CIVIL SERVICE QUARTERLY

FEATURE
WINNING THE STRATEGIC COMMUNICATIONS WAR WITH DAESH

SCIENCE IN EMERGENCIES

ACTIVE CYBER DEFENCE FOR THE UK

Civil Service

CONTENTS

EDITORIAL

Civil Service Quarterly 15: Security in government

Welcome to the 15th edition of Civil Service Quarterly (CSQ). which takes as its main theme, security in government, in a variety of aspects.

We lead off with an article from Dan Chugg, who describes the strategic communications operation he set up for countering Daesh propaganda. This is a crucial part of the work of the Global Coalition for the Defeat of Isis.

The role of the sciences in emergencies is the subject of an article by Christopher Whitty, in his capacity as interim Government Chief Scientific Adviser. He looks at the science-based response of the UK Government to four international and domestic emergencies, from the Ebola crisis in Sierra Leone, to the flooding of the Somerset Levels in 2013–14.

In **From crime scene to court – the science of explosives**, Charlie Stansfield gives first-hand insight into the little-known work of the Forensic Explosives Laboratory (FEL). The oldest facility of its kind in the world, but deploying state-of-the-art capability, the FEL has supported investigations into terrorist atrocities such as the bombing of Pan Am Flight 103 over Lockerbie and, more recently, the Manchester Arena attack.

Ciaran Martin, Chief Executive of the National Cyber Security Centre, considers the Government's response to what he calls, "the biggest problem facing the UK in cyberspace – the accumulation of high-volume, low-sophistication, automated attacks from criminals and states". In **Active Cyber Defence for the UK**, he outlines measures in the Active Cyber Defence programme, launched in mid-2017, which focus on protecting the Government and public services from such attacks by improving the basic level of defences.

Other articles in this edition include:

- **Civil Service transformation** – John Manzoni, Chief Executive of the Civil Service, looks at the forces driving profound change and improvement in the UK Civil Service and how they are challenging the organisation to accelerate towards its goal of becoming the best civil service in the world.
- **Supporting the rise of experimental government** – Dr Jen Gold, Head of the What Works Team at the Cabinet Office, considers the opportunities for government departments to generate more of their own evidence on what works to inform decision-making. And she asks: "What if policy teams routinely made policy in a fundamentally different way?".
- **Policy Propeller: transforming policy-making in the Department for Transport (DfT)** – DfT's Ana Costea and Pauline Reeves provide a progress report on the Policy Propeller scheme and how it is meeting the challenge for the department to test its own thinking and generate fresh policy ideas.

The subject of the CSQ Interview, which closes this edition, is Campbell McCafferty, the Government's first Chief Security Officer. In responding to a question about the major security threats facing the UK, he pinpoints keeping pace with – and even staying ahead of – the rapid pace of change in technology as the biggest challenge to government and the country at large.

I hope you enjoy this issue. You can give us your views and comments on the Civil Service Quarterly blog (https://quarterly. blog.gov.uk/), by email (csq@ cabinetoffice.gov.uk), or via #CSQuarterly on Twitter. If you would like to submit an idea for a feature in a future edition, please get in touch.

Chris Wormald

Sir Chris Wormald, Permanent Secretary, Department of Health

WINNING THE STRATEGIC COMMUNICATIONS WAR WITH DAESH

Dan Chugg, former Head, C-Daesh Coalition Comms Cell, describes the work of the unit set up specifically to counter Daesh propaganda.

THE CHALLENGE

In the summer of 2014, headlines were being made by a terrorist group we have come to call Daesh. They were taking over large swathes of land in Syria and Iraq; looting gold and cash from banks; and commandeering arms and ammunition from the stores of the fleeing Iraqi Security Forces. In part, the secret of their success as a brand was their success on the ground. They had promised to create a caliphate; stand up for Sunni Muslims; and impose a strict form of conservative Islam on their territory – and they were doing it.

But the other reason for the tremendous growth in their global brand – and the reason they were able to attract tens of thousands of people from around the world to join them – was because they put strategic communications at the heart of their operations and had a simple plan to "weaponise the media".

INTERNATIONAL RESPONSE

Daesh made the news all over the world with its creatively gruesome methods of murdering innocent people, filmed in high-definition, with slick, multi-angle editing. The media wasted no time in inadvertently amplifying Daesh's propaganda by reporting and publicising its atrocities. They gave the murderers nicknames, and created a sense of power and awe around the organisation. They even granted them a kind of bogus authority and respectability, and gave credence to their aims, by calling them 'Islamic State'. These were the very things that Daesh wanted the public to hear.

Then, of course, there was social media. Daesh systematically created social media accounts and used them to share information and specially designed content across the globe in the blink of an eye. Social media companies were largely unconcerned.

We had to do something.

In the first half of 2015, the international community started to get its act together. The UK was instrumental in creating a global coalition, which had five lines of action to defeat Daesh. One of these was strategic communications – and the UK was one of three countries jointly leading on this strand of work. However, we weren't doing enough to stop Daesh; partly because our systems were not designed for fighting on a virtual battlefield.

In September 2015, the then Prime Minister, David Cameron, announced to the UN General Assembly that he would establish a Coalition Communications Cell

AUG 2015   OCT 2017

IN OCTOBER, DAESH PROPAGANDA OUTPUT WAS 85% LESS THAN IT WAS AT ITS PEAK IN AUGUST 2015
SOURCE – UK GOVERNMENT ANALYSIS

DAESH IN DISARRAY

التحالف الدولي
GLOBALCOALITION

Global Coalition graphic for digital channels
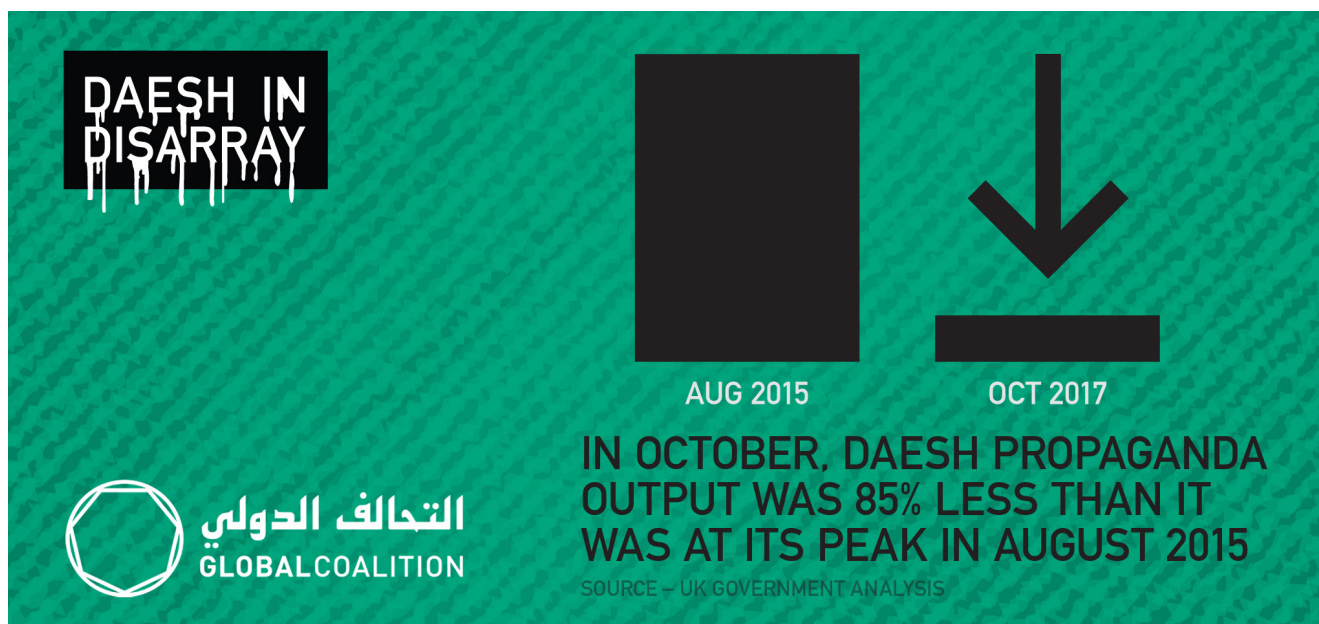
Meeting of the Ministers of the Global Coalition, Washington, DC

in London. The aim would be to undermine Daesh propaganda and to damage its brand. I was asked to make this happen.

To succeed, we had to change the global narrative and, in the terminology of the profession, contest the information space, rather than ceding it to Daesh.

THE GLOBAL NARRATIVE

I created a team using Conflict, Stability and Security Fund (CSSF) finance. Additional staff and resources were provided by coalition partners (15 secondees from 11 different countries, so far).

