CHAPTER 5

DENIAL OF SERVICE ATTACKS

5.1 INTRODUCTION

It often occurs that when hackers or crackers gain access to or interfere with computers or computer systems, legitimate users cannot gain access to the system or use the system. The denial of service attack, also known as a DOS attack, causes a computer system to be inaccessible to legitimate users.\(^1\) DOS attacks disrupt service to legitimate users or completely deny service to legitimate users for a period of time.\(^2\) A distributed denial of service attack occurs when the victim network are simultaneously attacked by various sources or machines.\(^3\) These malicious attacks can cause millions of rands of damage to corporations due to a loss of revenue because their computer systems cannot be accessed. It is reported that in February 2000 denial of service attacks were launched against the web sites of CNN, eBay, Yahoo and others.\(^4\) A fifteen-year old Canadian pupil that used the pseudonym Mafiaboy was arrested and convicted of inter alia the Canadian offence of mischief in

---


\(^3\) Scambray (footnote 2 supra) 499; Marchette (footnote 2 supra) 252.

relation to data as a result of these DOS attacks and sentenced to a period of detention in a juvenile detention centre.

There are many methods through which a denial of service can be achieved. A computer system can be bombarded with instructions or data that causes its resources to be overwhelmed and constitutes a denial of service. For instance a person wants to access a specific website and his computer sends a communication or connection request to the website server. The website server responds and sends a communication to the Internet address acknowledging further communication. The hacker, however, *spoofs* or forges the Internet address or uses an unreachable Internet address and the website server gets no reply from the forged or unreachable address. The server continuously attempts to communicate with the Internet address and uses resources that may lock legitimate users out from use. An Internet service provider can be flooded with false requests to access a certain web page which could also deny service to authorised users. If a planned continuous attack is lodged against such a server it may even cause the server to crash and it will be inoperable and inaccessible. Another method that may result in a denial of service is so-called *e-mail bombing*. A cyber criminal may repeatedly sent thousands of e-mails to an e-mail address, or send a very large e-mail to an e-mail address or a specific email address is targeted by various users. This causes the e-mail server to be bombarded with messages that it cannot handle and it becomes inaccessible. *Smurf attacks* involve a denial

---

5 See paragraph 5.2 *infra*.  
6 Standler (footnote 4 *supra*).  
7 Ebersöhn (footnote 1 *supra*) 25 *et seq.*  
8 Ebersöhn (footnote 1 *supra*) 27.
of service attack during which the attacker fools intermediary computers to actually mount the attack.⁹

5.2 INTERNATIONAL RESPONSES

5.2.1 The United States of America and the United Kingdom

In the State of North Carolina in the United States any person who wilfully and without authorisation denies or causes a denial of computer system services to an authorised user is guilty of an offence.¹⁰

Section 3 of the United Kingdom Computer Misuse Act of 1990 provides for the criminalisation of the unauthorised modification of the contents of any computer. It has been argued that a denial of service attack does not modify the contents of the computer.¹¹ The term modify means to change or alter data. Some denial of service attacks do not change or alter data in a computer system but only cause the system to be overwhelmed and therefore inaccessible. It appears that these types of denial of service attacks will not fall within the ambit of section 3 of the Computer Misuse Act. Certain DOS attacks however could result in the deletion or altering of data which causes the system to be inaccessible. This will constitute an unauthorised modification in terms of section 3 of the Act.

In the case of Aaron Caffrey it was alleged that the defendant launched a denial of service attack against the computer system of the Port of

---

⁹ Marchette (footnote 2 supra) 95.

¹⁰ Section 14-456 of the North Carolina General Statutes.

Houston. Caffrey alleged that a Trojan horse application, that installed itself on his computer, launched the DOS attack. No trace of any Trojan horse program could be found on his computer and he argued that the Trojan horse program deleted itself. Caffrey was acquitted.\footnote{12}{Hill (footnote 11 \textit{supra}) 31.}

\subsection*{5.2.2 Canada}

In Canada the offence of \textit{mischief in relation to data} contains certain provisions in respect of the denial of service to legitimate users.\footnote{13}{Section 430(1.1) of the Canadian Criminal Code.} A person is guilty of the offence of mischief in relation to data if he wilfully obstructs, interrupts, or interferes with the lawful use of data.\footnote{14}{Section 430(1.1)(c) of the Canadian Criminal Code.} Similarly a person will be guilty of the offence if he wilfully obstructs, interrupts or interferes with any person in the lawful use of data or access to data to any person who is entitled to access thereto.\footnote{15}{Section 430(1.1)(d) of the Canadian Criminal Code.}

\subsection*{5.2.3 Council of Europe}

The Council of Europe’s Convention on Cybercrime\footnote{16}{Convention on Cybercrime, ETS No. 185, Council of Europe, Budapest 2001.} recommended that \textit{system interference} should be criminalised and provided that “each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting,
deteriorating, altering or suppression of computer data”. The *hindering* refers to conduct that interfere with the proper functioning of a computer system. The hindering must be *serious* which will include the sending of data to a computer system “in such a form, size or frequency that it has a significant detrimental effect on the ability of the owner or operator to use that system”. This will also include programs such as viruses that constitute a denial of service.

