Transnational organised crime as a national security threat

Keith Bristow QPM, Director General of the National Crime Agency

George Washington University, 29 January 2015

Ladies and gentlemen, good afternoon. It is a pleasure to be here, and my thanks to the staff at George Washington University - and particularly to Professor Lemieux - for inviting me to speak to you today.

Organised crime is a transnational phenomenon which demands a coordinated, transnational, response. It is also increasingly recognised - at the highest levels within government - as a threat to the national security of our countries.

Over the next thirty minutes I aim to set out why I think that recognition is fundamental to our ability - as partners - to ensure the response to organised crime remains proportionate, and effective.

The UK's National Crime Agency has been operating for over a year now, and we have already conducted multiple successful operations with our US law enforcement colleagues. I appreciate, though, that not everybody here will be familiar with the NCA, so let me briefly describe what we do.

The NCA is the first agency ever to be given responsibility for leading the UK's fight to cut serious and organised crime. That represents a significant change in the way the UK coordinates and prioritises its law enforcement activities. We are intelligence-led operational crime fighters, who carry out our own investigations, support the investigations of our law enforcement colleagues, and coordinate joint activity. The UK media like to call us the UK's FBI. I don't object – this is helpful shorthand for a UK audience, despite some fundamental differences. We don't have a federal system as you do, for example. We don't have a counter terrorism policing remit – although of course we work closely with our partners in the space where terrorism and organised crime overlap. We are not police, but we work alongside the 45 regional UK police forces, and with other specialist national agencies. The NCA has an international network, with officers based in over 40 countries worldwide, including the US, and covering around 120 countries in total. And we hold specialist capabilities, which we share with our partners. This means that high end knowledge, tools, and techniques – for example in the fields of kidnap and intelligence collection - do not have to be retained separately by every one of the UK's regional police forces. Our partners in the UK security and intelligence agencies also share capabilities with us, which we use to support our own operations and those of wider law enforcement. As Director General of the NCA I have the power to direct the chief officers of police forces and law enforcement agencies in England and Wales to undertake specific operational tasks to assist the NCA or other partners. That power represents a significant shift. But since the NCA began operating in 2013, that power of direction has never been needed. Perhaps just the fact that it exists – and that I would use it if I needed to – is what matters. But in reality, good partnerships are achieving the same result – which is that the UK's law enforcement agencies are joined up, as they have never been before, to maximise the effectiveness of our national capability. This enables the UK – and indeed our international

partners – to make best use of collective resources, and so have maximum impact against organised criminals, both domestically and globally. At a time of global austerity, this approach also has clear benefits for using our collective resources not just effectively, but efficiently.

The NCA is, in part, a result of the evolution which takes place as criminal threats change, and policing and law enforcement changes alongside them. The law enforcement model in the UK has reflected for some time the fact that criminals – particularly organised criminals - do not neatly contain their activity within geographical and jurisdictional boundaries. Five decades ago, the UK set up regional crime squads, in response to the activity of organised criminals across police force boundaries. When criminal groups began operating on an increasingly national and international basis, the UK responded in the late 1990s by creating the National Crime Squad and the National Criminal Intelligence Service. And in 2006, the response developed again, with the creation of the Serious Organised Crime Agency, which had a specific focus on tackling high end criminal activity. But SOCA did not have a national leadership role, and it operated in an environment where the end-to-end response was therefore not always coordinated effectively. So the NCA is the next stage in a tradition stretching back 50 years. It is the logical law enforcement response to an evolving criminal threat.

This evolving response has been mirrored by a corresponding recognition, at the highest levels of government, that organised crime is a national security threat, whatever the nation. In the UK, for example, that recognition is enshrined in the government's Serious and Organised Crime Strategy, which informs the NCA's operational responses.

Organised crime attacks our way of life, undermines national institutions, and directly threatens the safety of thousands of our citizens. But the breadth of its impacts is still not understood universally, in the way that the impacts of other more 'established' national security threats are. In part, this is because they are not as visible. More often they are insidious, creeping, and corroding. They rot the wood beneath the painted surface. By the time something happens which exposes the rot, a lot of damage has already been done. At the same time, how we perceive the proximity of organised crime can distort our appreciation of its dangers. We understand the danger we face from a man in the street with a gun. But, standing in the same street, do we understand the danger we face from an organised criminal based in Albania? The damage can be just as great, and the risk is no less real. But the perceived lack of proximity means we see it as less of a threat. Organised crime has implications for health, welfare, taxation, education, social cohesion, and more. It affects the very fabric of our societies, at all levels. I believe it is in all our interests to ensure that the understanding of these impacts continues to grow. Because there is huge value in formulating our approach to organised crime alongside the approach to other national security threats. Let me explain why.