Our first task was to change the narrative around Daesh from one of success to one of failure. We needed to damage the Daesh brand by showing that, contrary to its own propaganda, Daesh was failing to win battles, failing to provide services to people in the territory under its control, and failing to live up to its promises.

We started sending a daily media pack around the coalition. This now goes directly to well over 1,000 officials every morning in more than 60 partner countries. We give updates on the latest news and suggest how to respond to atrocities. We provide bits of digital content and suggested tweets and retweets. We also run a website and various social media channels, which help coalition countries tell the story of Daesh's failures. We receive constant

positive feedback about the value of this activity, reflected in the fact that our content appears in global media, while the prime ministers of Spain and Australia have used our lines.

In addition, I co-chaired international working group meetings of over 30 coalition countries every quarter, to encourage consistency in our messaging; to upskill countries with less communications experience; to engage with the private sector; and to share content. This has resulted in numerous partners using strategic comms much more effectively to counter extremism and radicalisation in their own countries.

The narrative has, indeed, changed. Following the fall of Mosul, in Iraq, and Raqqa, in Syria, Daesh has, for some time now, been seen globally as a failing, disintegrating organisation.

FULL SPECTRUM EFFECT

Working to put communications at the heart of HM Government policy to counter Daesh was an important subsidiary objective. We have worked on a full-spectrum approach across government, with the Ministry of Defence, Home Office and others involved in tackling various parts of the Daesh propaganda operation. Having an overarching meta-narrative of 'Daesh is failing' has helped us focus this activity and make it complementary.

IMPACT

Two years on, Daesh, which was considered a threat to the stability of the whole Middle East, has failed to create a state. It is no longer able to recruit thousands or even hundreds of people to join it each month. And its propaganda is a pale shadow of what it previously was. It has resorted to inspiring low-tech attacks aimed at smaller groups of people. While this creates anxiety among the public, the threat to national security is a good deal less than if Daesh had the resources of an entire state at its disposal.

Much of the credit for this failure lies in the military efforts in Iraq, in particular the incredibly courageous efforts of the Iraqi Security Forces. However, the successful end of that battle was undoubtedly hastened and aided by the efforts of communications practitioners in the coalition, and particularly in the UK. We undermined Daesh's narrative, contested the information space and damaged their brand. We did this by making them appear less cool, less credible and less competent. Consequently, they found it more difficult to convince people to join them, both from among the local population in Iraq and from third countries.

Daesh is not yet defeated. As the organisation fragments, so its propaganda becomes less centralised and less consistent. While this diminishes its power, it also makes it more difficult to counter.

Daesh will be defeated eventually, but it will not be the last terrorist group to use Islam as the ideological underpinning for its crimes. This threat is persistent, organic and generational. New organisations will learn from Daesh's media operations, examine their shortcomings and improve on them. They will use the full gamut of communications tools in their efforts to harm us. Our experience with Daesh underlines the need to acknowledge that communication is a key battleground in preserving our nation's security. We need to improve our capabilities and increase our resources in this area if we are to stay safe.

There is much to do.

SCIENCE IN EMERGENCIES

Christopher J. M. Whitty, interim Government Chief Scientific Adviser (GCSA), and CSA at the Department of Health, looks at how scientific capability has been applied during national and international crises.

(Picture: Simon Davis/DFID)

Preventing an emergency from turning into a disaster requires political, operational and technical elements. The extent to which each is important varies according to the risk, but almost all emergencies require all three in some ratio.

A sure-footed political response and good technical analysis cannot make up for poor delivery. Good politics and operational skills will still lead to failure if the scientific or other technical basis on which the emergency is addressed is flawed. This applies to all elements of an emergency, whether in prediction, mitigation, response or recovery.

For the majority of the potential emergencies in the UK National Risk Register, the technical issues are scientific in part or whole. For most significant risks,

multiple sciences from different disciplines, including the social sciences, need to be integrated and deployed before, during and after an emergency. Historically, the UK Civil Service has been better at integrating science into emergency response than that of most other governments, in part because its scientific advisory system is stronger.

To illustrate some of the issues, this article highlights the scientific elements underpinning the Government response to four recent emergencies; two where the potential impact was primarily domestic, and two where it was predominantly international. What all have in common is that several sciences needed to be understood by civil servants to inform the UK Government response.

THE EBOLA CRISIS 2014 – BIOLOGICAL AND SOCIAL SCIENCES

The Ebola epidemic that hit West Africa three years ago had a terrible impact on the countries directly affected. It could, however, have been significantly worse if there had not been a rapid, science-driven response by UK public servants in support of African colleagues. This included major inputs from civil servants in the departments for International Development (DFID), Health (DH), and Defence (MoD), the Foreign Office, Cabinet Office, and Public Health England (PHE), as well as many NHS and armed forces professionals.

The failure of the international community to respond to

the early warnings has been well documented: this was not a failure of science, but of translating the science into action. Without the benefit of hindsight, the epidemic could not have been predicted, but could have been mitigated in its early stages. Once a UK response was underway, however, it combined scientific, operational and political elements across government extremely effectively.

The initial sciences involved were: mathematical modelling, to estimate the scale and speed of the epidemic and predict its future course; public health sciences, to determine ways to reduce transmission; and laboratory virology, to help improve diagnosis.

As the epidemic response got underway, three usually unrelated sciences were central. Social science was needed to reduce transmission, because many of the issues were around deeply rooted behaviours such as burial rites and health-seeking behaviour. Clinical science helped improve the initially dire survival rates of Ebola victims. Vaccine science accelerated the development of three highly effective vaccines that will substantially reduce the chance of an epidemic of Ebola on this scale occurring again.

UK science was central to all of these. Scientific advice fed into the Government's COBR crisis-response process, using the Scientific Advisory Group in Emergencies (SAGE) system, co-chaired by the Government Chief Scientific Adviser and the Chief Medical Officer.

FLOODING IN THE SOMERSET LEVELS 2013–14

The flooding in Somerset in the winter of 2013–14 caused substantial damage and economic shocks for families and firms.

Civil Service work, led by the Department for Environment, Food & Rural Affairs (Defra) through several technical agencies, supported by Cabinet Office and MoD, helped event prediction, mitigation, response and recovery. The Met Office provided projections of further rainfall; and the British

An Environment Agency official on duty during the Somerset floods

Geological Survey assessed likely groundwater drainage rates based on local geology. Academics made hydrological assessments to predict the rate of water movement through the local river systems. This helped provide a basis for government emergency response and factual communication with the public, which is so important in emergencies. The same agencies working with engineers are helping to repair and improve flood defences to mitigate future emergencies in this historically flood-prone area.

THE EYJAFJALLAJÖKULL VOLCANO AND AIR TRANSPORT 2010

The majority of the British public were surprised that ash from

a volcano in Iceland could so suddenly disrupt air transport for UK business and holiday travel. Eruptions in Iceland will happen again, potentially for prolonged periods (of a year or longer) and with more severe effects on human health and agriculture. The eruption of Laki in Iceland in 1783 sent clouds of ash and sulphur dioxide gas over Europe, and may have killed around 20,000 people in England alone. Fortunately, the Eyjafjallajökull eruption of 2010 was relatively small by comparison.

Predicting where eruptions will occur is much easier than predicting when – and the volcanoes of Iceland are well studied. In this instance, the initial sciences that civil servants needed, in particular from the Department of

Transport, were: volcanology, to predict the scale, height and composition of the ash cloud; and monitoring and modelling by meteorologists in the UK and Iceland to track and forecast the location of characteristics of the resultant volcanic ash plumes. Geophysicists from the British Geological Survey provided updates on seismic activity and possible follow-on eruptions affecting UK airspace. Engineers from Rolls-Royce helped determine the effects of different concentrations of ash on engines. This allowed policy teams to strike a reasonable balance between ensuring the safety of people and aircraft flying through ash clouds and minimising travel disruption.

Multiple government departments, coordinated by the Cabinet Office, have recently undertaken an exercise in how we would respond to a larger or more prolonged volcanic eruption affecting health and agriculture in the UK, as well as transport.

THE NEPAL EARTHQUAKE 2015 – GEOLOGICAL SCIENCES AND ENGINEERING

The Nepal earthquake devastated parts of Kathmandu, and caused widespread loss of life. DfID, FCO and MOD responded. The location, although not the timing, of this earthquake had been predicted, along with extensive preparation, which to some extent mitigated

its impact in terms of the loss of life. UK scientists in the Earth sciences had led much of this effort.

Immediately after the first earthquake, which only released around half the energy in the fault, UK university geologists helped map the direction of aftershocks to help plan relief efforts.

