# Denial of Service Attacks: Trends in Criminalization

**Quazi MH Supan***

## Introduction

In the early nineties many cybercrimes predominantly fell in the grey area of law. The frequent exclusion of these crimes outside the grip of law may be attributed to weak or lack of legislation or poorly equipped investigators. Among these crimes, the smartest, most sophisticated and elite one that tops the list of 'untouchable' cybercrimes is DoS (denial of service) attack. A variety of new trends in legislation can be seen since the early tens of the 21st century to criminalize DoS attacks that were otherwise immune from criminal or civil justice systems. This article examines those trends. In doing so, the article first characterizes various DoS attacks and then scrutinizes the criminal law responses to those attacks and identifies the trend.

For the purpose of this article I will examine the legislations of selected countries from all the continents, namely, Asia, Europe, North and South America, Africa and Australia and I will categorize DoS related criminal laws in the following three groups:

(a) Explicit criminalization: Generally the recent cyber legislations fall in this category. This trend explicitly refers to DoS attacks, defines a DoS activity and penalizes it.

(b) Criminalization through broadly-worded provisions of illegal access and diminishing utility: Technologically advanced states could foresee many facets of future cybercrimes and accordingly their drafters had defined 'future cyber activities' with precision to criminalize them before they appeared.

(c) Ambiguous criminalization: Legislations that took place before the advent of DoS attacks have given rise to confusion and controversy in penalizing DoS attacks. Some legislations of this trend may be capable of penalizing a few variants of DoS attacks, but for most variants they have proved ineffective.

## Dos and variants

Denial of Service (DoS) Attack is a criminal attack where the goal is to prevent a computing resource from being used. In other words, Denial of Service is an attack against an organisation's service that aims to prevent legitimate users from accessing it. Perhaps the situation has been best described by Graham Cluley's metaphor of '15 fat men trying to get

* Associate Professor, Department of Law, University of Dhaka.

through a revolving door at the same time'.[1]More sophisticated DoS attacks may include other variants like DDoS[2] and DDoS.[3]

Kevin Mandia et al categorized DoS attacks in the following manner:[4]

> Destructive – Attacks which destroy the ability of the device to function, such as deleting or changing configuration information or power interruptions.
>
> Resource consumption – Attacks which degrade the ability of the device to function, such as opening many simultaneous connections to the single device.
>
> Bandwidth consumption – Attacks which attempt to overwhelm the bandwidth capacity of the network device.

In a denial of service attack, a hacker can prevent authorized or intended users from accessing resources and services. The hacker can target the computers or network connections. By carrying out the attack, the hacker can prevent users from accessing several websites, using email, video conferencing, banking services and online shopping. In effect, a denial-of-service attack prevents users from accessing any content from computers and networks that are affected by the attack. One of the most common ways of performing a denial-of-service attack on a website is to flood the website with a huge number of information requests. This will prevent other users from accessing it, as each website can accept only a limited number of requests. [5]

In most denial of service attacks, malicious users exploit the connectivity of the Internet to cripple the services offered by a victim site, often simply by *flooding* a victim with many requests. A DoS attack can be either a *single-source* attack, originating at only one host, or a *multi-source*, where multiple hosts coordinate to flood the victim with a barrage of attack packets. The latter is called a distributed denial of service (DDoS) attack.

---

1 Graham Cluley, *Naked Security*, <nakedsecurity.sophos.com> December 2010.

2 Distributed Denial of Service Attack: a DoS attack where the source attacker is not one computer or device, but several of them, typically located in disparate locations.

3 Distributed Reflector Denial of Service Attack: a DDoS attack that is amplified by a reflector. A reflector is typically an uncompromised device that unwittingly participates in a DDoS attack. Due to the design of the attack, it sends several times more traffic to the victim than what was sent to it. For a general understanding, see Verisign Public, Distributed Denial of Service (DDoS) Attacks: Evolution, Impact & Solutions, Verisign White Paper, 2012.

