DoS Criminalization: Impact of Budapest Convention on Domestic Legislation

Quazi MH Supan*

(I)

Dealing with DoS and DDoS attacks is no easy task. In the recent past the endeavor in mitigating and preventing these attacks was primarily focused on technological aspects and measures. Various institutional policy documents, assessment studies and risk handling manuals, both governmental and non-governmental, rarely made reference to legal measures. This phenomenon explains why these institutions and enterprises collectively failed to form a pressure group to motivate the lawmakers to put robust anti-cybercrimes laws in place. Even where there were cyber legislations in place, DoS attacks continued to remain outside the grip of law and this was mostly due to flawed or ambiguous definitions of DoS activity. Heavy reliance on technological solutions is evident in many studies. To quote from one those studies:

> To mitigate the risks of DoS and DDoS attacks, a best-practice approach is required that includes an overarching strategy combined with operational and technical measures. Processes, procedures, software and hardware can be put in place that will protect systems prior to attack, detect malicious activity as it occurs and support the organisation in reacting appropriately as required. As a result of the nature of DoS attacks, it is often the case that strong reactive mechanisms are the best form of defence.[1]

The DoS umbrella is very broad and may cover a massive range of attacks and this impairs an organization's ability to know when it is under attack. In the DoS case, the effects are likely to be immediate and result in a system or subsystem becoming unavailable. A naive DoS attack is relatively easier to identify than a Distributed DoS attack. The symptoms of a DDoS attack may take longer to appear and are usually apparent in slow access times or service unavailability. A DDoS attack is also very difficult to detect as in this case multiple hosts (sometimes at different locations) are compromised to exhaust the resources of the victim server by the same group of crackers. Each connection established by the compromised machines behaves exactly like a normal user making a legitimate request although aggregated requests from these compromised machines can overwhelm the capacity the victim server can sustain.[2] This may explain an organization's over-reliance over technological defence against DoS attacks.

The legislative trends of the first decade of the present century indicate many states' reluctance to legislate or amend existing laws to cope with the DoS menace. Two different factors may be identified for this phenomenon, firstly, some states consider it as a rare and less serious threat and secondly, legislators in many countries think that existing legislation

---

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

1 Trusted Information Sharing Network for Critical Infrastructure Protection, Denial of Service / Distributed Denial of Service: Managing Dos Attacks, TISN, Australia, 2006, p. 6.

2 Dong Hyuk Woo and HsienHsin S. Lee, Analyzing Performance Vulnerability due to Resource DenialofService Attack on Chip Multiprocessors, School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, 2007, p.2.

is sufficient to prosecute DoS attacks if the investigators are equipped with advanced technologies and legal skills. The combination of these two factors led many to believe that 'the existing legislation already covers denial of service attacks without any need for amendments'[3] and 'the better preparation of cases and more sophisticated evidence gathering techniques, rather than legislative change, hold the key to combating the rising wave of cyber-crime'.[4]

Technology alone cannot always solve the problems associated with DoS attacks as 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.

While the importance of 'a combination of the use of intrusion detections systems, logging and monitoring systems, and honey-pots' to significantly increase an organization's ability to accurately detect and identify DoS and DDoS attacks cannot be undermined, various legal responses, including inflicting criminal, tortuous and contractual liability on the attackers, are coming to front to complement technological approaches in fight against the DoS menace.

In the last one decade we have seen a systematic effort to enact comprehensive laws relating to cybercrime and develop national cybercrime investigating capabilities. These initiatives and efforts were spearheaded by international and regional organizations by adopting various texts in the form of treaty, resolution, declaration and guidelines. These texts[5] constitute a unique and comprehensive model for cybercrime legislation and many countries all over the world have relied on this model in their domestic cybercrime legislations. Among other common initiatives, these texts share a common emphasis on prevention and penalization of DoS and DoS-like cybercrimes intended to render certain online services unavailable and undoubtedly such emphasis was first supplied by the Budapest Convention. The current global trend indicates that countries are using the Convention as a guideline for the development of cybercrime legislation.[6] For a good number of countries the Convention may be seen as a model law as their newly adopted

---

3 Ahmad Kamal, The Law of Cyber-Space: an Invitation to the Table of Negotiations, United Nations Institute for Training and Research, Geneva, 2005, pp.41-2.

