Transcript of Panel 4: Innovation and Technology: Re-writing the rules?
Margaret Thatcher Conference on Security
Guildhall, London
Tuesday 27 June 2017

The video recording of this panel is available on the CPS YouTube channel.

Deepak Lal: Good evening everyone. I'm Deepak Lal. We're going to talk about innovation and technology. This morning, we've been hearing a lot about social media and various other forms of new technology. Most of them seem to be threats. Anyway, we've got a very distinguished panel. On my immediate left is Commissioner Ian Dyson of the City of London Police, then there is ... Who's next? The Rt. Hon. Matt Hancock who's the minister of estate for digital, then Robert Hannigan who is a former director of GCHQ, and then Lara Poloni who's incoming Chief Executive of AECOM who is sponsoring this conference. I'm going to begin by getting Robert Hannigan to talk about it, because he can give us a global view. He's been in GCHQ for a long time. He just retired as Director. He can tell us what technology is doing to keep us safe or leading to us being attacked.

Robert Hannigan: Thank you very much, Deepak. Great to be here. I thought what I'd do is just say a few words about the shifts in power that have been referred to in various sessions during the day, that are caused by, or accelerated by technology. And then say something about the impact that's having particularly on global security and then a couple of thoughts on how we might approach that.

On those shifts, two in particular I wanted to pull out. One was the shift from government to private sector. If you look back over the 20th century and most of the history of GCHQ, their great innovations in technology were government driven, so nuclear efficient in the US, digital computing here, the arrival, the creation of the ARPANET and then internet, and things like GPS, which have transformed all our lives and probably helped people get here this morning, but underpin our security, were government generated, very often military backed innovations with academia against security threats.

I think if you were to ask anybody today whether they look for that sort of innovation and technology, they don't look to governments anymore. There's been a fundamental shift in the last 30-40 years away from government control. Part of that's been linked to Margaret Thatcher, her deregulation telecoms in the '80s led to a very dynamic tech sector here and other factors in the US drove that, and of course, the end of the Cold War was a factor too.

There is a pretty fundamental change, and it has implications, which I'll come to in a second. The second obvious change, which Henry Kissinger and others have referred to today is the technology shift from West to East, or the rebalancing of West to East. If you look at a map of the internet, physical

internet, the fibre optic cables that go under the sea from 15 years ago, it pretty much mirrors the imperial telegram cables of the turn of the 19th, 20th century, which in themselves mirrored global trading centres. The US and Europe were right at the centre of that. If you look at those fibre optic cable maps over the last 10 years, they have changed radically, and gradually the centre of gravity is moving further East. Partly because more people are coming online now, but partly because of the sheer dynamism and innovation that is going on in the far east.

The computing capitol of the world now in hardware terms is China. It isn't the West. That will have implications for our security because we may kid ourselves that we're buying a branded US router, it's almost certainly made in the Far East somewhere. It is blurring the lines of sovereignty in the way that other parts of globalisation are also. What does that mean for global security, and there's been a lot of talk today about what it means for other aspects and disruption of traditional ways of making money, disruption of politics, disruption of our social lives, but what's it mean for security? A couple of things I would pick out.

One is the obvious fact, the internet itself was not designed with security in mind. It was designed by an enthusiast and engineers and security has been thought about in retrospect. The attack that we're seeing and the cyber security industry that is now being generated and the messages from government to change culture, are all attempts to retrofit security onto something that was never designed with security or resilience in mind. That's a fundamental problem because it has opened up this network well as a little free gift for people who want to do bad things, particularly criminals but also terrorists and to some extent nation states and authoritarian states. We see examples of that all the time, I gather another one this afternoon. I don't know what the origin of that was, but in general we're seeing a trend of people taking advantage of what was essentially an open platform.

If you add to that the fact that technology has been democratised, if that's a word, and what was high grade encryption for example, only available to governments during the Cold War is now available by default on many of your apps on your mobile phone. That's a problem for government. It means the bad people can anonymise themselves in a way they couldn't before. At the same time, as those shifts in threat, the levers available to government have changed. Most of the things the governments need to meet either cyber-attacks or extremism online are not in the hands of governments anymore. The data, the technology and the skills are all most certainly in the private sector. That private sector may not be in our jurisdiction. Once again, sovereignty is becoming blurred by the internet and indeed the internet is by its essence not a sovereign domain. It's cross jurisdictional. That presents huge problems, which I know the minister is going to talk about in a moment.

The levers are not necessarily there. If you're excited as I am, or alarmed about that development over the last 50 years, it's going to become even

more fast paced and exciting and possibly alarming over the next 50, as billions of devices start producing data, the so-called internet of things, on the world around us as the other half of the planet comes online in the south and the east. As artificial intelligence, as some were referred to this morning, begins to make sense of that data and do really fantastic things with it, which the human brain can't at the moment do. Of course, under pinning all that quantum computing, which is possibly the most excited breakthrough of our generation, and it will arrive, I think in the next 10-20 years.