While the initial deaths caused by earthquakes come from trauma, usually due to collapsing buildings, the predictable next wave of mortality comes from a combination of factors. These include exposure (where meteorology to predict temperatures helps direct relief efforts); and disease, due to water and food disruption. In the latter case, epidemiology

Image of Eyjafjallajökull eruption, taken on 17 April 2010 Photo credit: Arni Sigurdsson. © Icelandic Met Office

and public health expertise are essential to the response. Mapping groups were established to analyse satellite imagery in order to identify locations for temporary camps and new building work.

Satellite mapping was also used by the British Geological Survey to assess delayed damage due to landslides – which often occur later when the monsoon rains arrive – allowing UK aid to be deployed early.

For long-term recovery and to mitigate the impact of earthquakes, the key science will be engineering. The majority of fatalities can be reduced by earthquake proofing to buildings, as Japan has shown. The trade-off during reconstruction

between making buildings safe and over-engineering, which increases the cost of building in poorer countries, is a difficult one. UK advice helped colleagues in the civil service of Nepal create a logical structure for addressing these difficult policy choices.

CONCLUSIONS

Emergencies will always occur. Some can be averted by prediction and the mitigation of risk based on science. However, the Civil Service has to predict, prepare for and respond to a whole range of possible eventualities. For some emergencies, such as the flooding in Somerset, much of the scientific

expertise lies within government and its technical agencies. For others, including volcanic eruptions, earthquakes and the Ebola crisis, the Government has to use the extensive scientific capacity in the UK academic sector and integrate it into Civil Service policy and operations.

Most government departments will at some point have a requirement for science in an emergency. The extent to which scientific advice is already integrated into their systems under routine conditions will usually determine their ability to predict the effects of the emergency. It will also determine how rapidly they can respond, making use of the science available to them to mitigate those effects.
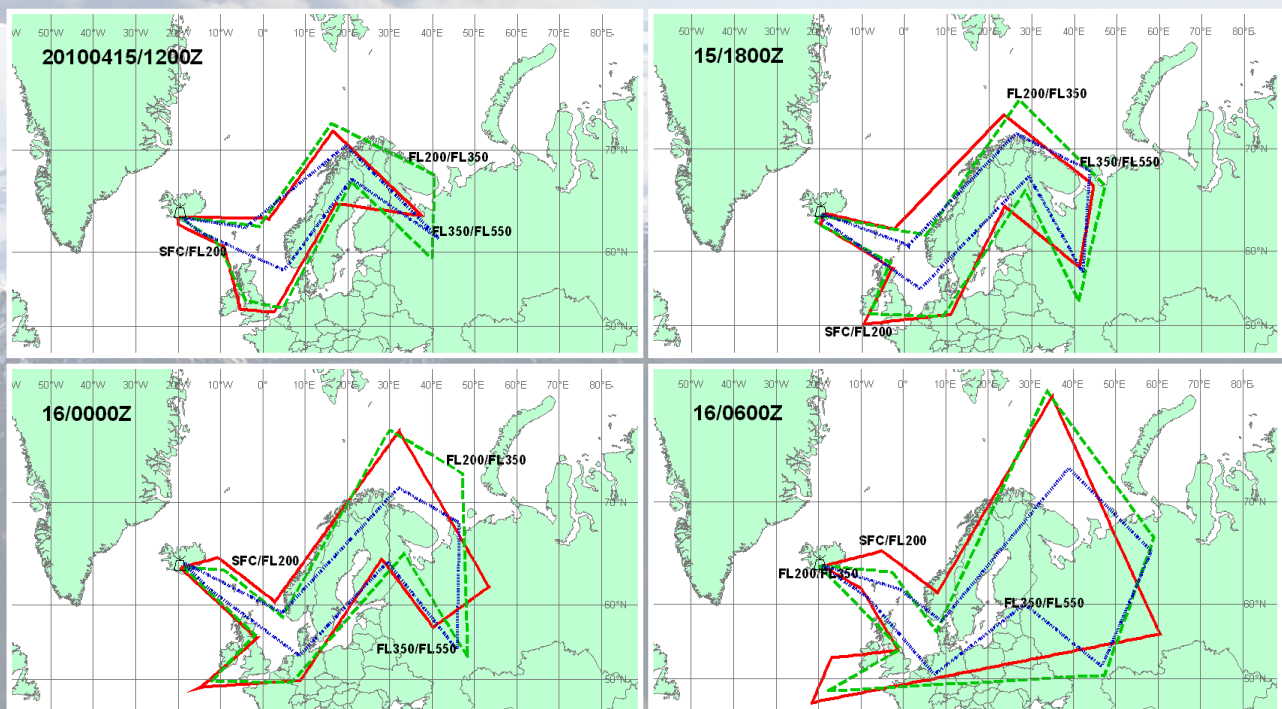
VA ADVISORY
DTG: 20100415/1200Z
VAAC: LONDON
VOLCANO:
EYJAFJALLAJOKULL
PSN: N6338 W01937
AREA: ICELAND

SUMMIT ELEV: 1666M
ADVISORY NR 2010/006
INFO SOURCE: ICELAND MET OFFICE
AVIATION COLOUR CODE: RED
ERUPTION DETAILS: SIGNIFICANT
ERUPTION CONTINUING. PLUM
REACHING 6KM, BUT POSSIBLY
OCCASIONALLY TO 11KM.

RMK: ASH CONCENTRATIONS
WITHIN THE INDICATED AREAS
ARE UNKNOWN
NXT ADVISORY: 20100415/1800Z

FROM CRIME SCENE TO COURT – THE SCIENCE OF EXPLOSIVES

Charlie Stansfield, Content Manager, Defence Science and Technology Laboratory Communications Team, gives an insight into the little-known work of a world-leading forensic science facility in keeping the UK safe.

From fireworks to fuselages, if explosives are involved in a crime, the Defence Science and Technology Laboratory's (Dstl) Forensic Explosives Laboratory (FEL) will be involved in analysing the material. With world-leading facilities, some unique in their capability, run by a team trained in-house, FEL exemplifies what Dstl is here for: delivering high-impact science and technology for the UK's defence, security and prosperity.

The FEL has existed in some form since the 1870s. It is the world's oldest laboratory of its kind and has been around longer even than its current base, Fort Halstead, on the Kentish North Downs, overlooking Sevenoaks.

Today, its experts are being called upon to help in the fight against terrorists and criminals. Every criminal or terrorism case that involves explosives in Great Britain, or involving British nationals overseas, is investigated by FEL's scientists.

FEL is funded by the Office for Security and Counter Terrorism (OSCT) at the Home Office to provide an impartial laboratory that supports the needs of the criminal justice system. Each year, the lab investigates around 200 cases, involving around 2,000 pieces of evidence.

FEL scientists have supported the investigations into terrorist atrocities such as the bombing of Pan Am Flight 103 over Lockerbie in 1988, the London 7/7 bombings in 2005, and the Manchester Arena bombing in 2017. The range of issues the lab covers also includes the illegal use of fireworks to cause harm to people and property, or people illegally producing explosives in their sheds or kitchens from recipes found on the internet.

CASE BY CASE

FEL's work is split into four main categories:
- post-explosion scenes;
- improvised explosives devices;
- finds and caches of explosives and related materials; and
- examination of suspects, property or premises for trace levels of explosives (that is, amounts that cannot be seen by the naked eye, as opposed to bulk levels, which can be seen, handled and weighed).

Work on a post-explosion scene focuses firstly on establishing whether an explosive material was involved. If yes, what type and how much; what type of device was used and how it was constructed; and where the device was placed before the explosion.

When a device is found intact, explosive ordnance disposal (EOD) experts will have rendered it safe before any assessment by FEL. It is then up to FEL to establish whether the device is explosive or an elaborate hoax. If it is real, then we need to determine what the explosive content is; whether the device could have functioned (and, if so, to what effect); and whether there is any link with previous devices.

Following a find of explosives or bomb-making materials, FEL looks to determine its significance. What types of

Scene of the 7/7 bombing, Tavistock Square, 2005

explosives are present or could be made from the materials? Does this tie in with any documentation or previous incidents? Is there evidence of 'new' technologies?

As well as being able to provide key evidence on the cause of an explosion, traces of high explosives aren't commonly found in the everyday environment and, therefore, can have forensic significance if we find them. If, for example, we can detect a trace of explosive, no matter how small, on an item of clothing, we can conclude that the person wearing those clothes is likely to have been in an environment contaminated with explosives. There may be no other evidence linking them to a scene.

WORLD-CLASS TECHNOLOGIES

Scientists at FEL have been involved in developing innovative new technologies and procedures. These include a sample collection kit, which makes it possible for property of all kinds, from cars to carpets, to be sampled at the scene. That is not to say that items of this kind have never been examined at Fort Halstead – vehicles, doors, and even parts of Hammersmith Bridge, have been sampled for high explosives.

FEL also developed a forensic aid known as a TERK – Trace Explosives Recovery Kit. This is used at crime scenes by police officers to collect material that might otherwise be lost or contaminated. The TERK can gather samples as small as one billionth of a gram; and the laboratories can detect levels 100,000 times less than a single grain of sugar.

