APPG ON CYBER SECURITY MEETING MINUTES 23RD March at 09.30

1. **Present:** Simon Fell MP (Chair), Lord Arbuthnot, Alun Cairns MP, Baroness Pauline Neville Jones (Vice Chairs), Stephen Metcalfe MP
2. **Apologies:** Greg Smith MP, Lord West
3. **Speakers:**

Maria Axente, Responsible AI and AI for Good Lead, PwC UK:

Began by talking about the state of AI in the business world. There are many statements made by leaders of industry but what are the main trends? How can those who are tasked with reviewing AI understand where it is going? What has happened over the past 12 months? PWC ran a survey[1] across three continents and approached executives working in AI Most interesting stat: pandemic has accelerated focus on AI. Only 5% of those questioned are not using AI, down from 43% in 2019, so industry is investing in AI.

Most clients are struggling to work out how to make AI strategic rather than tactical. There is an understanding that AI needs to be included in business strategy. Need to be ahead of the market and investing in technology.

Clients have also signalled that the risk associated with AI: the real and present dangers such as discrimination, bias, enhancing other problems such as inequality, job losses and other societal problems. We can see that the risks are now better understood and taken more seriously.

We also asked our clients about the challenges of adoption. Data Privacy is a top priority. Cyber concerns are nowhere to be seen because the questions focussed on AI, PWC did other cyber security surveys so there is a bit of a disconnect. There is a growing interest between the two domains of AI and Cyber Security. Data privacy remains a key concern.

Legal backlashes can be triggered and algorithms can create discrimination so clients are thinking more carefully about the ethics of AI.

Another important study is the CEO survey[2]. Usually interview around 3000 CEOs but have now managed to interview around 5000. Significant increase in cyber security is a concern. In addition, misinformation around AI is a concern that has increased, this is a clear signal that CEOs understand the risks.

Every other day we see a report on the mis-use of algorithms. This draws attention to AI, it comes with strings attached! This does help to educate the public that AI is here and being used now in both the public and private sectors. We need to re-think how we use AI and monitor the use of algorithms. We know the fiasco of the A Level results in 2020, this drew attention to how algorithms can be used. It gave a lesson in how not to use an algorithm in AI. These headlines can be intimidating, need to focus on the positive, on where we have problems in society and use AI to help right these wrongs.

Important to keep in mind how AI is used in the commercial world. We have seen an explosion of use cases across the value chain. Technology is now used across all areas of business including HR which is a growing field. Technology was generally confined to certain areas of a business but is not

[1] AI: an opportunity amidst a crisis - PwC India
[2] UK CEOs plan a 'no regrets' recovery - 24th Annual UK CEO Survey - PwC UK

used throughout the enterprise. Some industries are used to managing risk such as Financial Services, but others are not and there is a low awareness of the risks associated with AI.

AI has to be done responsibly. Users need to understand the right values and embed these in the life cycle of the use of AI. Those who use it and develop the algorithms need to be cognisant.

Jorge Blasco, Senior Lecturer and MSc in Information Security, Course Director in the Information Security Group at Royal Holloway, University of London.

Slides 1 to 4: Want to cover the potential of AI to harm. Maria has mentioned many issues: bias; use of algorithms but will focus on what happens when we do bad things intentionally.

In the Academic world we talk about machines that will do what we want them to do. What is the process that they use to reason? They learn from data hence machine learning. When we create the algorithms the experts who write them have a huge level of input into how they work. AI systems can be purely designed to codify the experts' knowledge rather than learn.

Defensive AI is used today for example for most of the anti-virus software we use. This is based on the defensive AI concept. The opposite is offensive AI when we use our knowledge to attack systems or when AI is used to attack other kinds of systems.

Slides 5 – 6: To attack you need to know how a system works. When we want to build a system it starts by acquiring data and learning from this. Scientists try to obtain malware samples and use these to feed the algorithm. An attacker would use data poisoning to foil the AI. It could be done by an insider or the platform that is being used. The aim is to confuse the AI and ensure that it is therefore inaccurate. This creates distrust.

