APPG ON CYBER SECURITY MINUTES OF THE MEETING
26th January 2022 at 3.30 p.m.

Title: The UK Government's Cyber Security Strategy – keeping its own house in order.

Chairman's welcome: Lord Mackenzie welcomed everyone to the meeting.
Apologies: Simon Fell, APPG Chair
Present: Baroness Neville-Jones, Lord Mackenzie of Framwellgate (Chair), Alun Cairns MP (represented by Corrie Driscoll), Bim Afolami MP (represented by Laura Bailey), Damien Moore MP (represented by Will Frost)
Speakers: Pete Cooper, Deputy Director Cyber Defence within the Government Security Group in the UK Cabinet Office. His role covers the Government sector cyber security, the Government Cyber Security Strategy, standards and policies as well as responding to serious or cross government cyber incidents.

First ever Government Cyber Security Strategy (GCSS) for the UK Government and public sector that looks across the whole sector. The National strategy focuses on the UK as a whole and how we get all sectors working together.

The GCSS is focused on the Govt sector and how we drive the step change in protecting citizens, services and data. Formally launched yesterday 25th January.

Aim – increase cyber resilience in all public services from a cyber security perspective. Runs until 2030, long term strategy for long term change. Government's digital estate is complex, like so many organisations, and the scale and the challenges mean putting long-term foundations in place are a key first step. Priority has been given to areas of higher risk.

By 2025 critical functions / systems are set to be hardened to cyber attack and the rest of Government by 2030.

Two main pillars:
1. Foundation of strong organisational cyber security resilience to cope with, for example, ransomware. Their business model is best disrupted by resilience, good practice and hardened security. As threat actors move on, being grounded in cyber security resilience means we can grow and adapt over time.

2. 2nd pillar (Defend as one) is focused on how to work better as the Govt and Public Sector in communicating and collaborating around cyber security. There are a lot of inter-dependencies across all government organisations. This pillar aims to work together to share information and best practice as well as vulnerabilities to help beat attacks. Foresees a collaborative approach which will bring benefits.

Key challenge is understanding the state of cyber security in your organisation at the moment. There is an ongoing effort to create a mature assurance process to assess Government cyber security. In the past we have had a minimum standard for cyber security in Government. We want to mature that through the Cyber Assessment Framework (CAF). This lays out the key areas of cyber security and what good looks like. This involves significant collaborative work with NCSC to deliver the risk profiles. This will transform the Government's cyber estate for the better.

770 incidents reported to NCSC in the past year, 40% of which were Government related. The Framework will help to solve these attacks.

The resilience pillar, number One, is based on breaking down the challenge of cyber security risk within organizations. Cyber Security teams work hard and with passion to meet their objectives. Throughout the development of the strategy we have considered how the burden on departments can be reduced. The strategy pillars map across to the pillars of the CAF. This means that when organizations report back using the CAF, progress against the GCSS can be measured more easily as results will map to the various elements of the strategy.

What does "good" look like? Got to manage the risk on a by-Department basis. Departments will need to engage and support organizations under their purview. Education, Health and local Authorities are specific target areas.

Now that we have understood those structures, how do we protect those areas that need protection from cyber-attack. Has to be proportionate and make sure that Departments have the right tools, capabilities and people. Work with Departments and across the Government to protect against attacks. Need also to detect attacks and coordinate campaigns as early as possible. Adversaries with enough resource and time can usually get anywhere.

Incidents will happen, so have to ensure that the tools are in place to manage both departmentally and across the Government as a whole. Not just breaches but also critical vulnerabilities. PC cited a recent incident and how they worked to reduce the risk and tell everyone about the vulnerability in question. This is about "defend as one", no one part of the Government should feel that they are alone.

Across all of these pillars, we need the right people and skills. The final objective therefore is to ensure that we have the right skills and culture across all organisations. This also means having

the right level of understanding at a senior level as well as industry specialists. Currently running a project to look at improving security via innovation with UK SMEs.

