APPG ON CYBER SECURITY MEETING MINUTES 13TH JULY 2021

Title: The meeting will look at the electricity market and the cyber threats.

Chairman's welcome – 11.00a.m. This is a meeting of the APPGs on Cyber and on Energy security. Calls for greater diversity in the system, interesting to find out how cyber threats are fought off.
Present: Alun Cairns MP (Chair of the meeting), Simon Fell MP (APPG Chair), Lord Mackenzie of Framwellgate
Apologies: Lord West
Speakers:

1. **Simon Jenner, Chief Information Security Officer, National Grid**
   Active level of engagement from Board and CEO in cyber security, executive engagement is essential for success. National Grid provides critical services to the UK and security accordingly is very important to our organisation.

   Approach is threat led, need to know who the bad actors are and how they operate and we work closely with NCSC to help prioritise investment and priorities.

   Risk and threats are common across sectors but the impact is different. Cross sector we see a lot of financially targeted attacks such as business email compromise and associated fraud and ransomware. Ransomware has the effect of disruption of service e.g. Colonial Pipeline. Criminals have been hitting public infrastructure, particularly in the US for the past two years. A threat-led approach is critical to enable an effective defence and security needs to be dynamic to meet these threats and deal with them.

   Perpetrators operate across borders, beyond the reach of the law. This is the major issue and crime does pay. Govt could focus on the right legal framework, work with local law enforcement where the attacks come from. Every UK business is a subject of these threats so this approach would benefit the whole of the UK.

   Glenn Bluff –
   1) Do you think that the regulatory framework for cyber security is robust enough? Is it effectively enforced?

   We have the NIS[1] regulation and a national CERT which NCSC provides, requires us to ensure that we have a robust process to assess risk. Ofgem will audit us against this. Ofgem has worked over the last 2 years with the industry and held a recent meeting to talk to industry about the obligations and the enforcement mechanism. National Grid works very

[1] The NIS Regulations 2018 - GOV.UK (www.gov.uk)

closely with Ofgem on this. The role of Ofgem is very clear in terms of sanctions and policies. Framework is evolving and there is a clear path.

2) How does it compare to cyber security in Financial Services, which is the most mature?
FS is more mature, about 2014 the Bank of England launched a new framework which initiated mandatory testing in the sector. Big believer in how to manage risk, testing is objective, takes subjectivity out of things. Opportunities to improve and learn from other sectors.
In the US it is quite different. The regulator has a prescriptive set of requirements. Audits are annual, companies do get fined but quite small ones.
SJ prefers a principle based measure with enforcement.

Sarb Sembhi – what is particularly unique for your organization? Would you favour unannounced Pen Testing?
Most importantly in favour or testing e.g. CBEST[2] and TBEST. Doing it unannounced is not particularly helpful. If governed well it is good such as using an independent company and at a time that is responsible.

2. **Dr Stefanie Kuenzel is a Senior Lecturer in the Electronic Engineering department at Royal Holloway University of London.**

Worldwide power systems are changing with the inclusion of more renewable generation. This ranges from large installations to household ones. We are getting more High Voltage Direct Current (HVDC) transmission for remote wind farm sites, international power connectors etc. We also need more energy storage in the network. There is also a change happening in the home with more electric cars, demand-side management, smart meters etc.

These changes introduce complexity and need more telecoms infrastructure to make it work. You get a feeling that there is a lot more scope for attacks and unintended consequences.

For a system in a steady state, introducing a step change can lead to a new steady state or the oscillations grow and grow and lead to catastrophe. Will change lead to more problems? We need to be aware of unintended consequences and the risk of attacks on the system.

[2] https://www.bankofengland.co.uk/financial-stability/financial-sector-continuity/cbest-threat-intelligence-led-assessments-implementation-guide

Recently worked as part of a Sprite+ project team to understand shadow infrastructures , including for power systems such as smart meter data, how that is used by bad actors; energy theft; role of the Grid as Critical National Infrastructure. Constant need to match demand and supply to keep the frequency around 50 hertz. Cited work done by Prof Mayes and Imperial on secure chips as well as smart meters.

With modern machine learning you can disaggregate household level consumption into individual appliances. This is a lot of personal information! When systems are designed, we need to consider data privacy rather than "data greed". Has a Ph. D. student looking at data collection from smart meters. Thinking about the frequency of data e.g. 30 minutes rather than 1 minute and should one aggregate households?

Petras project – looking at IOT risks in demand side management.

Systems are more complex with more devices so privacy and security need to be looked at very carefully. The same works for IOT.

Keen to talk to industry about helping with research.

Sarb Sembhi – co-chairs IOT Foundation and produces guidance for different audiences. What guidance have you found which would be useful? Where have you identified vulnerabilities or attacks in the way that systems interact? Cited control of thermostats.

One of the main points is data minimization which is an important and good thing. Full pathway of thinking about the functionality that you are trying to achieve is not always fully carried through. Once you have gathered information you need to look after it. A mistake to gather data that you will not use.
With demand-side management the hope is that the consumer will not be impacted but it is a step too far when households complain about it.

