DG National Crime Agency, Graeme Biggar

RUSI 4th Annual Security Lecture

31.10.23

Good afternoon.

Thank you, RUSI, for inviting me to give this year's annual security lecture.

I've spent almost all my career working on national security issues, mostly in the Ministry of Defence, then at the Home Office and then at the National Crime Agency. Engagement with RUSI has been a constant for me in that time: as a source of advice, inspiration, and as a voice for reason. Indeed, looking back, it was 25 years ago that I stood in this hall with my contemporaries on the graduate intake into the Ministry of Defence and gave a presentation on autonomous warfare. And looking forward, in just a few weeks' time, the NCA and RUSI are jointly running an academic conference here on serious and organised crime.

So it is a privilege to be asked to give your fourth annual security lecture, and I am delighted to be following three colleagues and friends. Last year, Jeremy Fleming discussed the cyber espionage threat to western industry from the Chinese state. Two years ago, Lindy Cameron highlighted the threat of ransomware from cyber criminals. And, back in 2020, Cressida Dick spoke of the role of data and technology, notably facial recognition, in policing, and the need for public debate and consent.

One theme united all three lectures, and that was technology. Which means that this will be the fourth year in a row where the core theme is technology – a point we should perhaps reflect on. For I, too, am going to talk about technology – the extent to which it now enables crime, and has to be fundamental to our response. And – spoiler alert – I will conclude that we need to recognise that, world leading though we are in some areas, we need a step change if we are to deal effectively with the criminality we face today, let alone what we can see coming in the future.

I will cover three areas: how organised crime has evolved in recent decades and how our structures have developed to respond to it; serious and organised crime as we see it now and as we see it developing; and finally, what I believe needs to change to better tackle it.

But first a word on the NCA. Having been established in 2013, we celebrate our tenth anniversary this month. We are an intelligence-led, law enforcement agency with an international presence. Our mission is to protect the UK public from serious and organised crime: principally drugs, guns, child sexual abuse, organised immigration crime, fraud, money laundering and cyber crime.

We do that in two ways. We gather intelligence, and investigate and arrest the most serious, hardest to reach offenders. And we have a statutory role to lead the operational system, pulling together law enforcement, intelligence agencies, regulators, the broader public sector and indeed the private sector and charities to create a whole-system response that is greater than the sum of its parts.

It is that collective impact that matters to the public, and I applaud the brilliant work that takes place right across policing and our other partners.

But let me give you some NCA only statistics. In our ten years, we have recorded 23,000 disruptions – actions that have had a material impact on serious and organised crime. That is over six disruptions each and every day for ten years, averaging more than three arrests, half a tonne of drugs and a firearm every day. In the last year alone, we have safeguarded more than 1000 children. And right now, we have over 800 live operations against criminals causing the highest harm.

Figures can appear a bit remote. You can hear the human stories behind these figures in – quick plug – our new podcast series: *Underworld: behind the scenes of the NCA*, which we launched last week and is available across all major podcast streaming platforms. We are proud to make a massive difference to keeping the public safe. We are all too conscious there is more to do.

Our successes are down to our almost 6000 officers, who are based all over the UK and in over 50 countries around the world. Each of them, every day, brings their expertise and passion to the

mission of protecting the public. It is my privilege to lead them, and I would like to take this opportunity to pay tribute to them.

Of course, we did not emerge from a vacuum in 2013. We are the product of an evolution that has taken place over decades as criminal threats, and our response to them, have changed. It is worth understanding that history, if we are to chart an effective course for the future.

Crime, of course, is as old as humanity. For most of history it has required the offender and the victim to be in the same place. Organised crime – in the form of robbery and smuggling – emerged in the ungoverned spaces between settlements: bandits or highwaymen on land; pirates at sea. Then, as now, the latest technology, as well as violence, was adopted to commit crimes and avoid capture, in the form of weapons, fast ships and secret messages.

Customs organisations – the original organised crime fighters – and navies played a role in combatting that crime. But for most of history, the vast majority of crime was local and dealt with by local communities and then local police forces.

That balance between local and national has shifted. In the '60s, criminals increasingly crossed police force boundaries as road networks improved, and so Regional Crime Squads were established. As the economy evolved, so did criminals, leading to the National Crime Squad and National Criminal Intelligence Service in the '90s. In the same decade, the National High Tech Crime Unit was established to investigate emerging crimes on the internet – technology having created a new ungoverned space.

