changed beyond all recognition. The scope of communication technology that is available, the way in which this is used globally, has completely transformed what is available to all of us here tonight engaged in law enforcement, in detection, in prevention. But it has also transformed and made available those same technologies to organised criminals.

We used to have a slogan when I was in local government, which was to "Think Global, Act Local". I think this is an appropriate slogan for this evening in terms of taking in the breadth of change, the enormity of what is available, the way organised crime has developed across the globe, and the way that boundaries mean nothing to those who are able to use the resources available to them to face us with the challenge of new ways of committing crime, and new ways of bringing insecurity.

We need to be able to develop that alongside the way in which we tackle crime on our streets so that people feel safer and are safer. The opportunity to commit crime being reduced by the use of technologies and forensic science. But at the same time to recognise that there is an interchange between the work of the organised criminal and the way that others feed off that at the very local level. So we too have to be at the cutting edge of technology, of methodology, of the ability to switch and change rapidly in the way that organised criminals do.

I am involved, of course, with a number of hats on, with organised drug trafficking and what that means in terms of availability on the street. I am also involved with the issues around the trafficking of people, both in terms of asylum and prostitution, and it is amazing how the same criminal gangs, using the same networks, are able to switch from one form of trafficking to another. They are able to switch routes in terms of the way in which we attempt to close down particular lines. This is particularly true of drugs. And the way, therefore, that you see the closure of a particular supply route immediately opening up new opportunities for them elsewhere.

We have to be as agile, as quick afoot as they are, in terms of the way we tackle this, the intelligence we use. But we also have to be as quick on the uptake in terms of using the technologies that are available to us.

We are therefore challenged by the way ahead in terms of not only being on top of the game as it is at the moment, but also asking the questions, putting in place the provision of research, opening up the debate in terms of the challenge of tomorrow.

Intelligent, rational debate – not yah-boo about the very difficult issues of balancing individual rights and freedoms versus our mutual security and safety. Protecting ourselves individually from intrusion and the erosion of our rights, is and always will be paramount – but balanced by common sense in terms of the way the latest science is used by criminals who respect no human rights, or personal protections, and know no boundaries in terms of what they are prepared to do.

DNA is an obvious and classic example of what has changed over the years. I just thought tonight that I would illustrate that I am not afraid of this by showing you my own DNA profile, which I acquired at the forensic science service laboratories. It may not mean anything to me, and I doubt if it means anything to you, but I just thought I would illustrate that a few squiggly lines can make the difference between getting my identity right or wrong.

It is of course true that we are developing all the time methods of achieving and understanding, whilst at the same time securing people's confidence that we use it properly. Therefore when we are, as we are doing, changing the way in which this can be used, by ensuring that at the time of arrest we can take the DNA and have the fingerprints available, rather than when we have already determined who we believe the criminal to be at the point of charge, we can transform the technology and the science from being an affirmation of what we have already understood, into being a key tool of understanding what we need to know in order to be able to find the criminal.

That is a substantial difference. Not in the technology, not even in its availability, but in its usage. It is in that usage that we can make real the available tools at our disposal.

So tonight I want to talk about three key areas. Exploiting existing technology and its usage more effectively – that is about whether we are really getting to grips with some very simple technology and using it well, in the way that is true of the rest of the world outside policing and law enforcement.

Secondly, the identifying of both the threat of new technology and science to us, and the opportunities it brings to get on side and to use the two sides of the coin for our benefit. It is about looking to the future and the opportunities that it gives us without fear.

The third is to be much better prepared to be able to respond more quickly - in a way that I was describing a moment ago - to all sorts of threats around us. Including the terrorist threat and the organised crime that is often funding and facilitating that, including of course financial crime, which has been an absolutely key element in terms of what we know about the organised terrorist networks.

So let me take the first one. The issue of DNA is obviously paramount here. The use of a technology based on science that was first revealed 50 years ago this year. We are celebrating that 50 year anniversary, and the way in which that has been sophisticated since to make it more readily available and more useable.