None of those things will belong to governments in the way they would've done 100 years ago. That is a huge challenge, I think for the West. What should we do about it? Well, I'm always conscious that if, at the risk of offending half the audience, looking around the room we are all of a certain generation, I myself included. If this was an audience of people in their early 20s, you would probably get very different answers. I think there is a danger that we fall into the Luddite begrudgery category. We have to get the balance right. This is overwhelmingly a good thing for the progress of freedom, as well as the progress of humanity. We shouldn't do what authoritarian states do. We shouldn't start trying to balkanize or nationalise the internet. The dead hand of government is not going to be a good thing for the freedom of the internet and of the worldwide web. We should avoid that.

Most people involved in the technology business, and I know many of them, and those who've generated the internet and the web understand that it cannot be a values-free and law-free domain. They are interested in that how we get there is the difficulty. I know others will talk about that, but it is perfectly possible for us to reach an accommodation. The internet is still young. It's still developing. There is time to do that. It's best done with the private sector.

Government will need to regulate, I think especially on cyber security in the future, but it needs to do so in a light touch way. It will also need to protect those who are going to lose out from this new machine revolution over the next 50 years. It may be that our political leaders may need to jump a generation in many countries and be from the generation that really understands this technology. It is a huge challenge I think that we have a generation, ourselves included who haven't grown up with the internet.

Finally, I'd say we need to keep ahead in innovation. We absolutely need to, partly because the answers to the technology problems we're facing, including on cyber security can be technology itself. Technology has the answers to most of our technology problems. We should invest in that and make sure that the West stays ahead of the game in innovation. There are lots of ways of doing that that we might talk about in questions.

Finally, we should have the confidence to do that. There is a clear relationship between the creation of this technology, particularly the internet and web and the values of the free West. These would not have been created in

authoritarian regimes, and they would not have flourished in them, and they are not flourishing in them. There is an absolute relationship between the free-flow of ideas that we've talking about all day and the creation of this technology. That ought to give us confidence that the future is through investment and innovation in the best technology of the West. The people who fear this technology, most are authoritarian regimes. There is a self confidence that we need to have, both in our technological innovation, but also in our values that underpin it. I think I'll leave it there.

Deepak Lal: Thank you. Our next speaker is Matt Hancock, who's the Minister of State for Digital.

Matt Hancock MP: Thank you very much Deepak. Unfortunately all of my best lines have just been stolen by Robert. I might start by saying what a fantastic contribution that was. It's absolutely classic of Robert, who's been an amazing public servant over many, many years and brought great thought and integrity to this topic. It's good to be able to be on a platform with you rather than having these discussions behind closed doors. Now that you've been fully unleashed onto the public, and your brain whirring in open view.

It's commonplace to say that technology is changing almost every aspect of our lives. I sometimes think whether we always say that. I think of a child born in the 1820s when the fastest you could go was on the back of a horse. The fastest information could travel was on the leg of a pigeon. If you think of somebody born in the 1820s, whether they would say more had changed in their lives than somebody born say, in the '70s like me, or especially in the '80s or '90s. There's no doubt that we're living through enormous changes. Ultimately these digital changes are underpinned by one thing, which is the cost of storing and transmitting information has collapsed over a generation in a way that has been unprecedented since the invention of the printing press in 1454.

Now, communication is of course all the way around the globe, almost costless, so long of course as you can get a signal on your phone. This has created huge advantages. I think it's very important that we hold onto and understand those advantages, the spread of ideas, the collaboration between people, it entertains us, it saves us time, it brings people together. But yes, it has replaced jobs and changed jobs and created new jobs as well. But having said all of that, I think we're only on the cusp of this. The artificial intelligence, machine learning, the automation of the means of production distribution and exchange, not just by hand but increasingly by brain is what we face.

I come at this from a tech background before I went into politics. I think it's both exciting and daunting. There's two areas that I just want to comment on briefly. The first is getting the response right in terms of the impact on jobs. You mentioned this briefly. Throughout history, new technology has disrupted the world of work. Today, people worry about in seemingly equal measure

about the problem that we've got of how to fill the countless jobs that are being created by technology, and also what we're going to do with the countless people made unemployed by new technology. This argument's been run throughout the ages by Harold Wilson who feared that machines would take all the jobs, by John Maynard Keynes who lamented the future of technological unemployment.

You mentioned the Luddites. The Luddites smashed looms because they were replacing the hand weaving technologies of their times. When I was doing some research into this, I discovered that the leader of the Luddites was a man in Nottinghamshire called Richard Hancock from whom the Hancocks are descended. I would say that over the past 200 years or so, the Hancocks have learned a bit or two about the advantages of new technology. So yes, jobs are being destroyed and they're being changed, but so too are jobs being created and indeed employment's at a record high. We need to square this circle. Some say that the new blue-collar job is coding and I think that's a really interesting way of thinking about it.

