Council of the European Union

Brussels, 7 February 2018
(OR. en)

6001/18

LIMITE

GENVAL 2
CYBER 22

NOTE

From:	The UK delegation
To:	Delegations
No. prev. doc.:	10952/2/15 REV 2
Subject:	Evaluation report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combatting Cybercrime" - Follow-up to the Report on UK

As a follow-up to each Round of Mutual evaluations, each Member-State is requested to inform the General Secretariat of the Council of the actions it has taken on the recommendations given to it.

This follow-up should be submitted within the 18 months of the adoption of the report concerned. Delegations will find in the Annex the follow-up of the United Kingdom regarding the recommendations that were made in the report 10952/2/15 REV 2 for the Seventh Round of Mutual Evaluations.

ANNEX

Responses to the 12 recommendations for the UK set out in the Report entitled 'The Practical implementation and operation of European policies on prevention and combatting cybercrime'

Investigation and Prosecution

Recommendation 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.

Response: The Crown Prosecution Service (CPS) has delivered a full and comprehensive training package for all of their prosecutors. This includes 8 e-learning modules of which two modules cover cyber crime specifically, whilst others cover digital evidence, online fraud, online grooming, social media, cyber-stalking and prohibited sexual images. This training continues to be regularly updated in order to address the ever increasing and fast moving threat of cyber criminality. In addition, the CPS have bespoke face-to-face training to enhance existing knowledge and expertise and they make training available to those prosecutors who require it, such as Heads of Complex Casework Divisions. This face to face training started towards the end of 2015 and is repeated from time to time and where deemed necessary.

In order to tackle the most complex cases the CPS have specialist cyber prosecutors in International Justice and Organised Crime Division (IJOCD) who handle all cases investigated and referred by the National Crime Agency. The Specialist Fraud Division (SFD) handles all serious and complex cases of fraud, including cyber fraud. The CPS have also published legal guidance to assist prosecutors in understanding how cyber crime is contextualised in relation to existing legislation. It provides prosecutors with a holistic package of tools to support them in this area of work. This guidance is also available to the public, defence lawyers and the judiciary.

Training for Judges is undertaken by the Judicial Studies Board which remains separate and independent from the CPS. Under the Constitutional reform Act 2005, responsibility for the training of the judiciary rests with the Lord Chief Justice and is exercised through the Judicial College. Under the adversarial system in the UK, the judge's main role is to manage the trial, ensure a fair hearing takes place, to sum up the case to the jury, and to pass sentence if a guilty verdict is returned. In that respect, it would be Police and CPS expertise in cyber crime that will be the important issue in order that a clear case can be presented to the Court.

There is no history of the judiciary training jointly with the CPS on any matter, nor is there likely to be in the future, as it could be considered to contravene the requirements of maintaining judicial independence.

Recommendation 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.

Response: The CPS has specialist prosecutors within the organised crime division. These are required to have a breadth of experience across all crimes and are not specifically trained solely to be cyber crime prosecutors. The same applies to other areas such as the Specialist Fraud Division. The CPS act on National Crime Agency referrals across all complex organised crime cases and they need to be able to use any of their specialist prosecutors at any time. The specialist prosecutors are the most experienced cyber crime prosecutors in the CPS and handle the most complex cases, as well as delivering the training to all the other prosecutors. However, prosecutors with the most experience of cyber dependant cases would be allocated a cyber crime case whenever possible.

Recommendation 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.

Response: Action Fraud does provide a service for Scotland, and fraud and cyber crime victims in Scotland reporting to Action Fraud receive the same service as the rest of the UK. However the primary reporting route for fraud and cyber crime in Scotland is direct to Police Scotland. Any decision on whether to formally extend the Action Fraud service to cover Scotland would be one for the Scottish Government.

Recommendation 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.

Response: In the financial year 2017/18 the UK government allocated one million pounds of National Cyber Security Programme funding to the College of Policing who are tasked with increasing the skills of law enforcement and mainstreaming a range of skills for all police areas. The aim is to implement a new cyber/digital pathway to professionalise the skills that law enforcement require. This will support the continued professionalisation of law enforcement, and increase attractiveness to remain in law enforcement with an accredited career pathway available. In addition, police forces throughout the UK recruit unpaid volunteers from relevant industries with specialist cyber skills as well as using Special Constables in order to support police forces with technical expertise to boost capabilities to tackle cyber crime at a local level.