4 Ibid.

5 Draft African Union Convention, COMESA Draft Model Bill, Commonwealth Model Law, Council of Europe Cybercrime Convention, ECOWAS Draft Directive, EU Decision on Attacks against Information Systems, EU Directive Proposal on Attacks against Information Systems, ITU/CARICOM/CTU Model Legislative Texts, League of Arab States Convention, League of Arab States Model Law, and Commonwealth of Independent States Agreement.

6 For example: Argentina, Brazil, Colombia, Egypt, India, Indonesia, Morocco, Nigeria, Pakistan, Philippines, Botswana, Dominican Republic,Sri Lanka and most European countries.

cybercrime legislations are uniquely in line with the convention.[7] This article aims to examine the Convention's impact on domestic DoS legislation and for this purpose it will examine DoS legislations of 25 countries, among them 22 have ratified/acceded to the Budapest Convention and the rest 3 are signatory states.

(II)

Denial of service (DoS) attacks on cyber-resources are complex problems that are difficult to completely define, characterize, and mitigate. DoS attacks involve a process, not a single event, that comprises multiple activities through time and space from its origin to its victim. Recent evidence suggests that perpetrators are continuing develop and explore innovative ways to enhance the effect of their attacks.[8]

A Denial of Service (DoS) attack is a type of attack focused on disrupting availability. Such an attack can take many shapes, ranging from an attack on the physical IT environment, to the overloading of network connection capacity, or through exploiting application weaknesses.A simple definition of Denial of Service is an attack designed to render a computer or network incapable of providing normal services. A Distributed Denial of Service attack uses multiple computers to launch a coordinated DoS attack against one or more targets.[9]Denial-of-Service is a common network attack method in which a malicious user intentionally makes a flood of requests to a targeted Internet service, rendering the victim server unavailable to legitimate subscribers.[10]

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 organization'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 through a revolving door at the same time'.[11]More sophisticated DoS attacks may include other variants like DDoS[12] and DDoS.[13]

---

7 For Example: USA, UK, Italy and Australia.

8 Timothy Draelos, Mark Torgerson, Michael Berg, Philip Campbell, David Duggan, Brian Van Leeuwen, William Young and Mary Young, Distributed Denial-of-Service Characterization. Networked Systems Survivability and Assurance Department, Sandia National Laboratories, Albuquerque, NM, 2003.

9 See Table A.

10 Dong Hyuk Woo and HsienHsin S. Lee, Analyzing Performance Vulnerability due to Resource DenialofService Attack on Chip Multiprocessors, School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, 2007, p.2.

11 Graham Cluley, Naked Security, nakedsecurity.sophos.com, December 2010.

12 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.

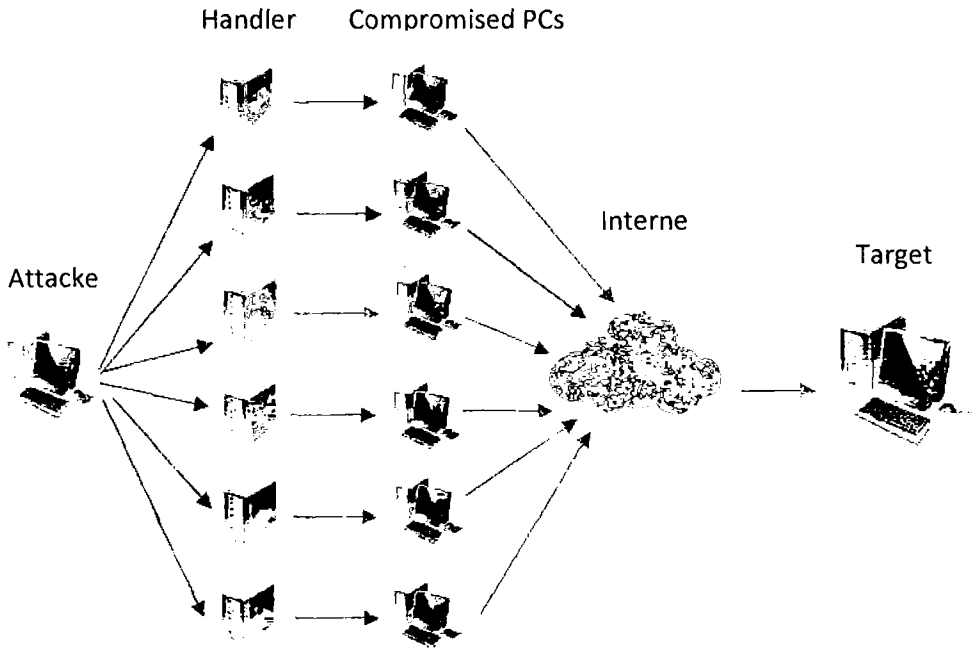
13 Distributed Reflector Denial of Service Attack: a DDoS attack that is amplified by a reflector. A reflector is typically an uncompromised device that unwittingly participates in a DDoS attack. Due to the design of the attack, it sends several times more traffic to the victim than what was sent to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