The task for government is to ensure that we see redeployment not unemployment, that we automate work but we humanise jobs. Ultimately, harnessing new technology to save money, to improve safety and to build the UK as an industry for technology where we can develop the best technologies in the world. This being a Margaret Thatcher Conference, I thought it was interesting to see what Margaret Thatcher herself thought about this. She said, "Technology is the true friend of full employment, the indispensable ally of progress, and the surest guarantee of prosperity." Our job is to make that true today, not by burying our hands in the sand, but by equipping people with the skills they need to thrive.

The second area I just wanted to touch on is the impact of technology on society. While the internet brings incalculable benefits, it also brings some harms. To harness the benefits, we've got to mitigate the harms. Parents worry that their children might be vulnerable online in ways that they simply don't understand. Customers worry what tech companies are doing with their data. Citizens worry about what terrorists can do in using the internet to plan, apparently with impunity. The basic problem, and it's a serious problem, is that technology is developing faster than the speed at which society is building the rules to deal with the challenges that the technology creates.

We don't yet have a shared understanding of what is and isn't acceptable online. I think that it is the role of government to lead the way in closing this gap and ensuring the right balance between freedom and security in the new digital age. Ultimately, the internet grew up as a libertarian idea. The dream that a lack of rules would mean that it would bring out the best in everyone, and it's true that it brings out the best in most people. But just like offline, it doesn't bring out the best in everyone, and that's human nature. We need to ensure that people are free and are kept safe online as well as offline.

That's the thinking behind the new digital charter that was announced in the Queen's speech. The aim is to set out a rules-based framework for how businesses, individuals, wider society should act in the digital world. The starting point is this, if you think about it, offline there's been a careful balance honed over generations of what is the limitations of freedom and how you balance that with security. For instance, and these are very practical examples. We cherish the long-held principle of free speech, but that principle has boundaries which stop people inciting terrorism or violence. These boundaries need to apply equally whether is somebody is using a pen and paper or using social media.

We've got to make sure we get these balances right. It is the role for government to do that. But I think that the reward is really significant if we can land this right. The aim is to provide a world leading framework for an understanding of the best way to bring the balance throughout the free world. The stakes are really big because I think that the first country that gets this right will have a huge positive benefit. No country has managed to do it yet. Because ultimately, business done right is a force for good in the world. Technology harnessed right can solve human problems on an unimaginable scale, using data well and according to sound ethical principles is fundamental to maximising those benefits, and to limiting the harms and making sure we get the most of the innovation.

It is a big job to do that, but it's a big goal that is not only a practical goal, it is a deeply ethical goal too, to improve the human condition by harnessing this technology for the good. I look forward to working to try to make that happen.

Deepak Lal: Thank you. The next speaker, Lara Poloni who is the incoming Chief Executive of AECOM. We see them all over the place. She's going to tell us how smart cities and safe cities can survive in this cyber age.

Lara Poloni: Thank you so much, Professor. It's an absolute privilege to be here today. Obviously, you can tell through my accent that I am coming from the end of the Commonwealth, but will soon be living in London. It's great to be here. It's interesting being part of the panel at the end of the day today because the conversation about security has progressed from a very captivating discussion, philosophical discussion if you will in terms of ... at a higher societal level in terms of where we're trying to go with this discussion. I think just now, even some of the minister's comments are a nice prelude to some of the comments that I'm going to make, which all descend straight into the city level infrastructure issues and city planning considerations, because that's what AECOM, our firm is all about. We are in the business of infrastructure, and cities and defence. I've got a few comments from me, if you will.

There's no question, everyone who's talked today about us being part of an era of rapid daily technological change and advancement. What we're seeing now is that each of us as citizens and organisations, making the most of

some of those opportunities that come through the internet of things, and artificial intelligence. It means that at a planning level, for example that we now have the opportunity to understand in a virtual reality way the impact of new city shaping proposals and ideas and infrastructure schemes. But at the same time, obviously as we move around the cities and we are experiencing greater mobility than we've ever seen before through some of the gadgets and the technology that we have. At the same time, the security risk in tandem is becoming more mobile. We are facing a number of challenges on that front.

Every day there is greater digitalisation occurring in terms of not just our personal lives, but how social and economic infrastructure is planned, built, maintained, operated. We're seeing those impacts in terms of business and trading relationships. Indeed, in some of the comments that were foreshadowed, in terms of how we deal with that from a governance and national security perspective. What we've recognised, in firms like ours is obviously we need to adapt to that in terms of technology systems, processes, data analytics, the way that we plan, anticipate, respond, and put real money towards building up our resilience particularly as cities.

I think at the same time, one realisation that we've had at AECOM is that this truly requires a different mindset, a cultural mindset. Even when you look at the world that we come from, which is all about infrastructure and defence, we've always operated in this mantra of we have to design and plan things that are built to last. Now we're finding that we need to change the culture and the conversation. It's about building things that are adaptable and resilient and able to change. It's a very different paradigm in terms of how we as city planners go about our business.

The same time, obviously we've acknowledged today, even in the last six months, 12 months that we've seen the prevalence of some of the most significant risks in terms of our own security. There's for example, the more and more incidents happening from lone and group suicide bombers in the last 12 months. In the city that I've come from, Melbourne, we've had incidents. It's not just London. It's not part of something that's happening in a very widespread manner. As I said, the security risk has become far more mobile.