4 Kevin Mandia and Chris Prosise, *Incident Response: Investigating Computer Crime*, (Osborne/McGraw-Hill, Berkeley, 2001) 360-361

5 Hevin Houle and George Weaver, Trends in denial of service technology (CERT Coordination Center at Carnegie-Mellon University, October 2001). See also, David Moore, Geoffrey Voelker, and Stefan Savage, 'Inferring Internet denial of service activity in Proceedings of the USENIX Security Symposium' (Washington, DC, USA, August 2001)

Sophisticated attack tools that automate the procedure of compromising hosts and launching attacks are readily available on the Internet, and detailed instructions allow even an amateur to use them effectively.[6]

The perpetrators may even penetrate wi-fi networks with DoS attack tools.[7]One does not have to be an expert to initiate a DoS attack since attack tools are available free of cost.[8] For this reason many countries have criminalized production, distribution and procurement of DoS tools.

Hackers may launch a DoS attack by several ways including the take over computer resources, such as bandwidth, disk space, or processor time or disrupt configuration information, such as routing information. Basically, the hackers overload the website's system with so many online traffic requests that the website can't function and regular users can't access it. Often in denial of service attacks, the computers used to bombard the targeted web sites with traffic, have actually been hijacked or taken over by hackers. The computers are often infected with malware that give attackers control over the computer, usually without the website's knowledge. Such attacks may result in unusually slow network performance beyond the norm, unavailability of a particular website, inability to access any web site or dramatic increase in the number of spam emails received by the website.[9]

The reasons of DoS attacks are varied. They may include political conflicts, economic benefits for competitors, curiosity of some computer geeks and even cyber terrorism.[10]

Malicious hackers can commandeer thousands of computers around the world, and order them to deluge a website with traffic - effectively clogging

---

6 Alefiya Hussain, John Heidemann, and Christos Papadopoulos, 'A Framework for Classifying Denial of Service Attacks' ISITR2003569, Date: 25 Feb 2003 [This material is based upon work supported by DARPA via the Space and Naval Warfare Systems Center San Diego under Contract No. N66001-00-C-8066 ("SAMAN"), by NSF under grant number ANI-9986208 ("CONSER"), by DARPA via the Fault Tolerant Networks program under grant number N66001-01-1-8939("COSSACK") and by Los Alamos National Laboratory under grant number 53272-001.]

7 The infiltration may take place against the guest network infrastructure and also against the infrastructure responsible for the Wi-Fi roaming services. See Romain Robert et al, Wi-Fi Roaming: Legal Implications and Security Constraints (2008) 16(3) *International Journal of Law and Information Technology* 205-41, 227.

8 For discussions and analysis of various DoS tools, see Fafinski, S., Access denied: computer misuse in an era of technological change", (2006) 70(5) *Journal of Criminal Law* 424-442;, G. Kon, P. Church , 'A denial of service but not a denial of justice' (2006) 22 *Computer Law & Security Report* 416-417 ; J. Mirkovic, S. Dietrich, D. Dittrich, and P. Reiher, *Internet Denial of Service: Attack and Defense Mechanisms* (Prentice Hall, 2005) ; P. Hallam-Baker, *dotCrime Manifesto* (Addison Wesley, 2008).

9 Mark Koba, Denial of Service Attack: CNBC Explains, CNBC, 24 Jan 2013.

10 Ahsan Habib, Mohamed M. Hefeeda, and Bharat K. Bhargava, 'Detecting Service Violations and DoS Attacks' (Concept paper, CERIAS and Department of Computer Sciences, Purdue University, West Lafayette, IN 47907, 2007) 1-2.

it up, preventing others from reaching the site, and bringing the website to its knees. They may even urge internet users to volunteer to attack, for example, recently they have urged internet users to voluntarily join a botnet by downloading a DDoS attack tool called LOIC (Low Orbit Ion Cannon).[11] Supporters of WikiLeaks have orchestrated DDoS attacks on a number of websites who they feel have turned their back on the controversial whistle-blowing website.[12] In response to Stop Online Piracy Act (SOPA) and Protect Intellectual Property Act (PIPA) the sympathizers of Anonymous and Megaupload orchestrated DDoS attacks against multiple entertainment industry and US government websites has been dubbed 'OpMegaupload' by Anonymous supporters. Among the victims of the attacks were websites for the Department of Justice, the White House, the FBI, the US Copyright Office, Universal Music Group, the RIAA, the Motion Picture Association of America and a bunch of other sites.