I mentioned the Bill and the way that fingerprinting has developed. It is only recently that we have had, through Livescan, the ability to be able to use fingerprints quickly and easily and electronically, rather than the old methodology when I first went into a police station as a Member of Parliament and had the ink pads and all the mess, the time it took, the trouble it was, the difficulty and the unreliability. This is now

gradually being replaced by pretty basic technology in terms of what the private sector would use, but absolutely crucial in terms of making a difference. And for DNA itself, the two millionth sample on the database available in a couple of weeks time. I don't think we are going to ask the person to celebrate their two millionth sample , not least because we may not have actually proved their guilt at the time and they wouldn't thank us for it.

But it raises all sorts of issues. We will be debating in July in the House of Lords the issue about double jeopardy and whether we should be able to, having found new scientific evidence – new evidence that is – actually reopen those cases (with the triple locks that we are putting in place to protect the innocent).

There are some famous ones for those of you who are very old. I was very interested a few weeks ago to hear about Hilda Murrell, the old lady as she was in Shrewsbury, who we all believed (those of us who were in CND anyway believed) had been done over by who knows in the Secret Intelligence Services (one of which of those services I am now in charge of, so it's a strange old world that we get into). And would they have done it? Of course not, I can assure you that they wouldn't have done anything of the sort.

Anyway, it is very reassuring to know that the possibilities exist 30 years on of finding out what really happened. It is true of the families in South Wales who can at last have some peace, having discovered who did kill the three teenage children, and having exhumed the body being able to use DNA effectively.

It is true in relation to being able to get a criminal who committed rape 15 years ago, when two years ago he was picked up for a £10 theft of groceries, and the DNA was now able to be matched in a way that enabled us to find the perpetrator of a rape. Not only important for those offended against, for the victim, but actually crucial as we know for those who are likely to be the future victims in terms of repeat offenders.

So there are real areas here of self-protection, of justice being shown to be done, of brining peace and comfort to individuals and communities. One thousand individuals a week, 2,500 matches because obviously many individuals are matched to more than one crime, which is transforming what we can do.

70% can be turned into detected offences we believe. At the moment it is just under 50%. I am afraid the rates of usage and proper detection are very low in some police force areas. It was as low as 10% until recently. It is 17% at the bottom end, over 90% at the higher end, which means that some forces are using the facility extremely well and effectively, with proper sampling at site at the point of detection and at the site of the crime. Others are doing very badly indeed.

So I think the challenge of the usage of old technology, as well as new, is the ability to sample, to use experience and expertise, with the way in which we can develop non uniformed staff to learn the trade and to be able to do the proper sampling on site, the processing of those samples, the careful matching. The speed with which we expect each element of the process to be dealt with, including the Forensic Science Service, where at the moment we have an average turnaround date of 14 days, with very much longer turnaround in some areas (far too long in terms of being able to move quickly to arrest and to charge).

In the West Midlands where we have had a fast track system, there has been a phenomenal improvement both in the usage of the science and in the gains it has made, particularly in dealing with repeat offenders. Burglary is a good example –

20% improvement in terms of cutting burglary rates in the West Midlands. A tremendous effort has gone into making the technology usable.

Now we need to move to the use of newer technologies to be able to detect all kinds of crime, including vehicle crime, with ANPR being gradually made more available. With the NAFIS fingerprinting system. With the better use of CCTV, which has a video in it rather than empty cameras, because that has been a problem, as well as the inadequate use of the cameras, with video technology used so badly that it could not be used in court. Where it is available we have had the most enormous turnaround rates of people pleading guilty.

All of this technology is helping to get both the lawyers to co-operate and the perpetrators to admit their guilt at a much earlier stage. I was speaking at a Law Society Dinner earlier this year and I thought I was doing very well until I made the mistake of making a remark which upset the table of barristers who were visitors there that night, by saying that we wanted to get rid of the syndrome of late guilty pleas because it was costing us all a fortune. I discovered from the boos that emanated from the barristers' table, which only reinforced all my prejudices you'll understand, that I was obviously taking a fortune away from them by speeding up those guilty pleas.

We have also got, of course, the use of technology worldwide. Operation Ore has had some difficulties, but it is a tremendous example of data sharing and the use of technology to be able to ascertain what was taking place in the awful crimes around pornography and the misuse of children, as well as of women. I hope we will be able to sophisticate that still further so that criminals will know that because of the use of technology, wherever they are in the world, whatever their crime, they will not be free from detection and the sharing of that data.