We're also seeing the very institutions and things that maintain the livability of our cities, so some of the cultural events, sporting events, concert events, they are also under threat. I think some of the more progressive cities in terms of how they're responding to this, absolutely not just trying to tackle it at a sole government level, but they are looking very much to the private sector to help them form partnerships about how can we make the most of rapid advances in technology? How can we partner with academic institutions? How do we partner with those private sector organisations at the leading edge of technology? There are some great examples in the US that our firm has been involved with, quite progressive cities like San Diego, which I think is featured in one of the publications that you have at your seat today.

San Diego is a great example of a very progressive, proactive county that has said, "We're actually going to become a centre of excellence in terms of cyber security. We are going to partner with private sector organisations such as AT&T and Hewlett Packard, and we're going to be well-equipped for this. We are going to, for example, have a day of just practising a whole lot of drills about what would happen in the event of a major cyber-attack?" How do we then build and cascade that level of resilience down through the grassroots at a community level? There are a number of community groups that are also taking up the charge to do this as well.

Look, there are similar examples. When we think about some of the other critical infrastructure in our cities, again using another American city is a great example that we're familiar with. The city of Chicago, which operates two of the largest wastewater treatment plants in the world, has invested significantly in terms of its cyber security and resilience and converge resilience planning. That has meant that through the installation of metres, through a whole lot of other mechanisms, that they are giving this some serious attention. We all know the devastating impacts that cyber-attacks and other intrusions on critical assets like a city's power supply and water supply would mean. It would bring those cities to a standstill.

What we're seeing in an info technology sense is, we've seen this evolution from simple malware disruptions to increasingly sophisticated attempts using social engineering, capitalising on these opportunities that are happening through the internet of things. More and more spear phishing and a dramatic increase in random ware attacks in particular.

Just one final point, the same publication that I pointed to, the better safer secure document, just again to magnify the importance of why this is so important to our cities and so important that it features prominently in terms of government policy agendas and that partnership that needs to happen with the private sector, some of the impacts of that publication that I mentioned talk about $2.1 trillion is the estimated cost of data breaches and cyber-crimes that global businesses will feel by the year 2019. Just in the UK, $34 billion will be spent defending some of these cyber and security attacks. Almost half of the firms in the US have experienced serious data breaches in the last couple of years. A concomitant figure for the UK is about 15%, but we know that that's already out of date.

$445 billion is lost annually to cyber security and espionage events around the world. 317 million pieces of malware were created just in 2014, and that's already obviously out of date. There are in excess of more than one million new threats that exist everyday as reported by some of the private sector firms like Verizon, in terms of their vantage point on this challenge.

Look, just a couple of comments in terms of solutions. I think what we're saying is there is no one size that fits all, but what is important is that particularly in terms of some of the converge resilience approach that we talk

about in AECOM, is that you must focus on all three important domains, the physical aspects, the cyber, not just cyber on its own but the wireless aspect as well. It's very important that those three elements are linked closely because if there is a breakdown in any one of those elements of planning, any one of those critical city assets, such as a water supply system, or a mass transit system, they become instantly at risk.

As I said, obviously what is critical going forward is that policy frameworks reflect the importance of this and those partnerships between private and public sector, and indeed the community, are emphasised in particular.

Deepak Lal: Thank you. My final panellist is Commissioner Ian Dyson, who is the Commissioner of the City of London Police. He's going to talk to us about cyber security and how one can deal with unconventional attacks like people driving lorries if we walk out of the Guildhall.

Ian Dyson: Thank you very much. That's a good steer for my talk. I'll probably cover that bit right at the end. Thank you very much for inviting me to speak to you today. What is my role? I'm the Commissioner of the City of London Police. That's the local police force that covers this area of London. My responsibility is to keep you all safe while you're here. I also deal with a whole range of policing issues that affect any police force in any part of the country, and probably any part of the world. However much technology changes and develops, the reality is people will still want to fight each other. People will still want to do damage to people they love or people they live next door to. People will still want to acquire property that other people have. We still need to deal with all those things.

But what makes the City of London Police quite special is we also have had for about the last 10-12 years, a national responsibility in the UK for fraud in policing, to lead the fight against fraud nationally because it was recognised that fraud was a growing crime problem and it was beyond force boundaries. What we're seeing now is 70% of the frauds that we're seeing are cyber enabled. We are getting very much into the cyber security space as part of that lead role responsibility.

We also have a national responsibility in policing for what we call Cyber Protect, which is the role that we play in helping both businesses and individuals to better protect themselves against the cyber threat. I'll come back to that shortly. What is the challenge of new technology for Law Enforcement? I think it's worth saying, I'm not going to comment and I wouldn't feel qualified to comment upon issues such as state actors trying to attack other countries and that sort of thing. That's very much the world that Robert was involved in. At the other end of the spectrum, I'm not really going to talk to you much about the teenager sitting in their back room piled high with pizza boxes, trying to hack into systems because it's an intellectual challenge or because they can.