Legislation

Recommendation 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.

Response: In the Serious Crime Act 2015, participating in activities of an organised crime group is an offence which carries a maximum of 5 years imprisonment. The crime itself has to constitute an offence in England and Wales punishable or conviction on indictment with imprisonment for a term of 7 years or more.

Therefore the most serious offences under the Computer Misuse Act (Sections 3 and 3ZA) would be captured by the participation offence in the Serious Crime Act.

The less serious offences in the Computer Misuse Act 1990 (Sections 1, 2 and 3A) would not be captured by this participation offence as they attract sentences of less than 7 years. It would not be reasonable or proportionate to increase the penalties for these less serious offences to 7 years or more. However, these less serious offences may be used to commit further offences which may be more serious, either under the Computer Misuse Act itself or which could fall under other legislation such as the Fraud Act; in such cases, these offences would attract higher sentences and may be captured by the participation offence.

Recommendation 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.

Response: The UK government remains committed to securing the maximum number of convictions in terrorism and serious crime cases.

The last review of the use of intercept as evidence, published in December 2014, concluded that the costs and risks of introducing a legally compliant intercept as evidence regime in the UK would outweigh the potential benefits.

Whilst the UK keeps the position under regular review, we do not assess that there have been any significant changes which would alter the current position. This was considered during development of the Investigatory Powers Act 2016 where Parliament agreed that maintaining the current bar was the correct approach.

The UK government will continue to keep this position under review with a view to developing an intercept as evidence regime when the potential benefits outweigh the risks and where it can be done in a way which is compatible with both an individual's right to a fair trial and the operational requirements set out in previous reviews.

Recommendation 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.

Response: The Scottish Government proposed abolishing the corroboration requirement in all criminal proceedings in the Criminal Justice (Scotland) Bill. Part of the intention behind this was to improve access to justice for victims of crimes committed in private. There was however some concern that additional safeguards and changes to law and practice may be needed to the criminal justice system following the planned abolition of the corroboration requirement. Lord Bonomy was appointed to head an independent reference review group to consider what changes might be necessary.

Given the complexity of Lord Bonomy's recommendations in his Post Corroboration Safeguards Review, and the lack of consensus on the abolition of the corroboration rule, the Scottish Government decided not to take forward the corroboration reform. One of the Review's recommendations was that any changes to the jury system should only be made on a fully informed basis by undertaking research into jury reasoning and decision making. The Scottish Government is taking forward this recommendation and the commissioning of Jury Research is now subject to a formal procurement process. The Jury Research is likely to take two years once it begins. Future consideration of corroboration reform needs to await the findings of that research and be considered in the wider context of that and the other recommendations of Lord Bonomy's group and any other related reforms.

Recommendation 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.

Response: In the Tackling CSE Progress Report which was published in 2017, the UK made a commitment to introduce full national roll out of video recording of all vulnerable/ intimidated witness cross-examination to commence in early 2017 and be completed by the end of 2018. The aim is to improve the experience of child and adult survivors of sexual abuse giving evidence, allowing them to do so in advance of the full trial and for their evidence to be recorded and played back at the trial.

The roll out of pre-trial cross examination (s28 of the Youth Justice Criminal Evidence Act 1999) commenced in Crown Court Centres in January 2017 for vulnerable witnesses. This allows those witnesses who are eligible for the provision to be cross examined on video before the trial takes place and the recording is then played to the jury at the trial. This means it is unlikely the witness will have to attend the trial as their evidence has already been taken. Further roll out is planned for intimidated witnesses in Crown Court Centres for victims of sexual abuse and modern slavery offences as well as a phased approach roll out of Section 28 to vulnerable witnesses.

Mutual Legal Assistance/International Cooperation

Recommendation 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).

Response: The separate functions between the police and prosecution services reflect the common law system in England, Wales and Northern Ireland. UK law enforcement are operationally independent and they can only initiate criminal investigations either through intelligence or crime reported to them. The UK values the role of Eurojust and routinely cooperate with Eurojust once it is clear an investigation that has cross border links.

Recommendation 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.