Kevin Mandia et al categorized DoS attacks in the following manner:[14]

> 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 authorised 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.[15]

Table A: Distributed Denial of Service Attack



[14] evin Mandia and Chris Prosise, Incident Response: Investigating Computer Crime, Osborne/McGraw-Hill, Berkeley, 2001, pp. 360-361.

[15] evin 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.

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. 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.[16]

The perpetrators may even penetrate Wi-Fi networks with DoS attack tools.[17]One does not have to be an expert to initiate a DoS attack since attack tools are available free of cost.[18] 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.[19]According to TISN, Internet and other network infrastructure components are at risk of DoS for two primary reasons:[20]

1. Resources such as bandwidth, processing power, and storage capacities are not unlimited and so DoS attacks target these resources in order to disrupt systems and networks.
2. Internet security is highly interdependent and the weakest link in the chain may be controlled by someone else thus taking away the ability to be self-reliant.

---

16 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.]

17 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 in International Journal of Law and Information Technology Vol. 16 No. 3, Oxford University Press, 2008, pp. 205-41 at pp.227.

18 For discussions and analysis of various DoS tools, see Fafinski, S., Access denied: computer misuse in an era of technological change", (2006) Journal of Criminal Law 70(5), 424-442; Kon, G., Church, P., A denial of service but not a denial of justice, (2006) Computer Law & Security Report 22, 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.

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

20 Trusted Information Sharing Network for Critical Infrastructure Protection, Denial of Service / Distributed Denial of Service: Managing Dos Attacks, TISN, Australia, 2006, p.5.

Malicious hackers can commandeer thousands of computers around the world, and order them to deluge a website with traffic - effectively clogging 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).[21] 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.[22] 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.

Many motivations exist for DoS attacks. They include financial gain through damaging a competitor's brand or by using extortion, raising one's profile in the hacker community, or even simple boredom. Recently, politically and revenge driven attacks designed to disrupt an organization's—or indeed a country's—operations have become more prevalent. They may also include political conflicts, economic benefits for competitors, curiosity of some computer geeks and even cyber terrorism.[23]Denial of service attacks cause significant financial damage every year, making it essential to devise techniques to detect and respond to attacks quickly.[24]The costs of DoS attacks to critical infrastructure organizations can be

---

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

22 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)

23 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, pp. 1-2.

24 According to Laudon and Laudon, the most economically damaging kinds of computer crime are denial-of-service attacks, where customer orders might be rerouted to another supplier. See Laudon, K.C. and Laudon, J.P., Management Information Systems: Managing the Digital Fin Eleventh Edition, Pearson Education, London, UK, 2010. See also Petter Gottschalk, Policing Cyber Crime, Petter Gottschalk & Venus Publishing ApS, 2010, p. 9.

extremely. A respondent to the 2005 Australian Computer Crime and Security Survey reported a single-incident loss of $8 million arising from a DoS attack.[25] For many critical infrastructure companies, a significant and prolonged period of system unavailability could result in losses an order of magnitude higher than this.

In addition to the potential for significant financial loss, the make-up of some critical infrastructure organizations means that the impact of downtime may not be limited to lost revenue and goodwill but will extend to social and human costs through an inability to deliver essential services. In extreme cases, this could indirectly include a loss of life — such as through a DoS impact on the health system, or delays in emergency service dispatch. Other costs may include those suffered due to litigation and contractual violations, stock price fluctuations and even intangibles such as decreased morale and loss of reputation.

