Council of the
European Union

Brussels, 25 November 2015
(OR. en)

10952/2/15
REV 2 DCL 1

GENVAL 26
CYBER 72

DECLASSIFICATION

of document:	10952/2/15 REV 2 RESTREINT UE/EU RESTRICTED
dated:	30 September 2015
new status:	Public
Subject:	Evaluation report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combatting Cybercrime" - Report on the United Kingdom

Delegations will find attached the declassified version of the above document.

The text of this document is identical to the previous version.

Council of the
European Union

Brussels, 30 September 2015
(OR. en)

10952/2/15
REV 2

RESTREINT UE/EU RESTRICTED

GENVAL 26
CYBER 72

REPORT

From:	General Secretariat of the Council
To:	Delegations
Subject:	Evaluation report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combatting Cybercrime" - Report on the United Kingdom

ANNEX

Table of Contents

1 EXECUTIVE SUMMARY

The UK Cyber Security Strategy identifies priorities and actions to combat cybercrime. It provides strategic guidance on strengthening law enforcement capacity, upskilling police and prosecutors, raising awareness and improving cooperation with all relevant national and international parties including the private sector.

The Office for Cyber Security and Information Assurance (OCSIA) in the Cabinet Office is responsible for the implementation of the National Cyber Security Strategy; this includes the management of the National Cyber Security Programme (NCSP), which funds and coordinates activity across Government to protect the UK in cyberspace.

The National Cyber Security Programme is supported by £860 million of Government investment from 2011 to 2016, 10% of which has been committed to enhancing law enforcement capabilities in England and Wales (and nationally through the National Crime Agency) to tackle cybercrime. This is on top of funding from the general policing budget. As a result of devolved funding streams, Northern Ireland and Scotland are not allocated funding in the same way as England and Wales.

There is a robust legal framework in place in the UK, with the key piece of legislation being the Computer Misuse Act 1990. The UK legislation is kept under review and has recently been amended by the Serious Crime Act 2015. The UK is party to the Budapest Convention, which contains provisions on MLA. The UK is also party to other Council of Europe Conventions, UN Conventions, EU instruments, and nearly 40 bilateral treaties on MLA. The UK has implemented the Freezing Order Framework Decision in relation to evidence, but in practice it is rarely used. The UK has also recently implemented the Confiscation Order Framework Decision.

From a practical point of view, fulfilment of the UK strategy on cybercrime is carried out by different stakeholders, including law enforcement agencies, prosecution and judiciary, Department of Business, Innovation and Skills, the Home Office, the Foreign and Commonwealth Office and other government bodies. Its objectives are also progressed via public-private partnership.

There are many initiatives arising from the Strategy worth mentioning: the establishment of the National Cyber Crime Unit located within National Crime Agency as the lead law enforcement agency; the enhancement of the centralised reporting body Action Fraud; and the ongoing efforts to improve public-private cooperation particularly through the creation of the Cyber-security Information Sharing Partnership (CiSP) under CERT-UK, to name but a few.

There is no mandatory reporting of cyber attacks for the private sector as the UK considers this burdensome to industry but instead encourages the private sector to share threat information. On the prevention of child sexual exploitation, search engines (Google and Microsoft) have introduced changes to their search engines to block images, videos and pathways to child abuse from blacklist search terms used by pedophiles, supplied by the National Crime Agency. The Internet Watch Foundation (IWF) also assist in the 'take down' of these indecent images of children.

The UK is actively engaged with Europol, EC3 and is presently chairing the Joint Cybercrime Action Taskforce (J-CAT) at EC3. It makes good use of JITs and makes significant efforts to facilitate links with other international partners. It also uses Mutual Legal Assistance with the Home Office having received over 700 requests from third states and having sent over 350 requests to third states in 2013; however, it identified challenges faced when using MLA in cybercrime cases, particularly the time the process can take.

The UK law enforcement agencies have substantial powers and investigative techniques at their disposal to investigate cyber offences and deal with digital evidence and encryption. E-evidence is treated as ordinary evidence, however, with no special rules in place to determine the handling and presentation of such evidence in criminal proceedings.

Part of the Strategy's objectives is to upskill law enforcement agencies and in this respect a National Training and Development Working Group has been established to oversee the content and delivery of cyber training to law enforcement agencies. The Police, key Government departments and other stakeholders are represented on this group. A range of training has been developed for various levels of LEA, ranging from specialist courses for those investigating sophisticated online crime to awareness raising courses and e-learning modules for first responders.

In addition, the UK, through its numerous stakeholders, provides a plethora of awareness-raising and prevention programmes to inform the public and industry about the risks of cybercrime and encourage the safe use of the internet. Many campaigns are offered to children as part of the school curriculum and the Department of Business Innovation and Skills works with Universities and the Higher Education sector to improve awareness and cyber security. There is a particularly advanced programme offered in Scotland.

On the whole, the evaluators could conclude that the UK Government is committed to tackling cybercrime and has taken a series of measures to meet this objective. The team was very impressed by the number of key initiatives in place and considers that many of these projects serve as models of good practice and could be used by other Member States to bolster their own efforts to tackle cybercrime.

The team did, however, identify some areas which need further improvement and has made some recommendations to the UK in this regard (See Chapter 9). The team invites the UK to implement these recommendations in order to further improve its efforts in the fight against cybercrime.

1.1 Models of Good Practice Case Studies

1. National Strategy - UK Cyber Security Strategy

In November 2011, the UK published the UK Cyber Security Strategy. The Cyber Security Strategy set out the UK Government's vision of "a vibrant, resilient and secure cyberspace" and set out 4 objectives:

- making the UK one of the most secure places in the world to do business in cyberspace
- making the UK more resilient to cyber attack and better able to protect its interests in cyberspace
- helping shape an open, vibrant and stable cyberspace that supports open societies
- building the UK's cyber security knowledge, skills and capability.

To support the Strategy the Government put in place a National Cyber Security Programme backed by **£860 million** of investment to 2016. Through the Programme the Government is working to: further deepen national sovereign capability to detect and defeat high-end threats

- ensure law enforcement has the skills and capabilities needed to tackle cyber crime and maintain the confidence needed to do business on the Internet
- ensure critical UK systems and networks are robust and resilient
- improve cyber awareness and risk management amongst UK business
- ensure members of the public know what they can do to protect themselves, and are demanding good cyber security in the products and services they consume
- bolster cyber security research and education, so it has the knowledge and expertise to keep pace with this fast-moving issue into the medium-term
- work with international partners to bear down on havens for cybercrime and build capacity, and to help shape international dialogue to promote an open, secure and vibrant cyberspace

The UK has made significant strides towards all these goals throughout the course of the Programme's existence. The long-term economic plan of the government continues to make the UK one of the most secure places globally for cyber innovation and commerce.

Governance of the Strategy

- The Office for Cyber Security and Information Assurance (OCSIA) in the Cabinet Office is responsible for the implementation of the National Cyber Security Strategy. The Home Office, the Department for Business, Innovation and Skills (BIS) are also key government stakeholders.
- The National Crime Agency's (NCA) National Cyber Crime Unit (NCCU) leads supports and coordinates the UK response to the cybercrime threat.
- In Scotland the government liaises closes with the Home Office, UK institutions and Police Scotland to fulfil the objectives of the Strategy.
- In Northern Ireland, the Department of Justice Organised Crime Taskforce (OCTF) coordinates prevention strategies with industry and statutory agencies.

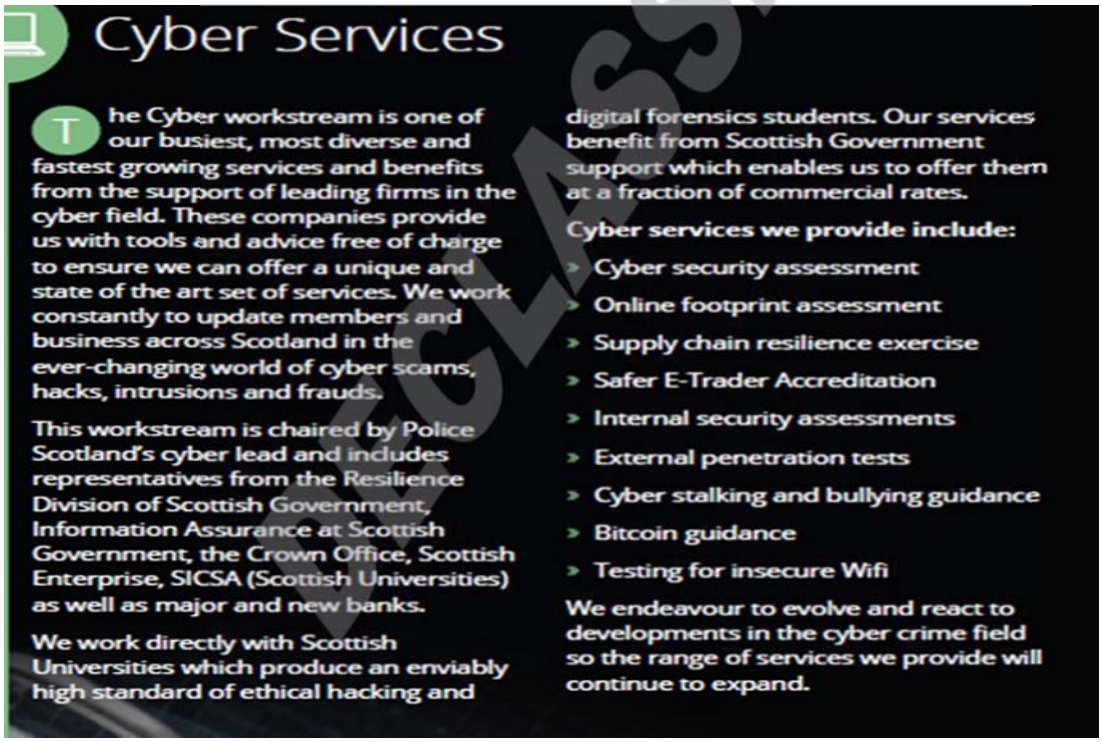
2. Scottish Business Resilience Centre

The Scottish Business Resilience Centre has established itself as a hub of innovation and business improvement in support of its partners and the business community.

Its objective is creating a secure Scotland for business to flourish in. In effect, creating a secure environment where business can trade and prosper securely, regardless of size and sector. This encompasses everything from premises and employee safety to cyber security.

It is a unique organisation comprising contributions and secondments from Police Scotland, Scottish Government, Scottish Fire and Rescue Service, major banks, industries, investors and private membership. It aims to provide its members with a wide ranging one stop shop for business security services and advice. It is uniquely placed to act as an advocate for commerce across Scotland and to be an independent voice for our members. Ultimately it is aiming to create a safer Scotland in which to thrive, live and do business.

Specific Packages on Cyber Security - SBRC Cyber Services Workstream



3. Cyber-security Information Sharing Partnership (CiSP)

The Cyber-security Information Sharing Partnership (CiSP), part of CERT-UK, is a joint industry government initiative to share cyber threat and vulnerability information in order to increase overall situational awareness of the cyber threat and therefore reduce the impact on UK business.

CiSP allows members from across sectors and organisations to exchange cyber threat information in real time, on a secure and dynamic environment, whilst operating within a framework that protects the confidentiality of shared information.

CiSP members are also able to receive network monitoring reports. This free service allows users to receive tailored feeds of information from CERT-UK covering any malicious activity that we see on your network.

Users can sign up for this service when they join CiSP or register your interest and a member of the team will get back to you when you have the necessary information.

Fusion Cell

CiSP members receive enriched cyber threat and vulnerability information from the '**Fusion Cell'**, a joint industry and government analytical team who examine, analyse and feedback cyber information from a wide variety of data sources – ultimately adding value to CiSP members and helping those organisations of all levels of cyber maturity. The Fusion Cell also provides a range of products and services including alerts and advisories, weekly and monthly summaries, as well as a capability to conduct bespoke malware and phishing email analysis on behalf of CiSP members.

Since launch in March 2013, the value of this collaboration for the benefit of the UK has been recognised by industry, with CiSP continuing to grow considerably with over 950 organisations and 2500 individuals signed up for this free service as of March 2014.

Benefits of CiSP

CiSP members benefit from:

1. Engagement with industry and government counterparts in a secure environment
2. Early warning of cyber threats
3. Ability to learn from experiences, mistakes, successes of other users and seek advice
4. An improved ability to protect their company network
5. Access to free network monitoring reports tailored to each organisations' requirements

4. Action Fraud - Centralised Fraud Reporting Centre

http://www.actionfraud.police.uk/

Action Fraud is the UK's national reporting centre for fraud and cyber crime where the public can report fraud if they have been scammed, defrauded or have been a victim of cyber crime.

It provides a central point of contact for information about fraud and cybercrime. The service is run alongside the National Fraud Intelligence Bureau by the City of London Police who are responsible for assessment of the reports and to ensure that your fraud reports reach the right place. The City of London Police is the national policing lead for economic crime.

Reporting of fraud and cyber crime

The Pubic can report fraud or internet crime using its reporting service any time of the day or night; the service enables the public to both report a fraud and find help and support.

When a member of the public reports to Action Fraud he/she receives a police crime reference number. Reports taken are passed to the National Fraud Intelligence Bureau. Action Fraud does not investigate the cases and cannot advise on the progress of a case. Action Fraud will always offer feedback to the complainant and sends letters to them to outline how the information they provided was used.

City of London Police also engages in some preventative work by means of producing preventative alerts to educate and inform the public on the threat of fraud.

