Serious Crime Act 2015

Fact sheet: Part 2: Computer misuse

Background

1. In 2010 the National Security Strategy identified hostile attacks on UK cyber space by other states and large scale cyber crime as a 'tier one' threat to national security. In response, the National Cyber Security Programme ("NCSP") was established to help meet the objectives of the strategy. It is underpinned by £860 million of government investment over five years to 2016, around 10% of which has been invested to build law enforcement capabilities to tackle cyber crime. A coordinated approach is needed to tackle serious and organised crime, including cyber crime. The Government set out how we plan to achieve this in the Serious and Organised Crime Strategy, published in October 2013. It is essential that in tackling cyber crime the right framework of offences is in place and that there is clarity in how the powers that are used to investigate cyber crime interact with the offences designed to catch cyber criminals.

The Computer Misuse Act 1990 as amended

2. The Computer Misuse Act 1990 ("the 1990 Act") sets out the offences associated with interfering with a computer (that is, hacking) and the associated tools (such as malware) that enable computer systems to be breached. It does not contain any powers. The 1990 Act, which applies UK-wide, makes unauthorised access to, or modification of, computer material unlawful.

3. Part 2 of the Serious Crime Act 2015 amends the 1990 Act to:

   - create a new offence of unauthorised acts causing serious damage;
   - implement the EU Directive on Attacks against Information Systems; and
   - clarify the savings provision for law enforcement agencies.

New offence of unauthorised acts causing serious damage

4. The new offence in section 3ZA of the 1990 Act addresses the most serious cyber attacks, for example those on essential systems controlling power supply, communications, food or fuel distribution. A major cyber attack of this nature could have a significant impact, resulting in loss of life, serious illness or injury, severe social disruption or serious damage to the economy, the environment or national security. However, hitherto the most serious offence under the Act was the section 3 offence of unauthorised access to impair the operation of a computer. The maximum sentence of 10 years' imprisonment which this offence carried did not sufficiently reflect the level of personal and economic harm that a major cyber attack on critical systems could cause.

5. The new offence applies where an unauthorised act in relation to a computer results, directly or indirectly, in serious damage to the economy, the environment,

national security or human welfare, or a significant risk of such damage (where damage to human welfare encompasses loss of life, illness or injury or serious social disruption). A significant link to the UK is required, so that at least one of the accused or the target computer at the time of the offence or the damage must have been in the UK, or the accused must be a UK national at the time of the offence and the conduct constitute an offence under the law of the country in which it occurred. The accused must have intended to cause the serious damage, or to have been reckless as to whether it was caused.

EU Directive on Attacks against Information Systems (2013/40/EU)

6. The EU adopted a Directive on attacks against information systems in August 2013. The aim of the Directive is to establish a set of minimum rules within the European Union on offences and sanctions relating to attacks against information systems. It also aims to improve cooperation between competent authorities in Member States.

7. The Government has until 4 September 2015 to transpose the Directive into UK law. The UK is compliant with the Directive save in two respects: tools used for committing offences (Article 7) and jurisdiction (Article 12). The amendments in the Serious Crime Act address these gaps.

Obtaining tools for use

8. Article 7 of the Directive covers the tools used to commit computer offences (for example malware). This Article states that Member States should have offences in their legislation to criminalise the intentional "production, sale, procurement for use, import, distribution, or otherwise making available" of tools with the intention that it is used to commit any of the further offences in the Directive.

9. Before the amendment to this offence, section 3A (making, supplying, or obtaining articles for use in offences under sections 1 or 3) of the 1990 Act covered all of the provisions under Article 7 with the exception of the offence of "procurement for use" of such tools. The prosecution was required to show that the individual obtained the tool with a view to its being *supplied* for use to commit, or assist in the commission of an offence under section 1 or 3 of the 1990 Act, in other words the offence required the involvement (or intended involvement) of a third party.

10. Section 42 of the Serious Crime Act now extends section 3A of the 1990 Act to include an offence of obtaining a tool for use to commit a section 1, 3 or 3ZA offence *regardless* of an *intention to supply* that tool – thus removing the requirement of the involvement, or intended involvement, of a third party and ensuring that the offence covers individuals acting alone.

Extending the extra-territorial jurisdiction of the 1990 Act offences by nationality

11. Article 12 of the EU Directive covers jurisdiction and requires Member States to establish their jurisdiction with regards to a cyber offence being committed by one

of their nationals. Before the amendment, the arrangements for the extra territorial application of the offences (that is, the ability for the UK courts to try cases in respect of conduct committed outside their jurisdiction) within the 1990 Act required the prosecution to show a significant link to the UK – that being that either the individual or the affected/intended affected computer needed to be present in the UK at the time of the offence.

12. In response to Article 12, section 43 of the Serious Crime Act extends the categories of "significant link to the domestic jurisdiction" in section 5 of the 1990 Act to include "nationality". This provides a legal basis to prosecute a UK national who commits any section 1 to 3A offence whilst outside the UK, where the offence has no link to the UK other than the offender's nationality, provided that the offence was also an offence in the country where it took place.

Savings

13. Section 44 clarifies the savings provision at section 10 of the 1990 Act and is intended to remove any ambiguity for the lawful use of powers to investigate crime (for example under Part 3 of the Police Act 1997) and the interaction of those powers with the offences in the 1990 Act. The changes do not extend law enforcement agencies' powers but merely clarify the use of existing powers (derived from other enactments, wherever exercised) in the context of the offences in the 1990 Act.

Home Office
March 2015