| Title: Investigatory Powers Bill: Equipment Interference<br>**IA no:** HO0199<br>**Lead department or agency:** Home Office<br>**Other departments or agencies:** FCO, Cabinet Office, MOD, NIO, GCHQ, MI5, SIS, NCA, MPS, PSNI, Police Scotland and wider law enforcement agencies. | **Impact Assessment (IA)**<br>**Date:** 4 November 2015<br>**Stage:** Consultation<br>**Source of intervention:** Domestic<br>**Type of measure:** Primary legislation<br>**Contact for enquiries:** investigatorypowers@homeoffice.gsi.gov.uk |
|---|---|

## Summary: Intervention and Options

**RPC Opinion: Not applicable**

**Cost of Preferred (or more likely) Option**

| Total Net Present Value | Business Net Present Value | Net cost to business per year (EANCB on 2009 prices) | In scope of One-In, Measure qualifies as One-Out? | |
|---|---|---|---|---|
| £0m | £m | £m | No | NA |

**What is the problem under consideration? Why is government intervention necessary?**

The internet and related forms of technology are now used extensively by terrorists and criminals to organise and carry out their activities. In order to keep pace, it has been necessary for law enforcement agencies the armed forces and the security and intelligence agencies to develop techniques to enable them to gain access to computers, devices and other web-based activities to gather evidence or intelligence. These techniques are known collectively as equipment interference (EI). New legislation needs to be clear about how equipment interference is being used and the robust safeguards that apply.

**What are the policy objectives and the intended effects?**

To provide a clearer and transparent framework for the exercise of EI for the acquisition of electronic communications and other private data by law enforcement agencies, armed forces and security and intelligence agencies. It will provide robust oversight and safeguards by consolidating the existing legislative basis for the use of this capability and improve public understanding of the need for and the use of these important and sensitive techniques. It will provide for the continued use of EI to investigate terrorism and serious crime, including cyber crime and online child sexual exploitation. It will set out how agencies work with communication service providers (CSP) when their assistance is required and the robust oversight that applies to this obligation. The policy will refer to both targeted equipment interference, directed at a particular person, group or premises; and bulk equipment interference, which collects untargeted data from outside of the United Kingdom, a small amount of which will be analysed in the interest of national security.

**What policy options have been considered, including any alternatives to regulation? Please justify preferred option (further details in Evidence Base)**

Option 1: No new legislation. All law enforcement agencies, armed forces, and security and intelligence agencies continue to operate under existing legal framework.
Option 2: Re-legislate for the use of targeted and bulk EI for the acquisition of electronic communications by security and intelligence agencies only along with associated CSP obligations.
Option 3: Re-legislate in the Investigatory Powers Bill for the use of targeted EI for the acquisition of electronic communications by law enforcement agencies, armed forces, and security and intelligence agencies and bulk EI reserved for use by security and intelligence agencies, along with associated CSP obligations.

**Will the policy be reviewed?** It will be reviewed. **If applicable, set review date: December 2021.**

| | | | | | |
|---|---|---|---|---|---|
| Does implementation go beyond minimum EU requirements? | | | N/A | | |
| Are any of these organisations in scope? If Micros not exempted set out reason in Evidence Base. | **Micro** No | **< 20** No | **Small** No | **Medium** No | **Large** No |
| What is the $CO_2$ equivalent change in greenhouse gas emissions? (Million tonnes $CO_2$ equivalent) | **Traded:** N/A | | **Non-traded:** N/A | | |

***I have read the Impact Assessment and I am satisfied that (a) it represents a fair and reasonable view of the expected costs, benefits and impact of the policy, and (b) that the benefits justify the costs.***

Signed by the responsible Minister ..... Date: 3 / 11 / 15

# Summary: Analysis & Evidence

Policy Option 1

**Description:** No new legislation.

**FULL ECONOMIC ASSESSMENT**

| Price Base Year 2015 | PV Base Year 2015 | Time Period Years 10 | Net Benefit (Present Value (PV)) (£m) | | |
|---|---|---|---|---|---|
| | | | Low: 0 | High: 0 | Best Estimate: 0 |

| COSTS (£m) | Total Transition (Constant Price) | Years | Average Annual (excl. Transition) (Constant Price) | Total Cost (Present Value) |
|---|---|---|---|---|
| Low | 0 | | 0 | **0** |
| High | 0 | | 0 | **0** |
| Best Estimate | 0 | | 0 | **0** |

**Description and scale of key monetised costs by 'main affected groups'**

This is the baseline option. There are no additional monetised costs associated with this option.