5.3 SOUTH AFRICAN RESPONSES

5.3.1 South African Law Commission

The South African Law Commission did not investigate this aspect specifically but recommended that the denial of service or access to legitimate users should be criminalised. The following offence was proposed in the Computer Misuse Bill:

> “Any person who –
> 
> (a) prevents or hinders access to any application or data in a computer system;
> 
> (b) impairs the effectiveness or reliability of any application or data in a computer system, or
> 
> (c) impairs the operation of a computer system,
> 
> is guilty of an offence.”

17 Article 5 of the Convention on Cybercrime (footnote 16 supra).


19 Explanatory Report to the Convention on Cybercrime (footnote 18 supra) paragraph 67.

5.3.2 The Electronic Communications and Transactions Act

Section 86(5) of the Electronic Communications and Transactions Act provides that:

“A person who commits any act described in this section with the intent to interfere with access to an information system so as to constitute a denial, including a partial denial, of service to legitimate users is guilty of an offence.”

The act or conduct is very widely defined and consists of any of the actions criminalised in sections 86(1) to 86(4) of the Act that results in a denial or partial denial of service to legitimate users. These actions will include unauthorised access, unauthorised modification or the utilising of a program or device to overcome security measures. A cyber criminal could interfere with or alter data in the computer system that may cause legitimate users to be locked out from access. A partial denial of service will also fall within the scope and ambit of this offence. It is submitted that ping flooding would also fall within the ambit of this subsection. The cyber criminal interferes with the data indirectly, which causes the computer system to become inoperable or inaccessible. This will constitute a denial of service to lawful users.

---


22 Discussed in chapter 3 supra.

23 Discussed in chapter 4 supra.

24 See chapter 7 infra.

25 In general see G J Ebersöhn Internet law: Port scanning and ping flooding – a legal perspective (2003) 66 THRHR No. 4 565 et seq. and paragraph 4.7.1 supra.
The absence of authority or permission is an indication of unlawfulness. Culpability in the form of intent is required by the Act. The intention is further specified as the intention to interfere with the access to an information system so as to constitute a denial or partial denial of service to legitimate users and can be determined from the specific facts of a case.\(^{26}\)

A person that is convicted of contravening this subsection may be sentenced to a fine or imprisonment not exceeding 5 years.\(^{27}\) An attempt to commit the offence is also criminalised\(^{28}\) and the aiding and abetting of another to commit the offence is criminalised in section 88(2) of the Act. Cyber criminals may conspire with or incite others to commit these types of offences and will be criminally liable in terms of the provisions of the Riotous Assemblies Act.\(^{29}\)

The provisions of section 86(2) and 86(5) of the Act are very closely related and certain actions will fall within the ambit and scope of both these offences. For example a virus may also cause a denial of service to legitimate users. When essential data configurations are deleted the system cannot operate properly and legitimate users will not be able to access the system. A problematic issue is whether an accused may be convicted of both such offences or whether it will constitute a duplication of convictions. The wording of section 86(5) refers to the proscribed actions in the rest of the subsections of section 86 and it could certainly

\(^{26}\) See Watney (footnote 21 \textit{supra}) 243.

\(^{27}\) Section 89(2) of Act 25 of 2002.

\(^{28}\) Section 88(1) of Act 25 of 2002.

\(^{29}\) Section 18(2) of Act 17 of 1956.
be argued that an accused should rather be convicted of an offence in terms of section 86(5) of the Act. It is however argued that the elements of subsection 2 and 5 are essentially different. Subsection 5 has the additional element that the initial action should be accompanied with the intent to interfere with a computer system so as to constitute a denial of service. This element noticeably distinguishes this offence from the other offences contained in section 86 of the Act. A person that deletes data usually has the intent to cause damage. In addition this person has the further intent to lock legitimate users out from access. It is submitted that in such instances the perpetrator could be convicted of contravening both these subsections.