CPS Cybercrime Strategy

Introduction

1. Cybercrime is an umbrella term used to describe two closely linked but distinct forms of criminal activity: **cyber-dependent** crime and **cyber-enabled** crime, applying equally to domestic and international offenders.

2. **Cyber-dependent** crime comprises acts unique to computer and computer-enabled systems, and primarily targets computer systems. **Cyber-enabled** crimes are typically traditional crimes transformed in scale or form by their use of the internet or communications technology. The growth of the internet and advancements in technology has enabled these crimes to be carried out on an industrial scale. Cyber-dependent crimes may also have the potential for secondary cyber-enabled attacks, such as the theft or personal information or fraud.

3. Cybercrime is not limited to only crimes involving financial gain; it can also involve the exploitation of technology to harm others, for example, the distribution of indecent images of children, or the use of technology to commit harassing or threatening behaviour. There has been a significant rise in cyber-enabled crimes targeting individuals such as revenge pornography, cyber-stalking and harassment. The use of the internet, social media platforms and other communications technology as an extension of offline behaviour to perpetrate violence against women and girls (VAWG) is also particularly prevalent. Prosecutors will need to consider online as well as offline activity when considering these cases.

4. The nature of the cyber landscape means that the traditional constraints of time and location of a crime need to be viewed differently. An offender based in one continent, victims in multiple locations across various countries and the crime conceived or executed from a communications device mean that almost all cybercrime will cross national jurisdictions – further still data involved in these crimes may have passed through multiple jurisdictions, via numerous communications service providers.

The CPS Cybercrime Strategy

5. This CPS Cybercrime Strategy supports the National Cyber Security Strategy (published in November 2016) and Serious Organised Crime Strategy (October 2013). It aims to:

    1. reduce the threat posed by cyber criminals who can commit crimes against the UK Government, businesses, and citizens from anywhere in the world; and

2. prosecute those who conduct such attacks, in line with the 'Deter' strand of the National Cyber Security Strategy. The strategy states that one measure of success will be 'higher numbers of cybercrime convictions.'

6. We will achieve this by:

   1. **allocating cases** in line with internal expertise;

   2. **building capability** within the CPS and across law enforcement partners;

   3. providing regular up-to-date and relevant **training for prosecutors**;

   4. using our **international network** to prosecute cybercrime criminals overseas; and

   5. improving our **service to victims** of cybercrime.

7. We will keep this strategy under review and work with our partners to ensure the law keeps pace with developing technology and the way it is exploited by criminals.

Case Allocation

8. The CPS deals with a number of prosecutions of cyber-dependent and cyber-enabled crime. Depending on the levels of complexity, these cases are handled at different levels across the organisation:

   - prosecutors in the Organised Crime team in the CPS International Justice and Organised Crime Division (IJOCD) will handle all cases investigated and referred by the NCA;

   - the Specialist Fraud Division (SFD) handles all serious and complex cases of fraud, including cyberfraud;

   - Area Complex Casework Units (CCUs) will handle all other serious cybercrimes investigated by local police forces, and

   - our main Area offices will deal with all other cyber-enabled cases.

Building Capability

9. We will work closely with law enforcement partners to enhance and increase cybercrime prosecutions through the mutual sharing of skills, knowledge and experience.

10. We will also conduct debrief conferences on complex cybercrime prosecutions to identify lessons learnt for all parties involved.

Training Prosecutors

11. We have developed two core cybercrime e-learning packages, explaining the various forms of cybercrime and relevant technical tools. The training also focusses on how to manage vast volumes of data and how to present evidence clearly in court. This will ensure prosecutors are properly skilled to deal with cybercrime.

12. Four new modules of e-learning training packages to accompany those which are already in use will be developed in the following areas:

    - digital evidence gathering;
    - online grooming;
    - online fraud; and
    - social media.

13. We have also developed consolidated legal guidance for prosecutors, providing an overview of existing guidance and practical advice for the various types of cybercrime. The guidance is published alongside this strategy.

14. We have bespoke face-to-face training to enhance existing knowledge and expertise and we will endeavour to make training available to all prosecutors who require it, such as Heads of Complex Casework Divisions.

International Engagement

15. The CPS has a number of staff based in various countries working as Liaison Magistrates or Criminal Justice Advisers. But even when key individuals responsible for the most damaging cyber criminal activities against the UK are identified, it is often difficult for the UK and international law enforcement agencies to prosecute them when they are located in jurisdictions with limited, or no, extradition arrangements.

16. Nevertheless, we will work with our overseas partners to form joint investigation teams, ensuring we fully understand the investigative methods and procedures of the country in question, and support capacity building, to bring criminals overseas to justice wherever possible.

17. We will continue to work closely with partner agencies overseas to promote international cooperation and work towards the development of effective protocols managing global investigations to tackle cybercrime.

Improve service to victims

18. As part of the CPS priority to improve the service provided to victims and witnesses, we will ensure victims of cybercrime are supported throughout their case, including by our dedicated victim liaison units and CPS staff at court where appropriate.

Crown Prosecution Service
November 2016