**Other key non-monetised costs by 'main affected groups'**

This is the baseline option. There are no additional non-monetised costs associated with this option.

| BENEFITS (£m) | Total Transition (Constant Price) | Years | Average Annual (excl. Transition) (Constant Price) | Total Benefit (Present Value) |
|---|---|---|---|---|
| Low | | | | |
| High | | | | |
| Best Estimate | 0 | | 0 | **0** |

**Description and scale of key monetised benefits by 'main affected groups'**

This is the baseline option. There are no additional monetised benefits associated with this option.

**Other key non-monetised benefits by 'main affected groups'**

This is the baseline option. There are no additional non-monetised benefits associated with this option.

Key assumptions/sensitivities/risks — **Discount rate (%)** 3.5

That the current legislation would stand and powers would continue to be exercised under existing statutory frameworks. There is a risk that public confidence in the application of these powers may be degraded.

**BUSINESS ASSESSMENT (Option 1)**

| Direct impact on business (Equivalent Annual) £m: | | | In scope of OIOO? | Measure qualifies as |
|---|---|---|---|---|
| **Costs:** N/A | **Benefits:** N/A | **Net:** N/A | No | NA |

# Summary: Analysis & Evidence

Policy Option 2

**Description:** Re-legislate for the use of equipment interference for the acquisition of electronic communications by security and intelligence agencies only.

**FULL ECONOMIC ASSESSMENT**

| Price Base Year 2015 | PV Base Year 2015 | Time Period Years 10 | Net Benefit (Present Value (PV)) (£m) | | |
|---|---|---|---|---|---|
| | | | Low: | High: | Best Estimate: 0 |

| COSTS (£m) | Total Transition (Constant Price) | Years | Average Annual (excl. Transition) (Constant Price) | Total Cost (Present Value) |
|---|---|---|---|---|
| Low | | | | |
| High | | | | |
| Best Estimate | 0 | | 0 | 0 |

**Description and scale of key monetised costs by 'main affected groups'**

The only identified costs associated with the change in policy will be those associated with greater transparency and reporting of compliance with the legislation. The costs of increased compliance are contained within the oversight impact assessment and are not reflected here.

**Other key non-monetised costs by 'main affected groups'**

N/A

| BENEFITS (£m) | Total Transition (Constant Price) | Years | Average Annual (excl. Transition) (Constant Price) | Total Benefit (Present Value) |
|---|---|---|---|---|
| Low | | | | |
| High | | | | |
| Best Estimate | 0 | | 0 | 0 |

**Description and scale of key monetised benefits by 'main affected groups'**

-

**Other key non-monetised benefits by 'main affected groups'**

Increased public confidence and understanding of the legislation and how it provides a clear and transparent statutory framework underpinning the activities of the security and intelligence agencies. Continued ability to investigate terrorist activity, and serious crime including cyber crime and online child sexual exploitation. Improved understanding of how CSPs may be required to work with organisations carrying out EI and increased confidence due to the safeguards that are applied.

Key assumptions/sensitivities/risks — **Discount rate (%)** 3.5

Technology may continue to evolve and develop rapidly, outpacing legislation. By consolidating existing legislation criminals and terrorists may be more aware of the capabilities of the law enforcement agencies, armed forces, and security and intelligence agencies to prevent and detect terrorism and serious crime, and may take new or additional measures to evade discovery.

**BUSINESS ASSESSMENT (Option 2)**

| Direct impact on business (Equivalent Annual) £m: | | | In scope of OIOO? | Measure qualifies as |
|---|---|---|---|---|
| Costs: N/A | Benefits: N/A | Net: N/A | No | NA |

# Summary: Analysis & Evidence

Policy Option 3

**Description:** Re-legislate for the use of EI for the acquisition of electronic communications by law enforcement agencies, armed forces, and security and intelligence agencies.