Some of the impacts of organised crime, and its transnational nature, are self evident. The heroin injected on the streets of Liverpool is from Afghanistan. The cocaine taken at middle-class London dinner parties is from Colombia. The new psychoactive substance that kills teenagers in Manchester is produced by chemists in China or India. Criminal money is laundered in the UAE. The boiler

room scam that robs the elderly in Birmingham is perpetrated from Indonesia. The immigrants held in slavery or sexual servitude in leafy suburbs or on Scottish fishing boats are from the Philippines or Vietnam. The cyber crime that threatens the bank accounts of those in Cornwall originates in Russia, and guns are imported from the USA to rob or kill.

In the UK we estimate that, every year, serious and organised crime is responsible for the deaths of several thousand UK nationals, and that it costs the economy over 36 billion dollars. Some impacts are only beginning to be understood fully though – particularly in the areas of economic crime and cybercrime, including the online sexual exploitation of children.

Part of understanding those impacts better is being able to quantify them - but that in itself is challenging. In the case of economic crime, for example, a huge range of activity can potentially meet the definition of organised crime. The vast majority of criminal enterprises - however complex, whatever techniques they employ or commodities they involve – have money at their root. Criminals want to make it, and keep it, for their status and lifestyle. They need it too - to bankroll, reinvest, and keep their criminal networks functioning. And in order to keep it, they need to hide it, and launder it. That means many of the economic crime threats, described by the NCA in our National Strategic Assessment, underpin a far wider spectrum of criminality, from cyber crime, through to drug trafficking, and modern slavery. And it means too that the impacts of those cross-cutting threats can be far reaching. The UK has a leading role in developing the international standards to tackle money laundering. Despite that, the scale of money laundering is a strategic threat to the UK's economy – and to its reputation. Many hundreds of billions of pounds of criminal money is almost certainly laundered through UK banks and their subsidiaries each year. The high transaction volume, language, developed financial services industry, and political stability of the UK, makes our financial system particularly attractive to money laundering – despite the measures to identify and stop it. The involvement of a small minority of complicit, negligent or unwitting professionals in the financial, legal and accountancy sectors, also facilitates money laundering – and unfairly damages the reputation of the large majority of professionals in those sectors. Losses through fraud by individuals, and by the private and charity sectors, now affect a large proportion of the UK population – and are growing. The National Fraud Authority's annual fraud indicator 2013 showed losses of nearly 32 billion dollars for the UK private sector, over 30 billion dollars for the UK public sector, and over 13 billion dollars for individuals. There is no question that there are areas of economic crime that traditionally law enforcement and government have not understood well. Some crimes, like high volume, low value, mass market fraud, haven't met certain thresholds, or have made it challenging to secure convictions. Others, like corporate fraud, have seen an inconsistent response. All this has presented criminals with opportunities, which they have been quick to exploit.

The challenges we face in trying to quantify the scale of economic crime also apply to cyber crime. The online environment has brought law numerous investigative benefits. But it has also revolutionised how criminals interact with each other and with their victims. This has fundamentally changed what law enforcement must do to keep people safe and bring criminals to justice. For example, the NCA and its partners have seized over ten thousand digital devices