This degree of precision is made possible by employing the newest cutting-edge technology in the trace lab – including a mass spectrometer operated using methods developed with support from partners at King's College London.

With this equipment, FEL can confidently separate a sample into its individual parts and provide information about the amounts of each part, even when the sample is vanishingly small. In addition, where most methods require the sample of interest to be compared to a known sample, in order to identify the separate components, this technology can look for and identify unknown materials.

EXHIBIT A: TELLTALE TRACES

During a safety search of premises occupied by a suspect, as well as knives, white crystals, small initiators and a respirator, EOD found a device taped to a cabinet. A test of the white crystals tested positive for peroxides; and the precursor chemicals for the high explosive HMTD (hexamethylene triperoxide diamine) were also recovered.

The suspect was apprehended, allowing FEL to sample his clothes for explosives. Traces of HMTD were recovered from his jacket, shirt, belt, watch, scarf and trousers. Further sampling around the wires of small fired initiators and analysis of the white crystals also identified HMTD, firmly connecting the suspect to the materials.

Documents suggested the individual had been testing the effectiveness of small initiators and listed plans for improvements. He was sentenced to two years' imprisonment.

EXHIBIT B: THE 7/7 ATTACKS

On 7 July 2005, four bombers attacked the London transport system, killing 52 people and injuring nearly 800. Teams from FEL attended each of the scenes, to determine where each device had been placed; the explosive used; the size of the device and its possible composition; and whether they were suicide bombs.

The variety and scale of hazards encountered across the four scenes were beyond anything previously seen in the UK. There were concerns over possible secondary devices, asbestos and a suspected gas leak; and the hot and dark working conditions were themselves challenging – not to mention the traumatic sights at each scene. The train between King's Cross and Russell Square tube stations was particularly difficult, being several hundred metres underground on the Piccadilly line.

The teams recovered trace samples and evidence to analyse at the lab. Thousands more items, including vehicles and trace kits, were also submitted to FEL in the following weeks. One vehicle, used by three of the suspected bombers, was recovered at Luton railway station. It contained components for a device, including packets of nails, as well as several complete devices containing HMTD, which were destroyed at the scene.

FEL scientists were deployed again five days after the attack to assist in a police raid at a property in Leeds, where it was suspected the bombs had been manufactured. They provided safety advice, ensured the right samples for analysis were taken, and prioritised more than 150 items for testing, including buckets containing a mysterious yellow-brown substance. FEL analysis showed the substance to be a novel explosive made from hydrogen peroxide and, probably, pepper.

By the end of the operation, more than 2,000 exhibits had been examined. The team's expert witness statements were used in coroner's court and at a separate trial of the accomplices, who received lengthy prison sentences.

EXHIBIT C: ASSASSINATION OF BENAZIR BHUTTO

As part of a team led by the Metropolitan Police's Counter Terrorism Command (SO15), FEL supported the investigation into the assassination of Pakistan's former Prime Minister Benazir Bhutto in 2007.

FEL analysis formed part of SO15's final report, which found that Ms Bhutto was killed by an explosion, causing a fatal impact with the roof escape hatch.

RECRUITMENT AND PROGRESSION

The team covering these roles is about 30-strong, supported by: colleagues who manage the labs within FEL and look after the technical resource; a pair of dedicated professional photographers to document evidence for the courts; and other skilled support staff and permanent researchers.

Most new recruits at FEL are science graduates in subjects such as Chemistry. Although previous experience in forensic science is not a prerequisite for graduate entrants, FEL also recruits experienced forensic scientists from other disciplines, who then retrain to gain expertise in explosives.

The requirements are: strong scientific ability; the capacity for hard work; and an absolute dedication to applying science rigorously and impartially to support justice.

The progression from graduate entry to becoming a Forensic Case Officer follows a structured path that typically takes at least four years. The entry-level role is Forensic Researcher. This involves two years learning the ways of the lab and developing and validating new forensic methods and techniques.

Some FEL staff choose to develop their careers as senior researchers or senior support staff; but for those who choose to become a court reporting scientist, the next stage is Forensic Analyst. It is in this role that the skills of the forensic scientist are developed, working under the tutelage of experienced reporting officers. Once they are considered to have enough experience, Forensic Analysts progress to become Forensic Case Officers, and are assigned their own cases.

HORIZON SCANNING

As well as analysing samples, giving advice and providing expert witness testimony in court, a crucial part of FEL's role is to constantly improve and stay 'ahead of the game'.

This means FEL staff keeping themselves informed of new explosives and emerging manufacturing methods, for example, on internet forums; and refining sampling and analytical techniques to enhance the lab's capability.

This is ever more important given terrorists' use of homemade explosives. The bomb-makers may be only amateur chemists with no scientific background, creating explosives that could be unstable or have unexpected properties. Constant research and analysis means fewer surprises and fewer unknown materials, and, if something new does emerge, FEL is more likely to have the capability to deal with it.

Forensic Case Officer analysing a car to recover traces of explosives, as part of a training exercise

" The requirements are: strong scientific ability; the capacity for hard work; and an absolute dedication to applying science rigorously and impartially to support justice. "

Forensic Case Officer working to recover evidence from a jacket in the laboratory

ACTIVE CYBER DEFENCE FOR THE UK

Ciaran Martin, Chief Executive, National Cyber Security Centre outlines the four measures already announced as part of the UK's Active Cyber Defence programme.

The Government cares about cyber security for two reasons. One is national security. Cyber attack can be (and occasionally, in other countries, has been) used as a way of damaging the security of a state, whether through interfering in electrical systems or elections. The second reason is economic. Britain is one of the most digitally advanced economies in the world. That's a vital national asset. But it won't continue if citizens don't think the digital environment is safe.

One thing the areas of national security and economic prosperity have in common, from the point of view of cyber security, is their vulnerability to attacks on basic weaknesses in defences. National security attacks can certainly be highly sophisticated (though not all are, and sophisticated attacks are difficult and costly to mount at scale). However, by far the biggest problem facing the UK in cyberspace is the accumulation of high-volume, low-sophistication, automated attacks from criminals and states seeking money or some form of competitive advantage.

This explains why the UK's record in cyber security to date is relatively good in terms of national security, though we've acknowledged that we have some way to go when it comes to our basic defences. Raising the standard of these defences is the most important thing we can do as a country, because, for the attacker, cyber attack is fundamentally about return on investment – what they will potentially get out of an attack compared to how easy or difficult it is to mount it. If it's easy to get in – and lucrative once the attacker is in – the attacker will come. If it's hard to get in and, once you do, it's hard to steal or tamper with stuff, the attacker may well go away, because there are plenty of other easier targets around.

This in turn explains, in part, why the National Cyber Security Centre (NCSC) was set up. We're proudly part of GCHQ, the near century-old government signals and communications intelligence agency. There isn't space here to outline in full the range of the NCSC's activities in leading the response to major cyber attacks affecting the UK – protecting our critical national infrastructure and raising our defences as a whole. Instead, I want to outline the world-leading programme we announced just after the General Election to protect the UK Government and public services by improving the basic level of defences.

One of the fundamental problems in cyber security is that it is shrouded in mystery. It was necessary to get across that the measures we believed departments should put in place are easy to understand. They are also easy to implement, and free. In due course, we will publish the data to show whether they work.

There are four measures already announced as part of our 'active cyber defence' programme.

1. BLOCKING FAKE EMAILS

Online spoofing – pretending to be someone you're not, usually by way of a fake email – is one of the biggest problems in cyberspace. Once someone opens the email, clicks on the link, and opens the attachment – the attack succeeds. But the organisation that is spoofed doesn't suffer any damage – if it's HMRC, for example, people are still going to pay tax because that's the law. This is a national problem, not an organisational one.

We've made spoofing much harder if bodies adopt the Domain-based Message Authentication Reporting and Conformance protocol – or DMARC. This helps determine whether a communication comes from the organisation it purports to. What DMARC does is tell the internet's distribution mechanisms how to recognise a genuine email from an organisation. We tried it out with HMRC in 2016. Instead of delivering the fake emails to the user with a warning, they were delivered to us. We got 300 million of them in 2016 alone. The best thing about this system is that ordinary computer users don't have to make a judgement about whether to open a 'dodgy'-looking email (please write and tell me if you know how to do that). So DMARC works, and is now freely available to all departments.

2. STOPPING GOVERNMENT SYSTEMS VEERING ONTO MALICIOUS WEBSITES

Cyber attacks also commonly involve redirecting a user away from the domain they intended to access, to somewhere that contains malware* or is fraudulent. We've worked with a commercial partner to set up a filtering service for public sector bodies that stops this from happening for registered users.