**FULL ECONOMIC ASSESSMENT**

| Price Base Year 2015 | PV Base Year 2015 | Time Period Years 10 | Net Benefit (Present Value (PV)) (£m) | | |
|---|---|---|---|---|---|
| | | | Low: | High: | Best Estimate: 0 |

| COSTS (£m) | Total Transition (Constant Price) | Years | Average Annual (excl. Transition) (Constant Price) | Total Cost (Present Value) |
|---|---|---|---|---|
| Low | | | | |
| High | | | | |
| Best Estimate | 0 | | 0 | 0 |

**Description and scale of key monetised costs by 'main affected groups'**

The only identified costs associated with the change in policy will be those associated with greater transparency and reporting of compliance with the legislation. These costs are likely to be small and are contained within the oversight impact assessment.

**Other key non-monetised costs by 'main affected groups'**

N/A

| BENEFITS (£m) | Total Transition (Constant Price) | Years | Average Annual (excl. Transition) (Constant Price) | Total Benefit (Present Value) |
|---|---|---|---|---|
| Low | | | | |
| High | | | | |
| Best Estimate | 0 | | 0 | 0 |

**Description and scale of key monetised benefits by 'main affected groups'**

-

**Other key non-monetised benefits by 'main affected groups'**

Increased public confidence and understanding of the way the clear and transparent statutory framework governs the activities of law enforcement agencies, armed forces, and security and intelligence agencies. Continued ability to investigate terrorist activity, and serious crime including cyber crime and online child sexual exploitation. Improved understanding of how domestic CSPs may be required to work with organisations carrying out EI and increased confidence due to the safeguards that are applied.

Key assumptions/sensitivities/risk — **Discount rate (%)** 3.5

Technology may continue to evolve and develop rapidly, outpacing legislation. By consolidating existing legislation criminals and terrorists may be more greatly aware of the capabilities of law enforcement agencies, armed forces, and security and intelligence agencies to detect and prevent terrorism and serious crime, and may take new or additional measures to evade discovery.

**BUSINESS ASSESSMENT (Option 3)**

| Direct impact on business (Equivalent Annual) £m: | | | In scope of OIOO? | Measure qualifies as |
|---|---|---|---|---|
| Costs: N/A | Benefits: N/A | Net: N/A | No | NA |

# Evidence Base

## A. Define the problem

A1. Background

Equipment interference (EI) is the term used to describe a range of techniques used by the security and intelligence agencies, armed forces, and to a lesser extent law enforcement agencies– primarily the police, HM Revenue and Customs and the National Crime Agency – to gain covert access to computers and other devices to gather intelligence or evidence, in connection with investigations or operations.

Developments in technology have transformed the way that we all communicate and carry out our daily business. They have also provided endless opportunities for criminals to exploit in planning, organising and carrying out their illegal activities. For some criminals, technology provides a means to communicate more effectively with contacts in a way that is harder to detect or trace. Others have found ways to use technology to evade other investigatory techniques such as interception of communications. It is vital that investigatory capabilities continue to be available to law enforcement agencies, the armed forces and the security and intelligence agencies in order to protect the public from the atrocities of terrorist attacks, protect our armed forces from those who would do them harm, and to guard against the devastation serious and organised crime can have upon communities and individuals. In order to keep pace with the changing methodologies of criminals, law enforcement agencies, the armed forces and the security and intelligence agencies have had to develop techniques to enable them to gather intelligence and evidence and respond to the changing environment in which terrorists and criminals now operate. These techniques are collectively referred to as EI.

EI operations vary in complexity. At the lower end of the scale, an individual may use someone's login credentials to gain access to information. More complex operations may involve exploiting vulnerabilities in software to gain control of devices or networks to remotely extract information, monitor the user of the device or take control of the device or network. These types of activities can be carried out illegally by hackers or criminals. These types of operations may also be carried out lawfully by law enforcement agencies, the armed forces and the security and intelligence agencies in limited and carefully controlled circumstances.

Using these techniques it is possible for law enforcement agencies and the security and intelligence agencies to locate subjects of interest, find out who they are working with, understand how they are financing their illegal operations and gather evidence where computers or other devices are used to plan or carry out their illegal exploits. This enables law enforcement agencies and the security and intelligence agencies to try to keep pace with advances in the technology by criminals to communicate with each other, such as use of the "dark web", a highly encrypted area of the internet. EI is one of the tools and techniques that law enforcement agencies, the armed forces and the security and intelligence agencies deploy to look to ensure that there is no safe space for criminals and terrorists online to plot atrocities and cause us harm.