in a single operation, targeting people who access indecent images of children online. Some of those devices contain *terabytes* of data, which need to be forensically analysed. This means several months of work by digital specialists. Anyone who is active online is a potential victim of cyber crime. And as individuals and businesses we don't always do everything we can to protect ourselves. In our new interconnected world, people voluntarily share the kind of data that, in the past, would have been kept under lock and key in a file or desk drawer. Even if it isn't given up knowingly and willingly, that data is vulnerable to intrusion and theft. Not long ago we were told never to write down our passwords for online accounts. The result is that we came up with ones that were easy to remember – and easy for automated programmes to break. Now the advice has changed. Perceived wisdom is that you are safer creating complex and hard to remember passwords, and writing them down somewhere on a piece of paper in your house. In other words, it's more likely your passwords will be de-coded by online criminals than that your house will get broken into. The idea of Russian organised crime groups selling stolen data to Nigerian fraudsters would simply not have occurred to law enforcement officers twenty years ago. The groups were culturally different, geographically separated, and unlikely to mix. The internet has made that criminal interaction possible. The implications are not only personal and domestic. Every business with an online presence is exposed to risk. A survey of British retailers showed that 79% of those who responded had suffered a cyber attack in a single year, including denial of service attacks, malware, hacking, and 'scraping', where criminal web sites masquerade as a retailer's site. Anti-virus providers generally conclude that cyber attacks globally are currently numbered in the billions - and increasing. Symantec reported blocking 5.5 billion attacks globally in 2011, and saw a 42% increase in targeted attacks in 2012. A UK newspaper reported last year that, in one month, there was a 370% increase in high-bandwidth, high volume distributed denial of service attacks on the UK, and that those attacks had increased their power by over 200%. One of the reasons cited was the easy availability of 'toolkits' which enable criminals to launch attacks from just a handful of servers. The cyber security company behind the findings said "Anyone can go out there and generate these really large attacks with really no skill sets. It has essentially become a service". Cyber crime is evolving more quickly than any other threat. It will continue to do so. I am sure the small minority of the next generation which is inclined to criminal behaviour is more likely to be operating in an online environment than smashing windows and grabbing television sets. This is an era when intelligent, well-educated young people perceive that the wealth gap is widening, that job opportunities are harder fought for, and that the burden of caring for older generations will fall heavily on their shoulders. Throughout history, feeling disenfranchised and disempowered has driven young people to demonstrate their frustration – and now cyber attack is a new tool by which they can do that. Indeed, however it may have mutated in the years since, the hacktivist group Anonymous began life as a protest movement.

In the case of child sexual exploitation online, high speed internet access has enabled the real-time live streaming of child abuse to order. Individual offenders can target multiple children in different time zones, simultaneously. From the anonymity of a computer, the shadowy loner we were told, as children, that we should not talk to, can now masquerade as a child himself. The online environment makes it easier to seek out potential targets. Children post

information about themselves online freely, and abusers know what to look for in a profile to determine how vulnerable that child might be to victimisation. And online networks enable the sharing of indecent images of children on an industrial scale, re-victimising a child every time an image is shared.

These are tangible, and often life changing, impacts. The sheer scale of economic crime and cyber crime makes them national security threats. But there is also a crossover between organised crime and other national security threats – including terrorism – which reinforces my view that the response to organised crime cannot be considered as somehow separate and distinct. We need to collaborate and share capabilities with agencies looking at other national security threats, and use the intelligence we hold on all national security threats, to inform our response across the piece. The biggest cocaine trafficker in the world is FARC. Hezbollah launders money and engages in global criminality. The Taleban raises 45% of its income from opiate trafficking. Al Qaida in the Islamic Maghreb, and others, make money from kidnap for ransom. This is not new. In the UK the Provisional IRA engaged in extortion and fraud to bring in revenue. And some of the same financial transfer systems used by organised criminals to launder money in the UK are used by terrorist groups, both domestically and overseas.

In some parts of the world, organised crime exploits or exacerbates international crises - trafficking people who have been displaced from their homes by violence, encouraging the flow of weapons, or seizing control of vulnerable states to use them as a base for criminal activity. In extreme cases, we see what we might call 'hybrid insecurity', where insurgency, plus organised crime, plus terrorist activity, added to social and economic pressures, creates instability which has transnational implications. Our approach to Afghanistan – for example - can therefore have a real and lasting impact in terms of crime at street level, certainly in the UK. And failure to act can have real and lasting damage in the same space. Our chances of success are limited further if we fail to address the potential for corruption to take root - especially in fragile or vulnerable states when instability leaves a vacuum. Corruption is one of the most pervasive and most damaging manifestations of where organised crime meets national security. We already have the UN Transnational Organised Crime Convention, which considers corruption and its impacts. And 2015 will see agreement on the post-2015 Millennium Development Goals at the UN. This matters, because goals which address organised crime – in particular, corruption - could be accepted by all states. Former Secretary General of the UN, Kofi Annan, was succinct and articulate in his description of the global implications of corruption: "Corruption undermines democracy and the rule of law, leads to violations of human rights, distorts markets, erodes the quality of life and allows organised crime, terrorism and other threats to human security to flourish. Corruption hurts the poor disproportionately by diverting funds intended for development, undermining a government's ability to provide basic services, feeding inequality and injustice and discouraging foreign aid investment". This is a devastating list, and every single person here will be concerned about at least one of the things on it - probably several of them. That is why the NCA's Economic Crime Command is providing strategic leadership and coordination to UK law enforcement efforts - and is working in partnership globally, including with the FBI - to tackle this insidious crime, which denies entire nations the ability to fulfil their potential.