Denial of Service attacks have existed since the early days of computing and have evolved into complex and overwhelming security challenges. Although the methods and motives behind Denial of Service attacks have changed, the fundamental goal of attacks, to deny legitimate users of some resource or service, has not. Similarly, attackers have always, and will continue to look for methods to avoid detection. The evolution in the technology of DoS attacks originates from this fundamental premise: establish a denial of service condition without getting caught. Malicious actors constantly explore new ways to leverage today's technology to meet their goals. Attackers work hard to engineer new techniques to distance themselves from the victim while amplifying the impact of their attack. Much of the evolution in DoS attacks goes hand-in-hand with the use and popularity of botnets. Botnets provide the perfect tool to help magnify the impact of an attack while distancing the attacker from the victim.

Denial of service attacks cause significant financial damage every year, making it essential to devise techniques to detect and respond to attacks quickly. Development of effective response techniques requires intimate knowledge of attack dynamics, yet little information about attacks in the wild is currently published in the research community.[13] DoS attacks are constantly evolving. The very recent DoS attacks showed extreme sophistication in attacking techniques and stealth attributes. Strict legal response, along with sophisticated defence technologies, is necessary to stop the menace.

---

[11] Are DDoS (distributed denial-of-service) attacks against the law? Graham Cluley, naked security, December 2010, nakedsecurity.sophos.com.

[12] There are numerous other stories, for example, a man was jailed in the USA who launched a DDoS attack against the Scientology website. Mitchell L Frost, 23, of Bellevue, Ohio, was given a 30 month prison sentence for a series of DDoS attacks he launched against the websites of high profile US right-wingers Bill O'Reilly, Ann Coulter and Rudy Giuliani. (See the references on internet)

[13] David Moore, Geoffrey Voelker, and Stefan Savage, 'Inferring Internet denial of service activity' in *Proceedings of the USENIX Security Symposium*, Washington, DC, USA, August 2001.USENIX.

**Direct Criminalization**

Laws penalizing DoS activities enacted in the last twelve years fall in this category. This trend specifically refers to 'denial of service' or 'denial of access'. South Africa, India and Bangladesh are good examples of states that have followed this trend. The South African legislators made their intention very clear in defining and penalizing DoS attack. Section 86(5) of the Electronic Communications and Transactions Act, 2002 provides:

> 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.

Thus under this section intention to interfere is a precondition to constitute a denial service attack. Obviously it is possible that someone, with no detailed knowledge, while experimenting with DoS tools, may initiate a DoS attack though he might not have any intention to commit such attack. Under this section such a person remains outside the gambit of law. It seems that an accused may use this 'lack of intention' as a good defence in an action for DoS attack. In an attempt to compensate this weakness the legislators have provided for provisions to penalize those who write or distribute codes or programmes to initiate a DoS attack. Section 86(3) states:

> A person who unlawfully produces, sells, offers to sell, procures for use, designs, adapts for use, distributes or possesses any device, including a computer program or a component, which is designed primarily to overcome security measures for the protection of data, or performs any of those acts with regard to a password, access code or any other similar kind of data with the intent to unlawfully utilise such item to contravene this section, is guilty of an offence.

Thus the South African law not only bans DoS attacks, it also declares illegal procurement, adaptation, design, distribution or possession of any programme that may be used in implementing a DoS attack.

The most relevant legislation to prosecute a DoS attack in Bangladesh is the Information and Communication technology Act, 2006. Section 54.(1)(f) defines a DoS attack as denying or attempting to deny access to any person authorized to access any computer, computer system or computer network by any means without permission of the owner or any other person who is in charge of a computer, computer system or computer network. As this provision does not explicitly refer to intention or knowledge, strict liability may not be ruled out. Again, it does not specifically declare possession or distribution of DoS tools illegal. Whether possessing or distributing DoS tools may be regarded as 'attempting to deny access' will remain to be seen. Criminalization of possession of DoS tools may give rise to interesting problems for investigators and law enforcers. For example, in Aaron Caffrey, Aaron was accused of launching a DoS attack against the computer system of the Port of Huston. Aaron denied the allegation and claimed that a Trojan that installed itself on his

computer launched the attack. No Trojan was found on Aaron's computer and he argued that the Trojan deleted itself and Aaron was acquitted.[14]

The DoS legal regimes of Bangladesh and India are identical as it appears that section 54.(1)(f) of the Information and Communication Technology Act, 2006 is an exact reproduction of section 43(f) of the Information Technology Act, 2000 of India.