The scale of EI operations also varies. Some operations target a single device belonging to a single person whilst larger 'thematic' operations may target a number of devices that share particular characteristics. 'Bulk' equipment interference involves EI on a larger scale without the same thematic link between targets. In other bulk regimes, once the data has been collected only a small amount of that data is then analysed. The ability to conduct bulk EI in this way will become increasingly important as technology continues to change the way in which people communicate. Only the security and intelligence agencies may exercise this bulk power.

The current legislative framework provides a statutory basis for EI, both targeted and bulk. However, it could be made more transparent. We intend to provide a clearer and transparent statutory basis for both targeted and bulk EI. The legislation would also include greater and robust oversight of EI and heightened safeguards including handling, destruction and retention arrangements (to be published in the associated Code of Practice) to ensure that the power is

used proportionately, fairly and with the appropriate protection that minimises potential incursions of privacy. The regime of increased safeguards are addressed primarily in the oversight impact assessment.

The current use of equipment interference by law enforcement agencies is under the property interference provisions in the Police Act 1997 with its use by the security and intelligence agencies authorised under the Intelligence Services Act 1994. The Government has recently undertaken a consultation on a draft Code of Practice on equipment interference which set out the robust procedures and safeguards governing EI techniques that the security and intelligence agencies already apply.

There have been three independent reviews of investigatory powers, which include equipment interference for the purposes of acquiring electronic communications. The first is the review conducted by David Anderson QC, the Independent Reviewer of Terrorism Legislation who was commissioned during the passage of the Data Retention and Investigatory Powers Act, to carry out a review of Investigatory Powers. Two others were conducted in parallel: the Intelligence and Security Committee of Parliament looked into the activities of the security and intelligence agencies, and published a report in March 2015; and the Royal United Services Institute established a panel to review the impact on civil liberties of Government surveillance, which concluded in July 2015. Anderson's report was published in June 2015. All of the reviews concluded that the legislative framework for equipment interference needed to be updated and modernised to make clear the statutory basis for its use.

While the exercise of EI by law enforcement agencies, armed forces and the security and intelligence agencies is conducted in full compliance with the current statutory framework, it could be made more transparent and further safeguards applied to its use. EI is a fundamental intelligence gathering and investigative capability for law enforcement agencies armed forces and the security and intelligence agencies, and it is important to ensure that new legislation is clear and transparent. Moreover the Government wishes to ensure that there is clear consistency in the robust safeguards that will apply to law enforcement agencies, armed forces and the security and intelligence agencies.

## B. Rationale

In order that Government can protect its citizens, it must ensure that law enforcement agencies, armed forces and the security and intelligence agencies have the necessary powers to protect national and safeguard public security by preventing terrorism and tackling serious and organised crime. Equally, the Government must ensure that the use of these powers are scrupulously overseen, and subject to robust safeguards. It has a responsibility to ensure that law enforcement agencies, the armed forces and the security and intelligence agencies can be held to account for their activities and that those activities are transparent, whilst protecting sensitive techniques. It is also important that there is public understanding as to what types of activity may be undertaken, in what circumstances, and that the public has confidence that the appropriate safeguards are in place.

EI is an investigative technique that is important for the detection and prevention of serious crime, including organised crime and terrorism, and for the protection of national security. It is vital that these techniques continue to be available to law enforcement agencies, armed forces and the security and intelligence agencies in order to protect the public from the atrocities of terrorist attacks and the devastation that serious and organised crime, such as drug trafficking or child sexual exploitation, can have on individuals and communities. At the same time, the Government recognises that these can include highly sensitive and potentially intrusive investigatory techniques, and that they must be subject to appropriate controls, safeguards and oversight. Separating EI from other forms of property interference and creating a free-standing EI provision for law enforcement agencies armed forces and the security and intelligence agencies will enable a regime to be created that sets out clearly the circumstances in which EI can be deployed and the checks and controls on its use.

