These notes refer to the Serious Crime Act 2015 (c.9)
which received Royal Assent on 3rd March 2015

SERIOUS CRIME ACT 2015

EXPLANATORY NOTES

TERRITORIAL EXTENT

Part 2: Computer Misuse

Summary and Background

126. Sections 1 to 3A of the Computer Misuse Act 1990 ("the 1990 Act") provide for a number of criminal offences to tackle cyber crime, as follows:

- Section 1 - unauthorised access to computer material or data (commonly known as "hacking");
- Section 2 - unauthorised access with intent to commit or facilitate commission of further offences;
- Section 3 - unauthorised acts with intent to impair the operation of a computer (this offence includes circulating viruses, deleting files and inserting a "Trojan Horse" to steal data as well as effectively criminalising all forms of denial of service attacks in which the attacker denies the victim(s) access to a particular resource, typically by preventing legitimate users of a service accessing that service, for example by overloading an Internet Service Provider of a website with actions, such as emails);
- Section 3A - making, adapting, supplying or offering to supply an article ("hacker tools") intending it to be used to commit, or to assist in the commission of, an offence under sections 1 or 3; supplying or offering to supply an article believing that it is likely to be used in this way; and obtaining an article with a view to its being supplied for use in this way.

Other provisions of the 1990 Act make limited provision for extra-territorial jurisdiction and a saving for certain law enforcement powers so that relevant conduct by law enforcement agencies does not fall within the section 1 offence.

127. The Government's UK Cyber Security Strategy[1] included a commitment to "review existing legislation, for example the 1990 Act, to ensure that it remains relevant and effective". Following that review, this Part introduces a new offence in respect of unauthorised acts in relation to computers causing serious damage.

128. On 12 August 2013, the European Parliament and European Council adopted Directive 2013/40/EU on attacks against information systems[2] ("the Directive") and replacing Council Framework Decision 2005/222/JHA. The Act makes two amendments to the 1990 Act to ensure that the UK law is fully compliant with the Directive. The Government announced that it intended to opt in to the Directive in an oral statement on 3 February 2011 (Official Report, House of Commons, columns 1051 to 1058).

---

1 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf
2 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF

Commentary on Sections

Section 41: Unauthorised acts causing, or creating risk of, serious damage

129. *Subsection (2)* inserts new section 3ZA into the 1990 Act which creates a new offence of impairing a computer such as to cause serious damage. The existing offence of impairing a computer under section 3 of the 1990 Act carries a maximum penalty of ten years' imprisonment. This maximum penalty is not considered adequate by the Government in those cases where the impact of the action is to cause serious damage, for example to critical national infrastructure. The new offence addresses that gap in the criminal law.

130. New section 3ZA(1) sets out the elements of the offence. The *actus reus* (or conduct element) is that the accused undertakes an unauthorised act in relation to a computer (as in section 3(1)(a) of the 1990 Act) and that act causes, or creates a significant risk of causing, serious damage of a material kind. The *mens rea* (namely the mental elements of the offence) is that the accused, at the time of committing the act, knows that it is unauthorised (as in section 3(1)(b) of the 1990 Act) and intends the act to cause serious damage of a material kind or is reckless as to whether such damage is caused. An unauthorised act is defined in section 17(8) of the 1990 Act as an act where the person doing the act does not have responsibility for the computer in question, which would thereby entitle him or her to determine whether the act is undertaken, and does not have the consent of the person responsible for the computer to commit the act.

131. The term "material kind" is defined in new section 3ZA(2), read with new section 3ZA(3) to (5), as damage to human welfare, the environment, the economy or national security. The other terms used in the definition of a material kind take their normal everyday meaning. It would, in the normal way, be for the jury to determine whether, for example, there had been damage to national security and whether that damage was serious.

132. The offence will be triable on indictment only. As a result of new section 3ZA(6) and (7) the maximum penalty is life imprisonment in respect of threat to life, loss of life or damage to national security. In respect of damage to the economy or environment, it will be 14 years' imprisonment.

133. *Subsection (3)* amends section 3A of the 1990 Act. The amendment ensures that the offence provided for in section 3A also applies to the making etc of hacker tools intended to be used to commit the new section 3ZA offence.

Section 42: Obtaining articles for purposes relating to computer misuse

134. Article 7 of the Directive requires Member States to criminalise certain activities in relation to the commission of the substantive offences at Articles 3 to 6 of the Directive (those Articles relate to illegal access to information systems, illegal system interference, illegal data interference and illegal interception). It provides as follows:

> "**Tools used for committing offences**
>
> Member States shall take the necessary measures to ensure that the intentional production, sale, procurement for use, import, distribution or otherwise making available, of one of the following tools, without right and with the intention that it be used to commit any of the offences referred to in Articles 3 to 6, is punishable as a criminal offence, at least for cases which are not minor:
>
> (a) a computer programme, designed or adapted primarily for the purpose of committing any of the offences referred to in Articles 3 to 6;
>
> (b) a computer password, access code, or similar data by which the whole or any part of an information system is capable of being accessed."