2 INTRODUCTION

Following the adoption of Joint Action 97/827/JHA of 5 December 1997[1], a mechanism was established for evaluating the application and implementation at national level of international undertakings in the fight against organised crime. In line with Article 2 of the Joint Action, on 3 October 2013 the Working Party on General Matters including Evaluations (GENVAL) decided that the seventh round of mutual evaluations should be devoted to the practical implementation and operation of the European polices on preventing and combating cybercrime.

The choice of cybercrime as the subject for the seventh Mutual Evaluation round was welcomed by Member States. However, due to the broad range of offences which are covered by the term cybercrime, it was agreed that the evaluation would focus on those offences which Member States felt warranted particular attention. To this end, the evaluation covers three specific areas – cyber attacks, online child sexual abuse/pornography and online card fraud – and should provide a comprehensive examination of the legal and operational aspects of tackling cybercrime, cross-border cooperation and cooperation with relevant EU agencies. Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography and replacing Council Framework Decision 2004/68/JHA[2] (transposition deadline 18 December 2013), and Directive 2013/40/EU[3] on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (transposition deadline 4 September 2015), are particularly relevant in this context.

Moreover, the Council Conclusions on the EU Cybersecurity Strategy of June 2013[4] anticipated the swift ratification of the Council of Europe Convention on Cybercrime (the Budapest Convention)[5] of 23 November 2001 by all Member States and emphasised in their preamble that "the EU does not call for the creation of new international legal instruments for cyber issues". The Convention is supplemented by a Protocol on acts of xenophobia and racism committed through computer systems[6].

1 Joint Action of 5 December 1997 (97/827/JHA), OJ L 344, 15.12.1997, pp. 7-9.
2 OJ L 335, 17.12.2011, p. 1.
3 OJ L 218, 14.8.2013, p. 8.
4 12109/13 POLGEN 138 JAI 612 TELECOM 194 PROCIV 88 CSC 69 CIS 14 RELEX 633 JAIEX 55 RECH 338 COMPET 554 IND 204 COTER 85 ENFOPOL 232 DROIPEN 87 CYBER 15 COPS 276 POLMIL 39 COSI 93 DATAPROTECT 94.
5 CETS no. 185, opened for signature on 23 November 2001, entered into force on 1 July 2004.
6 CETS no. 189, opened for signature on 28 January 2003, entered into force on 1 March 2006.

Experience from past evaluations shows that Member States will be in different positions regarding the implementation of the relevant legal instruments, and the current evaluation process could also provide useful input to Member States that may not have implemented all aspects of the various instruments. Nonetheless, the evaluation aims to be broad and interdisciplinary and not to focus solely on the implementation of various instruments relating to fighting cybercrime, but also on the operational aspects in the Member States.

Therefore, apart from cooperation with prosecution services, this will also encompass how police authorities cooperate with Eurojust, ENISA and Europol/EC3 and how feedback from those organisations is channelled to the appropriate police and social services. The evaluation focuses on implementing national policies with regard to the suppression of cyber attacks, fraud and child pornography. The evaluation also covers operational practices in the Member States with regard to international cooperation and the support offered to people who fall victim to cybercrime.

The order of visits to the Member States was adopted by GENVAL on 1 April 2014. The UK is the third Member State to be evaluated during this round of evaluations. In accordance with Article 3 of the Joint Action, a list of experts in the evaluations to be carried out has been drawn up by the Presidency. Member States have nominated experts with substantial practical knowledge in the field pursuant to a written request to delegations from the Chairman of GENVAL on 28 January 2014.

The evaluation teams consist of three national experts, supported by two staff from the General Secretariat of the Council and observers. For the seventh round of mutual evaluations, GENVAL agreed with the proposal from the Presidency that the European Commission, Eurojust, ENISA and Europol/EC3 should be invited as observers.

The experts charged with undertaking the evaluation of the UK were Mr Geert Schoorens (Belgium), Mr Timo Piiroinen (Finland) and Ms Mairead Cotter (Ireland). The observers were also present: Mr Michael Palmer (Commission), Mr Lionel Ferette (ENISA), Mr Hari Tiesmaa (Eurojust) and Mr Benoit Godart (Europol/EC3), together with Ms Monika Kopcheva and Ms Nicola Murphy from the General Secretariat of the Council.

This report was prepared by the expert team with the assistance of the General Secretariat of the Council, based on findings arising from the evaluation visit that took place in the UK between 20 and 22 January 2015, and on the detailed replies from the UK to the evaluation questionnaire, together with their detailed answers to ensuing follow-up questions.

3 GENERAL MATTERS AND STRUCTURES

3.1 National cyber security strategy

The UK published its National Cyber Security Strategy[7] in November 2011. The first objective of the strategy is 'to tackle cybercrime and be one of the most secure places in the world to do business in cyberspace.'

The strategy aims to consider all of the threats to the UK from cyberspace collectively, through the UK's National Cyber Security Programme. Under the programme, individual departments and agencies are assigned responsibility to address specific aspects of the strategy. The UK Government is of the view that as all segments of society benefit from the use of cyberspace, all of society has a responsibility to ensure it is used responsibly and should help protect it. Therefore, the strategy applies to the private as well as public sector.

Since its publication, significant progress has been made to implement objective one of the strategy, most notably to meet the following objectives:

- **Strengthen law enforcement capacity** - This has been achieved through the establishment of the National Cyber Crime Unit (NCCU) within the National Crime Agency (NCA) and accompanying enhanced cooperation at regional and local policing levels.
- **Increase business awareness of the risk -** A new Cyber-security Information Sharing Partnership (CiSP) has been created as part of the national CERT to help achieve this aim.
- **Improve reporting arrangements -** A centralised service for reporting fraud has been established by the City of London Police called 'Action Fraud' which creates a simplifed reporting system to make it easier for the public and businesses to report fraud.
- **Upskill Law Enforcement and prosecution authorities -** Work is underway to identify the police force requirements and to build the required skills through training. Training is also being further developed for prosecutors.
- **Increase Public Awareness of the risk -** Public awareness has been raised through the introduction and promotion of a number of campaigns such as CyberStreetWise, 'Make IT happy', ThinkuKnow and Get Safe Online.

[7] Available at (https://www.gov.uk/government/publications/cyber-security-strategy)

Governance of the Strategy

England and Wales

- The Office for Cyber Security and Information Assurance (OCSIA) in the Cabinet Office is responsible for the implementation of the National Cyber Security Strategy. This includes the management of the National Cyber Security Programme (NCSP), which funds and coordinates activity across the UK Government to protect the UK in cyberspace.
- The Home Office (Strategic Centre for Organised Crime, OSCT) leads on the objective to tackle cyber crime as part of its responsibilities to areas such as counter-terrorism, policing, drugs, crime and immigration. The Department for Business, Innovation and Skills (BIS) is responsible for working with industry to protect businesses on-line.
- The National Crime Agency's (NCA) National Cyber Crime Unit (NCCU) leads supports and coordinates the UK response to the cybercrime threat.

Scotland

The Scottish Government is responsible for policing within Scotland, including cybercrime. In this area it liaises closely with the Home Office, UK institutions and Police Scotland. The Serious Organised Crime Taskforce (SOCTF) ensures that law enforcement agencies and others in Scotland work together in addressing serious organised crime

Northern Ireland

The Organised Crime Taskforce (OCTF) (chaired by the Minister of the Department of Justice Northern Ireland) coordinates prevention strategies with industry and statutory agencies. This includes engagement with industry and academia and the implementation and development of legislation as well as raising public awareness. Significant liaison has been established with national law enforcement agencies. Local policing enforcement and cyber response falls to the Police Service Northern Ireland (PSNI) to investigate.

The NCA became fully operational in Northern Ireland on 20 May 2015. Officers are now able to exercise the powers and privileges of a Northern Ireland constable, in accordance with General Authorisation agreed between the Director General and Minister of Justice Northern Ireland.

3.2 National priorities with regard to cybercrime

Cybercrime forms part of the first objective of the National Cyber Security Strategy.

The UK's Serious and Organised Crime Strategy [8] (2013) is designed to deal with the challenges faced from serious and organised crime. It was published to coincide with the launch of the National Crime Agency (NCA) and reflects changes to the threats presently faced and lessons learnt from previous strategies. It is the product of extensive consultation with law enforcement, the UK intelligence agencies, local authorities, the private sector and academia.

The Serious and Organised Crime Strategy aims to substantially reduce the level of serious organised crime that affects the UK, including cyber crime. It promotes a 4 'P' framework; prosecuting and disrupting people engaged in serious and organised crime (PURSUE); preventing people from engaging in this activity (PREVENT); increasing protection against serious and organised crime (PROTECT); and reducing the impact of this criminality where it takes place (PREPARE).

The new strategy has tried to address identified shortcomings of previous strategies in particular by ensuring that there is cross-government responsibility for its implementation. This approach has netted tangible results and public-private cooperation has greatly improved as a result of the role of the Department of Business, Innovation and Skills (BIS) under the Strategy.

3.3 Statistics on cybercrime

Official Crime Statistics

Historical trends are not available because the responsibility for centralised recording of fraud and cybercrime only moved from local police forces to the National Fraud Intelligence Bureau (NFIB) in 2013/14. Prior to this, the police recorded such offences, but did not separately distinguish cybercrime.

[8] https://www.gov.uk/government/publications/serious-organised-crime-strategy

The total police-recorded crime from June 2013 to June 2014 was **3,717,089** offences. Of these offences, the National Fraud Investigation Bureau (NFIB) recorded that **18,416** fell under the Computer Misuse Act offences (i.e. cyber-dependent crimes), meaning the proportion is **less than half a per cent** of all recorded crime.

However, this does not include cyber-enabled crime (e.g. fraud), or crimes with an online element. It is not currently possible to identify these crimes specifically. For example, for the 12 months to June 2014, a total of **209,667 fraud offences** were recorded by NFIB, but it is not possible to identify which of these were cyber-enabled fraud.

Public Surveys

Available survey data suggests that experiences of viruses among adult internet users appears to be falling, since peaks in 2005/06[9], 2012/13 shows that 24% of adult internet users experienced a virus, down from 41% in 2005/06 and experiences of phishing emails are also down from a peak of 22% in 2011 to 19% in 2013[10]. However, the proportion of individuals surveyed who have had their personal computers accessed or hacked without their permission appears to be increasing since the 2000s, from 2% in 2006/07 to 8% in 2012/13.[11]

Looking at cyber-enabled fraud, data from Financial Fraud Action suggests that internet-enabled card-not-present (CNP) fraud increased rapidly in the early 2000s, began to fall in 2008, but has risen again since 2011. The most recent figures show that in 2013, **£163.2 million** was lost due to online CNP fraud, **up 16% from 2012.**[12]

Similarly, losses from online banking fraud declined since 2009, but began to rise again in 2012. In 2013, **£40.9 million** was lost to online banking fraud, an increase of **3% on 2012 losses**.

9 the Crime Survey for England and Wales (CSEW)
10 Oxford Internet Survey, 2013
11 CSEW data
12 Fraud the Facts, 2013.

3.4 Domestic budget allocated to prevent and fight against cybercrime and support from EU funding

The National Cyber Security Programme is supported by **£860 million** of Government investment over a five year period from 2011 to 2016. 10% of the overall budget goes towards enhancing law enforcement capabilities in England and Wales (and nationally through the National Crime Agency) to tackle cybercrime. This is on top of funding from the general policing budget.

This funding has been used to establish the National Cyber Crime Unit within the National Crime Agency to provide the national lead against the most complex cyber criminals; setting up cyber teams in each region in England and Wales; funding the Action Fraud/National Fraud Intelligence Bureau reporting and analysis center; and providing training for police officers in regional police units.

Northern Ireland and Scotland

A proportion of the NCSP funding is provided to Scotland and NI through their baseline funding but is not ring-fenced. NI and Scotland also benefit from national capabilities through National Cyber Security Programme.

3.5 Conclusions

- The UK has established a comprehensive, robust national Cyber Security Strategy which enjoys cross-government and industry support. It comprehensively covers the most important aspects to be taken into account when tackling cybercrime, such as prevention, legislation, capacity building and training, public awareness, public-private and international cooperation. The UK has clearly defined its national priorities with regard to tackling cybercrime and the Strategy contains clear objectives, measureable targets and a good governance structure.

- Significant funding has been made available to implement the Strategy which is indicative of the UK Government's commitment to tackle cybercrime. However, the team noted that the funding provided to Scotland or Northern Ireland is not ringfenced to deal with cybercrime and as a result the efforts to tackle the issue may not be consistent UK wide. The team considered that this could result in a gap in the implementation of the Strategy as a whole.

- It is clear that several concrete steps have been taken as a result of the Strategy, including the creation of the National Cyber Crime Unit (NCCU) under the National Crime Agency, the development of the centralised reporting service for fraud (Action Fraud) and programmes to upskill and equip law enforcement agencies (LEAs) to deal effectively with emerging trends and technological developments in cybercrime.

- In the opinion of the evaluators, the strategy, along with the defined priorities developed in the UK, is a solid basis to effectively tackle cybercrime with many good models having been developed. Close cooperation between the private sector and public organisations creates a unique opportunity to involve a wide range of entities working together.

- The team noted that statistics are available for England and Wales on cyber-dependent crimes but there are no comparable statistics readily available from the other UK jurisdictions. Since cybercrime can take different forms and is not always the predominant factor in criminal activity, it is difficult to provide detailed, standardised and comprehensive statistics on cybercrime that would make it possible to check overall cybercrime figures. Consideration could be given to the best ways to improve the current statistics, for example, cyber-enabled fraud offences could be recorded by adapting the reporting template already available on the Action Fraud website.