We have Airwave and the use of basic communications technology on the one hand, and believe it or not the introduction of basic pagers to ensure that people don't have to be in court when they don't have to be, on the other hand.

We are miles off using old technology, as well as developing new, to be able to transform what the police can do. Their availability on the streets because they don't have to be tied up for hours in the station. The way in which laptop computers can be used (that are commonplace elsewhere) with proper training for the police. They can be linked into the mainframe, so that from the moment of arrest through to the court hearings and beyond, we can use the same database. Rather than constantly transferring information - often still in the police service by writing it up in books - and then having it transferred onto the computer.

We can cut down the bureaucracy and the time wasting, and we can free police time to do the jobs that they want to do. Giving them the tools so that the visible cops, the real cops (not the Robocops as one of my officials rather crudely put it when I was talking to them about preparing this speech), or as John Prescott would say "traditional values in a new setting".

None of the old techniques have to go away. The thoroughness, the proper investigation, the asking of the right questions, training people to do the detection. The observation that actually spots the things that technology can't spot. Or use the technology to spot the things that the human eye may not be able to spot. These are all about training people to identify, to use the technology better, to be complete in what we do in those day to day tasks.

And, of course, even the better use of hand-held communication and old-fashioned mobile phones to make the job better.

The scale is very different. The techniques can often be the same. But we do need to ensure that we are using them well and we are facing the future with courage rather than people actually fearing to use that technology.

We need the industries around us – and I am very glad that our sponsors are here tonight and are able to affirm that there is a new beginning in terms of reaching out, using the security industries more effectively, co-ordinating with what they are able to do and how they can feed into the family of policing that we are developing.

Not just with the security industry, but also with commerce, with business, with finance, to get it right. We are talking with the financial institutions about making sure that the data we collect is not so indiscriminate that it is unusable, that it is not so burdensome that they feel unable to co-operate in working with us, that we can get right what we ask and then how we analyse and use it better.

We are working with them – as with the experiment in Northampton – to research how best to tackle financial fraud. The four digit PIN number which is being trialled there in terms of the banking industry in a way that has been commonplace in other European countries, including France, for some time. The task of halving plastic card fraud as we call it within the next three years.

And I was interested in a recent visit to Barclays Bank to learn of the new equipment that is soon to be disseminated, and I wanted to link that with what we are doing inside the Home Office with the national hi-tech crime unit and the dedicated cheque and plastic crime unit (that takes some saying, it's a good job I haven't got false teeth) working with the industry in looking at and making real the commitment to overcoming what is a massive and growing problem for all of us as individuals and for the industry itself. It takes technology to tackle it, and it is of course because of technology and because of the way in which the plastic card can be used, that we have the fraud in the first place. This is why I mentioned the two sides of the coin – the technology makes the crime easier, the technology we can use needs to overcome the crime. Working together we can identify how we can tackle fraudsters more effectively, and I am in discussions with Cabinet colleagues in relation how we can avoid the theft of our identity and the way in which our identity can be used in terms of criminality. Biometrics will help us do this, as will, I believe, the effective use of identity cards, but with all the necessary safeguards that all of us would want for ourselves.

Challenges of the computer, of internet crime, of associated pornography which I mentioned a moment ago, are with us daily. Therefore, vigilance and work – linking all of us in the community with the potential to help the police do the job – will be crucial. Biotechnology and nanotechnology will also transform what is happening around us.

Which brings me really to very much the cutting edge of the future. The synthesising of production of drugs is a good example, but it can be of other products as well. Of stealing intellectual property. Of nanotechnology , with all the potential for miniscule machines as well as hardened toughening of the resilience of products, transforming not only what we can do to protect the individual, of target hardening, of the way in which we can protect our property in the future, but also the real dangers of sophisticated criminology.

Think of the way in which intrusion using nanotechnology could transform the ability of criminals to open up our property, commercial or domestic, in terms of intrusion. Not just remote control in terms of bugging and intruding on our privacy, but remote control being able to open up avenues for criminality. Michael Crighton's 'grey goo' may be fiction, but as a politician I am all too well aware that fact and fiction are very close indeed on occasions.

