

Chapter 11

Cyber and external threats

I want you to protect the transmission system from cyber and external threats

**Gas
Transmission**

nationalgrid

11. I want you to protect the transmission system from cyber and external threats

Summary

UK infrastructure faces many security threats. They are becoming more frequent, sophisticated and persistent in nature.

Threats include terrorism, criminality, espionage, actions by activists or extremists, vulnerabilities within systems and vulnerability from insider action. This chapter explains those threats and how we are responding.

Protecting the gas transmission system is critical to security and reliability of supply. It enables customers to use gas as and when they want to.

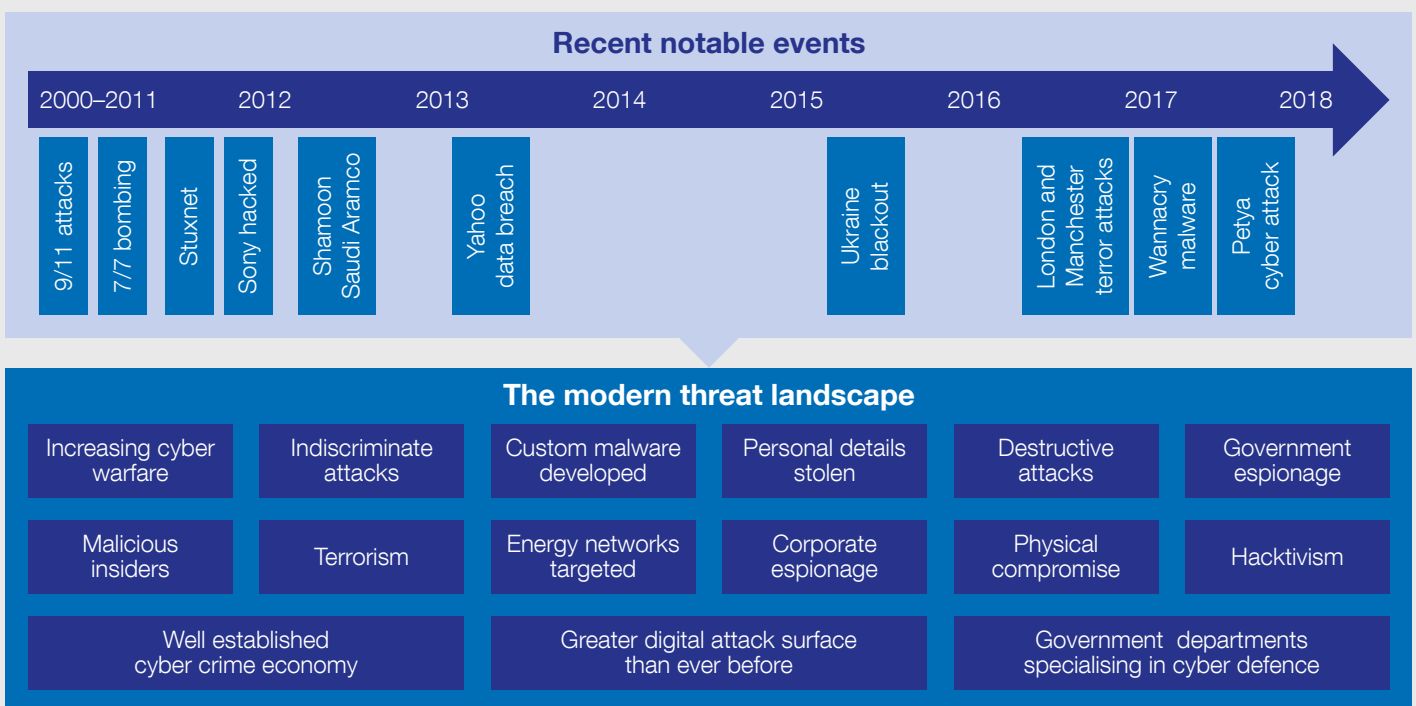
The UK Government is working with the Centre for Protection of National Infrastructure (CPNI) and the National Cyber Security Centre (NCSC) on this issue. It has set requirements for the levels of physical and cyber resilience that are in the national interest.

We work with these agencies to identify the most efficient way to meet these requirements. This requires operating and capital expenditure and will continue to do so in the future.

To protect national security, the Government restricts what we can say publicly about our current level of resilience and the specific measures we will take in the future to reduce vulnerability. For that reason, we have omitted specific details from this document.