New Zealand amended its Crimes Act of 1961[15] to define and penalize DoS attack. The Crimes Amendment Act 2003[16] repeals Part 10 of the Crimes Act 1961 and introduces a new Part 10. Under the heading of 'damaging or interfering with computer system', the substituted section 250(2)(c)(ii) defines a DoS attack. According to this provision, anyone who intentionally or recklessly, and without authorisation, knowing that he or she is not authorised, or being reckless as to whether or not he or she is authorised, causes any computer system to deny service to any authorised users, commits DoS attack.

The Canadian legislative trend falls both in direct criminalization and criminalization through willful inference of data. In 1985 Canada passed the Criminal Law Amendment Act. This amendment added Section 342.1 to the Criminal Code of Canada as well as adding Subsection (1.1) to Section 430 of the Code. The Criminal Law Improvement Act 1997 added Subsection (d) to Section 342.1(1).

The Canadian Criminal Code names an offence of mischief in relation to data that contains certain provisions in respect of denial of service to legitimate users.[17] A person will be guilty of this offence if he willfully obstructs, interrupts, or interferes with the lawful use of data.[18] Again he will be guilty of the offence if he willfully 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.[19] The newly introduced Subsection (1.1) to Section 430 of the Code reads:

> (1.1) Every one commits mischief who wilfully
>
> (a) destroys or alters data;
>
> (b) renders data meaningless, useless or ineffective;
>
> (c) obstructs, interrupts or interferes with the lawful use of data; or
>
> (d) obstructs, interrupts or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access thereto.

---

14 For more on this case see, Shelley Hill, 'Driving a Trojan Horse and Cart through the Computer Misuse Act' (2003-04) 14(5) *Computers & Law*

15 Act No. 43 of 1961.

16 Act No. 39 of 2003.

17 *Canadian Criminal Code*, s 430 (1.1)

18 *Canadian Criminal Code* s 430 (1.1) (c)

19 *Canadian Criminal Code* s 430 (1.1) (d)

Here provisions of Subsection (d) directly criminalize a DoS attacks while Subsection (c) introduces broad scope of criminalization for obstruction, interrupting or interfering with lawful use of data.

**Indirect Criminalization through Illegal Access and Diminishing Utility**

This trend does not refer to 'denial of service' explicitly rather it makes penal provision with broader ambit in a way that any type unauthorized access, both denying and non-denying access of service or to computer data, becomes an offence. Laws of the USA, Republic of Albania and Antigua and Barbuda are good examples of this trend.

The American legislation appears more advance in time than that of other countries having cyber legislation. The American law does not criminalize DoS attacks directly rather its broadly-worded provisions almost unquestionably criminalize DoS attacks.

The Computer Fraud and Abuse Act (The CFAA) prohibits a person from "knowingly caus[ing] the transmission of a program, information code, or command, and as a result of such conduct, intentionally causes damages without authorization to a protected computer."[20] Under this provision knowledge of transmission and intentional damage are two prerequisite to constitute a crime. The requisite "damage" element under the CFAA has been defined as "any impairment to the integrity or availability of data, a program, a system, or information"[21] and a "protected computer" means a computer "which is used in or affecting interstate or foreign commerce, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication."[22] The CFAA also criminalizes attempts to launch a DoS attack.[23]

The CFAA also has a civil liability component that permits "[a]ny person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunction relief." Thus the targets of the DoS attack can sue the individual(s) who were responsible for the damages incurred as a result of the attack (e.g., server downtime, costs to repair, and in some lost revenue.[24]

---

20 18 U.S.C. § 1030(a)(5)(A).

21 18 U.S.C. § 1030(e)(8).

22 18 U.S.C. § 1030(e)(2)(B).

23 18 U.S.C. § 1030(b).

24 18 U.S.C. § 1030(g). [There is a limitation that requires the damages exceed $5,000; however, some courts have liberally construed its calculation to include consultation services (e.g., IT/security persons) used to assess the extent of damage caused by the attack. Also, this provision does not require that a person ever be convicted before being sued for damages.]