4 NATIONAL STRUCTURES

4.1 Judiciary (prosecution and courts)

4.1.1 Internal structure

Cybercrime offences are prosecuted within the general court system. In England and Wales there are about 30 – 40 prosecutions under the Computer Misuse Act 1990 per year, and these are dealt with at either Magistrate or Crown Courts. Cases involving cyber crime offences and other criminal offences are often prosecuted under other Acts, such as the Fraud Act.

- **Prosecution**

The Crown Prosecution Service (CPS) is the sole prosecuting authority for England and Wales, acting independently in criminal cases investigated by the police. The CPS decides which cases should be prosecuted, determines the appropriate charges in more serious or complex cases and prepares cases and presents them at court. The UK does not have specialised prosecutors to deal with cybercrime, however, it does have a specialised prosecutor dealing with serious crime cases which are dealt with by the National Crime Agency.

Scotland

The Crown Office and Procurator Fiscal Service is the sole prosecuting authority for Scotland. Cybercrime acts do not fall under a specialised prosecution or Court in Scotland; they will in most circumstances be dealt with in the High Court or Sheriff Courts. Scottish courthouses are currently undergoing a digitalisation programme as part of the "Digital Scotland" agenda. This will make WIFI available in courtrooms and will assist in the provision of digital evidence during proceedings.

Northern Ireland

Prosecution of offences falls to the Central casework Section of the Public Prosecution Service who are responsible for the prosecution and direction of serious and organised crime cases.

- **Judges**

There are no specialist courts dealing with cybercrime. Criminal cases are tried either as 'on indictment' or by 'summary'. Summary trials take place in a Magistrates' court, while trials on indictment take place in the Crown Court. Despite the possibility of two venues for trial, almost all criminal cases, however serious, commence in the Magistrates' Courts.

4.2 Law enforcement authorities

National Crime Agency / National Cyber Crime Unit

The National Cyber Crime Unit provides the focus for the UK's national response to combating serious cybercriminals. It targets them by using its increased operational resources to investigate, disrupt and prevent cybercrime. It also makes use of the National Crime Agency's enhanced intelligence picture to proactively pursue criminals, targeting them where they are most vulnerable. Examples include recent operations between the UK and other international partners to combat the threat of malicious software ('malware') such as GameOverZeus and Cryptolocker.

The NCA is mainstreaming cyber and digital skills through training, new capability and recruitment of staff with specialist skills to work throughout the Agency to ensure the NCA has the right skills, capabilities and expertise to tackle organised crime in the digital age. The NCCU are also working with the College of Policing on the Digital Investigations and Intelligence Framework, streamlining training and delivery to meet needs nationally, regionally and locally across all levels of competence to develop a Skills Framework that mitigates the threat and exploits the opportunities.
The National Crime Agency has a UK-wide remit to fight serious and organised crime, but policing is devolved in Scotland and Northern Ireland.

Regional Organised Crime Units (ROCUs)

Police forces in England and Wales collaborate to form Regional Organised Crime Units (ROCUs). These units deliver specialist investigative and intelligence capabilities to help forces tackle serious and organised crime. They are also the primary interface between the police and the National Crime Agency, and are critical to successful National Crime Agency tasking and co-ordination. In 2013/14, the police embarked upon a programme of work supported by additional Home Office funding to significantly uplift ROCUs' capabilities in twelve core areas including cybercrime, fraud and witness protection.

During the evaluation visit the team learnt from officials that as recently as two years ago little attention was given to cybercrime across all the regional policing areas. Since then, the police response to cybercrime has been significantly enhanced. This has been facilitated by the creation of regional cybercrime units in each ROCU.

Scotland

Police Scotland has a single cybercrime investigation capacity within its Specialist Crimes Directorate located across three regions of the force. Police Scotland Cyber Crime Unit liaises closely at a UK level with the National Cyber Crime Unit and CERT-UK.

The Cyber Crime Unit is a national entity with local units based at 9 separate locations throughout the country. All of the units are line managed by senior officers within the Specialist Crime Division. In general terms, Police Scotland use the same legislation as the rest of the UK to investigate true cybercrime, but there are significant differences regarding legislation governing the detention, arrest and interview of suspects. Similarly, prosecutions are prepared and conducted by the Crown Office and Procurator Fiscal Service.

The Cyber Crime Unit has well developed partnership arrangements with National Crime Agency, CERT-UK, Scottish Government and Crown Office.

Northern Ireland

Northern Ireland's response to cybercrime is contained within the Crime Operations Branch of the PSNI. This Department uses investigators, forensic and technical staff, intelligence capability and covert officers who are trained in the cyber-tactics required.

Whilst this is not a single capacity, evaluations and proposals are being examined on the potential for a single cyber capability with management to coordinate the effective response. This will include the already established liaison and Organised Crime Task Force management. The Organised Crime Task Force was established in 2000. Its mission is to help secure a safe, just and prosperous society in Northern Ireland by confronting organised crime through multi-agency partnership between Northern Ireland Government Departments, law enforcement, the Public Prosecution Service, Policing Board, business community and the community at large.

The OCTF's structure, set out below, is a model for partnership working. The Stakeholder and Strategy Groups and the underpinning subgroups set priorities, develop strategies and agree actions to confront organised crime in Northern Ireland, from armed robbery to cyber crime and human trafficking to tax evasion. The OCTF undertakes regular threat assessments to identify key and emerging trends and threats and looks at how these may be tackled. The OCTF does not provide an operational response – that remains with individual law enforcement agencies.

STAKEHOLDER GROUP

Chaired by the Justice Minister

↓

STRATEGY GROUP

Chaired by the Department of Justice Director of Safer Communities

↓

SUBGROUPS

- Armed Robbery
- Criminal Finance
- Cross Border Fuel Fraud
- Cyber Crime

- Drugs
- Immigration and Human Trafficking
- Intellectual Property Crime
- Legal
- Publicity

4.3 Other authorities/institutions/public-private partnership

The UK Government and agencies work with a multitude of other authorities and private sector partners including the Serious Fraud Office (SFO); Financial Conduct Authority (FCA); Federation Against Copyright Theft (FACT); Government cyber security organisations such as Action Fraud – Get safe online (GSO), CiSP (Cyber information security partnership) as part of CERT-UK; Regulators such as Bank of England.

CERT-UK is active in the provision of advice on prevention and offers an electronic information sharing platform known as CiSP to encourage individuals and businesses to share information for this purpose. It is currently expanding this forum and is working towards having a node in each region which will allow the roll-out to regional small and medium enterprises (SMEs).

Scotland

CERT-UK is active in the circulation of prevention advice and CiSP also covers Scotland.

Scotland also boasts a Business Resilience Centre which is a unique organisation comprising Police Scotland, Scottish Government, Crown Office and Procurator Fiscal Service, Scottish Fire and Rescue Service, major banks, industries, investors and private membership. It aims to provide its members with a wide ranging one stop shop for business security services and advice including a specialist "workstream" on cyber services. This "workstream" is one of its busiest and includes the provision of: cyber security assessment; online footprint assessment; supply chain resilience exercise; safe E-Trader accreditation; internal security assessments; external penetration tests; cyberstalking and bullying guidance; bitcoin guidance and testing for insecure WIFI.

Northern Ireland

Northern Ireland under the OCTF control has developed a coordinated response involving the Public Prosecution Service (PPS), FACT, GSO, Action Fraud, CiSP and CERT-UK. This provides coordination to all these agencies and groups to effectively identify and develop efficient strategies to respond to cyber-threats and incidents. In addition, an OCTF 'Industry Engagement Group' has been developed which includes industry and academia and seeks to provide a collaborative environment to tackle the cyber-threats and response development.

4.4. Cooperation and coordination at national level

Legislation and policy is led by the Home Office. Operationally, at national level this is managed by the National Crime Agency, which replaced the Serious Organised Crime Agency. It became fully operational on 7 October 2013 and is a non-Ministerial government department. The National Crime Agency includes the Child Exploitation and Online Protection Command.

The NCA is the UK's lead agency against serious and organised crime; human, weapon and drug trafficking; cybercrime; and economic crime that goes across regional and international borders, but can be tasked to investigate any crime. It has a strategic role in which it looks at the bigger picture across the UK, analysing how criminals are operating and how they can be disrupted. To do this it works closely with regional organised crime units (ROCUs), the Serious Fraud Office, as well as individual police forces. It is the UK point of contact for foreign agencies such as Interpol, Europol and other international law enforcement agencies.

Collaboration with industry is critical to the NCA's approach to tackling cyber crime threats. The NCCU works closely with industry to share information, protect the UK from cyber threats, clean up UK internet infrastructure and deliver high impact operations targeting the most serious cyber crime threats. Supporting and strengthening existing cooperation mechanisms is critical to the NCA's approach to working with industry. The NCA works closely with CERT-UK to share threat intelligence, including time-critical alerts and complex bulk data disseminations. The approach in the past was to encourage industry to report on cyber attacks with a view to investigation and prosecution. However, it became clear that this was not an approach with which industry necessarily engaged, due to potential reputational damage which could result. The UK Government realised that instead it needed to build a trusted relationship with industry partners so it changed its approach. Now, it encourages industry to notify the National Crime Agency of attacks not necessarily with a view to prosecution, but to provide information to help against further attacks.

The National Crime Agency produces an annual strategic assessment which includes threat assessment and develops action plan/control strategy to deal with any identified cyber threats. The main document is the control strategy as it prioritises strategies, gaps in service and training requirements. The National Strategic Assessment draws together knowledge from across the whole law-enforcement community. It provides an objective picture of serious and organised crime threats, enabling UK law enforcement as a whole to prioritise, coordinate and target the response.

The preparation of the document therefore involves wide consultation across law enforcement, Government Departments and agencies including police forces in England and Wales, PSNI, Police Scotland, Regional Organised Crime Units, the National Crime Agency, Border Force, NOMS[13], HMRC, SFO[14], the Crown Prosecution Service, Immigration Enforcement, Cabinet Office, Home Office and GCHQ[15].

[13] National Offender Management Service
[14] Serious Fraud Office
[15] Government Communication Headquarters

The National Strategic Assessment summarises the current risk, key trends and knowledge gaps under each of the threats, including cybercrime. The National Control Strategy comprises a prioritisation of the risks and Strategic Action Plans summarising the planned response. This provides a framework to set priorities around the national response and is used to inform National Tactical Tasking and Coordination.

The National Intelligence Requirements are drawn from the intelligence gaps detailed in the National Strategic Assessment and represent the priority strategic intelligence requirements for the following year.

Scotland
Regular meetings are held between representatives of the Crown Office and Procurator Fiscal Service (COPFS) and Police Scotland to discuss issues pertaining to cybercrime.

Northern Ireland
In Northern Ireland the Organised Crime Task Force meets quarterly.

4.4.1 Legal or policy obligations

There are no legal obligations for the private sector to notify the UK authorities of cybercrime incidents , however in reality, if such a serious breach of personal data were to occur, the Information Commission is likely to be involved in terms of investigation and any subsequent enforcement activity. As part of this process notifications to affected parties is a common outcome.

On child sexual exploitation, law enforcement agencies have the powers to order the removal of indecent images of children, using standard legislation. In addition, the Internet Watch Foundation (IWF) has arrangements with industry that ensure URLs identified as being hosted in the UK are removed when the IWF notifies the host ISP, and URLs held on web pages outside the UK are regularly placed on the IWF blocking list.

4.4.2 Resources allocated to improve cooperation

Funding for tackling cybercrime is provided for out of the £860 million budget for implementation of the Strategy. In addition to that, the NCSP pays for a number of other work streams including private sector engagement and public awareness. These compliment the cybercrime work. NCSP funding is additional funding on top of existing funding to the police (e.g. main grant) and the additional funding from the Home Office to ROCUs and the NCA's core budget.

4.5 Conclusions

- Given the specialised nature and complexity of cybercrime and the increasing volume of cases, the evaluation team was surprised to learn that there are presently no specialised prosecutors dealing with cyber-dependent crime. The team noted that there are dedicated prosecutors for other types of crime. The appointment of dedicated prosecutors for cyber-dependent crime would ensure that the prosecution service is involved at an early stage of the investigation and cases are handled as effectively as possible.

- The team noted that there is a relatively low number of cases prosecuted under the Computer Misuse Act 1990 per year given the volume of cases reported to the NFIB and size of the UK, however, it was mindful that many cases may be prosecuted under other legislation such as the Fraud Act 2007.

- Prosecutors in England and Wales undergo training online via specialist courses available on the CPS website. The team considers, however, that more face-to-face training would be beneficial and should also be offered. This would also provide an opportunity for prosecutors to share experiences and enhance professional networks.

- Scotland has training with police, prosecutors and judges present. The team learnt that the Scottish police welcomed such training opportunities as judges indicate views on legal issues presented by cybercrime cases at those meetings.

- There is no specialised court dealing with cybercrime, and it does not appear that the UK sees any real merit in establishing these courts in the short to medium term. Whilst the team could understand this position, it noted that there is no systematic mandatory training provided for judges on cybercrime. The team considers that given the technical specificities of cybercrime, a high degree of understanding from the judge presiding over the case is required and training is fundamental in this regard.