So what more do we need to do? If I had to choose a single message today it is that, for me, partnership is at the heart of the answer. I am immensely proud of the work my agency has done with US partners – including the FBI, ICE, the DEA, and AFT - to tackle criminality and to bring down criminal marketplaces. In June last year, the NCA was one of the FBI's global partners in an operation against the Go Zeus and Cryptolocker malware. Law enforcement activity in eleven countries around the world disrupted the system used by infected computers to communicate with each other. We weakened the network enough that members of the public had an opportunity to put better protection in place. It was a groundbreaking achievement which a single agency could not deliver alone.

The NCA has been designed specifically to work in partnership – it is one of the things which distinguish it fundamentally from any of the UK agencies which went before it, and it is one of the reasons I believe the NCA will remain adaptable, relevant, and effective over time, where its predecessors did not. Those domestic and transnational law enforcement partnerships are crucial to our collective success - but mean that, undeniably, policy and legislation in one country impacts upon others. I think that is especially true of the US and the UK. Jim Comey and I have both spoken publicly about the threat to our response should we lose capability in terms of communications data and interception of communications. The data is there - but without access to it, certain prosecutions are simply not going to be possible, for example in areas like child sexual exploitation. I am not here today to promote the case for more powers. There must rightly be a public discussion about security and privacy. But I do not believe that this is necessarily about freedom versus security – indeed, I do not believe that the two are mutually exclusive. My children have the freedom to play by themselves in the park if law enforcement has been able to effectively target potential predators. My children have the freedom to go online and use social media if there is a law enforcement presence in that space which makes it safe for them to do so. Communications data, and the ability to acquire it, in necessary and proportionate circumstances, gives us more freedom. We can be free to go about our daily lives. However this debate plays out though, law enforcement needs public trust and consent to operate. Our police forces and agencies must be visible to the public in a community sense, representing the diverse nature of our society, and not – as has been reported in the US media – as a paramilitary force.

But recognising organised crime as a national security threat means the partnerships now go beyond law enforcement. Those with the private sector are becoming increasing vital. In the UK we have seen genuine innovation, within the economic crime environment, through the creation of the Financial Sector Forum. This unique development exemplifies the partnership approach we must take together if we are to succeed together. Chaired jointly by the Home Office, the NCA and the British Bankers' Association, the membership of the Forum includes banks, regulators and other financial institutions. The Forum's aim is to improve information sharing to tackle some of the most damaging and hardest to reach criminals operating in the UK. I don't think it is unfair to say that, historically, there has been a degree of mistrust between law enforcement, regulators and the financial sector, so it is a tribute to all those involved that this progress has been achieved. At the same time, the UK government's relationship with, for example, financial institutions and companies like Google, is

conceivably becoming as important as its relationships with some European countries. Indeed, businesses like Walmart have a greater equivalent GDP than some European countries, and all the influence that comes with this.

Partnerships with non-state actors and international institutions are also becoming increasingly relevant. The Internet Corporation for Assigned Names and Numbers, for example, is hugely important in the cyber landscape, as is the Financial Action Task Force in the financial one. Law enforcement engagement with opinion-makers and shapers, including universities like this one, think tanks and institutes, matters too. In the UK, the Royal United Services Institute and the International Institute for Strategic Studies have involved themselves heavily in organised crime debates over recent years. Law enforcement needs to do all it can to engage with, and learn from, those partners who are undertaking research in areas that matter to us. Multilateral relationships are useful, but can dilute the response, through expediency or consensus, when there are difficult choices to be made. Nevertheless, bodies such as NATO, and the Organisation for Security and Cooperation in Europe, can play an influential role where organised crime threatens a nation's stability. NATO's maritime commitments in the Mediterranean, and in the Gulf and Indian Ocean, are important to us in tackling trafficking – whether that is of heroin or people. NATO's plan for post-2015 Afghanistan matters to us. And NATO's cyber team is getting more and more active in the sphere of cyber crime. The Organisation for Security and Cooperation in Europe has a law enforcement remit, tactically, through deployments overseas, and strategically, through its Strategic Policing Unit in Vienna. It also produces an annual assessment of the organised crime impacts on Europe. Law enforcement needs to ask how it can work with these partners to best promote security in Europe.