This will also answer the recommendations of David Anderson, in respect of:

> *"1. ...a comprehensive new law, drafted from scratch which (b) prohibits interference with [communications] by public authorities, save on terms specified] 6. The following should be brought into the new law and/or made subject to equivalent conditions to those mentioned here: (b) equipment interference (or CNE) pursuant to ISA 1994 ss5 and 7, so far as it is conducted for the purposes of obtaining electronic communications (c.f. ISC Report Recommendations MM-PP)"*
>
> *"7. The new law should repeal or prohibit the use of any other powers providing for interference with communications. For the avoidance of doubt, no recommendations are made in relation to the use of court orders to access stored communications (e.g. PACE s9) or the searching of devices lawfully seized, save that it is recommended that oversight be extended to the former."*
>
> *"92 (d). There should be statutory provision for oversight of the operation of powers for interception and/or obtaining communications data other than in the new law to the extent that such powers survive, including the power to access stored data by order of the court under PACE s9."*

It will also go toward answering the recommendation of the Intelligence and Security Committee of Parliament, that:

> *"The Agencies may undertake IT Operations against computers or networks in order to obtain intelligence. These are currently categorised as 'Interference with Property' and authorised under the same procedure. Given the growth in, and intrusiveness of, such work we believe consideration should be given to creating a specific authorisation regime".* (Recommendation CC)

## C. Objective

To replace and consolidate legislation used to acquire electronic communications and other personal data by use of targeted and bulk EI, and update and modernise the legal framework. The intended effect will be to ensure the activities that law enforcement agencies, armed forces and the security and intelligence agencies undertake in respect of EI can be applied to protect national security and prevent and detect serious crime, including child sexual exploitation, cyber crime and other harms. The policy does not establish new powers in respect of EI, rather it makes clear where and how these important but sensitive techniques may be exercised, with a new regime for the authorisation and oversight applied to EI.

## D. Options

Three options have been considered. Option 3 is the preferred approach. As with all options, our basic assumption is that the Government must retain the ability to acquire electronic communications and other private data through EI.

### Option 1 - No new legislation

Under this option, no changes would be made to the legislation governing EI. The exercise of these powers would continue to be in accordance with the current legal framework: sections 5 and 7 of the Intelligence Services Act 1994 and section 93 of the Police Act 1997. The Equipment Interference Code of Practice would be put in place to cover the activities of the security and intelligence agencies use of EI and it would be possible to update the existing Covert Surveillance and Property Interference Code of Practice to provide further detail on the use of equipment interference by law enforcement agencies.

This option would not modernise the legal framework, not provide the safeguards requried for bulk EI and not respond to David Anderson's recommendation in respect of consolidating legislation.

**Option 2 - Re-legislate for security and intelligence agencies' activity**

Provision within the Investigatory Powers Bill would be in place to provide for the use and jurisdiction of targeted and bulk equipment interference by the security and intelligence agencies and armed forces. This would respond to the letter of Anderson's recommendation (No. 6) but not his principle that the legislation should, so far as is possible, prohibit interference with electronic communications outside of the legislation. Law enforcement agencies would continue to exercise powers under section 93 of the Police Act 1997 to provide for equipment interference.

This option would provide for increased transparency of the use of targeted EI by the security and intelligence agencies and armed forces, and the robust safeguards that would apply. It would also extend a heightened set of safeguards to oversee the use of bulk EI by the security and intelligence agencies. However, it would not provide for increased safeguards and robust oversight of law enforcement agencies use of targeted EI techniques as these would continue to be provided under existing legislation – including the present model for authorisation of these techniques. As a result the legislative framework for EI would remain inconsistent and lack coherency.

Equipment interference today will rely in some instances on the cooperation of CSPs. This option would create an obligation that would require CSPs to provide reasonable assistance and support the implementation of EI warrants when required. Any costs to industry would be reimbursed by Government. The cost of this process has not been monetised, but is expected to be small.