- The team was satisfied by the approach taken by the police to deal with cybercrime and the commitment to tackling the issue. The inclusion of cybercrime in Regional Police Control Strategies was considered a positive step and key to ensuring implementation of the National Strategy.

- The team welcome the work of Action Fraud which made the reporting of online fraud easier for citizens and industry. It noted, however, that Action Fraud did not cover Scotland.

- The UK authorities enjoy and foster positive relations with the private sector. It was clear that much thought has been given to identify the best ways of dealing with industry to encourage information sharing and better corporate response to the cyber threat. Dedicated funding under the National Cyber Security Programme and other innovative measures such as the development of CiSP, CERT-UK and the Scottish Business Resilience Centre have greatly enhanced this cooperation. This approach has yielded positive results and could be considered as a model of good practice.

- One of the challenges facing law enforcement bodies in the fight against cybercrime is the retention of specialised technical staff due to the limited funding available for public sector employees/agents. The National Crime Agency has been faced with competition from the private sector which can generally offer better remuneration to technical experts. The team was advised that the National Crime Agency has been exploring ways to retain technical experts by offering other perks and advantages such as management opportunities coupled with interesting and diverse work. These measures go some way to address the issue, however, it was clear that more needs to be done to retain these technical experts in a competitive field. Consideration could be given to increasing pay or creating new pay scales for these experts.

5 LEGAL ASPECTS

5.1 Substantive criminal law pertaining to cybercrime

There is no legal definition or offence of cybercrime in the UK, but a definition is provided in the Serious and Organised Crime Strategy:

"Cybercrime describes two distinct but closely related, criminal activities: cyber-dependent crimes, and cyber-enabled crimes:

Cyber-dependent crimes can only be committed using computers, computer networks or other forms of information communication technology (ICT). They include the creation and spread of malware for financial gain, hacking to steal important personal or industry data and denial of service attacks to cause reputational damage.
Cyber-enabled crimes (such as fraud, the purchasing of illegal drugs and child sexual exploitation) can be conducted on or offline, but online may take place at unprecedented scale and speed."

The main legislation relating to acts unique to information systems is the Computer Misuse Act 1990. The relevant sections for categories include;

Section 1 - unauthorised access to computer material
Section 2 - unauthorised access with intent to commit or facilitate commission of further offences
Section 3 – unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer
Section 3ZA – unauthorised acts causing, or creating risk of, serious damage
Section 3A - making, supplying or obtaining articles for use in offence under section 1, 3 or 3ZA

The UK does not use the term “child pornography" but rather the term “indecent images of children”. Furthermore it does not make a distinction between online and offline offending in relation to indecent images of children. The main legislation relating to indecent images of children is the Protection of Children Act 1978 and subsequent amendments. The legislation relating to grooming is s15 of the Sexual Offences Act 2003.

The UK does not distinguish between online and offline offending for fraud, forgery or identity offences. Within the UK (excluding Scotland) the Fraud Act 2006 covers both fraud and misrepresentation. The Forgery and Counterfeiting Act covers forgery. Spam is covered by the Privacy and Electronic Communications (EC Directive) Regulations 2003.

The UK has general legislation that can be used to hold legal persons liable for offences including cybercrime.

There are no criteria for "minor cases" in the relevant legislation. The decision on whether a case is minor or not is a matter for the Court.

Current Legislative Developments

The Serious Crime Act 2015 makes a number of changes to the Computer Misuse Act 1990, in particular to ensure that sentences for attacks on computer systems fully reflect the damage they cause. The amendments:

- Create a new offence of unauthorised acts in relation to a computer that result, either directly or indirectly, in serious damage to the economy, the environment, national security or human welfare, or creates a significant risk of such damage. The offence will carry a maximum sentence of life imprisonment for cyber attacks which result in loss of life, serious illness or injury or serious damage to national security and 14 years' imprisonment for cyber attacks causing, or creating a significant risk of, severe economic or environmental damage or social disruption.

- Extend section 3A (making, supplying, or obtaining articles for use in offences under sections 1 or 3) of the 1990 Act to include an offence of 'obtain for use' to cover the event of tools being obtained for personal use to commit offences under section 1 (unauthorised access to computer material), section 3 (unauthorised acts with intent to impair, or with recklessness as to impairing operation of a computer etc.), or the new offence above.

- Extend the existing extra territorial jurisdiction provisions in section 4 of the 1990 Act to provide a legal basis to prosecute a UK national who commits any 1990 Act offence whilst physically outside the UK, where the offence has no link to the UK other than the offender's nationality (provided the offence is also an offence in the country where it took place).

- Clarify the interaction between the offences in the 1990 Act and law enforcement powers (derived from other enactments, wherever exercised) necessary for cybercrime investigations through the clarification of section 10 of the 1990 Act.

The Computer Misuse Act 1990 applies UK-wide and the subsequent amendments included in the Serious Crime Act will also apply UK wide once these provisions are commenced.

Scotland

The importance of corroboration is a unique feature of Scots criminal law. The requirement for corroborating evidence means at least two different and independent sources of evidence are required in support of each crucial fact before a defendant can be convicted of a crime.

5.1.1 Council of Europe Convention on Cybercrime

The UK signed the Convention on Cybercrime on 23 November 2001 and ratified it on 28 May 2011.

5.1.2 Description of national legislation

A. Council Framework Decision 2005/222/JHA on attacks against information systems and Directive 2013/40/EU on attacks against information systems

The UK will become fully compliant with the Directive 2013/40/EU through the amendments made in the Serious Crime Act 2015 (see 5.1).

B. Directive 2011/93/EU on combating sexual abuse and sexual exploitation of children and child pornography

The UK transposed the Directive on time. There were no specific issues that arose as the UK was already largely compliant. A report of the transposition was submitted and is available on the Eur Lex database.

C. Online card fraud

Action Fraud is the UK's national reporting centre for fraud and cybercrime. The service is run by the City of London Police working alongside the National Fraud Intelligence Bureau (NFIB) who are responsible for assessment of the reports and to ensure that fraud reports reach the right place. The City of London Police is the national policing lead for fraud. There are two ways for the public to report fraud (i) through the dedicated call centres (based in Scotland and Manchester) or (ii) on line through the Action Fraud website.

Action Fraud separates the reports into two categories (i) information reports and (ii) crime reports. All reports are given a police reference number and are passed to the NFIB for consideration. Approximately 20,000 fraud and cybercrime cases are reported every month, and just under 10% of these are cyber dependant.

The NFIB assesses the criminal leads on the basis of three factors: (1) the viability of the enquiry; (2) an assessment of the level of harm to the victim; and (3) the potential for solving the case. More broadly it also considers repeat victimisation and prevention. It will refer potential cases to the most appropriate law enforcement agency and also to non-police bodies such as the trading standards agency for further action where appropriate.

Action Fraud will always offer feedback to the complainant and sends letters to them to outline how the information they provided was used. It does not investigate the cases and does not advise on the progress of a case.

From the on site visit it was clear that practitioners felt that disruption work is key to the work of Action Fraud. In addition to this core work, Action Fraud also engages in some preventative work by means of producing preventative alerts to educate and inform the public on the threat of fraud.

The team was advised that there were issues around bulk reporting in the past as each report had to be entered into the system individually. This caused problems especially for big retailers who could be hit thousands of times so were not in a position to report each incident individually. To address this, Action Fraud has now updated its system and is piloting a bulk upload facility.

Action Fraud accepts reports from outside UK and exports this information through SIENA to contacts in the EU.

5.2 Procedural issues

5.2.1 Investigative Techniques

All of the following investigative techniques are available under UK law;

- search and seizure of information system/computer data;
- real-time interception/collectionof traffic/content data;
- preservation of computer data;
- order for stored traffic/content data;
- order for user information

Most of these would be dealt with under the Regulation of Investigatory Powers Act 2000 (RIPA). Other legislation that can be used includes the powers in the Police and Criminal Evidence Act 1984 (PACE) and the Police Act 1997.

Section 19 of PACE gives a general power of seizure to a Police Constable lawfully on the premises, including in section 19(3) what he reasonably believes to be evidence in relation to an offence he is investigating and where seizure is necessary to prevent its loss or destruction. Section 19(4) specifically extends this to requiring electronic information fitting those criteria to be produced in a form to be taken away and to be visible and legible. Section 20 extends the powers of seizure in any Act (as well as PACE) to enable the police (or authorised civilian investigating officer) to require this in relation to electronic data.

Section 50 of the Criminal Justice and Police Act 2001 also enables police to 'seize and sift'- i.e. a power to remove material for the purpose of sifting it elsewhere to determine whether it includes material the police are authorised to search, where it is not reasonably practicable to do so on the premises. There is also a power to do this where the relevant material cannot reasonably be separated from something else - this could include for example a computer containing relevant data on a hard disk. Schedule 1 lists a wide range of seizure powers to which section 50 applies, not just police powers under PACE, but also other law enforcement activities and authorities.

While real-time interception of content data is possible the data collected cannot be used in criminal proceedings.

Scotland and Northern Ireland
Similar legislation and powers exist within Scotland and Northern Ireland.

5.2.2 Forensics and Encryption

- **Forensics**

The NCCU undertakes a wide range of forensic examinations, i.e.

- Digital media seized from crime scenes
- Victim devices to identify crime, cyber threat, malware etc
- Live data seizure at scenes capturing volatile evidence (Cloud, open encryption, RAM)
- Behavioural analysis and code examination on malware and viruses

Scotland

All forensic examinations of digital systems are undertaken by Police Scotland, who have trained staff throughout the country to provide evidence for court purposes. Capability exists to conduct these examinations covertly but not by remote means.

Northern Ireland

Forensic examinations are undertaken by trained staff within the PSNI e-crime facility. Remote forensic examinations are being developed but this is not operational at this time due to lack of funding.

- **Encryption**

Part III of the Regulation of Investigatory Powers Act (RIPA) 2000 provides for access to information protected by encryption. If an individual is issued with a notice under section 49 of RIPA they are required to disclose the key.

Notices can only be sought in the interests of national security, for the purpose of preventing or detecting crime or in the interests of the economic well-being of the UK (where it relates to National Security). Failure to disclose the relevant information can result in a fine, imprisonment or both.

The UK has independent commissioners who oversee the use of this provision regarding its proportionality and other aspects. The National Crime Agency advised that decisions to make use of this power are only taken after consultation with its team of in-house lawyers who consider whether fundamental rights are protected. In practice, the use of this provision is generally restricted to more sensitive cases.

Scotland

When faced with encryption, Scotland makes use of Section 49 Regulation of Investigatory Powers Act 2000, when required. It also uses forensic tools to try and "crack" a password before sending the device(s) to National Technical Assistance Centre (NTAC).

Currently it is unable to decrypt certain mobile devices which have encryption turned on as standard without recourse to this legislation.

Northern Ireland

Section 49 of RIPA is being used more often but increasing encryption of devices and data is also a growing challenge for PSNI.

5.2.3 e-Evidence

There is no separate classification for electronic evidence. There are guidelines (Policy Bulletin SPD/LI/2011) for law enforcement to use when they gather electronic evidence and the team was informed that the national policing lead on cybercrime is also examining the digitalisation of investigation and evidence gathering.

5.3 Protection of Human Rights/Fundamental Freedoms

The UK Human Rights Act supports freedom of expression . Law enforcement agencies are required to operate in accordance with the relevant provisions of the Human Rights Act , the Data Protection Act and other relevant legislation. In addition, section 3.5 of the UK Cyber Security Strategy provides that cybersecurity policies will be pursued 'while preserving UK citizens' right to privacy and other fundamental values and freedoms.

5.4 Jurisdiction

5.4.1 Principles applied to the investigation of cybercrime

The Computer Misuse Act 1990 allows for extra-territorial jurisdiction where the offence committed has a significant link to the UK – that being the suspect or the affected computer was in the UK. Recent changes to the Computer Misuse Act have extended the existing extra territorial jurisdiction provisions in section 4 of the 1990 Act to provide a legal basis to prosecute a UK national who commits any 1990 Act offence whilst physically outside the UK, where the offence has no link to the UK other than the offender's nationality (provided the offence is also an offence in the country where it took place).

5.4.2 Rules in case of conflicts of jurisdiction and referral to Eurojust

The resolution depends on the case, and the circumstances. The factors involved may include i) the location of the offender; ii) the location of the evidence; iii) where the harm was done. It is for prosecutors to determine where the case should be heard in accordance with the guidance issued by the Director of Public Prosecutions.

Scotland

Conflicts of jurisdiction are usually resolved in an amicable manner through bilateral discussions and meetings. These can be resolved through direct correspondence through many forms of communication or face-to-face meetings. The evaluation team was advised that this has recently been evident in a cybercrime case involving 3 Member States as well as two third states. A number of telephone conferences and face-to-face meetings established a common ground for the preferred jurisdiction of a single prosecution and discussed the arguments for and against separate prosecutions. This was conducted in an amicable atmosphere and the grounds for each option were properly discussed prior to any decisions being made.

The team was also advised that where this way forward is not possible for linguistic or practical reasons, coordination meetings at Eurojust have been called for the matters to be discussed.

5.4.3 Jurisdiction for acts of cybercrime committed in the "cloud"

The UK has no specific rules to address this issue. A specific problem when dealing with offences relating to the "cloud" is to establish where the offence is actually happening. Even the owners of data don't know where it is located and it can be located in more than one jurisdiction. Once the location has been established then the UK uses domestic legislation such as the Computer Misuse Act 1990 to allow for extra-territorial jurisdiction.