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.[26]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.

(III)

In one of its communications to the Council and the European Parliament, the Commission emphasized on the possible harmonization of substantive private law, and in particular contract law of its member states.[27] This communication was an articulated, systematic and timely response to the then intensified discussion on the issue.[28] While exploring some important substantive private contract law issues, the commission highlighted the possibilities offered by the Internet for electronic commerce and other technical developments that 'have made it easier for economic actors to conclude transactions over long distances.'[29] This communication may be regarded as a starting point raising and highlighting the possible legal issues concerning internet contracts and realizing its importance, this Communication was included in the Commission communication on E-Commerce and Financial Services within the policy area of ensuring coherence in the legislative framework for financial services.[30]Several later communications, reports and Council decisions deal with creating a safer information society and trustworthy e-commerce environment by, among others, tackling cybercrimes and in several instances

---

25 Meiring de Villiers (2007), Distributed Denial of Service: Law, Technology & Policy. Sydney: University of New South Wales Faculty of Law Research Series, Paper no 3.

26 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.

27 Communication From The Commission To The Council And The European Parliament On European Contract Law Brussels, 11.07.2001 COM(2001) 398 final.

28 See for example, Ole Lando and Hugh Beale (eds.), *Principles of European Contract Law Parts I and II*, Kluwer Law International, 2000; Hartkamp, Hesselink, Hondius, Joustra, Perron (eds.), *Towards a European Civil Code*, Kluwer Law International, 1998.

29 Supra note 28, paragraph 25.

30 COM(2001) 66 final, 7.2.2001, p. 11.

much emphasis has been put on the significance of defining and penalizing DoS attacks. The Council of Europe's*Proposal for a Council Framework Decision on attacks against information systems*[31] is a prominent example of this emphasis. Realizing that '[a]ttacks against information systems constitute a threat to the achievement of a safer Information Society and an Area of Freedom, Security and Justice, and therefore require a response',[32] the Council of Europe proposed this Framework Decision on approximation of criminal law in the area of attacks against information systems. Earlier the Commission of the European Communities made an important communication to the Council, the European Parliament, the European Economic and Social Committee and the Committee of The Regions - *Network and Information Security: Proposal for A European Policy Approach.*[33] This communication was the European Commission's response to the Stockholm European Council on 23-24 March 2001 request to develop a comprehensive strategy on security of electronic networks including practical implementing action. In setting up the generic security requirements of networks and information systems, the Commission proposed four interrelated characteristics: availability, authentication, integrity and confidentiality. The European, and later global, concern on DoS activities could be felt in Commission's understanding of availability:

> **Availability** – means that data is *accessible* and services are operational, despite possible disruptive events such as power supply cuts, natural disasters, accidents or *attacks*. This is particularly vital in contexts where communication network failures can cause breakdowns in other critical networks such as air transport or power supply. [Italics mine]

Now we know that there are certain attacks that are capable of making data inaccessible to legitimate users meaning denial of service. In those early days of DoS attacks the Commission intriguingly thought of '[c]ompanies relying on the network for sales or to organise delivery of supplies can be paralysed by a denial of service attack.' (p9) The Commission defined network and information security as:

> ...the ability of a network or an information system to resist, at a given level of confidence, accidental events or malicious actions that compromise the *availability*, authenticity, integrity and confidentiality of stored or transmitted *data* and the related *services* offered by or *accessible* via these networks and systems. . [Italics mine]

In order to lay the basis for the establishment of a policy framework to improve security, the Commission in its security threats overview specified six types of security risks: interception of communications, unauthorised access into computers and computer networks, network disruption, execution of malicious software that modifies or destroys data, malicious misrepresentation, and environmental and unintentional events. The Commission identified flooding and denial of service attacks as a network disruption risk as 'these forms of attack disrupt the network by overloading it with artificial messages which deny or reduce legitimate access.'