Slide 9: Feature extraction is mostly based on expert's knowledge. It uses permission to identify behaviour. An attacker could try to have the permissions be as close as possible to benign applications. It might try and mimic the permissions requested by Facebook for instance.

Slides 10 – 14: The algorithm needs to be trained so that it can be deployed across a system and detect / attack to bring a system down. We have not seen real cases like this.

Slides 15 – 16: The T shirt is covered in car registration numbers which could cause an ANRS to charge. The T shirt on the left is designed to confuse a facial recognition algorithm.

How can we use AI to attack? Slide 17 shows an exercise that was conducted. In Slide 18 we see that the teams qualified the knowledge and then inputted the results into the algorithm so that the AI did not learn. The humans are still better but not faster than the machines!

Are these feasible? They are mostly in academic settings. As we also know they not only use AI for improving business processes.

Conclusion – AI in attack mode is here but not yet being used outside of academia.

Colin Crone

How is AI used in Cyber security? ISO has only recently had an approach from the UK to use AI to develop guidelines for cyber security for AI. ENISA[3] has just set up a panel of experts on AI and Cyber Security. Standards and guidelines can take up to three years though to publish.

RUSI[4] was commissioned by GCHQ to see if there was a need for AI tools in national security. Concluded that there "may" be a need and they also addressed other issues such as ethics, data privacy etc. Answer was not that conclusive. We know that there is a huge budget for cyber security within national security budgets.

Govt is not a great example of cyber security, the National Cyber Security Strategy was criticized by the Public Account Committee in Feb 2019. The principal complaint was that the NCSC would only meet one of its targets. NCSC is the only part of the Govt which is concerned about publicising the production of safe systems. The NCSC website is heavily used by cyber security professionals but needs to be used by everyone. The mind set for seamless security should be the same as locking your car or house door, not difficult or exceptional.

Ask of the Government: Quantum computing will render current today's cyber security encryption useless, the security system that the world uses to protect data. The increasing use of IOT increases the level of risk. I would like to see a larger need or message to the general public to take cyber security more seriously. Look at the GDPR campaign and follow that as an example.

A quote from Joshua Burch head of Security at FTI Consulting, "try a mental experiment of a pre mortem and to imagine themselves standing in the ashes of a devastated business in the aftermath of the cyberattack, which most brutally exposed the weakest flank, and to ask yourselves: What do you now wish you had done in preparation for this moment?"

4. **Questions and answers**

a) Simon Fell MP and APPG Chair - Building on Colin's comment, the Online Harms bill talks about the need for transparency about the algorithms that sit behind AI. What is your view on the tension which this brings out? The more transparent we are the more risk there is of being attacked. How can we get the balance right?

   CC- what do you tell and what do you give away? There is a lot of theft and espionage in IT to try and get the advantage. Transparency itself is a need to make sure that we understand what people are doing is safe and that bias has been removed. Signing up to openness is not the same as giving away secrets. Important to follow the standards as they come out and to be audited. Having standards with a trustworthy authority will be important.

   JB – Big element of IP, do not want your algorithm to be fully transparent in case it gets stolen. Encryption algorithms are open in the sense that they are subject to scrutiny and inspection. In AI it is more difficult as you need to share the data that was used to create the algorithm, this may be secret or help to losE IP. Having independent authorities is fair.

b) Simon Fell MP and APPG Chair - is HMG naive to ask for transparency?

   CC – need to work out the mechanism. In one way it is naïve, unless you work in this environment, the awareness of how it works is difficult and businesses will want to keep their

[3] ENISA (europa.eu)
[4] Artificial Intelligence and UK National Security: Policy Considerations | RUSI

commercial edge. AI is expensive and requires investment. Govt needs to work out the mechanism for transparency.

c) Andrew Clarke - accountability and responsibility is a strong point here. You can give so much information out but it is like drinking from a firehose, need to be more diligent about how we educate the masses about AI and cyber security. All the information is no good to anyone if it is not structured. We talk about how private organisations can help the public but see no progress. What can be done to push this?