What sits in between those two extremes, in the volume piece is criminality. The cyber-attacks that you see, the frauds and the crime that is committed online, the vast majority of it is people out to make money and to acquire property or to acquire data. Criminality is the challenge. It is a volume challenged to law enforcement. As we see the statistics that have just been mentioned by Lara around some of the cost to industry, some of the volumes of attacks that you see, is a real challenge to us.

I think the other challenge around technology is it's developing and creating new business models. We're in a world where the world's biggest taxi firm owns no taxis, the world's biggest accommodation business owns no hotels, and the world's biggest retailer owns no stores. That changes the nature of the relationship between business and the public in my view. The traditional 'know your customer' to identify, are they legitimate? Are they vulnerable? All those sorts of things are challenged in a world of global business and transactions. The speed of transactions is ever reducing. Speed also brings with it then vulnerability in my view because if you go back to ... And I am old enough to remember the days when it took five days or five working days for a bank transfer to clear, that's just not acceptable to the public these days. They want it instantaneously.

What that means is, the criminal can move money as a result of that through the system at lightning speed. We also need, I think, in law enforcement to help people understand this world. If I think about the traditional crime types, if you've been the victim of a burglary, you kind of know why. You know that you left a door or window open, or a door or window is broken. But in either case, broadly you understand what you need to do to protect yourself in the future. What I find talking to lots of victims of crime is that they don't understand fully how the business models work. They don't understand how people can access their personal data. They don't understand the consequences of them putting information out online. Law enforcement has a role to play in that.

What are we doing? I think I'd start at the top and say Matt talked about the responsibility of government, and I think the creation of the National Cyber Security Centre is a really good initiative, really good. Not just because of the work that they do, and actually we work very closely with them and if you suffer a cyber-attack for example, on their website they refer you to us because we operate 24/7 cybercrime reporting through the City of London Police. But it also is important, I think, because it provides or starts to provide that sort of sense of the government is protecting its people because the confusion of where do I go? I've suffered this instant, I've suffered this crime, I've suffered this cyber-attack, the challenge for law enforcement is that in traditional crime you would automatically go to the police. My question and challenge to people is, if you suffer a cyber-attack, if you're a business, do you go straight to the police or do you look for the cyber experts to help you with that?

The government piece is really important, and they've also got Cyber Essentials, which is very straightforward advice that I wish more people would take up. It would help a lot. We, in the City of London Police, as you would expect with our responsibilities, I think are pretty cutting edge around some of the work we're doing. We're partnering with the United States around an initiative called the Global Cyber Alliance, which is a partnership between law enforcement and business to say, can we use the best skills in both of those different elements of life to actually try and address some of the systemic challenges that we face across the world?

The first one that we've done is looking at phishing emails and how can we stop those being brought into businesses. There is technology called DMARC, which I won't go into detail, but if you went onto gov.uk search under DMARC, it gives you some details. If you go to globalcyberalliance.org, will give you that information. It's very straightforward, it's free to load onto your systems as a business. It will protect you from a significant percentage of phishing. We're looking at other initiatives too that will help globally to protect against some of these things.

There is a perception, I think sometimes that if criminals are active in the cyber space, they're all abroad, they're all in jurisdictions that we can't touch. Well, that's not quite true. We look very carefully at where we can disrupt criminality. We've got a unit within the City of London Police, which is supported by the Intellectual Property Office. Looking, for example, at websites that are allowing people to download music and films for free illegally. We have done some terrific work with the industry to actually get a system whereby we can block and close those websites down, wherever they may be. We can take the fight to the criminal.

I think it's interesting that Matt mentioned in his talk that technology is going apace, and maybe legislation and regulation is slightly behind. My view might be that's always been the case, because you often have to shape your framework of regulation or legislation based upon where you see the developing and emerging threats. I don't think that that's necessarily a bad thing. I think the important thing is that we're aware of that and we're looking for the opportunities that we can.

Helping people understand, I mentioned that, is a really important piece of the work we do. Technology, I would say, is a force for good absolutely. But I think we are seeing new technology emerging that again, we have to help people understand what that means for them. The internet of things is, I think a very confusing concept for many people. I think understanding the implications of big data and just how a small piece of information that you give as part of your daily business online is fine and is limited, but it's the combination of that matched with everything else that somebody, should they choose to, to develop and build that picture of you, creates a very, very powerful tool. The criminal can use that as well as businesses.

Where do I think, in sort of coming to an end, that our focus should be? I think prevention is really important. If I take businesses first, there are emerging technologies and emerging businesses in that space. I think if you look at some of the more traditional industries, the banking sector and financial services is a really good example. There is a significant amount of regulation around those industries. I don't see that in the emerging social media industries, and I think what we're seeing is that gradual shift of public acceptance of what they can and can't do.