In its communication Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime[34]the European

---

31 Brussels, 19.04.2002 COM (2002) 173 final.

32 Brussels, 19.04.2002 COM (2002) 173 final, p. 2.

33 Brussels, 6.6.2001 COM (2001) 298 final.

34 Brussels, 26.1.2001, COM (2000) 890 final.

Commission made certain significant legislative proposals to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions. Among those proposals one was to further approximate substantive criminal law in the area of high-tech crime. This will include offences related to hacking and denial of service attacks.The Council of Europe Convention on Cybercrime (2001)[35]is an outcome of concerted efforts of all these years. The treaty is a historic milestone in the combat against cybercrime. The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception. Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation.[36]

Table B : Budapest Convention provisions covering DOS and DDOS attacks

Provisions	Relevance
Illegal access[37]	DOS and DDOS attacks may access a computer system.
Data interference[38]	DOS and DDOS attacks may damage, delete, deteriorate, alter or suppress computer data.
System interference[39]	The objective of a DOS or DDOS attack is precisely to seriously hinder the functioning of a computer system.

35 The Convention was opened for signature in Budapest on November 23, 2011 and entered into force on July 1, 2004 after satisfying the conditions of 5 ratifications including at least 3 member States of the Council of Europe.

36 4th Preambular paragraph: Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, *inter alia,* by adopting appropriate legislation and fostering international co-operation.

37 **Article 2 – Illegal access**

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 access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

38 **Article 4 – Data interference**

1 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 damaging, deletion, deterioration, alteration or suppression of computer data without right.

2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

39 **Article 5 – System interference**

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 suppressing computer data.

Attempt, aiding and abetting[40]	DOS and DDOS attacks may be used to attempt or to aid or abet several crimes specified in the treaty (such as Computer-related forgery, Article 7; Computer-related fraud, Article 8; Offences related to child pornography, Article 9; and Offences related to infringements of copyright and related rights, Article 10).
Sanctions[41]	DOS and DDOS attacks may be dangerous in many ways, especially when they are directed against systems that are crucial to daily life - for example, if banking or hospital systems become unavailable. A Party may foresee in its domestic law a sanction that is unsuitably lenient for DOS and DDOS attacks, and it may not permit the consideration of aggravated circumstances or of attempt, aiding or abetting. This may mean that Parties need to consider amendments to their domestic law. Parties should ensure, pursuant to Article 13, that criminal offences related to such attacks "are punishable by effective, proportionate and dissuasive sanctions, which include the deprivation of liberty". For legal persons this may include criminal or non-criminal sanctions, including monetary sanctions. Parties may also consider aggravating circumstances, for example, if DOS or DDOS attacks affect a significant number of systems or cause considerable damage, including deaths or physical injuries, or damage to critical infrastructure.

[40] **Article 11 – Attempt and aiding or abetting**

1 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, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.

2 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, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.

3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

[41] **Article 13 – Sanctions and measures**

1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.

2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

(IV)

The first legal response to DoS activities was criminalization and penalization of DoS attacks and such response had been seen before the adoption of the Budapest Convention, although the bulk of the criminalization of DoS activities could be seen since the early tens of the 21st century. Such criminalization has been categorized in three distinctive trends, namely, explicit criminalization, criminalization through broadly-worded provisions of illegal access and diminishing utility and ambiguous criminalization.[42]

Portugal's principal cybercrime law, i.e., Law No. 109/2009 is a good example of explicitcriminalization as it clearly defines a DoS attack. It is able to prosecute '[a]ny person who, without legal permission or without being authorized to do soby the owner, other right holder of the system or part thereof, prevents, stops, orseverely disrupts the operation of a computer system through the introduction,transmission, damage, alteration, deletion, preventing access or removal ofprograms or other computer data or any other form of interference in thecomputer system.'[43] Here both the prerequisites of DoS attack – illegal access (without legal permission or without being authorised to do soby the owner, other right holder of the system or part thereof) and denial of access (preventing access) – are present. Croatian law goes further ahead by using a combination of illegal activities like 'hindering' and 'rendering unusable or inaccessible'. Paragraphs 2 and 3 of Article 223 read as follows:

> (2) Whoever renders unusable or hinders the work or the use of computer systems, computer programs or electronic data and communication shall be punished by a fine or by imprisonment not exceeding three years.
>
> (3) Whoever damages, alters, deletes, destroys or in some other way renders unusable or inaccessible the electronic data or computer programs of another shall be punished by a fine or by imprisonment not exceeding three years.