135. Section 3A of the 1990 Act, in conjunction with sections 1 to 3 of that Act, meets the requirements of Article 7 save in one respect, namely the "procurement for use" of tools used for committing the Article 3 to 6 offences. Under the existing offence, the prosecution is 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 Act. This section extends subsection (3) of section 3A of the 1990 Act to include an offence of obtaining a tool for use to commit a Computer Misuse Act offence (including one under the new section 3ZA inserted by section 41) *regardless* of an *intention to supply* that tool. As amended, that subsection would provide that (additions shown in italics):

> "A person is guilty of an offence if he obtains any article with a view to *article* –
>
> (a) *intending to use it to commit, or assist in the commission of, an offence under section 1, 3 or 3ZA, or*
>
> (b) *with a view to* its being supplied for use to commit, or assist in the commission of, an offence under section 1 or 3."

Section 43: Territorial scope of computer misuse offence

136. Article 12 of Directive provides as follows:

> "**Jurisdiction**
>
> 1. Member States shall establish their jurisdiction with regard to the offences referred to in Articles 3 to 8 where the offence has been committed:
>
> (a) in whole or in part within their territory; or
>
> (b) by one of their nationals, at least in cases where the act is an offence where it was committed.
>
> 2. When establishing jurisdiction in accordance with point (a) of paragraph 1, a Member State shall ensure that it has jurisdiction where:
>
> (a) the offender commits the offence when physically present on its territory, whether or not the offence is against an information system on its territory; or
>
> (b) the offence is against an information system on its territory, whether or not the offender commits the offence when physically present on its territory....."

137. Sections 4 and 5 of the 1990 Act already provide for limited extra-territorial jurisdiction in relation to the offences in sections 1 and 3 of that Act. Under those provisions, it is possible to prosecute a person in this country for an act committed abroad which would constitute an offence under section 1 or 3 provided that there was a "significant link" to the appropriate jurisdiction in the UK. *Subsection (2)* amends section 4 of the 1990 Act to apply such extra-territorial jurisdiction to the offence in new section 3ZA inserted by section 41; *subsection (5)* amends section 5 of the 1990 Act to define what constitutes a "significant link" in the context of the new offence. A significant link is established if the accused was in the UK at the time of the offence, or if the affected computer or the intended affected computer was in the UK. Accordingly, it would, for example, be possible under the current law to prosecute a French national resident in England and Wales who hacked into a computer system in France or a UK national who hacked into a computer system in the UK whilst temporarily resident in France (but who subsequently returned to the UK). *Subsection (3)* inserts new subsection (4A) into section 4 of the 1990 Act, the effect of which is to apply extra-territorial jurisdiction to the offence under section 3A of the 1990 Act. *Subsection (4)* amends section 5 of the 1990 Act to extend the current extra-territorial jurisdiction in order to fully comply with Article 12; the effect of new section 5(1A) and (1B) is to permit prosecutions of a UK national for all offences under the 1990 Act even where the conduct concerned

has no other significant link to the UK, provided also that the offence was an offence in the country where it took place.

138. *Subsections (6) and (7)* amend section 13 of the 1990 Act. Subsection (6) sets out the criteria for when a sheriff court in Scotland will have jurisdiction to try an offence under sections 3ZA and 3A of the 1990 Act. A sheriff court will have jurisdiction if a person who commits an offence under section 3ZA is in the sheriffdom at the time they carry out any of the unauthorised act, or if the computer in relation to which the offence was carried out was located in the sheriffdom at the time of the offence. A sheriff court will have jurisdiction if a person who commits an offence under section 3A is in the sheriffdom at the time they carry out any of the acts set out in section 13(2B)(a). If a person was not in the sheriffdom, new section 13(2B)(b) provides the sheriff court will have jurisdiction to try the offence if the computer in relation to which the offence was carried out was located in the sheriffdom at the time of the offence. Subsection (7) provides that where a person commits an offence under section 1, 3, 3ZA or 3A of the 1990 Act outwith Scotland, he or she may be tried in any sheriff court district in which the person is apprehended or in custody, or in such sheriff court district as the Lord Advocate may direct, as if the offence had been committed there.

Section 44: Savings

139. Section 10 of the 1990 Act contains a saving provision. It provides that the offence at section 1(1) of the 1990 Act has effect without prejudice to the operation in England and Wales of any enactment relating to powers of inspection, search or seizure; and in Scotland of any enactment or rule of law relating to powers of examination, search or seizure. The amendment to section 10 of the 1990 Act made by this section is a clarifying amendment. It is designed to remove any ambiguity over the interaction between the lawful exercise of powers (wherever exercised) conferred under or by virtue of any enactment (and in Scotland, rule of law) and the offence provisions. "Enactment" is expressly defined to provide certainty as to what this term includes. The title of section 10 of the 1990 Act has also been changed to remove the reference to "certain law enforcement powers" (see paragraph 12 of Schedule 4). This is to avoid any ambiguity between the title and the substance of that section.