APPG ON CYBER SECURITY MEETING MINUTES

Date: 20th October 2020

Location: ZOOM CALL.

Present:
Simon Fell, MP, APPG Chair
Lord Mackenzie of Framwellgate
Tony Lloyd MP
Alun Cairns MP

Secretariat: Prof Keith Mayes and Andrew Henderson

Speakers: Paul Chichester, Emily Ferris and Matthew McCormack.

Chair's welcome
The Chair introduced the topic: Russian hacks into UK Covid-19 research and welcomed the speakers and the guests. Added that Parliamentarians need to keep abreast of these issues.

Apologies have been received from:
Lord Arbuthnot of Edrom
Sir George Howarth MP
Greg Smith MP

Presentations

1. **Paul Chichester MBE, National Cyber Security Centre**

Paul introduced himself: role at NCSC is to ensure that the UK and the NCSC has a good understanding of threats, is able to respond and deal with incidents. Deal with 600 per year, both state and criminal. Works at a deep technical level to understand the "how" of an attack as well as assessing the threat origins so that the Govt can make public attribution. PC reminded the meeting that this happened yesterday[1].

There are the Big Four (Russia, China, Korea and Iran) state actors but this does not preclude others and seeing an increase in a threat from other states. Driven by accessibility of high-end cyber capabilities and the ability to develop malware. Also look at cyber criminals.

Advanced Persistent Threat 29 cyber actors were attributed with activity against the UK from March onwards. The NCSC looked at what the actors were doing to make an impact on the UK's response. This was both State and Criminal activity. Saw a significant change of requirement from State actors supporting their national interests and needs. We saw a number of threat actors and called out APT 29 which is a Russian State group which targeted companies developing the vaccine. The capabilities

[1] https://www.ncsc.gov.uk/news/uk-and-partners-condemn-gru-cyber-attacks-against-olympic-an-paralympic-games

that the adversary was using were not well known in the public domain. Part of the NCSC role is to share the details of the technical capabilities that were being used.

Another key element is the international approach that we take. We collaborated with the US and Canada. This is a common theme and is true in our response to Covid. Try to build international coalitions and share this at scale.

2. Emily Ferris, Royal United Services Institute

Emily Ferris is a Research Fellow specialising in Russia's domestic policy. Emily's presentation gave the meeting some context for their cyber activities.

How Russia works – all know that Putin leads the country but there are many institutions which are overlooked that have say over policy areas. State Council is an advisory body to Putin (80 plus people), others in Putin's circle of trust which remains the same as it was in his early career. Putin's management process needs to be understood.

False to believe that everything happens because of Putin's say so. This is impractical. The Russian system, with its corruption, does not work well and this means that many goals do not map out as they were meant to and Putin often has to intervene. Russia can weaponise criminals but corruption within the body politic ensures that matters do not work as they are meant to do.

The perception is of Russia as hugely powerful and a significant policy actor. Matters like the Crimea annexation was an anomaly. There are a lot of unsuccessful foreign policy initiatives and Russia has been successful at convincing the West that it is better at policy than it actually is. Matters do go wrong frequently!

Take the Covid vaccine as an example – the hack that was reported in the UK Press may be more about sending a message to the Russian people than us in the UK. The Russian Government announced that a vaccine was available domestically, no evidence that this works though. Lot of economic pressures with important elections to the Duma due next year so it makes sense to undermine other countries efforts to obtain a vaccine so Russia does not look too far behind.

When we talk about Russian involvement in the UK there are many interest groups: business, spies etc. Russia has trade interests and intelligence ones in the UK. Brexit means an advantage for Russia as we have been vocal in pursing sanctions against Russia in the EU and taking a lead with this. Unilateral efforts against Russia by the UK are unlikely to have a major impact. The united reaction to the Skripal incident shows that a united front can be put together. The poisoning also shows that Russia must have calculated the inevitable diplomatic fallout with the UK and worked out that the breakdown in Anglo-Russian relationships would be a price worth paying.

3. Matthew McCormack, SVP & Chief Information Security Officer, GlaxoSmithKline

Matthew McCormack is the SVP & Chief Information Security Officer at GlaxoSmithKline. Has been fighting the Russians and the Chinese for around 20 years in cyberspace. Tech has changed but not the tactics. Lumps China and Russia together.

Contrasted the UK's NCSC with the FBI and the NSA who tell industry what they think whereas the NCSC partnership is more collaborative. Thank you to the NCSC.

When Matt looks at the challenges of Covid, the vaccine and Russia agrees that the way that the Russians approach hacking is different from the Chinese. The Chinese are loud and do not care that we know that they are there. They are not afraid to be caught. Chinese will deny even if caught.