Scotland

Scotland has not experienced any problems relating to cloud storage to date. This is partly due to the limited number of cases reported involving cloud storage. The cases have generally related to accessing images already on cloud storage as opposed to the creation of them. So far it has been able to claim jurisdiction by establishing where the cloud storage was accessed.

Northern Ireland

Whilst there are increasing instances of cloud storage being used there have been few instances of conflicts of jurisdiction. The PSNI have successfully used Eurojust and Joint Investigation Teams to overcome jurisdiction issues and primary prosecutions on cyber enabled offences.

5.4.4 Perception of the United Kingdom with regard to legal framework to combat cybercrime

The UK considers that as long as a nexus with national territory exists there is not generally a difficulty with establishing jurisdiction to prosecute.

It finds, however, that there are significant impediments to investigation outside national territory which pertains also to the context of digital evidence required to investigate crime committed within the territory.

- **Mutual Legal Assistance (MLA) procedures**

The UK recognises that MLA procedures were not designed for the digital age. It suggests that streamlined processes need to be developed for the acquisition of digital evidence which happens to be held by an overseas service provider.

➢ **Host Nation Authority (HNA)**

International law generally requires law enforcement to obtain the consent of the 'host nation' for any activity having significant overseas effects. This principle does not translate easily to law enforcement activity online. A Covert Internet Investigator (CII), for example, targeting a criminal online forum, will almost certainly be gathering intelligence on targets outside the jurisdiction. He/she is unlikely, however, to know all their different locations – in this and other context the principle of HNA needs reformulation in the context of online investigations.

➢ **Overseas law and capacity**.

The ability to investigate cybercrime committed overseas, and to gather digital evidence located outside the jurisdiction, will often depend on being able to secure appropriate cooperation from the host nation. Developing nations, in particular, may lack the capacity to provide effective cooperation. EU EAS and others need to work in collaboration to support the development of consistent, compatible international capabilities.

Scotland

The Scottish authorities described how the very nature of cybercrime removes international boundaries for the criminal but does not allow law enforcement to use legislation other than those that exist within their own territorial area. Strong partnerships and agreements exist worldwide and these work well to expedite cooperation via Europol and Interpol on most occasions.

In Scotland there is a willingness to prosecute an offender from outside the country if there is a clear jurisdictional link to Scotland in terms of the location of the victim.

5.5 Conclusions

- The Serious Crime Act 2015 has been recently enacted and the amending provisions to the Computer Misuse Act 1990 were commenced on 3 May 2015. This legislative reform extends some of the provisions of the Computers Misuse Act 1990, particularly around jurisdictional issues. The Computer Misuse Act 1990, as amended, provides jurisdictional grounds for many specific offences committed outside of the UK and establishes jurisdiction over almost all cybercrimes when committed by UK nationals abroad.

- The existing legislation does not provide a binding and common definition of cybercrime although a definition is provided in the Serious and Organised Crime Strategy. According to the evaluators, this may result in the use of a limited or different concept of cybercrime for statistical purposes. Consequently, stakeholders involved in combating cybercrime may not share a common understanding of or common approach to the same concept.

- The definition of organised crime, and in particular a crime of participating in a serious criminal offence, are provided for in the Serious Crime Act 2015 however this calls for the offences concerned to be punishable by a term of 7 years or more. Some of the offences under the Computer Misuse Act 1990, as amended, would not be covered if a criminal organisation participated in such offences. The UK should consider amending its legislation to address this issue.

- The UK has legislated for a large amount of the offences prescribed under Directive 2013/40 (attacks against information systems) by way of the Computer Misuse Act 1990, as amended. The territorial provisions encompassed in the Serious Crime Act, once commenced, should ensure compliance with the Directive's requirements.

- In relation to investigative techniques, there are a number of measures for seizing and retaining data for the purpose of gathering evidence (e.g. ordering a person who has access to relevant data to provide that data, or ordering a person to help with decryption of data), but also to prevent a criminal act from being committed (such as making data inaccessible to stop an activity). The team noted, however, that content data acquired using real-time interception was not admissible as evidence in criminal proceedings.

- It is unclear under UK law how the existing regulations on the use of investigative powers and techniques (RIPA and other acts) are to be applied in an online environment. Many unresolved issues remain concerning the authority and conditions under which policing and surveillance of the internet are possible (long term observations, covert operations, presence of a police officer in private chat rooms and participation to chats, trans-border access of stored data, etc.). This is a delicate matter that arises in many Member States. For the sake of clarity and certainty these unresolved issues instead of being left in the coming years to future case law decisions – should be addressed in specific instruction or at least in guidance notes from police and/or CPS describing the appropriate way to apply existing regulations in an online environment. In relation to attacks on critical infrastructure, amendments to the legislation are encompassed in the Serious Crime Act 2015.

- Cybercrime committed via the "cloud" was highlighted during the evaluation visit as an area creating issues for investigation and prosecution, particularly in relation to retrieving the actual physical location of data. The method of cloud computing creates a problem not only with regard to national law but also to international legislation which is based on the acknowledgement of states' independence.

  The UK Data Protection Act 1998 provides the legal framework for accessing personal data and the destruction of data when they are no longer relevant for a criminal investigation. Human Rights and Fundamental Freedoms are also protected by the UK Constitution.

- A general observation from the team was that the name of Action Fraud is a little misleading in so far as it doesn't cover its full remit which includes cyber-dependent crime. Also, on Action Fraud the team was advised that operational experience had highlighted that there were some difficulties with bulk reporting. To address this, Action Fraud has now updated its system and is piloting a bulk upload facility. The team welcomes this development and suggests the further roll out of pilot if successful.

- During the visit, the team was advised that the Scottish law of evidence requiring corroboration was being revised, however, since the visit the proposed amendment from the bill has been removed. The team considers this most regrettable and would encourage the Scottish Government to reconsider abolishing this rule as it was clear that this rule hampers investigation.

6 OPERATIONAL ASPECTS

6.1 Cyber attacks

6.1.1 Nature of cyber attacks

Cyber attacks are monitored in different ways in the UK and different agencies are assigned responsibility for this monitoring as follows;

- Cyber crime – Law enforcement authorities.
- Cyber security incidents – ongoing and not often reported, common for any large organisation to face constant attacks. CERT-UK has a monitoring role in this regard.
- Cyber espionage – intelligence and security agencies monitor hostile foreign action in cyberspace.

6.1.2 Mechanism to respond to cyber attacks

The UK uses multi-agency response and can leverage existing crisis management structures to respond to the most severe cyber incidents.

The coordination of agencies involved in the response is facilitated by the national CERT-UK. This response would typically include industry, law enforcement agencies, Home Office, Cabinet Office, intelligence and security agencies, the Foreign and Commonwealth Office and the lead department for any relevant critical infrastructure sector impacted.

Operators of critical infrastructure and information systems have primary responsibility for preparing and protecting their networks against attack. To aid this, the UK Government provides them with threat information and technical security advice. Specific sectors carry different regulatory requirements related to their provision of utilities and critical services.

6.2 Actions against child pornography and sexual abuse online

Search engines (Google and Microsoft) have introduced changes to their search engines to block images, videos and pathways to child abuse from blacklist search terms used by those with a sexual interest in children supplied by the National Crime Agency. The Internet Watch Foundation (IWF) also assist in the 'take down' of these indecent images of children. The UK uses all of these to prevent access to indecent images of children.

A range of tools are used by organisations to filter access to indecent images of children. The tools used by ISPs, other service providers and businesses are a matter for them, as the government does not specify what technical tools to use. The Government welcomes the work that Industry has done to help block the search returns for indecent images of children.

Law enforcement agencies have the powers to order the removal of indecent images of children, using standard legislation.

The IWF has arrangements with industry that ensures that the URLs containing the indecent images identified as being hosted in the UK are removed when the IWF notifies the host ISP, and the URLs outside the UK are regularly placed on the IWF blocking list.

In practice, most UK internet service providers that are members of the IWF will remove such material when informed of it being hosted on their systems by the IWF. The members of the IWF generally remove such material within one hour. Members of the IWF take the IWF list of web pages and upload it to their blocking mechanisms on a twice-daily basis. More than 98% of consumer broadband lines are covered by this blocking.

In cases where the server is located outside the UK, the web pages hosting the images are placed on the IWF blocking list. If there is a hotline in the country hosting it, they will be informed by the IWF of the webpage.

6.2.1 Software databases identifying victims and measures to avoid re-victimisation

The UK has developed a national capability for the collection, assessment and storage of indecent images of children for law enforcement agencies. The CAID (Child Abuse Image Database) provides law enforcement with effective tools to search seized devices for indecent images of children, reduce the time taken to identify such images, increase the ability to identify victims and share the hash set (the unique code associated with each image) database with the internet watch foundation, with the aim of removing such images from the network.

The National Crime Agency's Child Exploitation and Online Protection (CEOP) Command has a strict management system for the retention of indecent images of children doing so only for evidential and prosecutorial reasons. Additionally the UK has uploaded the 2nd highest number of victims to the International Child Sexual Exploitation (ICSE) database at Interpol. Additionally the CEOP Command, national policing and the Home Office are working together on the CAID (Child Abuse Image Database) to use images to assist in future investigations.

Any hardware which has had images/videos stored on it will not be returned to anyone convicted of the crime. They will be destroyed.

6.2.2 Measures to address sexual exploitation/abuse online, sexting, cyber-bullying

The UK has undertaken a significant programme of work to enhance the UK response to online child sexual exploitation, following the Prime Minister's speech on 22 July 2013 and Internet Safety Summit on 18 November 2013. In addition to continuing to support work to block indecent images of children, the measures taken include:

- **Made changes to search results**. Search engines (Google and Microsoft) have introduced changes to their search engines to block images, videos and pathways to child abuse from blacklist search terms used by paedophiles, supplied by the National Crime Agency.

- **UK-US Taskforce**: A Taskforce has been established by the UK and US governments to find new technological solutions to combat online child sexual exploitation by collaborating with the technology sector. In May 2014, an industry event branded WePROTECT 2014 brought 68 engineers from 47 companies together to generate new technological solutions for tackling these crimes.
- **WePROTECT summit**: An international summit was held December 2014 which was hosted by the Prime Minister and focussed on driving coordinated global action to protect children online. It resulted in a statement of action being agreed by over 45 countries to work against child sexual exploitation.

6.2.3 Preventive actions against sex tourism, child pornographic performance and others

The Internet Watch Foundation (IWF) is the reporting point for illegal content for the business and the public. The IWF was established in 1996 by the internet industry to provide the UK internet hotline for the public and IT professionals to report criminal online content in a secure and confidential way.

The Hotline service can be used anonymously to report content within its remit. It works in partnership with the online industry, law enforcement, government, and international partners to minimise the availability of this content, specifically:

- child sexual abuse images hosted anywhere in the world
- criminally obscene adult content hosted in the UK
- non-photographic child sexual abuse images hosted in the UK.

The National Crime Agency's CEOP Command runs the "Thinkuknow"" programme that provides information to children, parents and carers on how children can keep themselves safe online. CEOP Command also has a "Report Abuse" button, which is available on the CEOP website, and on social media and other sites, that allows children to report attempts at grooming.

6.2.4 Actors and measures countering real time dissemination of child pornography

The National Crime Agency's CEOP Command has close working relationships with industry and law enforcement to counter websites which are used for the live streaming of child sexual abuse.

6.3 Online card fraud

6.3.l Reporting of online fraud

Individuals and businesses report online card fraud directly to the relevant financial organisation. The financial institution may then forward the report to the police through Action Fraud and the National Fraud Intelligence Bureau which is the central fraud reporting and intelligence analysis system.

They can also report directly to Action Fraud through the dedicated call centres (based in Scotland and Manchester) or online through the Action Fraud website.

Scotland
Citizens and private companies can and do report online card fraud to Police Scotland. These reports can also be made via Action Fraud in London who forward information to Police Scotland using recognised points of contact.

Northern Ireland
Action Fraud became fully operational in Northern Ireland in May 2015. In addition an online reporting portal on the PSNI website has been developed to enable industry and businesses to report cyber incidents in live time.

6.3.2 Cooperation with industry to prevent online card fraud

There is a good level of cooperation between banks, private sector, industry and LEAs to prevent and fight online card fraud. The private sector (including banks and financial sector industry bodies) and LEAs meet routinely in a number of national forums focusing on fraud, including a threat group led by the National Crime Agency. The payments industry body (which represents banks and card schemes) funds a specialist law enforcement unit, the Dedicated Cheque & Plastic Crime Unit (DCPCU) which is dedicated to combating payment card fraud including online fraud. Industry partners identify trends and emerging threats, which DCPCU in turn uses to prioritise its workload. Both banks and LEAs issue alerts when new methods of abuse of payment tools appear. Work is ongoing to improve that process particularly to speed up the issuing of alerts and to ensure consistency of language. That work is being led by the National Crime Agency.

The banking industry has introduced measures to increase security of non-cash payment. Chip and PIN has been fully operational in the UK since 2006 and according to payment industry figures cardholder and issuer adoption of "3D secure" is growing strongly in the UK.

Scotland

The cooperation between industry, banks and LEA's is improving and a number of recognised groups have been established over the years to discuss and share information/intelligence to adapt working practices, prevent further crime and arrest offenders.

The financial sector has systems and processes in place to discuss and share information and intelligence without the need for law enforcement intervention.

Northern Ireland

Northern Ireland has been investing in increasing the capabilities of LEAs to raise the knowledge, skills and equipment available to investigate cyber and online criminality.