The legislation of Antigua and Barbuda is a combination of broadly worded criminalization and criminalization through diminishing utility. The legislators made their intention clear in the Preamble to the Computer Misuse Act, 2006 by describing the Act as 'an Act to prohibit the unauthorized access, use of or interference to any program or data held in a computer and to a computer itself...'

Section 12.(1) of the Act provides:

> A person who without authorization does any act-
>
> (a) which causes; or
>
> (b) which he intends to cause, directly or indirectly, a degradation, failure, or other impairment of function of a computer, program, computer system, computer network or any part thereof commits an offence...

Thus this provision does not specifically refer to denial of service attacks and a plain reading of the provision may be indicative of its vagueness. But if read with the Preamble, the act of causing degradation or other impairment of a computer network becomes an act of unauthorized act of interference and the language is broad enough to include a denial of service attack as it diminishes the utility of a computer network. The Act also criminalizes production, sale, procurement for use, import, export or distribution of any device or computer programme designed r adapted for the purpose of committing a DoS attack.[25]

Republic of Albania criminalizes DoS attack under the heading of 'interference in the computer transmissions, in the Criminal Code of 1995.[26] Under article 192/b '[i]nterference, in any way, in the computer transmissions and programs, constitutes a penal contravention'. The words 'interference, in any way, in the computer transmissions' are wide enough to include, unquestionably, DoS attacks.

Perhaps the Argentine provision is wider than that of Albania. In Argentina, destroying completely or partially, erasing, altering temporarily or permanently, or in any way preventing the use of data or programs through any means, whatever the medium containing them, during the processing of an electronic communication, is an offence.[27] The act of preventing the use of data or programs during the processing of an electronic communication undoubtedly refers to a DoS attack. And if this provision is not well enough to prosecute a DoS attack, an alternative provision is provided in the same legislation which penalizes interruption or obstruction of any communication through any means.[28] The sale, distribution or dissemination of DoS tools has also been criminalized.[29]

---

25 Section 13(1)(a), the *Computer Misuse Act 2006.*

26 Law No.7895, dated 27 January 1995.

27 *National Criminal Code* (Law No. 11.179 of 1984) s183¶ 2

28 Ibid s 197.

29 *National Criminal Code* s 183 ¶3

**Ambiguous Criminalization**

The cyber legislations that had taken place before DoS attacks were in existence fall in this category. Cyber laws in some countries were taken by surprise with the advent of sophisticated DoS attacks. The legal unpreparedness forced the law enforcers to apply the existing laws to criminalize the 'future crimes' and thus to meet the circumstances.

The original United Kingdom Computer Misuse Act of 1990 (CMC) is a good example of ambiguous criminalization. The CMA came into existence because legislation intended for other purposes did not always fit the particular facts before the court. While in some cases the prosecution succeeded in obtaining a conviction[30], in many cases prosecution failed.[31] As a result of the problems in prosecuting such cases a Royal Commission was set up and following their recommendations the Computer Misuse Act was enacted.

Although, the legislation was drafted before the Internet and Internet related crime became a major concern the courts have by statutory interpretation of key words managed to apply the Act to a variety of circumstances that could not have been envisaged by the original drafters of the legislation.[32] The CMA covered three distinct offences, namely, unauthorized access to computer material[33], unauthorized access with intent to commit other offence[34] and unauthorized modification of computer material.[35]

---

30 *R v Whiteley* (1991) 93 Cr. App. R. 25, CA. [Whiteley a computer hacker was convicted of criminal damage, he gained unauthorized access to a computer network and altered data contained on discs in the system, thereby causing the computers in question to be shut down for periods of time.]

31 See for example, *R v Gold and Schifreen* [1988] 2 W.L.R. 984. [Gold and Schifreen were hackers who gained unauthorized access to the Duke of Edinburgh's computer files contained on British Telecom Prestel Gold network. They were convicted of committing an offence contrary to section 1 of the *Forgery and Counterfeiting Act 1981* (FCA) for making a false instrument. On appeal their convictions were quashed as the court said that the electronic impulses that formed the password could not be an instrument within the definition of section 8 (1)(d) of the FCA.]