3. David Prince, Baringa Consulting

Future smart energy systems are of great interest. Hardly a day goes by without a cyber attack appearing in the media. Recovery costs a lot of money and demonstrates how destructive these events are. A US business suffering an attack is a good example of the global effects with a Swedish business having to close.

Fragility is the important factor. The frequency of attacks is unprecedented. Energy needs to have resilient systems with effective governance and risk management regimes.

Dean Kelshall, Baringa Consulting – over the last few years we have seen a move from a centralized energy control system to a more distributed one. Individual devices can impact the system on a microscale. If a large number of devices are compromised then this can have a big effect. Control is distributed and when you have large numbers of devices that can be impacted at the same time then you have an issue.

Need to ask: Who controls these devices? How well are the controllers secured? Interested in the regulations that may be needed to stop mass compromises of systems.

Macro industry constraints mean that you cannot move so quickly when cyber events happen. Need to consider this when you have future events esp. with IOT. Incentives such as low cost, competitive market for equipment does not align with security.

Open questions and discussion:

Alun Cairns – US has strong, prescriptive regulation – is this outcome focused or is it more a box ticking exercise?

SJ – US regulation is outcome focused and prescriptive in the bulk electric system specifying technical and procedural requirements. There is little latitude for non-compliance and requirements are updated regularly and inspected annually.

AC - Do tech innovators have an eye on the risks that they may well be adding to the system?

SK – I hope that some of them are but would not rely on them to build in security. Many, many companies in different countries are producing these devices. You have to make sure that your country's system is stable, cannot put the responsibility on the individual engineer who designs the fridge.

My perception is that the macro risk was the greater one, David has highlighted micro risk. Is Govt regulation strong enough in this area?

SJ – If you are a criminal entity or nation state that wants to disrupt UK energy targeting will be risk based and we need to defend CNI as a priority. Secondary risks such as IOT need to be designed secure by default and the holistic system design will need to contain the risks associated with distributed technology in energy to avoid disruption form decentralised technology.

As such need to think of the energy system as a whole rather than individual pieces. Think of lighting strikes[3] on the system last year which disrupted transportation. We need to look at the risk systemically and where a disruption will have the largest impact on the Grid and we need to plan on a multiple horizons' basis.

SK – completely agree that the major assets need to be secured first and foremost. If you measure the frequency of power supply through your household sockets you can see when the system is under stress.

DP – big advocate of prescriptive control requirements under certain circumstances. Namely, where the scope of applicability is limited, and the variability or desired variability is low. However, when we look at the Energy sector, having a regulation such as the NIS regulation, which favors a risk-based and more outcome-driven body of requirements, we see a consequence of organizational behavior change, and internal maturity growth. This is far more suited to complexity and large scope. Whilst this creates a lag, due to the need to build and train talent, it is overridingly preferable.

Contrast Energy and FS and the Operational Resilience of the two sectors. Do not see the same levels of scrutiny and would encourage cross-sector co-operations.

DK – important to paint a real picture of the micro world. Imagine a TESLA charger manufacturer who can control these remotely? That organisations could configure them to charge at the same time thus causing stress to the system is problem. If you have a homogenous network you have a higher risk profile.

Glenn Bluff – given that we move from an operational led industry to an information led one in electricity supply, it has not traditionally looked after cyber security . Why have we not seen more attacks given low level of maturity?

SJ – attacks are persistent we see this every day in the news. The intent of these is criminal and organisations generally have good defences against low level criminal activity.

SK – Successful attacks on power systems in the Ukraine for instance.

Apurva Saral – did her Masters under Prof Keith Mayes of Royal Holloway. Do you think that the current legislation is enough e.g. GDPR to cover smart meters?

[3] Thunderstorms Leave Trail of UK Broadband Connectivity Woes UPDATE2 - ISPreview UK

SK – thinks that GDPR does cover a number of these things, could be interpreted to be used to protect the consumer.

DP – need to distinguish between a principle-based regulation such as GDPR and enforcement and application in practice, Puts a huge emphasis on standards.

Prof Keith Mayes – as an observation SK mentioned some work that I have done with Imperial College around power systems. Based on distribution of highly secure chips into a power system on top of which you can build your protocols for communications and local resilience. Would fight off some remote cyber attacks and would be a secure system for taking measurements. At some point it would need to interact with the control system. Also explored a moving target defence whereby you intentionally create a disturbance in the system at a time when an attacker cannot predict this, creating your own alarm.

Is there any kind of active testing going on at the moment to disrupt the physical network and ensure that the monitoring systems pick it up and cannot be foreseen by an attacker?

KM – look at the more sneaky things, looking for criminals being prepared to do something physical such as a voltage change.

SJ – we use a methodology in the industry using technical testing methods which identify disruptions, fail overs etc. This is an interesting angle and I would love to know more.

KM – some of these things can be quite subtle. I have solar panels on my roof and if the local grid is too near the top then my solar panels can create an error. If we had local defensive monitoring with some local relevance then we could spot an attack on all the panels in a given area which would create an error.

Conclusions Breadth of risks because of complexity, regulatory lessons which we can learn from other places, micro and macro risks and how they come together, local defence mechanism. Tipping points on local levels and the design of systems to cope with new types of generation and technologies.
Next meeting – September – Is our health data secure?