What I mean by that is that they're very good, and apologies if anyone's in the social media world, I don't want to tar everyone with the same brush, but I think they're quite good at creating that they're very trendy and they're slightly anti-establishment, they never wear shirts and ties, they wear t-shirts. They're kind of quite cool. But actually, the data that they're developing and they're mining and they're using is significantly powerful. I think now in the light of certainly some of the terrorist incidents where there's been evidence that law enforcement has some challenges around accessing some of that data through phones, et cetera, I think there is a recalibration of that, that to responsibility of that industry. I think it's part of the fact that they're an immature industry in terms of life cycle.

Businesses can do more to protect themselves. Last year, TheCityUK did a survey with Marsh and it's on the website TheCityUK website, so you can have a look at it, around cyber in the city. There was some interesting data came out of that survey, which is really quite impactive. It surveyed city businesses, and you would've thought they would be at the forefront of some of this prevention of cyber. 70% of the businesses that surveyed didn't have cyber in its top 10 risks. Something like 60% had not considered the impact of a cyber-attack on their business. A similar percentage had no proven or tested plan to respond to a cyber-attack. Something like 40% of the businesses surveyed believe that cyber is an IT issue. Given those statistics, and I suspect if you looked at any sector anywhere, they would be similar statistics. We have a big challenge ahead of us to educate people to better protect themselves. Some of the learning coming out of things like 'wannacry' is, actual the patching and the technology to prevent some of these attacks and these viruses and these ransom wares already exists. You just need to make sure that you're using it.

When I get into the personal space, young people are far more relaxed ... I'll use that term ... about personal information than perhaps people of my generation. We've seen examples online of young people holding up a photograph and posting it on Facebook or other social media of their newly acquired driving licence, or their newly acquired passport, not realising the vulnerability that they have of the part that people can ... I go back to that bit I said earlier about being able to take small bits of information and build the picture that then can be used by criminality, and it's a vulnerability. Education is really important. In a world where the most commonly used password in this country is password. The second most commonly used is 12345. We have

a long way to go in order to educate the public and the individual citizen about their responsibilities around cyber.

Then I'll finish really with just technology impacts all crime, not just cyber. It enables the criminal much easier. Scale wise it's much bigger. Frankly, who would rob a bank now when you can go online and make significant sums of money. One just very quick example, if I may. We did recently a ticketing scam, is a big challenge now as the demand for these big concerts of significant singers and musicians. We set up a false account on Facebook saying that we had tickets for a concert of Ed Sheeran. I hope most of you know, played at Glastonbury, headlined my daughter tells me. We said, we targeted it and we said that these tickets were available at ridiculously low price. The old adage, "If it's too good to be true, it's not true," is really very valid. We advertised them really, really cheaply knowing that they've been sold out within minutes.

In something like six to eight hours, we had enough people coming online to try and buy them and instantly also we were asking for bank transfer, which is also a vulnerability. They were coming on and the point they clicked on the page to say, "We want to buy them," it said this is a page operated by the City London Police. This is a fraudulent site, beware of the risks, et cetera. We could've taken in eight hours, £75,000, had we chosen to. I didn't for the purposes of integrity, and the minister being here. That just shows you how the volumes are massive. It's changing the way criminality operates, and it's changing in that piece just to pick up what was said earlier around security.

The whole world of technology has changed the world of terrorism as well. I don't want to go into all the stuff about the money and how they generate money through criminality. A lot of that is generated online. But if you look at the pattern of the latest terrorist attacks, the days of conspiring together in a physical location, or even through communication whether it be email or telephone, have gone. There is the ability now online to do all your preparation without ever touching anyone else. You come together at a very, very quick time and it's very challenging for law enforcement to be able to anticipate some of that. If you look at the recent attacks, yes, the press has said, a number of them were known to security services or law enforcement. Personally, I'd me more worried if they weren't known, because that would suggest they were looking at the wrong people.

But actually, understanding how quick they can go from talk and thinking to actually something that results in an action has now just speeded up beyond anyone's previous knowledge. I don't say that to alarm you, I say that it's just a reflection of how all criminality is shifting. Thank you very much.

Deepak Lal: Thank you very, very much. Before going on to some of the questions, which have been sent on, I just want to say something about the dark side of the internet. Matt picked some of it up and the Commissioner just told us, I've real recently been watching Game of Thrones, and at the same time reading a

very old book by ... I think it was actually a monster, a chap called Elias Canetti. He won the Nobel Prize for the novel called *Auto-da-Fe* but he also wrote this other rather good book called Crowds and Power. The book starts off by ... What he's really trying to do is to look from what we as human beings, or incipient human beings were like when we were roaming about in the savages and bands in the Savannah. His starting point, he said "The most primal fear which human beings have is fear itself, and their fear of being touched." Because you imagine in the Savannah, you're in the dark and someone touches you, you don't know whether it's a leopard or a hyena, or your friend or a familiar stranger.