Domain Name Service (DNS) is the phonebook of the internet, and our new service focuses on data that GCHQ and commercial partners have acquired from malicious addresses. It then simply blocks the user from going there – providing automatic protection for staff visiting infected sites while using work systems.

3. Helping public bodies easily fix website problems

Attackers also learn what to target by scanning for vulnerabilities in Internet-facing services. The UK public sector has a huge digital estate to manage. This isn't easy and provides a useful set of targets for attackers. If an organisation doesn't know how to check for vulnerabilities – such as unused sites or those with out-of-date certificates – they provide an open goal for attackers. Web check is a free-to-use website configuration and vulnerability scanning service, available to all UK public sector organisations. It scans and then gives you a report in plain English on what needs fixing and how to fix it.

4. REMOVING BAD THINGS FROM THE INTERNET (PHISHING† AND MALWARE MITIGATION)

Since June 2016, the NCSC has been working with Netcraft, a private sector company, on a phishing and malware countermeasures service to protect government brands and UK service hosting infrastructure.

Government departments benefit automatically from this protection without having to do anything. Departments can boost the service by notifying Netcraft if they discover they are the target of a phishing campaign, or that there are malicious emails purporting to be from them. Netcraft will then issue takedown notifications to the hosts of the email and phishing sites. To help this work, departments and businesses should forward offending emails and any attachments to scam@netcraft.com.

Since Netcraft started this work, the average 'time to die' for phishing sites relating to government has fallen from 27 hours prior to the service's introduction, to under one hour; and for malware from 525 to 43 hours. For attacks on HM Government hosted outside the UK, 63% of Advance Fee Fraud sites spoofing the Government (where an email purporting to be from HMG asks for credit card details) are taken down within the first 24 hours, compared to 3% before.

ADVENTUROUS AGENDA

These measures are part of a new and adventurous agenda from the NCSC that is drawing attention from around the world. We're not claiming to get everything right, but we set out to use GCHQ's world-class expertise for the benefit of all UK internet users. We aim to innovate constantly; and to give users easy and cheap ways of making themselves that bit safer online – because every extra bit of protection counts. We're also serious about being open; and we want to work with partners in government, law enforcement, business, with citizens' groups and internationally. And we'll publish details of how we get on so you can judge for yourself.

---

* Malware is software designed to disrupt, damage, or gain authorised access to a computer system.
† Phishing is the fraudulent practice of sending emails that purport to be from reputable organisations in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

National Cyber Security Centre HQ

CIVIL SERVICE TRANSFORMATION

John Manzoni, Chief Executive of the Civil Service, explains why the Civil Service is transforming the way it works and why it needs to accelerate the change.

We have set ourselves the goal of becoming 'A Brilliant Civil Service', the best in the world.

How we measure up against this ambition will have a bearing on how successful we are in creating a fair, efficient and prosperous society, and a Global Britain that people want to visit, study in, invest in and trade with.

The Civil Service has great strengths. It is built on tried and tested principles that are also the basis of its international reputation for reliable and trusted public service.

In the new International Civil Service Effectiveness (InCiSE) Index – which compares performance on core functions such as policy advice, fiscal and financial management, and regulation, and attributes such as openness, integrity and inclusiveness – the UK Civil Service ranked fourth overall.

This is a good result. But – while the fundamental values (integrity, honesty, impartiality and objectivity) that underpin everything we do will stand us in good stead – it is not the whole story. The most effective organisations react positively, flexibly and practically to – and even anticipate – challenges. They change decisively to meet them and are always looking to improve. For the Civil Service, being the best means providing the best results for the people it exists to serve.

A MOMENT FOR CHANGE

Today, we find ourselves in one of those moments that demand change. The pressure for change has been building for some time, since the 2008 financial crash put a huge strain on budgets and a premium on greater efficiency and value for money. Even before that, the world was changing in ways and at a pace we could not afford to ignore. That pace is only increasing. Advances in technology have revolutionised how people buy goods and services and manage other aspects of their lives. They rightly expect to be able to deal with government in the same convenient and accessible way – online, and on demand. At the same time, society itself is changing – it's more diverse than it's ever been, and people are living longer, putting greater strain on health and welfare services.

> 66 For the Civil Service, being the best means providing the best results for the people it exists to serve.
> 99

On top of this, we now have Brexit, the nation's biggest priority. Therefore, our ambition for the Civil Service is fuelled by the realisation that, if we fail to change and improve, we will also fail the test of the times. If we get left behind, we risk forfeiting the trust of the citizens who rely on the services we provide. We must now seize the moment, spurred on by Brexit and the changes in society – to accelerate our transformation.

I say accelerate, because civil servants are already doing brilliant things that show what a transformed Civil Service, fit for the 21st century, can achieve. I see this at first hand when I visit teams across the country. They are collaborating more, delivering more for less, and building high-quality – increasingly digital – public services focused on what's best for the people who use them, not what's best for government.

Now, we have to go further to create government that works in smarter ways and is capable of keeping up with the rate of change in the world around us. This means not just quicker change, but transformation at a fundamental level in how and where we work and in the tools we use (both the hardware of technology and the software of data from which we draw evidence) to fashion services that improve lives. It also means changing our culture, the 'shape' of civil service careers and the look of the workforce, because a brilliant Civil Service is ultimately about people.

DIVERSITY AND INCLUSION

Our Civil Service should reflect the society it works for, in all its diversity. It must also be inclusive. An inclusive culture will allow us to tap into the talent, experiences and insights of civil servants from varied backgrounds that will provide better outcomes for citizens; while giving all our people the freedom to to be

themselves and the opportunity to reach their full potential.

We are committed to becoming the most inclusive employer in the UK by 2020. The proportions of ethnic minority (11.6%) and disabled civil servants (10%) are already the highest ever, with increased representation on Civil Service talent programmes. The graduate Fast Stream has recruited graduates from more diverse backgrounds than ever before, with 14.6% from an ethnic minority and 9.6% declaring a disability. Over 40% of senior civil servants are women – up 10% over the last 10 years.

We have also pledged to create 30,000 apprenticeships by 2020, opening the Civil Service up to talented people from a wider range of socio–economic backgrounds and helping us to build capability in key areas.

This is good progress, but the job is far from over.

Our new Diversity and Inclusion Strategy focuses very deliberately on representation and inclusion. It establishes measures based on the actual experiences of people from underrepresented groups that will help us to remove barriers to progress and create truly representative diversity.

'RESHAPING' CAREERS

As important as greater diversity and inclusion are, the change I want to see in the Civil Service is about something more. It's about engineering a fundamental shift in the balance of experience and skills of all civil servants. We are traditionally brilliant at policy, and there is a very good reason for this – we are geared to producing policy specialists. We need to reshape the next generations of civil servants around new career pathways that build professional expertise in key disciplines, the core government functions, while giving them the chance to broaden their practical experience. The goal is to make us as effective in delivery – of projects, services, procurements – as we are in policy-making. This broader, delivery-based experience, will encourage different approaches to the complex issues we face and the insight and judgement to produce and deliver different, workable solutions.

All the Government Functions are now mapping out their own career paths. Meanwhile, the graduate Fast Stream offers opportunities in 15 different schemes for new and existing civil servants, from Digital, and Data & Technology, to Project Delivery and Commercial.

MODERN WORKPLACES

Another essential component of continuous, deep improvement in the Civil Service - and the services we provide – is making sure we have modern workplaces, up-to-date equipment and the skills to make the most of them.

In major cities across the UK, we are creating around 20 strategic hubs. This programme will reduce the number of government buildings from around 800 to 200 by 2023. Hubs will allow us to locate teams from different departments in the same offices, enabling greater collaboration and a smarter, one-Civil-Service

approach, using mobile technology and focusing operations at a local and regional level.

The Department for Work & Pensions is already delivering more efficient services by concentrating its resources in co-locations with other departments and local government. And, by 2021, HMRC will set up 13 regional centres as part of transforming itself into a smaller, more collaborative, better equipped and more highly skilled operation for the digital age. These modern centres will replace the department's ageing network of 140 offices, which are expensive to run and create isolated pockets, doing a narrow range of work.

The One Public Estate programme is promoting joint working across central and local government and is on track to create at least 44,000 jobs and release land for 25,000 homes by 2020.

> 66 We need leaders who can explain the goal of transformation and take their people through it. Leaders who are confident beyond their own professional area, by virtue of their broad experience of government… 99

These changes are generating opportunities for civil servants at all grades: opportunities to learn the expert skills in digital, data, project management and commercial needed to deliver government priorities, and to take new professional career paths. For the time being, we will bring in external expertise where necessary, but our aim is to outgrow this need by developing our own people. In commercial, for example, we have brought in external specialists while also ensuring that existing staff have opportunities to develop through the commercial curriculum.