So all of this opens up new possibilities for us to counteract crime, to deal with terrorism, but it also opens up terrible avenues in terms of what can be done to us.

I want to set this in the context of the fact that there has been enormous social change. Crime changes the availability of the potential for committing crime and the opportunity changes, and so does our reaction to crime as our social life changes. Those close knit communities, those Neighbourhood Watches, that were actually part of the very thrust and core of the neighbourhood disintegrated as we moved apart, as housing changed, as family mobility changed. And yet we have to catch up with that in new ways without unnecessary intrusion.

Relationships between people and the police have changed. The developments that we are putting together reflect that - with the National Centre for Policing Excellence, with the work of the Association of Chief Police Officers, with what we are doing in the Home Office with the Police Scientific and Development Branch. These are changing the way in which we have to do our business. With surveillance, with protective equipment, with the chipping of goods in industry, with the target hardening and security in neighbourhoods. Even with the methodology for stopping faster and faster cars. They are all part of their business and we have to adapt quickly to changing circumstances around us.

And of course on the international crime and terrorism front, we are having to change daily to what is facing us. The greater sophistication, the networks using technology and satellite, the investment we need to make in tackling CBRN in the radiological protection that is necessary, in a way that was never thought in the past to be a possibility.

And of course the detection and the exposure to weaponry is something that all of us are having to take seriously every day.

All of this changes the nature of that attack. We have changed from the way in which traditionally armies met and war was conducted, as we saw in Iraq, to greater and greater sophistication. We see that in terms of the way in which we have to change our reaction to the use of technology and to the use of the terrorist threat. In the past the army was the threat, today we see the danger of the suicide bomber. In the past we would know where the organised criminals were, and we would know and be able to identify the gangs. Today, asymmetrically, an intrusion into a computer can disable the very network and technology designed to protect us and to stop that happening, but is one individual as a hacker that can transform that rather than an identifiable group.

All of this brings entirely different challenges, both in terms of the basic policing operation, the security and intelligence services. I just want to conclude by reflecting on this.

Last week I launched the new Joint Terrorism Assessment Centre bringing together the analysis and assessment of data from the intelligence and security services here and around the world. We were doing so to update the capacity of our intelligence

services to be one step ahead. We need to do so with the criminal fraternity (as the old fashioned phrase had it) with the National Criminal Intelligence Service and its links to the National Crime Squad and the 43 forces in England and Wales. We need to update the way we work on our border controls and with Customs and Excise.

In the end, it is intelligence in its widest sense, in its most profound usages, that will be the greatest security we have. Because prevention always has to be better than prosecution. It is patently true in terms of terrorism. Firstly, because terrorists, as with suicide bombers, are not often available for prosecution and don't care if they are. So it has transformed the nature of the purpose of prosecution, which of course has always been to apprehend and therefore to deter, to ensure that the detection becomes the greatest strength we have in deterring people from committing crime, and the punishment in terms of not just retribution, but the messages and signals we send in enforcement.

But actually in the new world prevention is critical to ensuring that the crime doesn't take place in the first instance, and if it does that we know what network is behind it, and we can crack that for the future. It changes that relationship between prevention and prosecution, and of course with it the debate around our protection, but also the balance of individual versus mutual rights.

And that is so crucial to the future. If we are prepared to use technology to help the witness come forward, because we can protect them from identity themselves in terms of the threat that they will face, by the use with them of better surveillance (not instead of them). If we can protect the victims better in the future so that they in turn will be co-operative in working with us, in bringing people to book, and to bearing witness themselves in court. If we can get the police to able to use the technology effectively in the 21st century, then we will transform what is available to us as a community in what we are doing in securing our wellbeing. Prosecuting those we have to. Enforcing the law and taking on the re-offender and the perpetual criminal.

It is a tremendous challenge. I think we are just at the tip over, the cutting edge point. I think that if we can get this right, and all partners engaged in this can work together, we will have a safer and better community in which to live, and a police force able to use their time and energy more effectively in terms of reassurance, visibility and availability, because the technology will have helped them and those working with them in the civilian services to do the job effectively.

It is a tremendous challenge, but it is also a tremendous opportunity. It involves teamwork as never before, and I would like your views and opinions – now or over the weeks ahead – in terms of both the challenge and the dangers and how we take them on together.