6.3.3 Role of the private sector

There is no mandatory reporting for the private sector as UK does not consider this beneficial but instead encourages the private sector to share threat information. In December 2013 it published Guiding Principles on Cyber Security which set out a number of minimum standards that each Internet Service Provider should voluntarily adhere to.
In March 2013, the Cyber-security Information Sharing Partnership (CiSP) was established. It now sits under CERT-UK and this voluntary scheme is open to UK Industry. This online portal allows members to share threat intelligence and to share experience in a secure and if needed, anonymous environment. Through this portal, Industry is able to share such information with law enforcement.

Internet Service providers may be required to retain communications data under the Data Retention and Investigatory Powers Act 2014. They can also be required to disclose communications data and assist with the interception of communications – both under the Regulation of Investigatory Powers Act 2000. Otherwise these types of business are subject to the general law. As mentioned in section 6.2 on child pornography, ISPs and others take action to remove indecent images of children when informed of it being hosted by them by the IWF or the police. For wider forms of crime, law enforcement can request that a website be removed using the Police and Criminal Evidence Act 1984 powers.

The National Cyber Crime Unit takes a pragmatic approach when dealing with private industry, which often reflects the internal structure or policy of the business in question. The National Cyber Crime Unit has a proactive and collaborative approach to working with industry, which involves a two-way dialogue and open discussion on how they can work closely together and the added value of collaboration.

Both the National Cyber Security Strategy and Serious and Organised Crime Strategy state a clear focus on working closely with the Private Sector to tackle and prevent cybercrime. This work is undertaken through a range of ad-hoc, formal and informal working arrangements including a specific Industry group within the National Crime Agency and the Cyber Growth Partnership and the Security and Resilience Growth Partnership, both attended by public officials and Industry.

Resources are focused on this work within the NCA and Government, across a number of Government Departments.

6.4 Conclusions

- The team was impressed with the establishment and use of the CiSP Forum which is achieving its objective of encouraging industry to share information and intelligence on cybercrime threats.

- The IWF provides valuable assistance to the UK in the fight against online child exploitation. The key to its success is the support it receives from the online industry and strong partnerships it has across the globe. It strives to meet the demands of evolving technology, industry developments, and public and government scrutiny and as a result seems to be making a significant contribution.

- The UK has taken several measures to raise awareness and prevent cybercrime which are well documented above. It engages regularly with the private sector and has been proactive in promoting international cooperation through the organisation of intergovernmental summits on child protection issues.

- Directive 2011/92 sets out under Article 20 paragraph 4 that interviews of child victims shall be audio-visually recorded and can be used as evidence in court. The terms of the directive are prescriptive and mandatory. Article 20 paragraph 3 calls for the use of specialist interviewers. Victims that are children are often groomed online, and thereafter abused or exploited off line. It became apparent during the visit that this practice has not been introduced into England and Wales although it is provided under the Victims and Witnesses (Scotland) Act 2014. Specialist interviewers are not mandatory either in the process. It is evident that Scotland has introduced some special measures in this regard, although it does not seem to be a mandatory procedure in that jurisdiction.

- Online reporting of fraud has been greatly facilitated by the establishment of a central reporting body, Action Fraud. It was clear from the visit, that this approach had yielded tangible results and made reporting of online fraud and cyber-dependent crime easier for the public and industry.

7 INTERNATIONAL COOPERATION

7.1 Cooperation with EU agencies

7.1.1 Formal requirements to cooperate with Europol/EC3, Eurojust, ENISA

The UK is one of the most active Member States participating in the fight against cybercrime at European level. In that regard, the UK's National Cyber Crime Strategy fits perfectly well with EC3's priorities and objectives.

- The UK is involved in the EMPACT[16] priority on cybercrime[17] as defined within the EU policy cycle 2014-2017[18]. In accordance to this latter frame, strategic objectives are defined in multi annual strategic plans and operational goals implemented via operational action plans All EMPACT meetings are regularly attended by experts from the UK competent authorities.
- The UK is associated to all Focal Points (FPs) dedicated to cybercrime which are operational projects developed by Europol/EC3 to support EU MS and third parties' investigations.
- A senior manager from the National Cyber Crime Unit chairs the European Cyber Crime Taskforce (EUCTF) initiative.
- The UK has supported the launch of the recently formed Joint Cyber crime Action Taskforce (J-CAT) with the head of the UK National Cyber Crime Unit chairing the oversight board. This initiative began in September 2013 and brings together around 14 countries to coordinate the operational response to a set of agreed operations affecting members. The National Cyber Crime Unit has attached a member of staff to Europol for this initiative.

16 European Multidisciplinary Platform against Criminal Threats.

17 Cybercrime – aiming to: combat cybercrimes committed by OCGs and generating large criminal profits such as online and payment card fraud, cybercrimes which cause serious harm to their victims such as Child Sexual Exploitation, and cyber-attacks which affect critical infrastructure and information systems in the EU.

18 Council Conclusions on the creation and implementation of an EU policy cycle for organised and serious international crime, doc. 15358/10 COSI 69 ENFOPOL 298 CRIMORG 185 ENFOCUSTOM 94.

- The UK is member of the European Financial Cybercrime Coalision (EUFCC) which has been established to foster relations between law enforcement and the financial sector.
- In addition, the UK is active in training activities developed by EC3. Recently, National Crime Agency supported a training course on Domain Name Resolution.

7.1.2 Assessment of the cooperation with Europol/EC3, Eurojust, ENISA

- ***Europol EC3***

The National Cyber Crime Unit has found EC3 a very useful partner which offers a good platform for bringing law enforcement together to discuss common threats and a base from which to coordinate global activity.

A recent National Cyber Crime Unit coordinated international operation into a malware variant involved close working with EC3. The operational centre for the associated day of action was located within Europol. This allowed much easier coordination of the response with European and other international partners.

- ***ENISA***

Cert -UK enjoys good cooperation with ENISA.

- ***EUROJUST***

The team noted that the UK engaged primarily with Europol when dealing with cybercrime with very little use made of the possibilities Eurojust could offer in this regard.

Scotland

Scotland has also made good use of EC3 and advised about an investigation into an online marketplace dealing in illegal commodities was completed at the beginning of November 2014 which led to the arrest of an individual in Scotland.

7.1.3 Operational performance of JITs and cyber patrols

The UK makes good use of JITs with the National Cyber Crime Unit presently having a number of active JITs in place. The UK experience is positive once these are in place but it recognises that the time taken to set up JITs and secure associated funding can detract from their overall usefulness.

As mentioned in 7.1.1, the National Cyber Crime Unit is participating in the J-CAT initiative which facilitates joint working with other Europol members. Three of the UK's operations are currently being run in cooperation with the J-CAT.

In addition, the UK has a number of ongoing joint initiatives where it is actively working with other Member States. The National Cyber Crime Unit is also contributing to the EMPACT programme and supporting Member State-led initiatives as part of this programme (see 7.1.1).

7.2 Cooperation between the British authorities and Interpol

The National Crime Agency has recently seconded a member of staff to the Interpol Global Complex for Innovation (IGCI) Interpol initiative in Singapore. This officer will manage the Cybercrime Fusion Centre.

7.3 Cooperation with third states

The UK strongly supports the Budapest Convention as a means of developing international cooperation on cybercrime. It supports capacity building work to develop national legislation, law enforcement capability, and international cooperation.

The EC3 and J-CAT programmes have facilitated joint work with 3rd parties who have been invited to join initiatives. A number of non-Member States are participating in the J-CAT.

7.4 Tools of international cooperation

7.4.1 Mutual Legal Assistance

The UK uses MLA. The Crime (International Co-operation) Act 2003 (CICA) and other existing bilateral mutual legal assistance arrangements provide a basis for applying the general principles of MLA. The UK believes that MLA should be used in appropriate circumstances, such as when action by a court is required, but that for other information, tools such as police-to-police cooperation should be used.

All incoming requests for MLA must be received and considered by a central authority (Home Office, Her Majesty's Revenue & Customs (HMRC), or Crown Office). Any action that can be requested under MLA can be requested for cybercrime with the most common investigative measures for MLA being requests for witness evidence, banking evidence or communications data. Incoming requests can be received electronically, but sensitive material should not be transmitted externally (from the UK) using unsecure methods (including unsecure email).

The Home Office (which receives the majority of incoming requests) received over 4,400 incoming requests for evidence from EU Member States in 2014. The top 5 EU Member States for incoming requests were Germany, Poland, Spain, Portugal, and Netherlands. Most requests were in regard to some kind of fraud, including cyber enabled fraud, and range from high value complex frauds to *de minimis* offences. The UK acknowledges that it can be slow in responding to foreign MLA requests but emphasised that the volume received coupled with the fact that almost all requests received are generally marked 'urgent' by the requesting state regardless of the nature of the request, leads to delays in processing of requests.

Outgoing requests may be issued and transmitted by any UK judicial authority or designated prosecuting authority to a competent authority of an EU Member State.

Data on outgoing requests to EU Member States is not held centrally.

Scotland

In Scotland all outgoing and incoming MLA requests go through the Scottish Central Authority, namely the International Cooperation Unit, Crown Office, Edinburgh. Although requests are generally submitted in hard copy to the requested state, they can also be transmitted electronically or by fax.

7.4.2 Mutual recognition instruments

- The UK is party to the Budapest Convention, which contains provisions on MLA. The UK is also party to other Council of Europe Conventions, UN Conventions, EU instruments, and nearly 40 bilateral treaties on MLA. The UK meets these provisions through the general UK legislation on MLA. The Home Office received over 900 requests from third states in the 2014 and has sent over 350 requests to third states in the same year.

- The UK implemented the Confiscation Order Framework Decision in December 2014.

- The UK has implemented the Freezing Order Framework Decision in relation to evidence and property.

7.4.3 Surrender/Extradition

Decisions about whether to seek extradition from other territories are a matter for the prosecuting authorities and the police. In terms of extradition, all the offences in the Computer Misuse Act 1990 carry a maximum sentence of at least 2 years so all are extraditable.

For receiving requests in the UK, in European Arrest Warrant (EAW) cases the National Crime Agency certify requests but final decisions lies with courts. For 'Part 2' cases the Home Office certifies requests, the courts and the Secretary of State consider whether extradition should be carried out (although the final decision generally lies with the courts).

For sending requests from the UK, in EAW cases the National Crime Agency is the channel of communication for requests from England, Wales and Northern Ireland. For 'Part 2' cases requests to and from England Wales and Northern Ireland go via the Home Office.

Scotland

In Scotland the Crown Agent is the designated central authority for the receipt and execution of European Arrest Warrants. In practice this function is carried out by prosecutors within the International Cooperation Unit, Crown Office. Prosecutors will represent the issuing judicial authority (IJA) before the Courts in Scotland and will liaise with the IJA over the course of the case.

Routes of transmission are through the National Crime Agency or, in cases of urgency, the European Judicial Network.

Extradition is covered by the Extradition Act 2003 and, where appropriate, multi-lateral or bi-lateral agreements. There are no specific conditions or procedures that need to be fulfilled regarding cybercrime. In urgent cases if the IJA undertakes to provide a full request within 48 hours of arrest then provisional arrest can be instructed. The average response time from receipt to arrest for a person located in Scotland is between 1 to 5 days. Provisional arrests are possible where allowed for by extradition arrangements. Even if provisional arrests are made, full papers are still required.

7.5 Conclusions

- It was well evidenced both in the replies to the questionnaire and the on-site visit that the UK engages well with European Partners, in particular EC3 which is demonstrated through its active role in the J-CAT and chairing the EUCTF.

- An ever-growing percentage of MLA requests are related to cyber-enabled or cyber-dependent crime. Most of the incoming letters of request are centralised within the Home Office, which acts as Central Authority (UKCA). Until very recently no adequate system existed that could track the execution process of these MLA requests and no reliable statistics are available. This being said both the requesting States and UK itself realise that the speed of execution of MLA request leaves a lot to be desired and could be improved greatly especially for cybercrime cases where e-evidence is volatile and must be handled efficiently. The work overload of UKCA is also partly due to the input of a great deal (appr. 30%) of insufficient MLAs (lack of information, dual criminality etc) that have to be sent back to the requesting States.

- From speaking with practitioners the team found that MLA channels are not always considered the most appropriate option due to the time these procedures can take. It was suggested that other fora such as J-CAT at EC3 could offer better opportunities to share information as several external partners such as the FBI, and US Secret Service are involved. Use of this channel could alleviate the need to use cumbersome MLA procedures although it was recognised that the validity of the data would have to be verified if less formal channels were used. On the whole, the team was advised that the UK try to use all opportunities available and try to make good use of MLAT.

- The team was advised that the UK only uses Article 26 of the Budapest Convention in a restricted way. The UK is encouraged to make better use of this provision which creates the possibility to spontaneously forward available information to other parties to the Convention which can be admitted as evidence in criminal proceedings.

- In addition it was understood that mutual legal assistance can be further restricted and limited by the UK's introduction of the '*de minimis'* rule (no execution of minor cases under £ 1,000). The team encourages the UK to consider the best way of dealing effectively and efficiently with MLA requests to ensure the best cooperation possible.

- The team considers that international co-operation is generally good on the investigation side. The UK has stated that MLA is a slow process both for incoming and outgoing requests. In the formal replies to questionnaire, it has indicated that it does not work effectively for cybercrime generally, due to the multi jurisdictional nature of computer technology. This issue should be tackled at both a national and EU level to identify the best way of dealing with it.