Russians are patient and quiet. They will wait until they need to in order to turn something on. Reflects spy statecraft. Can be difficult to trace back to Russia, have seen them outsourcing. The Sony breach was attributed to an outsourcing project to North Korea by China. Have seen Eastern European gangs trying hacks of both GSK and Astra Zeneca. GSK has thousands of 3rd party companies some of which have been hit by ransomware. A large Indian service provider to GSK was hit in April as were a number of healthcare services companies. This meant that GSK was locked out of own studies, had a shipping company hit so GSK medicine was marooned on the high seas on the way to South Korea and Japan.

GSK has a robust security operation so easier to hit much softer 3rd parties. Move to the Cloud means by many smaller firms who do not believe that they have to follow the same security requirements as large ones. GSK will be very dependant on many 3rd parties to deliver the vaccine to people. The Russians will go after the soft underbelly of 3rd parties.

GSK does business in China and Russia. In China any police officer can enter a building and demand to see everything on the server. This is also true of Russia. Trying to avoid putting servers into Russia and not have physical devices in situ. This means that a policeman could walk in of the street and potentially take the formula for the Covid vaccine.

Russians want to do their own thing like China's Great Firewall. Process in the EU called serialisation which tells you when and where a medicine was produced. Russia developed their own system to trace the provenance of their own systems. We know that they are coming after to us every day and we know that they outsource. They are also legitimate customers with legitimate needs for medicines. GSK is extremely paranoid about protecting data, fear is when the company has to start sharing with 3rd parties for manufacture, distribution etc.

Questions

1. Lord MacKenzie – interested in the aspects of hacking which can be proven.
    - Are we simply identifying the country of origin or can we prove the hack is form a particular organisation, person or location?

    - If blackmail is acceded to, do you actually get your information back or do you lose your money?

    - When is a hack a war crime or warranting a military response?

MM – Intelligence could do more. There are legal restrictions such as "Hackback". We do not hack back. Attackers will attack through various hops using a University system, Starbucks etc. Will typically turn the investigation over to the FBI or the NCSC. Sometimes the hacker signs his / her work, likes the victim to know who created it. The Security community can attribute to certain people.

If you pay ransomware, they will come back as they know that you will pay.

PC – attribution is talked about a lot in the cyber world. One of the NCSC core functions is to build up that evidence. NCSC uses certain language along the lines of the UK considers it almost certain that X state is responsible for Y hack. Very formal process by the NCSC that looks at probability and confidence in the result.

"Almost certain", "high level of confidence" are terms that mean the Government has both technical and other evidence. Usually the Govt has humint or signals intelligence to hand. We have been tracking some of these groups for 20 years which helps to make statements around attribution.

Work with law enforcement partners on ransomware attacks and use multiple sources of intelligence.

Worked with NATO on Skripal and share information with friendly parties. Very often the intelligence is obtained by methods that cannot be used in a court. People talk about false flagging and we see a lot more of this. Must penetrate the adversary well to understand this and usually a state related activity.

EF – Military response with Russia is not the most effective way. More means at our disposal that do have a high impact such as a withdrawal of co-operation, excluding Russia from certain decision making processes etc. Reinforces the Russian narrative that we are against them though. Take yesterday's sanctions (Navalny), the sanctioned are not necessarily directly responsible for the attack but are important figures in the Administration and close to Putin. Moreover, they are thought to be senior in the administration and have helped to create the system that allows actions like this to take place. Some sanctions can hurt e.g. hitting a UK-based business.

Simon Fell – are our reactions proportionate to these threats?

EF – impossible question as the community of observers is divided. The Government is divided as to whether or not we should engage with Russia. Theresa May's ultimatum to Putin played out well at home but was not realistic in Russian terms.

UK and Russian relationships are less close now than 15 years ago. The Russian and UK private sectors may be interested in a more co-cooperative approach but without a political change in Russia, will not happen.

2. Alun Cairns MP – APPG serves a really important purpose, Cannot recall a Cabinet meeting that discussed this topic specifically. Cyber Security does not have the profile that it warrants.

Does Paul feel that he has enough Government and Parliamentary support (financial and other)? If you think of the time that Parliament spends on Defence issues, not replicated in relation to cyber security.

PC – there is extensive Government interest esp. since the 2015 cyber security strategy. Cyber security is very much baked into Government processes. NCSC views It through a geo-political focus. Writes to Ministers on a weekly basis with an update.