Thus a willing prosecutor can seek help from both these provisions to prosecute a DoS attack. The law of Romania is identical as it declares illegal '[t]he act of causing serious hindering, without right, of the functioning of acomputer system, by inputting, transmitting, altering, deleting or deterioratingcomputer data or by restricting the access to such data.' The phrase 'restricting the access' takes away any doubt about the intention of the legislators.

The terms 'unusable' and 'inaccessible' are not synonymous in DoS terminology. A computer system may be in a usable state and still it may remain inaccessible. For this reason Armenia, Montenegro, Germany and Czech Republic will have to rely on broader analogy of their legal provisions to successfully prosecute a DoS attack as the nearest illegal activity that resembles a DoS attack in these laws is unauthorised act that renders a computer system unusable or useless. FYROM's law penalizes any act that 'will make unusable a computer data or program or device for maintenance of the computer system, or will make impossible or more difficult the use of a computer system, data or program or the computer communication.' Here the legislators have used three variations of 'use':

---

[42] See, Quazi MH Supan, *DoS Criminalization: Impact of the Budapest Convention on Domestic Legislation*, accepted for publication in the Dhaka University Law Journal, Volume 23, No. 2, December 2012.

[43] Article 5, Law No. 109/2009.

'unusable', 'impossible to use' and 'more difficult to use', albeit doubt remains regarding the future success of these provisions to prosecute a DoS attack. Albania and Cyprus rely on 'hindering of computer system'. Republic of Albania criminalizes DoS attack by under the heading of 'interference in the computer transmissions, in the Criminal Code of 1995.[44] 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. Italy, Australia and Finland put emphasis on 'interference with a computer system'. Ukraine, Lithuania, Bulgaria and France do not have any DoS legislation in place.

Argentina, neither a party nor a signatory to the Budapest Convention, has wider provisionthan 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.[45] 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.[46] The sale, distribution or dissemination of DoS tools has also been criminalized.[47]

It is interesting to explore that states that are neither parties nor signatories to the Convention have more explicit law in place, for example Bangladesh and India.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 authorised 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.[48] 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.

---

44 Law No.7895, dated 27 January 1995.

45 Second paragraph of Section 183 of the National Criminal Code (Law No. 11.179 of 1984).

46 Ibid. Section 197.

47 Third paragraph of Section 183 of the National Criminal Code.

48 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. For more on this case see, Shelley Hill, Driving a Trojan Horse and Cart through the Computer Misuse Act in Computers & Law Vol. 14 Issue 5 (December 2003/January 2004).

New Zealand amended its Crimes Act of 1961[49] to define and penalize DoS attack. The Crimes Amendment Act 2003[50] 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(1)(c)(i) 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 law of South Africa, a signatory state to the Convention, directly criminalizes DoS attacks. 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. The legislators have attempted to take away this weakness by penalizing 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 Canadian law attempts to criminalize DoS activities through willful inference of data. 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.[51] A person will be guilty of this offence if he willfully obstructs, interrupts, or interferes with the lawful use of data.[52] 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.[53]

---

49 Act No. 43 of 1961.

50 Act No. 39 of 2003.

51 Section 430 (1.1) of the Canadian Criminal Code.

52 Section 430 (1.1) (c) of the Canadian Criminal Code.

53 Section 430 (1.1) (d) of the Canadian Criminal Code.

The American legislation was capable of efficiently prosecuting a DoS attack much before the adoption of the Budapest Convention. 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."[54] 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"[55] 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."[56] The CFAA also criminalizes attempts to launch a DoS attack.[57]

Most of the examined legislations contain provisions for prosecuting misuse of devices with a variety of meanings of 'misuse' and 'devices'. There are certain activities, if accompanied by required *mensrea*, will constitute 'misuse'. Such activities include production, possession, selling, procurement for use, distribution, making available, import, circulation, dissemination, offer, and even carrying. Devices may include hardware or software or both. Laws of Cyprus, Czech Republic, UK, Slovakia and Turkey do not provide for any explicit provisions to deal with misuse of devices, rather they supply very remote provisions which may or may not be able to successfully prosecute any misuse of device activity.