The Serious and Organised Crime Agency subsumed them all in 2006, along with parts of Customs and Excise and its extensive overseas network, recognising the need to bring more national functions together, and to give it an international edge.

And the National Crime Agency was then set up in 2013, bringing in further national functions but also importantly taking on a new responsibility and authority to lead and task other agencies, recognising the need to join up and drive the whole system.

Over the last twenty years, and increasingly the last ten, technology has enabled a different shift, less geographic and more into a new domain. Crime has gone online. Technology has made it easier to conduct traditional crimes. And it has enabled new ones, in online child sexual exploitation, cyber crime and online fraud.

And again, we have responded, growing – with Government investment – new capabilities in each of those areas, in NCA, across policing and with new partners like the National Cyber Security Centre.

Of course, technology has helped law enforcement as well as criminals. The same decades have seen the development of fingerprints, DNA, ANPR, CCTV, and phone intercept and comms data analysis. All controversial in their time and rightly requiring a debate to get public consent. All needing to be introduced with care and safeguards and used proportionately. All now widely accepted and not just keeping us safer, but also, as Cress observed in her 2020 lecture, ensuring fewer miscarriages of justice than in the past. Facial recognition and AI are the two latest technical developments where we need to continue working through the right use by law enforcement. Essential that we use them. Essential that we get it right.

So, history has seen criminals taking advantage of ungoverned spaces and using the latest technology. And technology has seen crime shift from being predominantly local to also global, and from being real world to also online. In response, we, in law enforcement, have evolved our structures and – where we can – taken advantage of the *massive* opportunities technology has offered us to prevent and combat crime.

Where does this leave us? We find ourselves in the NCA faced with a broader range of threats than in the past, each important. I won't today set out the state of play on each of them. We do that every year in our National Strategic Assessment of serious and organised crime, which you can find on our website. But I will pull out three themes.

- First, every serious and organised crime we look at has a significant international nexus. Organised immigration crime, by definition, originates overseas, as do most drugs and

many illegal firearms. Three quarters of online fraud in the UK is partially or fully committed from overseas. Russian speaking groups continue to pose the biggest cyber threat. Many of the worst dark web child sexual abuse sites are hosted overseas. Careful international cooperation is therefore vital, and our border a key intervention point.

- Second – and this is the macro theme of the last decade as well as this lecture – criminals have exploited advances in technology, both to enhance 'traditional' crimes and to create new ones.

- Thirdly, not only are we faced with a broader range of crimes, they are also each more complex to investigate, with more of an international footprint, and exponentially more data involved, all of which must be presented to a court to an ever higher set of standards. In short, the cost per case has gone up.

Faced with these challenges, what is our response?

Of course, it is not just about law enforcement. It needs to be a whole of government and indeed societal effort. To my mind, it involves four Ds:

- Reducing Demand for illicit goods and services, such as drugs or passage on a small boat. This is a matter of public health and public policy and requires behavioural change.

- Raising our Defences, by designing out crime where we can, which is particularly relevant to fraud, cyber crime and online child sexual exploitation – and is a matter primarily for government, regulators and the private sector.

- Diverting young people from the possible lures of a criminal path, which, for example, we seek to do with our widely applauded Cyber Choices initiative.

- And finally, and most relevant to the NCA's own operational capabilities, Disrupting and degrading the organised criminals and groups who will seek to meet that demand and exploit any weak defences.

We work closely with the Home Office on all of this, and I look forward to their forthcoming Serious and Organised Crime Strategy.

Within the overall government approach, we have our own NCA strategy. And being here at RUSI – one of the homes of strategy – I thought I had better explain what it is, and do so in terms of ends, ways and means.

Our *ends* – our mission – as I mentioned earlier – is to protect the public from serious and organised crime.

We have four priorities.

The first two are *ways*. We lead the UK's operational response. And second, within that overall response, we in the NCA focus on degrading the most harmful organised crime groups, in areas the rest of law enforcement would struggle to reach.

The third and fourth are *means*: by transforming our capabilities and growing a highly skilled workforce.

Let me explain a little more about that second priority – degrading the most harmful organised crime groups. We are doing that by shifting our focus upstream, overseas and online to maximise the impact we can have for the public here in the UK.

- Upstream, to disrupt those at the *top* of the criminal chain, those who *enable* their activities and those who *launder the money* they make, targeting the links in the criminal chain that are hardest to replace.

- Overseas, to tackle the threat at source and en route to the UK.

- And Online, to combat that critical element of the organised crime business model and reflecting the fact, as I have said already, that more crime takes place online or is enabled by technology.