- The team noted that the UK engaged primarily with Europol when dealing with cybercrime with very little use made of the possibilities Eurojust could offer in this regard. Whilst the team could appreciate that this may reflect the role of the police as an investigative authority in the UK as a common law jurisdiction, it would still urge the UK to make use of all the resources available at European level.

8 TRAINING, AWARENESS-RAISING AND PREVENTION

8.1 Specific training

The National Training and Development Working Group, a policing led initiative that sits within the National Cyber Security Programme, has been established which includes ACPO and Government representatives overseeing the content and delivery of cyber training across the UK. A range of training has been developed for various levels of LEA, ranging from specialist courses for those investigating sophisticated online crime to awareness raising courses and e-learning modules for first responders.

Prosecution

The Crown Prosecution Service currently has four e-learning modules related to cybercrime:

- **Cybercrime basics-** introduces the different types of cybercrime and technology used;
- **Cyber stalking-** introduces the offences of cyber stalking and grooming;
- **Cybercrime intermediate-** builds on the information given in module one through case studies. It identifies common problems encountered in cybercrime cases and how to deal with them;
- **Prohibited Sexual material**- shows how to effectively prosecute cases involving indecent images of children.

In the Autumn 2015 it plans to expand this programme to include:

- **Digital evidence gathering-** this provides prosecutors with information about the different types of digital material and how they can be used to build a prosecution case;
- **Online fraud-** this raises awareness on how fraud, a mainstream crime, is committed online through cyber-enabled technologies;
- **Online grooming-** through a case study prosecutors are provided with key facts, definitions and relevant legislation;
- **Social media**- introduces a range of internet communications and social networking sites which are commonly used to perpetrate cybercrime.

The first two modules are mandated training which must be completed by all prosecutors. The Crown Prosecution Service is considering including the **Digital evidence gathering** module as part of the mandatory training. The other modules are dependent on the training needs of individual prosecutors.

Police

The College of Policing provides the following training:

- Numerous e-learning training packages
- Online research investigation course
- Mainstream Cybercrime Training courses

These form the basis of the basic cyber training courses for law enforcement agents. The College of Policing currently provides cyber training to Law Enforcement Agencies but the demand exceeds course availability and needs so other options for training through external providers are being explored.

Specialist Units also undertake;

- Core Skills Network Investigations course
- Core Skills Data Recovery course

which are delivered by the College of Policing or external providers.

A proportion of the funding for LEAs from the National Cyber Security Programme pays for training, both at the specialist and mainstream level. However this is in addition to funding already provided in the general policing budgets, and it is not possible to produce a figure that gives the overall amount of money that pays for cyber security training across policing.

Scotland

In terms of specialist training for Police Scotland Cybercrime Unit staff, it has been involved with Napier University, Edinburgh in developing a Network Investigation Course and a Fundamentals in Forensics Course. Twelve members of Police Scotland staff attended the first iteration of the network course, whilst 21 staff from Police Scotland and 3 officers from south of the border have attended 2 fundamentals courses. The delivery of these courses allows the Police to train a significant number of people at around £50,000 less than it would pay for other recognised training. Its work with Napier University and others in Scotland continues to maintain this drive towards efficient and effective training within Scotland at significantly reduced costs. The benefit for the universities is they gain from Police expertise and advice in the development of courses which they can then sell to the private sector and other LEAs.

Private Sector

Private Industry offers specialist courses across a range of training needs and requirements e.g. malware, coding, databases, scripting, live forensics.

The National Cyber Crime Unit works with additional providers as required to deliver specialist technical training.

Academia

The National Cyber Security Programme and the UK government works with academia, professional bodies, trade associations and industry to define a framework for the required learning outcomes in cyber security within computing science and related courses. Initially this will apply to all undergraduate courses accredited by the British Computer Society and the Institution of Engineering & Technology by 2016. The UK has six certified 'Master's degrees in General Cyber Security and have recognised Academic Centres of Excellence in Cyber Security Education.

Scotland

The Scottish Business Resilience Centre works directly with Scottish Universities to produce an enviably high standard of ethical hacking and digital forensics students. It benefits from Scottish Government support which enables it to offer the service at a fraction of commercial rates.

8.2 Awareness-raising

The UK has several ongoing awareness campaigns on cybercrime;

(i) The Government launched CyberStreetWise in January 2014 to improve cyber security amongst the public and small and medium enterprises. The CyberStreetWise campaign is informed by a steering group which includes industry partners and private sector support is provided to the campaign through financial and other means.

(ii) E-safety is taught in schools as part of the Personal Social Health & Economic Education (PSHE) curriculum from Primary education upwards. Part of this was development of the 'Make IT Happy' campaign which involved the creation of detailed lesson plans and other resources to help teachers instil internet safety skills in pupils aged 9-11.

(iii) The UK is overhauling the computer science (General Certificate of Secondary Education) GCSE exam, to focus on coding rather than office skills, including teaching why security is important in the design, development and implementation of information systems (including secure coding). It is also making available interactive teaching and learning materials for cyber security to all schools through the through e-Skills 'Behind the Screen' initiative, aimed at GCSE and A-Level students. Much of this work is focused on inspiring young people to consider science, technology, engineering and maths (STEM) careers and on ensuring the correct educational provision at all levels from aged 14 to postgraduate. This should ensure that all people leaving education have a basic understanding of cyber security before entering the workforce and also motivate those with the aptitude to pursue a career in cyber security.

(iv) The Department for Business, Innovation & Skills (BIS) has continued a partnership with Universities and the Higher Education sector to improve awareness and drive action to improve cyber security. It has worked with Universities UK to carry out a Cyber Security Governance Health Check for higher education institutions, in addition, internet safety (good cyber hygiene) principles feature in many of the induction programmes at UK Universities.

(v) The National Crime Agency CEOP Command has also developed an awareness-raising programme for schools called ThinkuKnow which assists teachers to help children to identify online risks. It also focuses on educating parents on how to ensure their children are safe on the internet.

(vi) Police Scotland has been working closely with Education and Scottish Universities to engage with the Computing Science Department at Kyle Academy in Ayr to deliver a series of modules over a 12 week period to 1st Year pupils at the school. The modules relate to online safety awareness, cyber security and an introduction to computing science. The collaborative developed the open badge programme in an attempt to raise awareness amongst pupils of the online threat but also to highlight opportunities in the cyber security world as a well-paid career. The pilot is complete and was very well received. There is significant interest in the programme across a number of schools who are keen to replicate this into their curriculum. The additional benefit of this programme is children returning home and educating their parents and grandparents on the use of online technology and how to keep it secure. By rolling the programme out across Scotland it hopes to reach a wide audience of all ages through the children.

(vii) Police Scotland is now involved with partners and the Scottish Qualification Authority (SQA) in the development of a National Progression Award module for Cyber Security. One of the Cybercrime Unit Detective Inspectors is writing one of the modules for the course.

(viii) A certified training course called "Introduction to Cyber Security" has been developed by the Open University with support from the UK's National Cyber Security Programme. This free online course is aimed at helping the public protect their digital life and recognise online cyber threats.

8.3 Prevention

(i) The Serious and Organised Crime Strategy and the National Cyber Security Strategy both set out clear objectives for reducing the risk of people becoming a victim, otherwise termed ‘Protect’. This is detailed in the links above, but includes the delivery of effective protective advice and messaging to the public, business and the public sector to encourage safe online behaviours.

(ii) A range of activity is ongoing across the UK Government in conjunction with the third sector and private sector partners to reduce victimisation. For example, the National Cyber Security Programme funds the national CyberStreetWise campaign which has been running since January 2013. This campaign is delivered in conjunction with external partners Phase 2 of the campaign commenced in October 2014.

(iii) The National Cyber Security Programme part-funds Get Safe Online, an advisory website and awareness raising initiative on online threats and safe behaviours.

(iv) The Home Office is also promoting safe behaviours against fraud through bespoke campaigns in targeted areas and through funding for Action Fraud, which provides advice and support through their website and call centre.

8.4 Conclusions

- The team was advised that through the national security programme, the Centre for Applied Science and Technology CAST has been considering developing an accreditation programme for new software. The team would encourage efforts in this regard and also possibly the provision of accredited training through the College of Policing.

- It is clear that cybercrime is a criminal area that is evolving faster than all others. Cyber criminals are learning and adapting. As mentioned in Chapter 4, the team considers that mandatory core cybercrime training should be provided for judges given the specific nature of the issue and that training for prosecutors should be developed further.

- The UK is encouraged to make maximum use of the training possibilities offered by the European Cybercrime Training and Education Group (ECTEG) whose biannual meetings are hosted by EC3.

- It was clear that substantial training is provided to police at entry level and for those dealing in operational positions. The team considers that due to the evolving nature of cybercrime and the diversification of criminal techniques and tools used it would also be of immense value to provide training to senior police officers as part of continuous professional development.

- The team was impressed with the range and type of awareness campaigns provided by the UK authorities and commends the UK for its efforts in this regard.

9 FINAL REMARKS AND RECOMMENDATIONS

9.1 Comments from the UK

The UK identified several issues which affect the successful investigation and prosecution of cyber offences. Many of these issues are not just UK specific but affect all Member States given the nature of the crime.

Obstacles for successful prosecution

The UK authorities consider the main obstacles to prosecution to be the difficulty of locating and obtaining evidence, and in identifying the perpetrator. These are significant challenges particularly where the offender and the evidence are outside the UK jurisdiction. This can cause difficulties in so far as electronic data may not be retained and that the jurisdiction in which it is held may not be easily identifiable or contactable.

Jurisdiction

The UK considers that there are significant impediments to investigation outside national territory which pertain also to the context of digital evidence required to investigate crime committed within the territory.

Mutual Legal Assistance (MLA) procedures

The UK recognises that MLA procedures were not designed for the digital age. It suggests that streamlined processes need to be developed for the acquisition of digital evidence which happens to be held by an overseas service provider.

Investigation overseas

International law generally requires law enforcement to obtain the consent of the 'host nation' for any activity having significant overseas effects. This principle does not translate easily to law enforcement activity online. A Covert Internet Investigator (CII), for example, targeting a criminal online forum, will almost certainly be gathering intelligence on targets outside the jurisdiction. He/she is unlikely, however, to know all their different locations – in this and other context the principle of HNA needs reformulation in the context of online investigations.

Overseas law and capacity.

The ability to investigate cybercrime committed overseas, and to gather digital evidence located outside the jurisdiction, will often depend on being able to secure appropriate cooperation from the host nation. Developing nations, in particular, may lack the capacity to provide effective cooperation. EU EAS and others need to work in collaboration to support the development of consistent, compatible international capabilities.

9.2 Recommendations

As regards the practical implementation and operation of the Framework Decision and the Directives, the expert team involved in the evaluation of the UK was able to satisfactorily review the system in the United Kingdom.

The United Kingdom should conduct a follow-up on the recommendations given in this report 18 months after the evaluation, and report on the progress to the Working Party on General Affairs including Evaluations (GENVAL).

The evaluation team thought it fit to make a number of suggestions for the attention of the UK authorities. Furthermore, based on the various good practices, related recommendations to the EU, its institutions and agencies, Eurojust, Europol and ENISA, are also put forward.

9.2.1 Recommendations to the United Kingdom

The team was extremely impressed by the measures taken by the UK to tackle cybercrime and the Government's firm commitment to prioritise this issue by way of the National Cyber Security Strategy. On the whole, the UK serves as a model of good practice for other Member States in this area, and the team suggests that several of the innovative measures established by the UK could be usefully adapted and applied in other Member States. That being the case, the team did find some areas which could be improved upon by the UK authorities and, therefore, makes the following recommendations;

Investigation and Prosecution

1. Significant effort, means and people are invested in law enforcement capacity building in the area of cybercrime. It seems however that prosecution and judicial process is a bit forgotten. As a result of this lack of investment, both institutions face greater challenges when handling the increased volume of cybercrime cases in the future. Training of prosecutors and judges is essential to improve efficiency and effectiveness in prosecuting and ruling on cybercrime cases. This includes not only e-learning sessions, but also in depth group sessions with an exchange of experiences and the analysis of real-life cases (issues of e-evidence, the use of online investigative techniques, jurisdiction etc). The team learnt that some training is offered to prosecutors but little is provided to judges. It is recommended that both prosecutors and judges receive specialist training on cybercrime. The joint training offered in Scotland could be a model for England and Wales to follow in this regard.

2. It is recommended that the UK should have specialised prosecutors for high end cybercrime prosecutions (cyber dependent crimes). This is particularly important in a system where the courts are not that well trained and equipped to deal with demanding cybercrime cases.

3. The team welcome the work of Action Fraud which made the reporting of online fraud easier for citizens and industry. In this light it recommends that consideration should be given to extending Action Fraud to also cover Scotland.

4. It is evident that it is difficult to retain valuable experience within the cybercrime area, as generally experienced police officers/computer experts are lured to the private sector by significant salaries. It is recommended that further attention be given to measures to retain expert staff for the greater good of policing in the area of cybercrime.

Legislation

5. The definition of organised crime, and in particular a crime of participating in a serious criminal offence, is provided for in the Serious Crime Act 2015; however, this calls for the offences concerned to be punishable by a term of 7 years or more. Some of the offences under the Computer Misuse Act 1990, as amended, would not be covered if a criminal organisation participated in such offences. It is recommended that the UK should consider amending the penalties for offences related to organised crime.