32 ICF Legal Subgroup, *Reform of the Computer Misuse Act 1990*, ICF, 30th April 2003.

33 Section 1: It is an offence to cause a computer to perform any function with intent to gain unauthorized access to any programme or data held in any computer. It will be necessary to prove the access secured is unauthorized and the suspect knows this is the case. This is commonly referred to as hacking.

34 Section 2: An offence is committed as per section1 but the Section 1 offence is committed with the intention of committing an offence or facilitating the commission of an offence. The offence to be committed must carry a sentence fixed by law or carry a sentence of imprisonment of 5 years or more. Even if it is not possible to prove the intent to commit the arrestable offence the S1 offence is still committed.

35 Section 3: An offence is committed if any person does an act that causes unauthorized modification of the contents of any computer. The accused must have

At least for DoS attacks, certain provisions of the Act were in the center of confusion and controversy from the very beginning. Section 3 of the Act criminalizes unauthorized modification of the contents of any computer. The question was whether the offence of doing anything with criminal intent "which causes an unauthorised modification of the contents of any computer" covered DoS attacks. While some DoS attacks may delete or alter data in a computer system, there are DoS attacks that will not delete or change data. If the term 'modify' means to change or alter data, the latter DoS attacks are not covered by section 3.[36] Although section 3 CMA does not specifically refer to DoS attacks, some argued that its lack of precision and technology-neutral language appears to provide sufficient flexibility for such a case to be prosecuted. Some government lawyers, with supports from academics, expressed the opinion that any sort of DoS attack was covered by existing legislation. Section 3 of the CMA does not require unauthorized access to a computer system, merely unauthorized "modification of the contents of any computer". The requisite intent that accompanies this offence is to render data stored on a computer unreliable, or impair its operation. And this loophole was first exposed by DPP v Lennon,[37] the first reported criminal case in the U.K. concerning DoS attacks.

David Lennon, a UK teenager of 18 and a disgruntled employee,[38] overwhelmed an email server of his former employee by sending over five million messages. The massive volume of email disabled the office server.[39] The Crown Prosecution Service brought criminal action against David Lennon under section 3 of the Computer Misuse Act, 1990. The CMA explicitly outlaws the 'unauthorised access' and 'unauthorised modification' of computer material. Lennon's lawyer had successfully argued that the purpose of the company's server was to receive emails, and therefore the company had consented to the receipt of emails and their consequent modifications in data. District Judge Kenneth Grant, who ruled that an email bomb did not violate the CMA because email servers were set up to receive emails. As such, each individual email could be ruled to make an 'authorised modification' to the server. District Judge

---

the intent to cause the modification and be aware the modification has not been authorized. There is no necessity for any unauthorized access to have been obtained during the commission of this offence. This offence is used instead of *The Criminal Damage Act 1971*, as it is not possible to criminally damage something that is not tangible.

36 Hill, above n 14

37 [2005] EWCA Crim 2150.

38 Lennon was employed by Domestic & General Group PLC (D&G) for three months until he was dismissed in December 2003.

39 To bombard D&G server with emails, Lennon downloaded a mail bombing program from the internet, the Avalanche v3.6, and set the Avalanche to mail until it stopped. The emails also spoofed the name of Betty Rhodes, D&G's Human Resources manager, therefore they appeared to originate from Ms Rhodes, rather than from Lennon.

Kenneth Grant concluded that sending emails is an authorized act and that Lennon had no case to answer, so no trial took place. The Director of Public Prosecutions (DPP) appealed against this ruling, that there was no case to answer. Lord Justice Keene and Justice Jack disagreed with Judges Grant's reasoning, allowed the appeal and remitted the case to the district judge to continue the hearing, stating that the district judge had erred in that ruling by "rather miss[ing] the reality of the situation by wrongfully finding that there was no case to answer". The unproblematic question the court had to answer was whether the addition to the data on D&G's server arising from the receipt of emails sent by Lennon was unauthorized within the meaning of s.17(8). Since Lennon was not the person entitled to determine whether or not such "modification" should be made, requirement of s.17(8a) was satisfied. Then, the question was whether Lennon "had consent to the modification from any person who was so entitled" according to s. 17(8b). The appeal court answered in the negative. Lennon eventually pleaded guilty and, in 2006, he was sentenced to two months' curfew with an electronic tag. But by that time, amendments to the 1990 legislation were already included in the Police and Justice bill.