Response:
Since 2014 the UK Central Authority (UKCA) has seen a large increase in the volume of requests for Mutual Legal Assistance (MLA) being received In 2016 the UKCA received on average 540 incoming requests for evidence each month, which equates to 44% more requests than 2014, the UKCA also received 57% more requests for the service of documents than were received in 2014. To allow the UKCA to efficiently process the high volume of requests for evidence and service of documents being received, the UKCA has made a number of key changes to the way it processes MLA requests to improve efficiency.

These changes have allowed the UKCA to half the time to create a case from 3 days to 1.5 days, the time to consider a new incoming MLA request for evidence has also decreased from 39 days to 12 days.

In 2014 the UKCA moved to new case management software (iCasework). Since 2015 the UKCA has continuously increased their understanding of this software allowing for better use of the available functionality. This increased understanding has helped increase productivity within the unit.

A key part of the changes made to improve efficiency by the UKCA has been to introduce a digital case working system, which was introduced in April 2016. As part of this process paper files are no longer created; all incoming and outgoing correspondence is stored, generated and processed digitally on the case management system.

To monitor performance within the UKCA, the UKCA has implemented internal end-to-end key performance indicators (KPI) which are monitored at weekly performance meetings to ensure that all cases are processed efficiently. These KPIs cover the process for receiving the request, registering it as a case on the UKCA case management system, consideration, referral to an executing authority and for responding to correspondence. All cases are assessed and prioritised to ensure the most sensitive and urgent cases are processed within appropriate timeframes.

The UKCA uses a continuous improvement programme to ensure new issues are recorded as soon as they arise. These issues are then reviewed by remedial work streams who implement the necessary improvements. Case working processes are also reviewed and improved on a regular basis to adapt to the ever changing pressures.

The European Investigation Order (EIO) requires acceptance of an order within 30 days and the providing of assistance within a further 90 days These deadlines should help continue to improve the time it takes the UK to provide assistance to requests for MLA from EU countries.

Other Issues

Recommendation 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.

Response: There have been improvements in how the UK collects and publishes their statistics on cyber dependent crime.

The Home Office and Office of National Statistics publish a breakdown of cyber dependant crimes (Computer Misuse Act offences) every quarter. Home Office data is based on the number of reported cyber crime offences, however only a small number of these are passed to police forces for investigation. The Ministry of Justice publish the data on the number of successful prosecutions and convictions under the Computer Misuse Act.

A number of complex reasons account for the difference between reported crime and subsequent prosecutions, including:

A lack of evidence or a change in how the case is processed.

Some offences may be dealt with a measure that is less than a conviction – such as a fine or police warning.

A crime which may have a cyber dependent element to it can often end up being prosecuted and convicted for a different offence. For example online fraud (depending on type of fraud) could be covered under the Fraud Act 2006 or Data Protection Act 1998; online sales of illegal items could be covered under the Copyright Designs and Patents Act 1988 or the Trade Marks Act 1994; malicious and offensive communication offences (depending on type) could be covered under the Malicious Communications Act (1988).

Cyber Crime Related Statistics in the Devolved Administrations:

From 1st April 2015 Action Fraud took responsibility for the central recording of fraud and cyber crime previously recorded by Police Scotland and Northern Ireland. Action Fraud became responsible for all such reports in England and Wales by 1 April 2014. Action Fraud is the UK's National Reporting Centre for fraud and cyber crime reported directly from the public and other organisations. Action Fraud figures relating to fraud and cyber crime occurring in Northern Ireland and Scotland are provided to both jurisdictions on a monthly basis.

Northern Ireland publish their police statistics monthly which includes cyber dependant offences and while these are broken down by offence type such as computer virus/malware/spyware there is no reference to the associated legislation. Work is currently ongoing within the criminal justice system so that prosecutions and convictions for offences that might be classified as cyber crime can be identified as such and reported upon.

Scotland now publish cyber dependent recorded crime data and have an additional line in their National Statistics bulletin on police recorded crimes against the Computer Misuse Act 1990. The Scottish Government is currently working with Police Scotland, HMICS and others to improve the evidence base on cyber crime and its impacts in Scotland. This includes working with Police Scotland to improve the accuracy of recording and to increase reporting of cyber crimes.

Data on prosecutions and convictions for specific offences under the Computer Misuse Act are not routinely published in either jurisdiction, as the numbers are very low, however this data is freely available on request.

Recommendation 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.

Response: Central funding is allocated via the Barnett Formula to the devolved administrations and it is for the devolved administrations to determine how this funding is allocated.