He builds on this and then he has a whole classification of these different types of crowds. But I picked up a couple and some of these you'll recognise immediately. Some of these that actually what Matt was talking about. One of these is what he calls the crowd which is baiting people. This goes back a long, long way. If you think of the coliseum where Christians were being fed to the lions, the guillotine mess, the mother and the father admitting away the French Revolution. He makes a point that, the fact that this is not ended at least in the West. We don't have collective cruelty, but there's a bunch of bad places in the world. You just look at the pictures of ISIS and what have you, this is still there.

But what he gauged then is he said that where you still have this in newspapers, because in newspapers we have baiting, people go out and ... But the main point about that of course is that ... so Freedom of Speech, but there we recognise the libel laws that there is a limit, you can't. The thing about the internet, things that you mentioned, bullying. My daughter is a school teacher and she tells me that these young school girls now, they look at their Facebook page and see how many likes or dislikes they have and then go into some sort of trauma as it's have to depending up on that. All that, but the main difference now between the old baiting and the newspapers, is that all of this is anonymous. If you're going to think of any chatter, one of the things which Facebook and Twitter once we forced to do is to add in anonymity of people who put the things on. You could track them down.

There's no reason why you can't take someone who's posted some bullying thing on this thing and you can take them to court. The second group, and this comes back to some of the political things we were talking about when people talking about dysfunction of politics and how social media has made things worse. Here again, and that is quite useful, he looks at the war packs, essentially if you look at the Game of Thrones, there are all these different war packs fighting each other. In the war packs, you would have two, one here and one on the other side, but whatever that ends at, they have a battle and you measure your success by how many people you have killed.

A very important point, he says, as you have parliamentary democracy, evolving then in America, this removed this need for people to die for their thing. You still have packs. You are part of one. You stand on different sides

of the thing, and the battle takes place, whatever it is, and it ends as soon as a vote is delivered. Once the vote is delivered, that's the end. But this time, there aren't any dead bodies lying around. That's a way which is civilised, if you like, these basic instincts. That's still there, but that's everlasting.

This fits in to a very important book by a chap called Norbert Elias, called The Civilising Process. He describes how ... Essentially in post renaissance Europe there were people, Erasmus, Montaigne, they civilised our basic instincts. They internalised various ways in which we contain them. One other thing which has happened, which you're describing, which is criminal instincts could be there. These have been aided in some sense. You're going back to being de civilised in some sense in all these social attitudes, et cetera. It's these aspects of the social media I think, which you need to consider. One of the most important ways of removing this, it seems to me, is ending anonymity.

I know that Facebook, they're already keen on anonymity because they think this is the way to get liberation movements. Now the liberation movements, why are people on there, they're trolls, there all these bullying kind of things, and some people losing their lives.

Matt Hancock MP: Deepak, if I may respond to that.

Deepak Lal: Yeah.

Matt Hancock MP: We have to be realistic that human nature is pretty unchanging. The thing about the impact of the internet is that it brings great promise, but it also brings with it dark new threats. These aren't new threats, because humans are different. It's because the technology changes the impact. My sense is that the internet has grown up. I love this phrase of Robert's that the internet grew up without security in mind. It was a great liberation. It is a great liberation. We mustn't lose that. But, fortunately we have a code. We have a description of the way forward. Loosely, it's called political philosophy. Because for centuries, people have been working how to deal with these balances in the offline world, the balance between freedom and security is at its heart. We now need to apply these to the new technology and not treat the internet as a values-free area.

I think that we've got a blueprint for how to take this forward. It's just a rather large task of implementing it.

Deepak Lal: Common law, it's what you need to apply. That means you can't have people anonymously twittering, "I dislike you. I hate you. You're this that or the other." If they do, we should take them to court justice like someone does at a newspaper. I think that's very important rule. One of the questions which I've got here, "When will we see a conflict conducted or concluded in cyber space?" I think this rather went to ...

Matt Hancock MP: Conflict? When we say what?

Deepak Lal: A conflict conducted or concluded.

Matt Hancock MP: What a day to ask the question since this morning the defence secretary affirmed our offensive cyber capability. Isn't the truth that cyber is one element of security. The link, as you were saying between cyber and the physical is actually where the action is.

Robert Hannigan: I think we're already in a conflict. We have been for a while. There is a lot of conflict going on, a lot of nation states doing things in cyber space, which is at Matt says, usually part of a wider foreign policy or foreign intervention. States do behave pretty much online as they behave in the real world. If Russia's going to invade part of Ukraine, why wouldn't they switch off power in Ukraine if they have ...

Deepak Lal: Yeah.

Robert Hannigan: North Korea robs banks because they need money. They protect their rulers, or reputation in their nuclear programme, online in the same reckless way they do in the real world. Conflict is already here.

Deepak Lal: Yeah. Well, another question, "Steven Hawking has warned AI could pose a serious threat to mankind. Why isn't this talked about more?" Elon Musk is trying to colonise Mars, isn't he? I suppose it's being talked about. What do you think? Do you it's a serious threat, AI?