Table C: 'Misuse' Activities and Devices

States	Misuse activities	devices
Albania[58]	production, possession, selling, procurement for use, distribution or otherwise making available, use	a device, including a computer programme, a computer password, access code or other similar data
Armenia[59]	development and manufacture	special hardware or software, special viruses

54 18 U.S.C. § 1030(a)(5)(A).

55 18 U.S.C. § 1030(e)(8).

56 18 U.S.C. § 1030(e)(2)(B).

57 18 U.S.C. § 1030(b). 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. See 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.]

58 Article 293/d, Law no. 9918, dated 19.05.2008, on electronic communications.

59 Article 255 of the Armenian Criminal Code.

Austria[60]	production, introduction, distribution, sale or otherwise making accessible	computer program or a comparable equipment, computer password, an access code or comparable data
Bulgaria[61]	circulation	computer or system passwords
Croatia[62]	production, procurement, selling, possession or making available	special devices, equipment, computer programs and electronic data created or adapted
Cyprus[63]	remote provisions	-
Czech Republic[64]	remote provisions	-
Estonia[65]	preparing, possession, dissemination or making available	a device, program, password, protective code or other data
Finland[66]	possession, import, manufacture, selling or otherwise disseminating or making available	a device or computer program or set of programming instructions
France[67]	import, possession, offering, transferring or making available	any equipment, instrument, computer programme or information created or specially adapted
FYROM[68]	production, procurement, selling, spreading possession or making available	special devices, means, computer password, viruses, access code and similar data

60 Section 126c of the Austrian Penal Code as amended by the Penal Law Amending Act, 2002 (Strafrechtsänderungsgesetz 2002, Federal Law Gazette I No. 134/2002; mainly entered into force on 1st October 2002).

61 Article 319e of the Bulgarian Penal Code.

62 Criminal Law, Article 223, paragraph 6 and 7 (OG 105/04).

63 Articles 6 and 7, Cyprus Law No. 22 (III) 04.

64 Criminal Code No 140/1961 Coll. – subject to re-enactment

65 Penal Code, Article 216.

66 Penal Code, Section 9a.

67 Article 323-3-1 of the French Criminal Code.

68 Article 251 of the Macedonian Criminal Code.

Germany[69]	producing, acquiring, selling, supplying, disseminating or making otherwise accessible	passwords or other security codes, software
Italy[70]	detention and diffusion	device or programs
Lithuania[71]	possession, production, carrying, selling or disseminating	devices, computer programme, passwords, access codes and other similar data
Montenegro[72]	making and planting	computer virus
Portugal[73]	import, distribution, production, holding, selling, or otherwise disseminating	any device that allows access, software, programs, a set of executable instructions, code or other computer data
Romania[74]	production, sale, possession,import, distribution or making available	a device or a computer program designed or adapted, a password, access code or other such computer data
Serbia[75]	making, introducing	computer virus, equipment and devices
Slovakia[76]	remote provisions: interference with the technical or program equipment of a computer	-
Ukraine[77]	production, distribution, sale, use	software and technical means
UK[78]	remote provisions	-

[69] German Criminal Code (Strafgesetzbuch), 2009 ("StGB"), Section 202c.

[70] Article 615-quater, quinquies c.p.

[71] Article 198-2, Lithuanian Criminal Code.

[72] Section 28 of the Criminal Code of Montenegro, Article 351 - Producing and Planting Computer Viruses.

[73] Law No. 109/2009 (15th of September), Articles 3-7.

[74] Articles 42-46 of Romania Law no 161/2003.

[75] Article 300 paragraphs 1, 2 and 3 and article 302 1 and 2 of CRRS.

[76] Section 247 (1) c of the Criminal Code Act no 300/2005 Coll.

[77] Article 361-1 of the Criminal Code of Ukraine (with amendments of June 5, 2003).

[78] Article 3(2/a, 6) of CMA 1990.

Australia[79]	manufacture, import, distribution, offer, providing, communicating	device
Turkey[80]	remote provisions	-

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 unauthorised 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 unauthorised 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 or adapted for the purpose of committing a DoS attack.[81]

The DoS legislative scenario in the UK can explain how the Budapest Convention can have a real impact on domestic legislation if accompanied by the political will of the state. The original United Kingdom Computer Misuse Act of 1990 (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[82], in many cases prosecution failed.[83] 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.