And, of these, in my mind, the biggest shift that we need to make is online.

So how are we making that shift?

Our adversaries are innovating enthusiastically, at pace, and in numerous ways.

Criminals are using AI to code ransomware, create indecent images of children, and craft fraud scripts. This is not a future threat; it is happening now – and so the Prime Minister's AI Safety Summit is more than welcome. It is essential that we have an international response to ensure public safety is built into technology.

Traditional drug criminals are also using: the dark web to trade commodities; encryption to communicate; and crypto currency to pay. They are downloading blueprints for 3D printed firearms. Organised immigration crime gangs are using social media to advertise their services and then encrypted comms to engage directly with prospective migrants.

These developments give criminals *reach* and they *lower the threshold* for entry. Put simply, the technology that we all rely on makes us *accessible* to criminals anywhere in the world. And technology also enables *scale*: criminals can contact *thousands* of people at once to see who responds, and then hone their approach much faster and more cheaply. Crime used to be local and one-to-one. It is now also global and one-to-many.

But these developments depend on *anonymity* and *trust*: criminals *believing* they are anonymous online; and *trusting* that the sites they are visiting and the people they are engaging with are also criminal.

So, as well as arresting the criminals where we can, our approach is to undermine the ecosystem they rely on by *removing that anonymity, undermining that trust, and disrupting that infrastructure*. We are doing that, and we are doing it together with partners in the UK and internationally.

Let me give some examples.

- Drugs criminals have been using bespoke phones or apps with a high degree of encryption. So we have targeted them. The French and Dutch took down Encrochat and Sky ECC. The FBI and Australian Federal Police ran the Anom operation. These operations led to multiple arrests worldwide (over 3000 in the UK alone); and we have more in the pipeline. The criminals *thought* they were anonymous and so they spoke freely. They thought they had a cloak of invisibility; it turned out to be their Achilles heel.

- Cyber criminals too thought they could operate in the shadows. We worked with the FBI to unmask the identities of the cyber criminals behind DRIDEX and ZEUS and then CONTI and TRICKBOT. They thought they could hide behind anonymous handles; they were wrong. They are now outed, indicted and sanctioned.

- We have hacked criminal infrastructure, taking it down, and identifying who has been using it. We supported the Met Police in the fantastic work they did taking down iSPOOF, which was enabling mass fraud, and identified all the users.

- And under Operation POWER OFF – and this is my favourite example – the FBI, NCA, Dutch Police and Europol took down 48 of the most popular DDOS Booter sites. But on this case, we did not *just* take down the sites and identify the users. The NCA *also* set up our *own* DDOS site, purporting to be criminal, to lure in several thousand cyber criminals before explaining to them that *they themselves* had been scammed.

- And why did we do that? We harvested their data of course, and there will be knocks on their doors. But the main objective was to sow distrust and fear among the broader cyber criminal community, so that they can never be sure who they are dealing with online.

So, we are having some success in removing criminal anonymity and undermining their trust in each other and the infrastructure they use. We are using the tech that they think is their greatest asset, against them.

This is the right direction of travel. But, to move on to my third and final theme: we are *not going fast enough*.

Elements of our response to the shift online have been world leading, but the pace of technological change is accelerating, and we are not adopting it as quickly as criminals. We are still too analogue in a digital age. We need to move further and we need to move faster, both in the NCA and law enforcement, and in Government and the broader system.

I would set *three* challenges for *each*.

For the NCA and law enforcement, we need to:

- First, grow the skills of our workforce. We have some world class experts, but we need more of them. And our generalist officers are more digitally aware than ever, but need to learn more. We intend to introduce a new technical stream to recruit and grow our specialists, and – funding permitting - an academy to grow our skills generally. And we are looking at how we can offer career pathways that move more seamlessly between the NCA, policing and the intelligence agencies. Between us, we can offer a compelling mission as well as the opportunity to use powerful tools in ways that otherwise would not be legal. But we will need to reform our pay model if we are going to be able to recruit and crucially retain the highly sought after skills that we need.

- Second, we need to transform our capabilities. Some are world leading but not all. We have built a bulk data exploitation capability, which is starting to deliver for us, but which has so much more potential. We need to develop further our digital intelligence collection capabilities and our digital forensics. We need to hone our ability to de-anonymise individuals online and to track crypto currency. We don't need to do all of this alone. We get support from the Home Office on building capabilities. And we benefit from the excellent work carried out by our intelligence partners and foreign allies. We can play to each other's' strengths and out-collaborate our adversaries. But we need to make sure we are playing our part and we need to lift our game.