**Option 3 - Re-legislate for security and intelligence agencies', armed forces and LEA activity**

The new legislation would consolidate the statutory framework for targeted EI for the purposes of acquiring electronic communications that provides for the activities and jurisdiction of law enforcement agencies, armed forces and the security and intelligence agencies. It would rationalise the powers exercised under the Police Act and under the ISA for equipment interference for acquisition of electronic communications and other private data and place them on a clear and transparent statutory footing. It would make apparent the robust safeguards and rigorous oversight that applies and improve public confidence and understanding of how and when these powers are exercised, in strict accordance with necessity and proportionality. It would extend a heightened set of safeguards to the provision of bulk EI, reserved for use by the security and intelligence agencies regarding matters of national security. A new Equipment Interference Code of Practice would illustrate the retention, handling and destruction arrangements for material acquired.

The Bill will also provide additional protections for the communications of Members of Parliament and other legislators. In addition to approval by a Judicial Commissioner, the Bill will state that the Prime Minister must be consulted before the Secretary of State can decide to issue a warrant to acquire an MP's communications through equipment interference. This will cover all warrants for targeted equipment interference that are carried out by the security and intelligence agencies. It will also include a requirement for Prime Ministerial authorisation prior to the selection for examination of a Parliamentarian's communications collected under a bulk warrant. It will apply to MPs, members of the House of Lords, UK MEPs and members of the Scottish, Welsh and Northern Ireland Parliaments/Assemblies.

Equipment interference today will rely in some instances on the cooperation of CSPs. This option would create an obligation that would require CSPs to provide reasonable assistance and support the implementation of EI warrants when required. Any costs to industry would be reimbursed by Government. The cost of this process has not been monetised, but is expected to be small.

This option would go furthest to answer the recommendations made by David Anderson, the ISC and RUSI, and is the preferred option.

## E. Appraisal (Costs and Benefits)

The legislation does not provide for new powers in respect of EI, or expansion of existing capabilities. It replaces the existing statutory basis for EI to acquire electronic communications and other private data, and provides for greater oversight and transparency.

### GENERAL ASSUMPTIONS AND DATA

While efforts have been made to understand the costs and benefits to all affected groups, it is necessary to make some assumptions. The Home Office has (as far as is possible) strengthened and confirmed the evidence base through information gathered through consultation with other Government Departments and operational partners including law enforcement agencies and the security and intelligence agencies.

### GROUPS AFFECTED

- Government Departments (Home Office, Foreign and Commonwealth Office, Ministry of Defence)
- Security and Intelligence agencies (Security Service, Secret Intelligence Service, GCHQ)
- Armed forces
- Law enforcement agencies: (National Crime Agency, police forces in England and Wales, Police Scotand and the Police Service of Northern Ireland, HM Revenue and Customs) and Services police)
- Intelligence Services Commissioner and the Office of the Surveillance Commissioners (covered in detail in the separate oversight impact assessment)
- Communication Service Providers (CSP)
- The public

**Option 1 is the baseline option, against which Option 2 and 3 are compared.**

**Option 2: re-legislate for use of targeted and bulk EI in application to the security and intelligence agencies**

COSTS

There is provision in existing legislation legislation for bulk and targeted equipment interference. The ongoing baseline costs of the technical systems and resource used to carry out EI would remain, with no cost incurred above those already established.

This option would create an obligation that would require CSPs to provide reasonable assistance and support the implementation of EI warrants when required. Any costs to industry would be reimbursed by Government. The cost of this process has not been monetised, but is expected to be small.

BENEFITS

There would be no monetary benefits to affected groups as a result of legislation. Non-monetary benefits would include: greater public confidence in the transparency and clarity of the legislation that applies to interference with equipment to acquire electronic communications and other private data as a result of the strengthened safeguards and additional overisight, through the introduction of a double-lock authorisation process, whereby a judicial commissioner approves warrants issued for equipment interference.

**Option 3: re-legislate for the use of targeted EI in respect of the law enforcement agencies, armed forces and the security and intelligence agencies; and bulk EI in respect of the security and intelligence agencies.**

COSTS

There is provision in existing legislation legislation for bulk and targeted equipment interference. The ongoing baseline costs of the technical systems and resource used to carry out EI would remain, with no cost incurred above those already established.

This option would create an obligation that would require domestic CSPs to provide reasonable assistance and support the implementation of EI warrants when required. Any costs to industry would be reimbursed by Government. The cost of this process has not been monetised, but is expected to be small.

BENEFITS

Non-monetary benefits would include: greater public confidence in the exercise of equipment interference by law enforcement agencies, the armed forces and the security and intelligence agencies, to acquire electronic communications and other private data as a result of the clearer, robust safeguards and oversight applied to the use of EI.