Matt Hancock: Ultimately, all this technology is invented by humans. Even artificial intelligence is designed, the mechanisms to generate it is designed by humans. That means that we've got the wherewithal to stop that from happening. I'm an optimist, but it requires not only the technologists to have a view, it requires governance and then ultimately government to have a view. Even as a freedom loving conservative, I believe in a strong framework around this. We've got to make sure that if we can't always be ahead of the curve, and I take you're very gentle chastisement over that, we've got to make sure we're up there ensuring that the freedom we enjoy exists within a framework.

Deepak Lal: Here's another question. If Mark Zuckerberg ran for president, would it be a step down?

Robert Hannigan: Certainly, financially it would be! I think there's a serious point that there is a generation of people who have grown up with and been part of this technology, who are part of the answer to what Matt has just been talking about. The internet is still relatively young. One of the problems is we still talk about the online world and the real world as if they're different things. Actually, there is one world and the great challenge for this generation I think

is to make civilization in the broader sense, so the freedoms we enjoy in the real world and the rule of law that we enjoy in the real world, apply online. The two should not be separate.

But because it's a new technology, that will take a while to get there, but I absolutely think that people like Mark Zuckerberg ... And it's interesting, in his generation, he's getting a bit older now and I think his generation are beginning to accept this, it's how you do it. I don't think necessarily the old generation have all the answers. I think if we had an audience of 20 year olds, they would have different answers, which wouldn't all be wrong. I wouldn't say that to my children, but I do think there is a dialogue to be had about how do we achieve exactly what Matt has been describing. Zuckerberg and others are part of that.

Deepak Lal: There are two others which are connected, what are the other sources of innovation that most excite you, and link to that what are the other threats from technology that most concern you? Who wants to answer that?

Lara Poloni: When you mentioned Elon Musk before, obviously there is ... We were talking about just how rapidly some of the technology is changing. Again, coming at it from an infrastructure perspective, some people think we're talking about some sort of Jetsons age of Hyperloop happening 20 years down the track. The reality is that here in this part of the world, there are active tests going on for Hyperloop in the US, that they're testing the test track for that as well. The Maglev technology is already here. I think whether you're talking about driverless cars or Hyperloop, I think the focus now should be on the regulatory aspect to accelerate the implementation. That's exciting, it's moving so fast, but I think we've all talked today about the importance of government policy settings and regulation. I think that's really a difficult frontier that we've got to tackle at the moment.

Matt Hancock: Undoubtedly, autonomous vehicles are one of the most exciting ideas. Not only because the straightforward convenience, but there is a potential future in which the impact of autonomous vehicles is that people don't have to waste tens of thousand pounds of their own capital by having a metal box that sits for 95% of its life outside your front door, or in your office parking lot. There's big positive economic impacts as well that essentially will make people better off by the fact that one day you might be able to summon a vehicle to your door at the moment that you need it, no matter where you are, and it will take you to where you want to get to.

But that also brings on to one of the big concerns and worries, which is undoubtedly that getting the cyber security of these great developments right, especially within the internet of things and especially once the internet of things starts to move. Then getting that right is incredibly important. We're really at the early stages of making sure that happens, but we've got a plan.

Robert Hannigan: But for me-

Deepak Lal: The other question for you Matt.

Robert Hannigan: Just to throw in my ... I think the advances of life sciences are spectacular.

Deepak Lal: Life sciences?

Robert Hannigan: Life sciences, and bioscience, biotechnology and nanotechnology put together with AI. You really offer extraordinary progress in healthcare in the next 50 years, which we will need.

Deepak Lal: Matt, this is for you. Is Theresa May right to emphasise the need for further intrusion for the sake of security?

Matt Hancock: That was more or less at the heart of my speech. The answer is of course to whether Theresa May is right is yes, because she's the Prime Minister and I'm a minister in her government. But, there's also a serious point here, which is that bringing this balance and making sure that freedom also is protected through good security, whether that's cyber security, whether that's making sur we have a prevention of harms, whether children are safe online, to ensure that terrorists do not have a safe space online. This isn't about intrusion in the internet. It's about ensuring that we protect people's freedom by protecting against those who would wish us harm. I think that the whole of the tech community is understanding that impact, and that movement.

We've got to work with not only government, but the private sector to make it happen. I think progress is being made, but I wouldn't characterise it quite as it was in the question.

Ian Dyson: I could just answer that. I think absolutely right, the old adage that one person's freedom is another person's prevention of freedom or loss of freedom, is quite important. We do need something which allows us to protect people and protect people's ability to go online and be safe, and to do their business online without the challenge of people harassing them or trying to disrupt their business. As a law enforcement officer, I'm absolutely supportive and up for, it's part of my DNA that I'm accountable for the powers that I exercise. There is a lot of mood music around the ability of law enforcement to intrude into everyone's lives. It's just a different space. It's no different to my ability in the past to in the extreme as to open mail and things like that. I have to be accountable for that. That's where I think the framework needs to show that law enforcement can exercise powers, but they have to be publicly accountable, and be seen to be accountable. These are also important.

Deepak Lal: Okay, I think we've fulfilled our duty. Thank you all very much.