The initial decision on Magistrates Court gave rise to heated debate and arguments that led to renewed calls for the CMA to be updated so as to deal with changes in technology and use. The first attempt to amend the Computer Misuse Act, to put the illegality of DoS attacks beyond doubt, was a Private Member's Bill to amend the Act was introduced by the Earl of Northesk in 2002, but like most Private Members' Bills, it failed to become law. In June 2004, the All Party Internet Group made an inquiry into the Act and the inquiry highlighted the possibility of a loophole for DoS like attacks. One of the key recommendations of this inquiry was that an explicit 'denial of service' offence of impairing access to data should be introduced. Although Ten Minute Rule Motions, like all Private Member's Bills, are very unlikely to become law, Derek Wyatt,[40] the Labour MP for Sittingbourne and Sheppey made a 10-minute pitch to Parliament (House of Commons) in March 2005 for changes to the CMA. In his speech he observed:

> Although high-profile DDoS attacks have been made against e-commerce and, especially, gambling sites, the UK Government and the country's critical infrastructure could also be attacked. It is essential for a law to be in place to make prosecution possible when offences are committed, because that will send the strong and unambiguous message that e-crime is treated with the utmost seriousness. International co-operation is also the key. Increasing sentences for section 1 offences to two years will create an extraditable offence, and bring the law into line with the European cybercrime convention.[41]

---

40 At that time he was the chair of All Party Internet Group (APIG).

41 Out-law.com, Parliament hears 10 minutes on Denial of Service law, http://www.out-law.com/page-5508, retrieved on 1 June 2013.

Changes were made to the Computer Misuse Act in 2006 but they were not made live at the time. In October 2007 they were adopted in Scotland, but not in England and Wales. The Statutory Instrument to bring them into force was finally passed on 24th September and the changes came into effect for England and Wales on 1st October 2008. The Police and Justice Act 2006 (s.36) amended s.3 of CMA criminalizing DoS attacks, punishable by a maximum of 10 years' imprisonment. This amendment brought the U.K. in compliance with A.5 of the Council of Europe Cybercrime Convention and A.3 of the E.U. Framework decision on Attacks against Information Systems.

The Philippine legislation defines hacking in its widest possible ambit. Under Electronic Commerce Act, 2000, hacking or cracking refers to unauthorized access into or interference in a computer system/server or information and communication system; or any access in order to corrupt, alter, steal, or destroy using a computer or other similar information and communication devices, without the knowledge and consent of the owner of the computer or information and communications system, including the introduction of computer viruses and the like, resulting in the corruption, destruction, alteration, theft or loss of electronic data messages or electronic document. Theoretically it is possible to incorporate a wide variety of cybercrimes within the heading of hacking and apparently such incorporation seems alright before actual application of the law in the real world. While this definition of hacking may well include a varied spectrum of cybercrimes, it will not include a DoS attack. The reasons are twofold: firstly, under this definition access or introduction of computer viruses is essential to constitute a crime and a devastating DoS attack does not need any access. Secondly, a DoS attacker will deploy malicious code or virus or BOTNET to launch an attack but the qualifier 'resulting in the corruption, destruction, alteration, theft or loss of electronic data messages or electronic document' eliminates any possibility of successfully prosecuting a DoS attack as most DoS attacks will not result in the conditions prescribed in the qualifier. This provision is yet to be tested in a court of law in the Philippines.

**Conclusion**

Many software commonly used to run and maintain internet infrastructures and access and manipulate internet benefits may contain severe design or coding flaws that make themselves vulnerable to DoS attacks. DoS attack history indicates that many hosts used as DoS attack agents are subverted[42] through well-known vulnerabilities in commonly used software.[43] Insecure design of common web browsers and email software are exacerbating the problem. Allen Householder et al observe:[44]

---

42 The Code Red worm and Power malicious code are two well-known examples.

43 Allen Householder, Art Manion, Linda Pesante, and George M. Weaver In collaboration with Rob Thomas, 'Managing the Threat of Denial-of-Service Attacks' ( CERT Coordination Center, Carnegie Mellon University, 2001) 22-23.