The Major Projects Leadership Academy has trained more than 300 senior project people; while the Digital Academy will train up to 3,000 people a year across government in the skills they need in data and technology as well as digital.

MODERN SERVICES

We are deploying technology to modernise public services, saving time and money for users. Her Majesty's Passport Office is sending millions of messages to users, updating them on passport renewals, with the aim of over 90% of passport applications being fully digital by 2020; and the Environment Agency is issuing up to 40,000 rod fishing licences a day, using the GOV.UK Notify platform for sending emails and texts.

We expect to have delivered at least 89 digital public services by 2020. To exploit the efficiencies and convenience of technology to the full, these services will increasingly be provided by a government that is digital – and digitally skilled – from its back-office operations to what citizens see and use on their computers and mobile devices every day.

By 2020, HMRC will have moved to a fully digital tax system, allowing businesses and individual taxpayers to update their information and pay their taxes when and where they want to and at any point in the year. And we've begun the biggest courts reform programme in the world, digitalising processes and introducing virtual hearings.

Through Government as a Platform, digital services are underpinned by common technology components, service designs and platforms such as GOV.UK Notify, and Pay (a secure payment service). Departments can use these as a base on which to build their own digital services, making it easier and cheaper to deliver customer-facing systems that meet the unique user requirements of each service.

As I write, we are delivering 40 major government transformation programmes, including:
• the new Childcare Choices website: this brings all childcare options together for the first time, so busy families can clearly see which offer works best for them; more than 260,000 parents have already opened a childcare account and are benefiting from new forms of childcare support; and
• Universal Credit (UC) full service, which will enable claimants to make a claim, check details of payments, notify changes of circumstance and search for a job through a single digital account – 99.6% of applications for UC are now made online.

MODERN LEADERS

Change of this scale and depth requires a new approach to leadership. We need leaders who can explain the goal of transformation and take their people through it. Leaders who are confident beyond their own professional area, by virtue of their broad experience of government, and whose first instinct is to collaborate, defying the silo mentality.

The new Civil Service Leadership Academy will strengthen these abilities, initially in leaders at senior level, but in due course through programmes open to all grades. Integral elements will be learning from leaders sharing their experiences – both good and bad - with immersive case studies of managing projects; and encouraging inclusive leadership that connects with people.

These are exciting times for everyone in government. The excitement is wrapped up in the challenges and opportunities of transformation. What we are saying to all civil servants is: embrace the changes and grasp the opportunities they are creating. There's a role for everyone in getting better at what we do, but everyone must take responsibility for their own development, doing things differently and inspiring colleagues.

For all civil servants, the prize at the heart of the change that's underway is to be 'A Brilliant Civil Service'; to be proud of what we do as civil servants every day, wherever we work; and for everyone in the country to take pride in us.

THE WHAT WORKS TEAM: SUPPORTING THE RISE OF EXPERIMENTAL GOVERNMENT

Dr Jen Gold, Head of the What Works Team in Cabinet Office, sees growing opportunities for departmental policy-makers to generate more of their own evidence of what works.

The idea that good decision-making should be informed by the best available evidence is hardly a controversial one. Yet there remain many gaps in the evidence available to government.

Take, for example, crime reduction. When it comes to organised crime, asset-focused interventions (AFIs) – such as confiscating property and recovering unpaid tax – are an increasingly popular law enforcement strategy. But while we know of around 300 studies on AFIs, none involves proper impact evaluation. This lack of evidence means that we have no certainty as to the effectiveness of AFIs in disrupting and deterring organised crime.

IMPROVING THE SUPPLY OF EVIDENCE

We can – and must – do more to encourage universities and other research organisations to help us plug gaps in our knowledge. We have made a start. Since March, some departments have begun issuing Areas of Research Interest. These set out 'the most important research questions' for each department that academic research could help address. First out of the blocks have been the departments of Health, for Transport, and for Environment, Food & Rural Affairs, as well as the Food Standards Agency. More will soon follow.

However, there are even bigger opportunities for departments to generate more of their own evidence on what works. What if policy teams routinely made policy in a fundamentally different way? What if their standard practice was to test variations in approach to a particular policy problem and then rigorously evaluate the results? What if it was business as usual for civil servants running frontline services to test new interventions before they are fully rolled out?

HARNESSING OUR COLLECTIVE EXPERTISE

Experimentation is certainly not new to government. The Ministry of Agriculture and Fisheries (1919–1955) was a big sponsor of experimental methods in farming research, much of it at Rothamsted Experimental Station in Hertfordshire. Departments such as Work & Pensions and HMRC also have a long history of running controlled trials to discover what works. And the Behavioural Insights Team that was set up in the Cabinet Office in 2010 (and now operates as a social purpose company) spearheaded the use of randomised controlled trials (RCTs) in parts of Whitehall that had previously shown little enthusiasm for such activities.

But testing and evaluation is still hugely under-used across government. We need to strengthen our capacity to test new and varied approaches, and to build in rapid and robust evaluation. Only then can we shift resources from less to more effective programmes.

This is where the Cabinet Office What Works Team – supported by David Halpern as the National What Works Adviser – can help. It supports civil servants working in both policy and operational delivery roles to generate and use more evidence. It also strives to put in place institutional structures that improve the supply of evidence.

The team understands how complex it is to design trials and impact evaluations in government. And at a time when budgets are constrained, it's never been more important to share in-house expertise.

That's why the What Works Team runs a cross-government Trial Advice Panel, bringing together some of the top trialling experts in the Civil Service. Panel members are on hand to offer free advice to policy teams on what sort of trial or test will generate the most useful results on what works. That might be an RCT, or equally it might be another type of experimental or quasi-experimental method. Panel members can also advise on evaluation design or be called on to offer guidance as challenges arise during a trial.

Thanks to support from the Economic and Social Research Council, the panel also consists of 30 UK-based academics from a range of disciplines, all of whom have first-hand experience of conducting high-quality trials and evaluations.

Since the panel was launched in 2015, members have assisted projects in 16 departments and public bodies. The team has seen plenty of examples – such as end-of-life care – where civil servants have been able to test new interventions in settings

END-OF-LIFE SUPPORT TRIAL, CABINET OFFICE

One of the earliest projects supported by the Trial Advice Panel was a Cabinet Office trial to test the evidence behind community-based end-of-life support – i.e. the use of volunteers to supplement state provision.

The Cabinet Office's Centre for Social Action was keen to understand the impact of befriending services. For example, did they improve quality of life? Did they reduce the experience of loneliness and the burden felt by family members caring for their terminally ill relatives?

Trial Advice panel members offered advice concerning:
eligibility criteria and consent; when to consider the trial complete;
how to communicate with volunteer organisations (many of whom were not used to, or necessarily comfortable with, research trials in this area); and how to liaise with the external organisations commissioned to evaluate the trial.

Befriending services were found to have a positive impact on slowing the decline in participants' physical health. The evaluation had important implications for the delivery of services. In terms of having a meaningful impact on quality of life, the trial pointed to targeting limited resources at certain groups who could receive more intensive support (e.g. older men who live alone) rather than spreading contact hours over a larger group of recipients.

THE EDUCATION ENDOWMENT FOUNDATION'S RCTS

Almost one third of all schools in England (a staggering 7,500 in all) have participated in trials funded by EEF. Nearly all of these were randomised control trials.

As a result, in just six years the EEF has more than doubled the amount of evidence we have from experimental trials in education in this country. When parents drop their children off at the school gates, they can now be assured that there's a much stronger evidence base to support their child's education.

We now know, for example, that the use of phonics is cost-effective in teaching young children to read (even more so if teachers receive formal training in phonics interventions). But older children who are struggling to read would likely benefit far more from other interventions such as meta-cognition and reading comprehension strategies.

often dismissed as being too problematic for experimentation by government.

The What Works Team also recognises that the key to stimulating greater interest in testing what works is to help civil servants understand experimental methods. With this in mind, it is collaborating with the Cross-Government Evaluation Group and the Policy Profession Support Unit to design and deliver training. The team is now involved in graduate Fast Stream inductions, the Future Leaders Scheme and the development of new course material through Civil Service Learning.

MAKING USE OF THE WHAT WORKS NETWORK

At the same time, it's important that policymakers, commissioners and those delivering programmes and services have as much access as possible to the evidence that already exists. To assist in this, the team coordinates a network of seven independent What Works Centres – covering crime reduction, health, education, early years interventions, ageing, wellbeing, and local economic growth.

Nearly all of these receive direct government funding. However, they are not like other research institutions. They provide practical advice on the available evidence on different interventions – drawing on and interpreting evidence that is often highly technical in nature, buried in academic journals, or unpublished. Their staff members (or the partner organisations they work with) comb the internet and academic databases, systematically assessing the existing evidence, and offering accessible summaries for policymakers, practitioners and commissioners.