The project has good support across the Government.

Questions:

Prof Benson: what is the cyber security culture project and how can other people get involved?

PC: Project is up and running now and have got six organisations who have pitched to their ideas about how to drive culture change across Government. Set them a number of hypotheses to test their offering / assumptions. At the end of March, we aim to have a blueprint for cyber culture in the Government.

Lord Mackenzie – is the biggest threat from State actors or lone wolves? Do you see a cyber attack as an act of war?

PC: the final one is not a small question! Tend not to use the word hacker to cover all such activity, as you can have good and bad ones. Hacking is more of a mindset and approach, harnessing and working with 'good' hackers can be very helpful. For example, as part of the strategy we will role out a vulnerability reporting service so that a hacker who finds a vulnerability within a government system can report it to us easily. When it comes to risks and challenges the effort that large scale actors can put into campaigns is significant and that is a huge challenge. There are different reasons why nation state actors engage in activity ranging from espionage type activities through to disruptive activity.

Ransomware gangs have significant capability and financial resources.

Durgan Cooper – how will the vertical alignment of the CAF be engaged? As you have the framework, I understand that you will look at different sectors and environments.

PC - when a sector wants to apply a CAF to their sector, they need to state what they want to achieve and the types of threat they are facing. We are developing threat profiles for government that can be mapped to CAF controls that would mitigate threat. There will be a baseline Government profile which everyone will be expected to achieve. An enhanced profile is being developed for more critical areas of Government, working with the NCSC and we are looking to align work with CNI.

Sanjana Mehta – works for a professional organisation for cyber security practitioners.
Given the scope of the strategy, where does the Government most need to strengthen its work force?

PC – There is no particular role that stands out. Technical teams and leadership are crucial, as well as policy and strategic teams. We need to think about how we can fill and shape gaps. Historically the effort has been on the technical skills and we need to develop the policy / strategy people as well.

Does the Govt experience competition with the private sector in hiring cyber security experts and what is it doing to mitigate this?

PC - Yes, there is competition with the Private Sector. The Government cannot compete on salaries and this is a challenge. We need to be creative, for example, show how easy it is for people to move between sectors and lay out a career plan.

Graham Mann – how will the Government keep the strategy fresh and up to date? It would seem sensible to have a centralized SOC with an overview of all departments, CNI, NGOs etc so that attacks are monitored and action taken.

Whilst the Government says that it wants to work with the Private Sector, there are some 3000 companies out there offering 10,000 + solutions, is there a mechanism in the Government to track these?

PC – Good change in cyber security takes a long time. The more that we can have a fixed direction helps the teams. We now have "what good looks like" with the GCSS and know that evolution will occur.

We can already do some centralized monitoring through NCSC and their ACD services. What we are trying to create through the cyber security co-ordination centre is a central management function. Not looking to have a 'SOC[1] of SOCs' though.

Throughout the writing of the strategy we had an external challenge panel to work with us from the private sector and academia. TechUK were also engaged as part of the development. All of this effort helped greatly.

[1] Secure Operations Centre

Simon Fell MP – started the day with the FCO talking through the threats that they are facing in cyber security. Struck by building in resilience and ensuring that the Govt is prepared for any shocks which might come. Concerned that we are reliant on a small number of Cloud providers. How do we build resilience into the market?

PC – hard to turn round quickly and be better in Cyber Security. Good to hear that the FCDO team are briefing on the GCSS. On the question of suppliers, scale and risk there is no one answer. A hyper scale cloud provider brings a huge amount of resource and capability to deliver services with significant resilience and back-ups. Also means that they can afford large scale cyber security teams. A bigger number of smaller providers brings the risk of whether or not these companies can supply the right levels of cyber security support.

Lord Mackenzie and Simon Fell thanked the speaker and those who asked questions.
Next meeting – 22nd March at 3 o'clock with Ciaran Martin