6. Legal interception of content data (voice) is not treated in a similar manner to other Member States in so far as it is not admissible as evidence in criminal proceedings. The team notes that the UK has assessed the possibility of changing its legislation to provide for this but rejected the idea. The team recalls that issue is provided for under Article 21 of the Budapest Convention and as a result recommends that the UK keeps this issue under review.

7. The team was advised that the Scottish law on corroboration used when giving evidence means that at least two different and independent sources of evidence are required in support of each crucial fact before a defendant can be convicted. The team noted that this practice can greatly hamper the provision of evidence, particularly in cybercrime cases. The team recommends that consideration be given to abolishing this rule to aid the prosecution of cybercrime offences.

8. In order to prevent secondary victimisation of children it is highly recommended that the UK introduces a scheme to effect compliance with the Directive 2011/93/EU in relation to the provision of audio-visual recorded interviews for child victims. This would reflect the wishes of the UK government in their document “Statement of Action: Webprotect Summit 10-11 Dec 2014” in which it seeks to protect victims in investigations and to adopt good practice in their treatment.

Mutual Legal Assistance/International Cooperation

9. The UK is conscious of the importance of a strong collaboration within Europe. In the area of cybercrime, UK law enforcement puts a lot of effort into the development of collaboration with EC3, J-CAT and Europol in general. This is commendable. It should not be forgotten, however, that the cooperation with many other Member States as well as the signing and financing of JITs are in the end a matter for the prosecution and Eurojust. Therefore more attention should be given to the early involvement of Eurojust in those cases where the international cooperation eventually envisages more than mere police-to-police cooperation but also measures that fall under the authority of prosecution services or even the signing of a JIT which is a matter for Eurojust and prosecution services (both in UK and in other States).

10. It is recommended that the UK makes further efforts to reform the work process of the UK Central Authority to enable the efficient and effective execution of incoming MLA requests.

Other Issues

11. Cybercrime related statistics should be collected in a comprehensive way. It seems that statistics on cyber-dependent crime are published in England and Wales but not in Scotland and Northern Ireland . In addition, the team noted that the statistics on reported crime when compared with the statistics on prosecutions and convictions show a surprising gap between the number of reported incidents and convictions. It is recommended that the collection and collation of statistics should be improved and published in the three jurisdictions.

12. Resource allocation between England, Wales, Scotland and Northern Ireland is not even. While this may be a reflection of differing risk environment it is recommended that the UK Government encourages the Scottish Government and Northern Irish Executives to use any future funding provided under the National Cyber Security Programme to further develop cyber resilience. The allocation of the funding could remain a matter for the respective administrations and therefore the devolved funding rules could be respected.

9.2.2 Recommendations to the European Union, its institutions, and to other Member States

1. Member States should improve the quality of the MLA requests they send to other countries, and particular regard should be taken to ensure they are sufficiently completed. Member States should also properly assess the necessity of the request given the nature of the offence and whether it is urgent or not.

2. It is recommended that the European Commission makes proposals for streamlining MLA systems for digital evidence and consider creating a specific definition of organised cybercrime groups.

3. The European External Action Service (EEAS) is recommended to continue working with third states to improve cooperation, the ability to investigate cybercrime committed overseas and the possibility of gathering digital evidence held outside the EU.

4. A concerted European effort needs to be made to tackle cybercrime. Issues such as how to collect e-evidence, jurisdictional issues and accessing data stored in the 'cloud' need to be considered at a European level.

5. The EU Cybercrime Strategy could be developed to explore ways to ensure the effective prosecution of cybercrime offences.

9.2.3 Recommendations to Eurojust/Europol/ENISA

1. The European Cybercrime Training and Education Group (ECTEG) should continue to offer and promote training for law enforcement authorities in the Member States on cybercrime.

2. EC3 should explore expansion and best use of J-CAT pilot particularly in the efficient sharing of information on cybercrime between LEAs of Member States and other partners at Europol.

3. Both Eurojust and Europol should consider ways to make JITs easier to set-up including access to available funding to ensure their effectiveness to the Member States.

ANNEX A: PROGRAMME FOR THE ON-SITE VISIT AND PERSONS INTERVIEWD/MET

UNITED KINGDOM EU Commission, Europol, Eurojust, ENISA and the General Secretariat.		
Monday 19th January 2015		
DATE/TIME	**SITES and ACTIVITIES**	**ATTENDEES**
Representatives to travel independently	Arrival of evaluation team and check-in at the hotel Premier Inn London Victoria	***Evaluation team**:* *Council–* *Miss Nicola Murphy* *Ms Monika Kopcheva* *National Experts* *Ms Mairead Cotter (Ireland)* *Mr Geert Schoorens (Belgium)* *Mr Timo Piiroinen (Finland)* *Observers* *Mr Michael Palmer (Commission)* *Mr Harri Tiesmaa Eurojust* *Mr Lionel Ferette (ENISA)* *Mr Benoît Godart (Europol)*

Tuesday 20th January 2015 Day 1: Home Office and Government meetings		
09:00	Departure from the hotel Premier Inn London Victoria to the Home Office HQ	
09:30-11:30	Introductory meeting with Home Office Strategic Centre for Organised Crime, *Leads Ian Caplan, Piers Harrison, Justin Millar, Ebrima Chongan* (*Conference Room 9, 2 Marsham street London SW1P 4DF*)	*Evaluation team* *Ian Caplan (SCOC)* *Piers Harrison (SCOC)* *Mike Taylor (SCOC)* *Ebrima Chongan (ID)*
11:30-11:45	**Coffee break** (*Conference Room 9, 2 Marsham street London SW1P 4DF*)	*Evaluation team* *Ian Caplan (SCOC)* *Piers Harrison (SCOC)* *Mike Taylor (SCOC)* *Ebrima Chongan (ID)*
11:45 – 12:30	Session on Computer Misuse Act, *Lead, Kathryn Roe(Conference Room 9, 2 Marsham street London SW1P 4DF)*	*Evaluation team* *Piers Harrison (SCOC)* *Mike Taylor (SCOC)* *Ebrima Chongan (ID)* *Kathryn Roe (SCOC)* *Samantha Ryb (HO Legal)*
12:30 – 13:15	Meeting with Home Office International Criminality Unit , *Lead Harvey Palmer (Conference Room 9, 2 Marsham street London SW1P 4DF)*	*Evaluation team* *Harvey Palmer (JCU)* *Ebrima Chongan (ID)* *Piers Harrison (SCOC)* *Mike Taylor (SCOC)*
13:15 – 13:45	**Lunch** (with informal opportunity to ask questions) *(Conference Room 9)*	*Evaluation team* *Harvey Palmer (JCU)* *Ebrima Chongan (ID)* *Piers Harrison (SCOC)* *Mike Taylor*

13:45	Departure to Cabinet Office	
14:00-15:30	Meeting at Cabinet Office, *Leads David Raw, Emma Dickens, (Room 419, 70 Whitehall London SW1A 2AS)* *Discussion on NCSS Obj 1, NCSP funding.*	*Evaluation team* *David Raw (CO)* *Emma Dickens (CO)* *Mike Taylor (SCOC)*
15:30	Departure to CPS	
15:45 – 16:45	Meeting at CPS, *Lead Alyson Sprawson, (Room TBC, Rose Court 2 Southwark Bridge London SE1 9HS)*	*Evaluation Team* *Alyson Sprawson (CPS* *Russell Tyner (CPS)* *Justin Millar (SCOC)*
16:45	Departure to Hotel Premier Inn London Victoria	*Evaluation Team*
18:50	Departure from hotel to restaurant	*Evaluation Team*
19:00-21:00	**Dinner at '*About Thyme' 82 Wilton Road London SW1V 1DL*.**	*Evaluation team* *Ebrima Chongan (ID)* *Piers Harrison (SCOC)*
21:00	Departure to hotel Premier Inn London Victoria	

Wednesday 21st January 2015 Day 2: Law Enforcement meetings		
8:20	Departure from the hotel Premier Inn London Victoria to Action Fraud	
9:00-10:30	Meeting with Action Fraud, *Lead: Peter ODoherty* *(Room: 5th Floor Conference, 21 New Street London EC2M 4TP)*	*Evaluation team* *Peter ODoherty (AF)* *Pauline Smith (AF)* *Christopher Felton (AF)* *Matthew Bradford (AF* *Piers Harrison (SCOC)* *Mike Taylor (SCOC)* *David Silke (SCOC)* *Sam Dowling (SCOC)*
10:30	Departure to the Home Office	*Evaluation team* *Piers Harrison (SCOC)* *Mike Taylor (SCOC)*
11:00 – 12:30	Meeting with National Policing Lead, *Leads DCC Peter Goodman, Terry Wilson(Conference Room 3b, 2 Marsham street London SW1P 4DF*)	*Evaluation team* *DCC Peter Goodman* *Terry Wilson (Police)* *Piers Harrison (SCOC)* *Mike Taylor (SCOC)*
12:30	Departure to NCA	*Evaluation team* *Piers Harrison (SCOC)* *Mike Taylor (SCOC)*
13:00 – 15:00	Lunch followed by CEOP session, *Leads Zoe Hilton & Paul Phillips (Room Vienna Unit 2, ground floor Spring Gardens, units 1-6 Citadel Place, Tinworth Street SE11 5EF)*	*Evaluation team* *Piers Harrison (SCOC)* *Mike Taylor (SCOC)* *Dominic Riddex (SCOC)*
15:00 – 16:00	Meeting with NCA / NCCU *Lead: Andy Archibald (Room Vienna Unit 2, ground floor Spring Gardens, units 1-6 Citadel*	*Evaluation Team* *Andy Archibald (NCCU)* *Paul Phillips (CEOP)*

	Place, *Tinworth Street SE11 5EF)*	*Zoe Hilton (CEOP)* *Piers Harrison (SCOC)* *Kathryn Roe (SCOC)* *Mike Taylor (SCOC)*
16:00 – 16:30	Optional wash up session (England & Wales) led by Piers Harrison / Mike Taylor *(Room Vienna Unit 2, ground floor Spring Gardens, units 1-6 Citadel Place, Tinworth Street SE11 5EF)*	*Evaluation Team* *Piers Harrison (SCOC)* *Mike Taylor (SCOC)*
16:30	Departure to hotel Premier Inn London Victoria *(free time in the evening)*	*Evaluation Team*
Thursday 22nd January 2015 **Day 3: Scotland and Northern Ireland meetings**		
6:00 (*i.e. British Airways flight at 7:50am)*	Departure from hotel Premier Inn London Victoria to London Heathrow Airport.	*Evaluation Team* *Piers Harrison (SCOC)*
London Heathrow 7:50 – Edinburgh 9:10	Delegates flying from London Heathrow to Edinburgh, Scotland	*Evaluation Team* *Piers Harrison (SCOC)*
Agenda **11:00- 12:00:** **12:00-12:45:** **12:45-13:30: lunch** **13:30-15:00:** **15:00-15:30: tea**	Meeting with the Crown Office, Police Scotland, PSNI and Scotland and NI officials (*Room: The Dome, New Register House Edinburgh)* *Scotland Leads: Det Supt Steven Wilson* *NI Leads: DCI Dougie Grant and Siobhan McKelvey.*	*Evaluation Team* *Piers Harrison (SCOC)* *Iain Logan (COPFS)* *Willie Cravens (Police Scotland)* *Keith McDevitt (Scottish Government)* *Clare El Azebbi (Scottish Government)* *Steven Wilson (Police Scotland)* *Andrew Richardson (COPFS)* *NI:* *DCI Dougie Grant (PSNI)* *Siobhan McKelvey (DoJNI)*

15:30-16:30: **16:30-17:15:** Wash up session	*Lead: Piers Harrison*	*Tricia Roulston (PSNI)* *As above*
17:15	Departure to Hotel in Edinburgh *Apex Waterloo Place Hotel, Free time*	*Evaluation Team* *Piers Harrison (SCOC)*
Friday 23rd January 2015 Day 4:		
Independent travel	Departure of evaluation team	

ANNEX B: LIST OF ABBREVIATIONS/GLOSSARY OF TERMS

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	ACRONYM IN ORIGINAL LANGUAGE	ENGLISH
CEOP		Child Exploitation and online Protection Command (within the NCA)
CERT		Cyber Emergency Response Team
CiSP		Cyber-security Information Sharing Partnership
CO		Cabinet Office
CPS		Crown Prosecution Service
EC3		European Cybercrime Center at Europol
EJTN	-	European Judicial Training Network
EMPACT	-	European Multidisciplinary Platform against Criminal Threats
ENISA	-	European Network and Information Security Agency
EUROJUST	-	The European Union's Judicial Cooperation Unit
EUROPOL		The European Police Office
GENVAL	*Groupe de travail "Questions Générales y compris l'Evaluation"*	Working Party "General Questions including Evaluation"
ICSE	-	International Child Sexual Exploitation
IWF		Internet Watch Foundation
J-CAT		Joint Cybercrime Action Taskforce at Europol
JCU		Judicial Cooperation Unit (Home Office)
JIT	-	Joint Investigation Team
LEA	-	Law Enforcement Authorities
MLA	-	Mutual Legal Assistance
MoJ		Ministry of Justice
NCA		National Crime Agency
NCCU		National Cyber Crime Unit

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	ACRONYM IN ORIGINAL LANGUAGE	ENGLISH
OCCRA		Organised Crime Research and Analysis (Home Office)
OCSIA		Office for Cyber Security and Information Assurance
OSCT		Office of Security and Counter Terrorism
SCOC		Strategic Centre for Organised Crime (Home Office)