Re-legislating for EI as part of the Investigatory Powers Bill will provide for continued use of investigatory techniques that help to achieve the following benefits below:

**Counter terrorism and protection of national security**

The use of EI can provide for the acquisition of communications and other private data via operations against a target's computer or network. In limited and controlled circumstances this might mean the security and intelligence agencies obtain authorisation to use a terrorist's e-mail credentials to log into their e-mail account and access e-mails with details of contacts and, potentially, attack planning. This can give access to material that would be encrypted if intercepted, or material which cannot be obtained because there is no CSP on whom a warrant can be served.

**Safeguarding children**

Many cases of child sexual exploitation rely heavily on use of computer technology to organise and carry out the crime, in an attempt to evade detection and identification by law enforcement agencies. Police make use of EI to gather intelligence and evidence on paedophiles operating on the internet, tracking the sharing of indecent images of children, and others exploiting children for these purposes. Similarly, the security and intelligence agencies may, in limited and controlled circumstances, be authorised to exploit a vulnerability in software which would give them access to a machine belonging to a serious criminal in order to obtain intelligence to disrupt a paedophile ring.

**Other serious crime**

Intelligence and evidence obtained through the use of EI is used to investigate and prosecute serious criminals (such as drug traffickers and illegal arms traders) and to protect UK cyber security. For example, the security and intelligence agencies may be authorised, in limited and controlled circumstances, to counter the activities of cyber criminals to prevent large scale disruption or compromise of computers in the UK.

The following case studies are presented to demonstrate the value of EI in previous operations:

**CASE STUDY A**

Equipment interference, when used with other intelligence gathering techniques, is vital in time-limited cases of threat-to-life when the police need to act quickly.

In one example, intelligence was received that several suspects were at large after being involved in an attempted murder. Equipment interference and other intelligence gathering techniques were used to identify and locate the suspects leading to their arrest before further offences could be committed. Due to the high quality of intelligence achieved through equipment interference, the suspects were arrested within hours of receiving the initial intelligence. Without the use of equipment interference it would not have been possible to arrest the suspects simultaneously which was critical to preserving the evidence.

**CASE STUDY B**

The ability to use equipment interference alongside other intelligence gathering techniques provides operational flexibility enabling the police to progress long term criminal investigations even when crime groups use specific tactics to try and disguise their activities.

A law enforcement operation into an organised crime group importing Class A drugs into the UK used equipment interference alongside other intelligence gathering to identify the criminal network. The intelligence was used to make numerous arrests and seize a significant amount of Class A drugs before it reached the streets. Through the combined intelligence approach law enforcement were able to dismantle the drugs network.

**DIRECT COSTS AND BENEFITS TO BUSINESS**

CSPs may incur costs as a result of the assistance they are required to provide but reimbursement will be made such that there are no net costs.

## F. Risks

There is an ongoing risk with all options outlined above that technology will continue to evolve and develop rapidly, outpacing legislation. There is also a risk that in consolidating existing legislation criminals and terrorists will be more greatly aware of the capabilities of the law enforcement agencies, armed forces, and the security and intelligence agencies to detect and prevent terrorism and serious crime, and will take new or additional measures to evade discovery.

## G. Implementation

The Government will Introduce a Bill following any revisions necessary after pre-legislative scrutiny, in the New Year. The Bill will need to be enacted by 31 December 2016, by which point the Data Retention and Investigatory Powers Act will fall away.

## H. Monitoring and evaluation

The proposed legislation will be scrutinised by a Joint Committee of Parliament, before being introduced in the early New Year. The application of the legislation will be scrutinised on an ongoing basis by the Investigatory Powers Commission, an independent body of the judiciary, who will provide yearly reports on the exercise of powers within the Bill. The Intelligence and Security Committee of Parliament will continue to oversee the activities of the security and intelligence agencies, including their exercise of investigatory powers. And the Investigatory

Powers Tribunal will provide a right of redress to any individual who believes they have been unlawfully surveilled.

## I. Feedback

The Government will consider carefully the recommendations of the Joint Committee before bringing forward revised proposals for Introduction. Public consultation will form part of the pre-legislative scrutiny process.