   JB – try to look at professionals. Maybe we focus too much on teaching professionals and not enough on more generally teaching the people about cyber security issues. Huge effort to teach my parents about scams for instance. Banks and FIs spend a lot on educating customers. If we can educate people from an early age, that would be a good investment. Need to make sure that is done well, need to set a good basis.

   CC – major problem for small firms and works in managing risks. Need for more education, awareness support and not many organisations can do this. GDPR is a good example of how to get a message over. Needs to be a lot more information flowing around.

d) Stephen Metcalfe MP – what is the average size of the business surveyed by PWC? Fear that it focused on large firms which have the resources to look at these issues. SMEs do not. What interaction is there between the trade organisations to try and educate members to risk and opportunities. Secondly would like to back the call for a wider public conversation about AI. People generally do not understand how their data is being used nor what they are giving away. How can we get the conversation going at scale?

   CC – T&Cs are a problem in that most do not read, I only skim through. Younger people tend to be more blasé, they want the app more than any risk implied. Angry Birds free version asked for all your contacts, there was a scandal and it was asked for less. People like it because it is fun. People do not value personal data as much as they should.

   JB – in terms of trade bodies, not aware of anyone helping small business or the self-employed. NCSC has cyber essentials and should spend more money on promoting these. Big business is prepared, small business cannot afford to defend themselves. Also need to reduce the costs.

   Apple has recently changed the way data is captured and stored. It presents this in a simple and easy to read way. Facebook was very angry with this. Needs to be easy to understand for the people. It has had an effect on the way apps are downloaded. Apple does check that data collection is done properly.

   If business model is based on data collection this creates a conflict. Need to find a solution to this. Apple uses this as a selling point as they do not make money from selling apps.

   SF – Vodafone issued a report to say that if an SME is hit by a cyber attack they cannot afford the costs of coming back. Huge education gap.

e) Malcolm Warr – drafting the FSB advice on this. Is also an advisor to IASME. Downside is that this information is there but not well publicised. Interested to know what people think about how AI will help us in the balance between defence, security and humanitarian Aid?

JB – UK is in a good position to be in the forefront of AI. What do we use AI for, more offensive or defensive capabilities? Other countries are developing these capabilities. It is well known that there are nations which have huge defensive capabilities. It is known that some attacks are created by foreign governments on commercial interests.

Where do we spend our resources? How can we make our defences more efficient using AI, that would be a good use of AI. Difficult balance with ethical considerations and public ones.

CC – agree with Jorge. AI should be used to improve. Economic element needs to be protected, a lot of the economy is based on small businesses. Affordable AI would be great, how many objects do we have in our houses such as Siri, Echo etc that are routes into attack us? Need to deal via education with the easy things.

JB – would like to add how can AI be used initially defensively. Home Office gave money to a company to identify extremist videos online and automatically classify them. Also need to think about whether this creates an automatic AI censorship system, do we want this? Could we use AI to help moderators who have to watch unpleasant and hard to watch videos and so save them from harm.

f) Prof Keith Mayes – observation – can remember working on automated systems 20 years ago. The concept is not new but has increased in scope and scale. Calamitous result scares the most, even years and years ago there was no shortage of people who wanted bias in decision making. Most of what we know about cyber security does not help us. If I look at AI, it has to have some learning and adaption in there. It could be that the learning gets targeted by a malicious 3rd Party. That creates instability which is a worry, think of stock market sell / buy systems.

Think of it like fire safety: a small fire can spread rapidly and go out of control. What are the fire doors or the sprinklers?

CC – this is a very real problem, the Microsoft TAY BOT[5] was meant to learn through experience and became a white supremacist chat BOT overnight. If things go wrong, humans need to be able to intervene. Removal of bias is very difficult. AI cannot control AI. AI does what it is told.

JB – need supervision and monitoring just as we do for a PC against malware for instance. If you know how the system works, you can exploit it. Huge challenge because the benefits of connecting up systems may outweigh the risks.

5. **Conclusion**: Simon Fell thanked the speakers for their time and answers.

[5] Why Microsoft's 'Tay' AI bot went wrong - TechRepublic