“Protecting the gas transmission system is critical to security and reliability of supply.”

Figure 11.1: The modern threat landscape



What our stakeholders tell us

Stakeholders tell us that the way we manage security threats should be a priority. We understand this is because they identify with the increasing threat to society and their own businesses.

Stakeholders recognise that disruption to the GT Network and to their energy supplies would have direct, adverse consequences for them. Examples of what our stakeholders have told us:

“Cyber security for the transmission system is a national security issue.”

“Cyber security should be considered alongside physical security.”

“Outputs need to include cyber security and this needs to be funded.”

We must also consider the feedback from stakeholders about taking gas on and off the network where and when they want to. Any disruption to supply caused by external threats would have a significant impact on businesses and consumers' day-to-day life. We speak about this more in Chapter 6.

Our activities and current performance

Background

Parts of the gas National Transmission System are classed as Critical National Infrastructure (CNI). This means that if they are compromised or not operating, it would have a major effect on essential services. There could be severe economic or social consequences and potential loss of life.

We look at this issue holistically. Our approach covers people, processes, site and data security. We understand that training, awareness and vigilance across our teams is just as important in reducing risks as headline expenditure on things like hardware and software.

Physical security

We review the need for physical security at our operational sites regularly. At each review the number of sites requiring extra protection is agreed with government.

Our RIIO-1 performance involves the ongoing delivery of this Physical Security Upgrade Programme. This work is mandated by government to protect the UK's critical infrastructure. Our approach is in line with the information and guidance on physical security published by CPNI. You can read more on the [CPNI website](#).

“We understand that training, awareness and vigilance across our teams is just as important in reducing risks as headline expenditure.”

Evolving cyber threat

The frequency and risk of cyber-attacks is increasing. The threats we face are varied. They include malicious reconnaissance, theft of intellectual property and malware dropping, potentially to be used later.

The rising threat level is evidenced by events such as the Stuxnet malware which hit an Iranian power plant in 2010 and blackouts on the Ukrainian grid in December 2016 thought to be linked to similar malware.

What is the scale of the threat?

Malicious emails with harmful links or attachments containing malware are a common method of cyber-attack. Between 1 June 2018 and 31 December 2018, 283.9 million email attempts were made to National Grid employees. Of these, 225.1 million were considered ‘threat messages’ and stopped from reaching the recipient. A further 19.7 million unsolicited messages or ‘greymail’ was blocked. Only 39.1 million ‘clean’ emails were allowed through our screening process.

For further information on cyber threats see this [video](#) from the NCSC CYBERUK 18 conference.

NIS Regulations

The NIS Regulations came into effect in the UK on 10 May 2018. They aim to minimise the risk of cyber-attack and the resulting impact on UK CNI and the economy. This is in line with the NIS Directive aiming to raise overall levels of cyber security across the EU.

The NIS Regulations apply to a defined list of ‘Operators of Essential Services’ (OES). Each of these has a relevant ‘Competent Authority’ (CA) supporting and monitoring compliance. NGGT is a designated OES and within the energy sector the CA is a joint role. It is held by Ofgem and the Department for Business, Energy and Industrial Strategy (BEIS).

As the UK’s energy system changes, the danger from cyber threats is growing. This is in part due to the rapid digitisation of energy assets and the merging of IT systems with operational technology (OT) used for industrial processes and equipment.

During the RIIO-1 period, we have invested in enhancing cyber security controls and capabilities. The aim is to identify, defend against and recover from existing threats.

However, we know that the threat from cyber-attack is continuing to grow globally. In response, the Government is implementing the Network and Information Systems (NIS) Regulations to coordinate the mitigation needed.

“The frequency and risk of cyber-attacks is growing.”

Dealing with change

As the level, nature and response to external threats is uncertain, a re-opener mechanism has been used during the RIIO-1 period. This governs approval of our reasonable costs of complying with enhanced security requirements that had not yet been defined at the start of the period.

The May 2015 and May 2018 ‘re-openers’¹ have been used to adjust our RIIO-1 allowances in line with the evolving scope, volume of work and costs entailed. During RIIO-1 we have responded to cost challenges set by Ofgem and found more efficient ways to reduce costs.