One area where the NCA and its predecessors have found particular value is in joining or forming transnational coalitions and taskforces to tackle crime. Whether it is the National Cyber Forensics and Training Alliance in Pittsburgh, the Interagency Operations and Coordination Centre in Afghanistan, the Organized Crime Drug Enforcement Task Force in Washington, EUROPOL in the Hague, Interpol, or any of the many others I might name, engagement in taskforces has been of clear mutual benefit. And the UK's key partner in these ventures is often the US. For a minimal investment, we have shown ourselves adept at building coalitions, encouraging partners to join, and having real effect against a threat - whether that's cocaine trafficking, Afghan heroin, cyber crime, or piracy. We share the risk and reward - as we share the intelligence - for maximum benefit.

Going forward though, this read-across into the national security picture raises important questions for law enforcement, which we cannot duck. Is it more beneficial, for example, to form bilateral relationships with the countries with whom we have most in common, such as the US, or with those who pose the biggest threat to us? How do we persuade politicians that law enforcement diplomacy, on an apolitical subject like organised crime, can succeed with politically challenging nations, where more traditional approaches have failed? We need to consider the point at which partnerships intervene to prevent a threat developing. The Arab Spring is seen as a triumph of democracy and the will of the people, but previous experience – in the former Soviet Union, the Balkans, and Afghanistan – shows us that when autocratic regimes collapse, the

vacuum in law and order means that within as little as two years a country will become a serious crime threat for the UK. In developing our operational response to that challenge, there is danger if we focus on arbitrary targets. By giving priority to criminal justice outcomes, for example, we may intervene too late, after the harm has already been done. So is it acceptable to undertake early intervention, before a UK threat and a law enforcement problem materialise, or do we wait, until the threat has arrived on our doorstep? How do we prioritise the promotion of democracy and human rights where there is a tension, or even a conflict, with issues of our own national security? For example, should a human rights issue prevent us engaging with another nation to find sexual offenders against children, murderers or kidnappers of British nationals, for fear of how the perpetrators may be dealt with?

In finding answers to those challenging questions – and others – and in delivering for our governments on national security issues, I am quite clear that the one thing we must do is engage. We need to do business with the politically and reputationally challenging, and with the ungoverned, unstable, fragile and fractured parts of the world. The key difference for law enforcement is that we do it apolitically, having mitigated as many risks as we possibly can. But equally, even in politically difficult places, part of the value is simply being there. Results and outcomes will oscillate over the years, but there are certain posts where we should hold our nerve and maintain our presence, in order to achieve change.

Organised crime is transnational, but how we tackle it as global partners has a direct impact on the streets of our cities, and on the people who live there. Organised crime attacks our way of life, undermines national institutions, and directly threatens the safety of our citizens – whatever our nation. It is a threat to our national security. The public expects to be protected from national security threats. It knows what it expects in terms of protection from terrorism, and the acts of unfriendly states. I am not sure the public yet knows as clearly what it expects in terms of protection from organised crime. And unless we help people to better understand the impacts of organised crime, its status as a national security threat probably remains fragile. This matters, because it is in all our interests - and particularly those of the people we are charged with protecting – to ensure we maintain that status. Recognising organised crime as a national security threat generates common language. If states A and B both identify a threat to their nation, that threat becomes a shared transnational concern. It means policy makers, across a broad range of policy areas, give it the priority they should. Which means that we can mobilise a broader range of responses. In short, if we integrate organised crime alongside the other national security threats, we can think more logically about how we deploy the collective armoury we already have, against all the threats. That helps us to keep people safer. Thank you for your time, and the opportunity to speak today.