Parliament is still on a journey in this space. Great to have a forum like the APPG. Since Parliament was attacked has seen more interest and would like to do more. In terms of scrutiny, a good question as the NSCS does appear in front of Parliamentary Committees in an increasing way

Emily – where are their really productive institutional relationships with Russia? You can imagine the co-ordination that we have with NATO, although there are tensions, we co-operate.

Plenty of business co-operation going on. Not a fantastic climate but companies are hanging on. Intelligence co-operation is at a minimum. Tends to be around emergency matters. Other problem is a lack of educational links which were cut due to sanctions. Hard to go to Russia, to get a job or

study there. Not enough funding for people to study Russian. Difficult to get that expertise in the UK. Better in Continental Europe.

Little co-operation with think tanks. Need to understand how they think. In sum a lack of contact at many levels makes it difficult to build links.

Matthew Lewis – do you believe that the private sector takes cyber security seriously and reports incidents?

The risk of a cyber security incident is what keeps them up at night. Does think that senior leaders in business take it seriously. Bank of America appends US$1 bn on cyber security. Has a team of 300 people at GSK Most companies cannot afford this. Estimates a shortage of 5M people across western countries for cyber security. For me, getting more people into cyber security is key. University programmes are not producing the people that we are need. The Master's or Bachelor's degree does not cut it, happy to take people from an audit, psychology or accountancy background.

Many CEOs rely on their insurance policy and hope. We, the industry, need to help people understand the risk, look at TikTok or Hua Wei. Get more people interested is key. It is a well paying sector so people should want to get into it.

Prof Keith Mayes – NCSC has done a good job in encouraging people to study cyber security. Interested in different ways of training such as Capture the Flag (supported by NCSC and DCMS0) initiatives. Cited one example of someone who approached cyber security like a game, some room for those types of activities and approaches.

MM – typically the annual training for cyber security is read a Powerpoint and tick the box at the end. Now using a gaming based training option.

Tony Lloyd MP – how we disseminate the culture of cyber security is interesting?
What is our capacity to match technological change in those who would do us harm?

PC – Govt has invested in the last spending review period a significant amount. The NCSC is invested in tis workforce and understanding technological change. Partners with Universities and research institutes to cover gaps in knowledge. By way of example, have done work on AI.

MM – personally speaking, starting to see some wise decisions about data nationalisation, keeping data in country for instance. A lot of energy is going into the security of driverless cars. These are great but I want to know where the database is? The data has to go somewhere. Changing how taxes and tolls are charged, so move towards a per mile rate. Scared that an Amazon might end up selling that information back to the Government. Govt needs to invest in public data stores first so that they so not need to be bought.

Is there any pathway towards the kind of relationship with Russia that we have with former Warsaw Pact nations?

Russians believe that they have a democracy. Also have a different world view, tendency is for the UK and Russia to speak past one another. They see us imposing democracy on Warsaw Pact countries which they do not want. Russia wants to maintain their political/economic/security stake in these countries. Will not change under current leadership. Important question: where is Russia going post-Putin? He will probably step down in 2024. Need to understand who is up and coming.

Need to understand how these people think of the West, democracy etc.

Glen Bluff – how would the NCSC get visibility of potential end points that companies might have in China or Russia?

PC – NCSC is heavily focussed on the threat end. News is a service offered as a type of early warning system. Automatic feed of vulnerabilities etc. Do a lot of knowledge sharing.

MM – one of the areas that occupies most of my day. GSK has grown by overnight acquisition so a constant challenge. Shadow IT is a nightmare.

Glen Bluff - Are you seeing an increase in protectionism around data privacy e.g. individual takes on GDPR?

MM - Yes, have more lawyers than ever before. My ability to deploy IT is delayed by this.

Jon Inns – made the point that reform of the Computer Misuse Act would be welcome. Matt mentioned that the supply chain is a concern due to vulnerability, do you see that people are attacking your supply chain to slow your progress?

MM - Not that, health sciences in general are being hit hard. Have to notify the Government if you pay off hackers for instance.

Keith Mayes – in the covid situation there are a lot of organisations that have been thrown together rapidly and do something vital which has value. You see Universities, small companies, health systems and none are renowned for resistance to nation state attack. Are we confident that this is not a losing battle?

PC – no, not a losing battle. From a UK perspective, one of the leading nations to understand the threat. NCSC spends a lot of time dealing with activity that could be fixed by a lot of companies directly. Want to focus efforts on nation state type attacks. Cannot expect companies to defend at scale.

Conclusions Simon Fell thanked the speakers for giving up their time and being so candid. Alun is right as we need to get more parliamentarians involved. Will circulate a note of this meeting and the future programme. Please do raise issues which you think that we should be discussing.

Next meeting: 3rd November: Doing business with the US Department of Defense: Cyber Security standards