¹ <https://www.ofgem.gov.uk/publications-and-updates/informal-consultation-riio-1-price-control-reopeners-may-2018>

Our direction of travel

We take our responsibilities as an Operator of Essential Services (OES) seriously. We will continue to take sensible measures to protect the integrity of the network in line with best practice and government requirements.

We intend to improve the safety and resilience of the transmission system. This will strengthen its ability to cope with and recover from malicious events that threaten GB energy supplies. This is what our stakeholders want and it supports consumers' desire to use gas as and when they want to.

We expect to extend our programme of cyber security resilience to reduce the risk of failure or compromise of our IT/Operational Technology estate. This is in line with the NIS Regulations.

We will also learn from the wider National Grid Group, where we own gas and electricity transmission and distribution networks across the north eastern United States.

Working closely with our US colleagues helps us to gain more powerful insights in our 24/7 analysis, and management of global security information and event data. We are competing to bring the best cyber talent in-house. We recognise that this is a new skill set needed in our workforce.

We will continue to put in place the enhanced physical security upgrades (capital expenditure) that are needed to protect our sites. Heading into RIIO-2 there will be higher ongoing maintenance activity. This relates to the increased security equipment that has previously been installed. We will also begin asset replacement for the older installations.


For the RIIO-2 period, we currently think that, where the scope of work is agreed in advance with the Government and Ofgem, funding should be included within our price control allowed revenue.

Where the scope is uncertain, or new requirements arise, we will seek to agree a suitable adjustment process. Finding the right way to work with the security agencies to monitor and adjust our delivery during RIIO-2 will ensure our effort and expenditure will benefit consumers even if circumstances change.

“Working closely with our US colleagues helps us to gain more powerful insights in our 24/7 analysis.”

“We are competing to bring the best cyber talent in-house. We recognise that this is a new skill set needed in our workforce.”

Our future costs for protecting the transmission system from cyber and external threats are uncertain because it depends on what threats emerge during the period. In the graphic below we have given the indicative cost of our known minimum response to the rising level and sophistication of external threats, especially cyber. To protect national security, the Government restricts what information we can share publicly about our current level of resilience and the specific measures we will take in the future to reduce vulnerability.




What it could cost

**T1
annual spend
£34m**

**T2 annual spend
£90m (known minimum)**

Key drivers for the changing trend and range:

- Increasing level and sophistication of external threats, especially cyber.
- The T2 indicative cost reflects known minimum response to mitigate increasing cyber threat.
- We are working with Ofgem and BEIS to confirm the scope of our work in response to new requirements of the NIS Regulations.



We welcome your views:

Chapter:
Cyber and external threats

Question:
15. The detail of our cyber and physical security plans will be developed confidentially with Ofgem and the Government. How would you like to be kept updated?

Submit your feedback online [here](#):

Initial planning assumptions

We are basing our initial planning on the following assumptions:

- **External threats.** Our planning is informed by the current level of threat advised by the relevant authorities. The nature of threats and our required response is kept under regular review as circumstances change.
- **Physical security.** The sites where enhanced physical security measures are needed remain as prescribed to date by BEIS.
- **Uncertainty mechanisms.** We use the same critical factors and interpretation of the measures needed to mitigate threats as currently. We assume a RIIO-2 adjustment mechanism will be included to ensure consumers continue to benefit as the situation evolves.

How to use this document

We want your feedback

Who is this consultation aimed at?

We are interested in the views of all stakeholders who are impacted by what we do and shaping the future of gas transmission. This includes the views of gas consumers, government and regulatory bodies, energy industry professionals and members of the public.

Tell us what you think

This consultation is open until 31 March 2019. You may give us feedback in the ways outlined below. We particularly seek your views in response to the specific questions we have posed. These are summarised on page 12. You may respond to all questions or just those relevant to your specific views.

Ways to feed back:

Make notes

Throughout the document, we have provided space for you to read and make notes at the start of each chapter (opposite). You can then type up your notes and send them in an email or submit them online.



Interactive pdf notes

Alternatively, we will be sending out editable pdf versions of this document with note fields for you to type directly into.

Email

We have a dedicated email address specifically for your feedback to this document. We welcome your thoughts at:

jennifer.pemberton@nationalgrid.com



Alternatively, you can put your thoughts in writing and send to: Jennifer Pemberton, National Grid House, Warwick Technology Park, Gallows Hill, Warwick. CV34 6DA.

Online

You can go directly to the website and submit your comments [here](#).



**Please share
your thoughts:**