44 Ibid 23.

> A significant number of these vulnerabilities allow attackers to gain root/or administrator access from a remote location. Attackers gain complete control over the computer and may use it to suit their purpose, which may be to use it as a DDoS agent. Current economic pressures lead vendors to focus on achieving a fast time to market rather than on designing secure networks and applications. Without some financial (or legal) incentive to behave more securely, developers will continue to produce vulnerable products.

The current legal trend does not seem to be ready to penalize the developers of these vulnerable products, though developers of the DoS tools may be prosecuted, albeit minimally.

Many states are reluctant to legislate or amend existing laws to cope with the DoS menace. Some do not consider it as a serious threat and some think that existing legislation is sufficient to prosecute DoS attacks if the investigators are equipped with advanced technologies and legal skills. Ahmad Kamal observes:

> There are many who take the view that the existing legislation already covers denial of service attacks without any need for amendments, and that the better preparation of cases nd more sophisticated evidence gathering techniques, rather than legislative change, hold the key to combating the rising wave of cyber-crime.[45]

Sole reliance on technology has its own problem. Providing protection against some types of DoS and especially DDoS attacks can be technically challenging. It is often hard to distinguish legitimate from illegitimate activity, which means that genuine traffic can be discarded through protective measures. The lessons learned from the North American and European experiences remind us that technological sophistication is not the lone way forward to successfully prosecute DoS attacks, advanced technology must be complemented by new or amending laws that will define DoS activities either specifically or by introducing broadly-worded provisions that will clearly and unambiguously include, among others, DoS activities.

---

[45] Ahmad Kamal, *The Law of Cyber-Space: an Invitation to the Table of Negotiations* (United Nations Institute for Training and Research, Geneva, 2005) 41-2.

**Table A: DoS Criminalization Trends**

| State | Criminalization Category | *Mens rea* | Criminalization of DoS Tools | Legislation | Punishment |
|---|---|---|---|---|---|
| Bangladesh | Direct criminalization | without permission of the owner or any other person who is in charge of a computer, computer system or computer network | No | Information and Communication Technology Act, 2006 | Imprisonment for a term not exceeding ten years or a fine not exceeding Taka ten lac or both. |
| India | Direct criminalization | without permission of the owner or any other person who is in charge of a computer, computer system or computer network | No | Information Technology Act, 2000 | Damages by way of compensation not exceeding one crore rupees to the affected person. |
| Republic of the Philippines | Ambiguous | without the knowledge and consent of the owner of the computer or information and communications system | No | Electronic Commerce Act, 2000 | A minimum fine of one hundred thousand pesos and a maximum commensurate to the damage incurred and a mandatory imprisonment of six months to |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | three years. |
| New Zealand | Direct criminalization | intention or recklessness, knowledge of non-authorisation | No | Crimes Act of 1961 as amended by the Crimes Amendment Act 2003 | Imprisonment for a term not exceeding 7 years. |
| South Africa | Direct criminalization | intention | Yes | Electronic Communications and Transactions Act, 2002 | A fine or imprisonment for a period not exceeding five years. |
| USA | Broadly worded provision | knowledge of transmission and intentional damage | No | Computer Fraud and Abuse Act (18 USC 1030) | A fine under this title or imprisonment for not more than ten years. |
| Canada | Direct criminalization and Broadly worded provision | willful action | No | Criminal Code of Canada | Punishment provided for mischief. |
| Argentina | Broadly worded provision | strict liability | Yes | National Criminal Code | Imprisonment of a term not less than one month nor more than two years. (2nd Para, Section 183); imprisonment for a term of not less than |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | six months nor more than two years. (Section 197). |
| Antigua and Barbuda | Broadly worded provision | Without authorization, strict, actual act is not necessary if intention can be proved | Yes | Compute r Misuse Act, 2006 | A fine of fifty thousand dollars and to imprisonme nt for ten years or to both. |
| Republic of Albania | Broadly worded provision | strict liability | No | Criminal Code of Republic of Albania, 1995 | A fine or imprisonme nt up to three years when the alleged brings about serious consequenc es, imprisonme nt up to seven years. |
| UK | Broadly worded provision | non-authorization | No | Compute r Misuse Act 1990 | Imprisonm ent for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both. |