For instance, the reviews undertaken by the College of Policing (who run the What Works Centre for Crime Reduction) suggest that CCTV, street lighting and the intensive policing of crime 'hot spots' all reduce crime. On the other hand, there's very little evidence that the electronic monitoring of offenders (through the use of ankle or wrist tags) has any overall effect on crime, despite being so widely used. Yet, in the case of one specific group – sex offenders – there is strong evidence to show that electronic monitoring reduces criminal activity.

Some of the centres also try to address gaps in the evidence base by commissioning their own trials. The Education

Figure 1: College of Policing's Crime Reduction Toolkit. Source: http://whatworks.college.police.uk/toolkit/Pages/Toolkit.aspx

Endowment Foundation (EEF) has had by far the biggest programme. The College of Policing is also supporting an increasing number of trials. Just recently, it has sponsored trials on stop-and-search and interventions to reduce domestic violence.

One of the biggest challenges remains the need to ensure that this evidence reaches decision-makers. This is critical if the What Works Network is to help practitioners improve the delivery of services and put decision-makers in a position to shift resources towards interventions that are achieving results.

A number of centres, including the College of Policing, have made their findings more accessible through a user-friendly toolkit (see Figure 1). They appreciate that policymakers and frontline practitioners rarely have the time to locate and analyse evidence systematically. These toolkits allow users to compare the effectiveness and cost of different interventions, as well as the strength of the available evidence.

The centres also have outreach programmes to help embed their learning in practice. To take one example, the College of Policing recruits 'evidence champions' within police forces and runs a High Potential Development Scheme that promotes evidence-based policing.

The What Works Team supports the communication of their findings through meetings and workshops across government, and via social media and publications. It also regularly brings the centres together so they can support each other as they develop their dissemination strategies.

The team would like to work with as many other teams and units across government as possible to drive this initiative forward. Why not:
• learn more about experimental methods by watching the team's online video;
• make use of the tools and resources produced by the What Works Centres; and
• consider using the Trial Advice Panel if you're thinking of running a trial in your area of work.

For more information on the What Works initiative, email: whatworks@cabinetoffice.gov.uk For regular updates, follow the What Works Team onTwitter: @WhatWorksUK

POLICY PROPELLER: TRANSFORMING POLICYMAKING IN THE DEPARTMENT FOR TRANSPORT

Ana Costea, Policy Profession Programme Lead, Department for Transport (DfT), and Pauline Reeves, Deputy Director, Road User Licensing Insurance & Safety, DfT, and Policy Fellow, Cambridge University Centre for Science and Policy (CSaP), look at a DfT initiative for generating fresh policy ideas

The Department for Transport is looking to challenge its own thinking and generate fresh policy ideas.

In August 2016, the department launched Policy Propeller as part of the novel Learning & Development process. It was inspired by the experience of Pauline Reeves, a Senior Civil Service (SCS) participant in Cambridge University's Policy Fellowship scheme.

Pauline was influenced by the academic input of the fellowship in suggesting a change in the policy direction on encouraging more people to cycle. She believed that other DfT policy staff should have the opportunity to experience the same stimulus and challenge that she had experienced through the Policy Fellowship.

The Policy Propeller scheme is a bespoke, departmentally funded scheme for DfT policy professionals, supported by DfT's Executive Committee of Director Generals and the Permanent Secretary. It has been developed in collaboration with Cambridge University's Centre for Science and Policy (CSaP), whose mission is to improve public policy through the more effective use of evidence and expertise.

The scheme consists of cohorts of up to 10 DfT policy professionals sourced from talent grids and nominated by directors. Its aim is to spark a mutually beneficial dialogue between the policy professionals and CSaP's wide range of researchers, academics and fellows. CSaP organises workshops for the Propeller programme, providing a forum for policy professionals to discuss high-priority issues and network with researchers.

These workshops allow decision-makers to test and shape their thinking by working through specific policy challenges with researchers. And networking can help to build longer-term connections between CSaP members in the academic/ research community and the policy-makers, supporting the sharing of good practice for evidence-informed policy-making.

THE MAKING OF COHORT 1

Every Policy Propeller cohort is allocated a director sponsor and a policy 'challenge'. The aim of the scheme is to widen the experience of policymakers' sources of evidence and their focus on academic research, and to exchange knowledge/skills with CSaP's contacts.

Each cohort takes part in three pairs of workshops, each pair addressing a different policy issue identified in advance by DfT.

Following every pair of workshops, teams present their findings to DfT ExCo (Executive

Joint DfT/CSaP meeting

Committee) and the DfT Policy Profession Steering Group, pitching policy solutions in partnership with their academic colleagues for the department to try out.

The first policy challenge to be set was the commitment in the 2015 Conservative Party manifesto to double the number of cycling stages (i.e. cycling as part of one point-to-point journey) from 800 million to 1.6 billion by 2025. This was combined with a later commitment for cycling to become the default for short journeys, aimed towards the 2040s.

Two workshops were held in Cambridge. The first focused on interaction with academics from CEDAR (Centre for Diet and Activity Research). They have created a Propensity to Cycle Tool to visualise evidence of cycle usage, and to inform the public (and policy officials) on existing measures of cycling data. This

also provided an opportunity to network with PhD students. Two small groups were formed to examine both the 2025 and the 2040 targets. Working with CEDAR researchers, the teams explored some of the barriers, opportunities, trends and evidence gaps to address some of the difficulties thrown up by the policy commitment.

The second workshop centred on refining the identified options and the advice on developing proposals and preparing pitches from experts in the field.

Between the workshops, discussions were held to address the options and the pitch session, and a chronological ideas planning process was conducted.

The workshops were completed as part of the officials' 'day jobs', and the enthusiasm and commitment of the teams was highly

commended. Cohort 1 ultimately influenced the Government's first statutory cycling and walking strategy, published in May this year.

Two cohorts, each of 10 DfT staff (with additional CSaP members), have been completed since the launch of the scheme. A further cohort followed this autumn.

DfT is so pleased with the outcomes that it wants to replicate the scheme, and is extending a tailored programme at Executive Officer level and making this part of the overall talent management and capability strategy for the department. Having senior buy-in from members of the DfT ExCo was and remains crucial to the scheme's adoption and continuation. They act as the final panel to approve policy ideas, some of which may feed into current policy thinking around the issues in question.

INTERVIEW WITH CAMPBELL McCAFFERTY, GOVERNMENT CHIEF SECURITY OFFICER

Campbell McCafferty was appointed as the first Government Chief Security Officer (GCSO) in July 2016. The GCSO replaced the role of Government Senior Information Risk Owner. The creation of the GCSO as functional head of government security is an important step towards strengthening and professionalising this critical area of work. The GCSO reports to the Chief Executive of the Civil Service.

In addition to his role as GCSO, Campbell is the Director of Cyber and Government Security in the Cabinet Office, and is responsible for delivery of the National Cyber Security Strategy (https://www.gov.uk/government/publications/national-cyber-security-strategy-2016–to–2021) and National Cyber Security Programme.

Prior to this appointment, Campbell led the Civil Contingencies Secretariat and has held a number of defence roles, including Head of Counter Terrorism and UK Operational Policy.

What are the biggest security challenges we face in government, and how are we tackling them?

The biggest challenge we, and I believe the UK as a whole, face in security is staying ahead of the rapid pace of change. By this I mean the speed at which technology is evolving; fewer government buildings and the shift from office-based to a far more mobile workforce; the migration of critical public services to the web; and changes in the wider society we recruit from.

Set alongside this is an equally fast-moving threat picture.

Reconciling the pace of change with the threat is the biggest challenge. For example, how can we safely maximise the huge opportunities provided by technology while appreciating that cyber offers the lowest-cost, lowest-risk way to steal from or disrupt government business?

A recent review of government security found too much duplicated effort across departments, and over-complicated practices. Government security has been delivered in a broadly similar way for the last 30 years.

To tackle this, the Cabinet Office has established a transformation programme to deliver a step change in government security.

The programme will create a security system that delivers a higher quality and more efficient service, one that is focused on enabling civil servants to work in a way that is secure.

At the same time, it will allow cross-departmental working and the use of modern technology.

What are your priorities as Government Chief Security Officer?

I see my top priorities as:
• delivering a government security transformation programme that ensures HM Government can rely upon a world-class security operation now and into the future;
• building a government security profession that develops, attracts and keeps the best talent and is seen as a key enabler for government business; and
• raising the level of ambition across all areas of security, with higher standards in cyber, personnel and physical security – to make HMG the hardest target it can be.

What are the biggest barriers to understanding the requirements of security in government?

The perception is often that 'security says no' and is a blocker, where it should be an enabler of new technology and ways of working. Civil servants I speak to often see security as opaque or confusing and a hurdle they have to cross before things can get done.