- Thirdly, we need to keep evolving *how* we tackle crime, adapting our doctrine to respond to and anticipate changes in criminal practice, becoming more innovative and agile in adopting new technology, and focusing on proactive, intelligence led disruption at scale. In doing so, we cannot afford to lose our traditional investigative skills and tradecraft, our humint and surveillance. Twenty years in Defence taught me that wars are not won by air power alone; in the same way, the fight against serious and organised crime cannot be conducted by technology in isolation. Just as in Defence, it is the blend of capabilities that matters.

For Government and the broader system, my three challenges are:

First, to adapt legislation and the criminal justice system for the digital age. The Online Safety Act, which was given Royal Assent just last week, is a *massive* step forward, and I congratulate all involved. The Computer Misuse Act, on the other hand, dates from 1990, and needs some fundamental changes. And the Criminal Procedure and Investigations Act was introduced when a phone might have a kilobyte of data on it. We now deal with phones that can store a terabyte – a billion times more. Disclosure risks becoming an overwhelming challenge for law enforcement and criminal justice, as ever greater efforts go into preparing for cases. Technology will provide part of the solution, but only part, so I am delighted the Government has asked Jonathan Fisher KC to review the position. He will need to think radically to find ways of meeting the enduring principles of CPIA in a digital age.

Secondly, review arrangements for sharing intelligence and evidence with international partners. We have investigations where the suspect is in one country, using servers or sourcing drugs in another, to target victims in a third, laundering the money in a fourth and accruing assets in a fifth. Technology enables much of this to happen or switch in an instant. The current processes for mutual legal assistance and international letters of request take months and sometimes years.

Government needs to work internationally to find solutions that are adaptable and flexible, whilst still protecting our principles. The UK US Data Access Agreement last year was an important step in that direction.

Thirdly, further strengthen relationships with the private sector, and where necessary set a new framework. These relationships are crucial. The private sector can of course be victims themselves, for example of cyber attacks, and needs to improve its own resilience. But their greater role is in designing out crime from the services they offer, be that in banking, in tech, in retail, in transport. Progress has been made with all of these but there is still an *acute* need for more progress with the tech sector.

Here we risk going backwards. I *strongly* support encryption. It is an important protection from a range of crimes. But the blunt and increasingly widespread rollout by the major tech companies of end-to-end encryption, without sufficient protection for public safety, poses a fundamental and negative implication.

It means they cannot protect their own customers, by identifying the most egregious illegal behaviour on their own systems. Each platform brings different risks, and the Online Safety Act recognises this, requiring companies to ensure safety within the services they are providing. If Facebook roll out end-to-end encryption their ability to spot child abuse will significantly reduce, as will the number of children we save from sexual abuse and the number of criminals we arrest on the back of their information. Let me be clear: this would be tantamount to consciously turning a blind eye to child abuse – choosing to look the other way.

It does *not* need to be like this. Despite the protestations of some, this does *not* need to be a binary choice: there *are* ways of providing for stronger encryption and privacy, and still protecting customers and enabling lawful access. Ultimately, it appears to me that fundamental decisions on the balance between privacy and security are for democratically elected governments to make, not multinational corporations.

To conclude, I believe that adapting to the digital age is the central challenge for those of us fighting serious and organised crime.

It is not just about recognising and responding to the fact that now over half of crime takes place online and ensuring we can respond to it. It is about recognising that technology is core to the conduct of almost all serious and organised crime, and is certainly core to our attempts to prevent it, investigate it, and bring to justice those who commit it.

Such a response needs to begin, as I said earlier, with an honest recognition that, world leading though we are in some areas, as an Agency and as a country, we need a step change if we are to deal effectively with the criminality we face today, let alone what we can see coming in the future.

The NCA must embrace becoming more and more an online agency, harnessing the best of technology, with the very best people. It is our future. We are uniquely placed to do so, sitting as we do at the juncture of policing, the intelligence agencies, government and international partners; and blessed with a wonderful blend of officers from a range of specialist backgrounds.

It is an urgent challenge, but one that law enforcement has risen to time and again throughout history. Faster ships; better code cracking; the ability and willingness to find and police those ungoverned spaces: these are challenges we have faced and overcome before, and, working with Government and broader society, I am confident we can do so again.

If we are to achieve our mission of protecting the public from serious and organised crime, we must.

Thank you.