We're now working much more closely with the HR, Digital and Commercial functions so that we understand their needs and they have a clearer understanding about what we do, and why.

There's a phrase I like that says, 'security just needs to be good enough'. Even done properly, security can add cost and reduce functionality, so it is incumbent on the security profession to focus on the things that really matter. There is also no such thing as absolute security: risk management is critical, as is expressing security risks in language the business can understand.
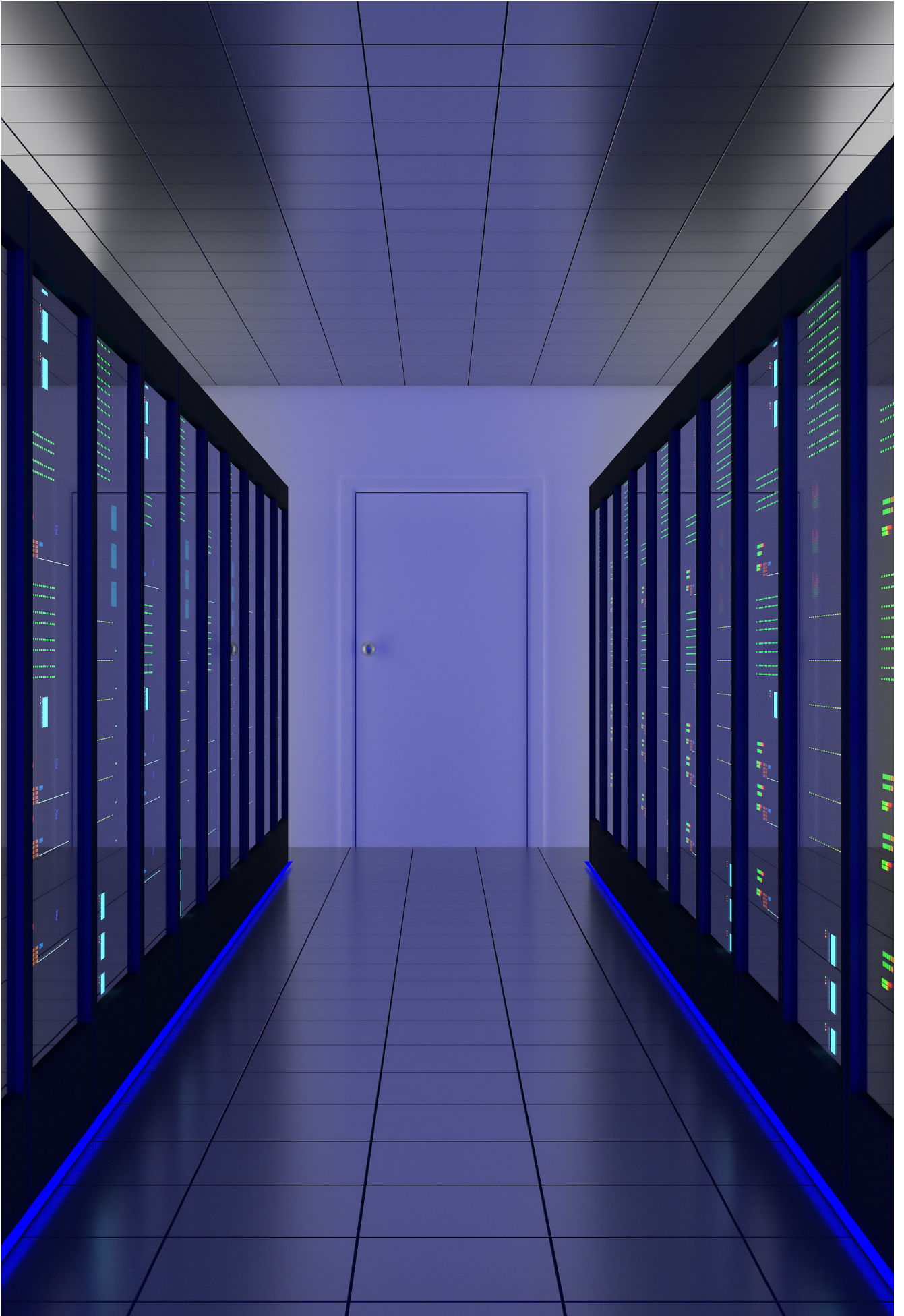
We constantly have to make risk decisions on how to balance security and business need. For example, the trade-offs between keeping a digital service up and available, versus taking it down in order to patch and secure it. Creating this transparency is vital to reducing barriers.

And those decisions also need to be reviewed regularly as the needs, the threat and the context change. And to help departments understand what 'secure enough' looks like, we are introducing minimum security standards for staff, buildings and technology.

How important are civil servants in keeping government safe?

People are our strongest defence when it comes to security, and almost all security incidents have a decisive human factor, such as clicking on a malicious link or leaving documents on the train.

While government is responsible for keeping its staff and information safe, civil servants also have an important role to play. This may sound daunting and many people are put off or confused by complicated security rules, but there are a number of simple things you can do to keep yourself safe at home and work. Most of this is just common sense and good judgement. Staff should refer to the Government Security Principles and Behaviours. You should also make sure you're aware of your department's security policies and who to notify if there's a problem.

Given the prominence of cyber threats and attacks in the media and elsewhere, is there a risk that we lose a holistic approach to security?

Yes, I think there is a danger that we lose our holistic approach. We have been doing personnel and physical security for so many years we sometimes see the cyber threat as something so new and different that it almost becomes a domain unto itself. In many cases, the people on the other end of the keyboard who want to do us harm have exactly the same intent as those who might try and steal public money or sensitive government information using more traditional means.

We must also be very aware that not all security threats fit into a neat box. There is a lot of crossover between cyber, physical and personnel security. A good example would be an improperly vetted contractor (personnel), gaining access to a government data centre that was poorly secured (physical) and plugging in a USB containing malware to enable an attacker to gain a foothold on the network (cyber). A system that is not joined up doesn't recognise this multi-pronged threat and leaves us more vulnerable as result.

What I'm trying to say is that our attackers don't think in silos of cyber, personnel or physical, so neither should we.

How joined up is government security?

The changes we are making over the next two years will deliver much more consistency, with security services being delivered by centralised units rather than separate services within each department. These bigger and more capable teams will ensure that skills and resources can be more evenly distributed across government enabling greater sharing of best practice, less duplication and more opportunities for security practitioners to develop and progress within the profession

We will also be introducing baseline standards and clear compliance processes across government. We recognise that, at the moment, security policies and standards are not applied consistently across government, which makes it hard to assess the risks that we face. The changes we will be introducing will result in more effective performance monitoring and a clearer picture of how we are dealing with security threats.

Security is also becoming a cross-government function, alongside digital, HR, commercial and finance. This is allowing us to create much greater integration and collaboration between the different functions and helps us learn from each other.

How closely do you work with other government security and intelligence agencies?

We work very closely with the intelligence agencies and other organisations to keep government safe. In particular, the National Cyber Security Centre (within GCHQ) and the Centre for Protecting National Infrastructure (MI5), which are the UK National Technical Authorities for cyber and personnel, and physical security respectively. This means they provide the advice and guidance that we base our policies and standards on. The intelligence agencies also provide crucial information on the threats to government, which helps our team and departments work out how best to protect ourselves.

How are we making sure we are recruiting and developing the best talent to counter the increasing sophistication of cyber and other threats?

We want to build the next generation of security professionals to include a diverse range of talent. Our recruitment approach will be to attract people from a wide variety of backgrounds, including bringing more women into the profession and those from groups of protected characteristics. We need people with a wide range of skills such as commercial, technology, HR, communications and risk management to name but a few.

A more diverse workforce will provide fresh perspectives, innovation and better reflect the businesses we support.

Why should people want to work in government security, compared with a role in a big private sector company?

Government can offer a scale and scope of challenge that far exceeds that found in the commercial sector. Government business involves dealing with millions of people and with billions of pounds – experience that can't be matched commercially.

It also offers an opportunity to tackle the most severe threats and build deep relationships with the security and intelligence agencies and wider national security community, both in the UK and abroad.

What is your vision of how government security will look in the future?

Our vision is to have a thriving security profession made up of subject matter experts who provide high-quality, dynamic security services that enable government to deliver now and in the future.

We want to empower our staff and we are committed to their development, so that they can have clear and exciting careers within government security. We want to ensure that government security is a brilliant area to work in to attract and retain the very best talent.

We must transform our security systems to modernise and protect against an ever-evolving range of threats. We want to bring together departments and security teams, and foster cross-government sharing of security services, best practice and expertise.

We will create a new culture where security is seen as an integral part of everyone's role, enabling them to do their job effectively.

We will create a new structure for government security with expert professionals providing high-quality, dynamic security services that protect and enable government to deliver now and in the future.

Security is an essential part of good government – we need to protect to enable.