---

[79] Section 132 APD of the Copyright Act, 1968. See also Article 478.3(1) of Criminal Code Act, 1995 (Act No.12 of 1995) of Australia.

[80] Article 244, paragraph 1, Turkish Penal Code no 5237/2005.

[81] Section 13.(1)(a), the Computer Misuse Act, 2006.

[82] R v Whiteley (1991) 93 Cr. App. R. 25, CA. [Whiteley a computer hacker was convicted of criminal damage, he gained unauthorised 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.]

[83] See for example, R v Gold and Schifreen [1988] 2 W.L.R. 984. [Gold and Schifreen were hackers who gained unauthorised 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.]

Table D: System Interference Provisions Relevant to DoS Attack

States	Provisions
Albania[84]	serious and unauthorised hindering of the functioning of a computer system by inputting, damaging, deforming, altering, deleting or suppressing of data
Armenia	obliteration (sabotage) of computer data or software, isolation or making it unusable, spoilage of computer equipment or destruction of the computer system, network or on storage media
Austria[85]	unauthorised serious interference with the functioning of a computer system
Bulgaria[86]	adding, changing, deleting or destroying a computer programme or data without the permit of the person who administers or uses the computer
Croatia[87]	rendering unusable or hindering the work or the use of computer systems, computer programs or electronic data and communication; damaging, altering, deleting, destroying or in some other way rendering unusable or inaccessible the electronic data or computer programs
Cyprus[88]	intentionally and without authority causes serious hinderingof the functioning of a computer system, by inputting, transmitting, destroying,deleting, altering, adding or suppress computer data
Czech Republic[89]	gaining access to a data carrier and with intent to cause damage toor to acquire unlawful benefit for oneself or another, and unlawfully using such data,damaging, destroying, altering or rendering useless such data, orinterference with the technical or program equipment or a computer or other telecommunication device
Estonia[90]	illegal interference with or hindering of the operation of a computer systemby way of uploading, transmitting, deleting, damaging, altering or blocking ofdata
Finland[91]	in order to cause detriment or economic loss to another, byentering, transferring, damaging, altering or deleting data or in anothercomparablemanner unlawfully preventing the operation of a computer system or causing seriousinterference in it

84 Article 293/c, Law no. 9918, dated 19.05.2008, on electronic communications.

85 Section 126b of the Austrian Penal Code.

86 Article 319b of the Bulgarian Penal Code.

87 Criminal law, Article 223, paragraphs 2 and 3 (OG 105/04).

88 Article 7 of Cyprus Law No 22(III)04.

89 Section 257a of the Criminal Code No 140/1961 Coll.: Harming and Misusing Record on Data Carrier (subject to reenactment).

90 PC Article 207,237.

91 Penal Code, Chapter 38, Section 7a Interference in a computer system.

France[92]	fraudulently accessing or remaining within all or part of an automated data processing system
FYROM[93]	without authorization, erasing, changing, damaging, covering or inother way making unusable a computer data or program or device formaintenance of the computer system, or making impossible or more difficultthe use of a computer system, data or program or the computer communication
Germany[94]	interference with data processing operations which are of substantialimportance to another byentering or transmitting data with the intention of causingdamage to another; ordestroying, damaging, rendering unusable, removing or altering a dataprocessing system or a data carrier
Italy[95]	interference concerning information andtelecommunication systems that have a public utility
Lithuania[96]	illegally destroying, damaging, removing or replacing thesoftware in a computer, or disrupting or changing the operation of a computernetwork, database or information thus causing serious damage
Montenegro[97]	entering, destroying, deleting, altering, damaging, concealing or in anyother manner making useless a computer datum or a computer system in theintention to obstruct the operation of the computer system
Portugal[98]	without legal permission or without being authorised to do soby the owner, other right holder of the system or part thereof, preventing, stopping, orseverely disrupting the operation of a computer system through the introduction,transmission, damage, alteration, deletion, preventing access or removal ofprograms or other computer data or any other form of interference in the computer system
Romania[99]	the act of causing serious hindering, without right, of the functioning of acomputer system, by inputting, transmitting, altering, deleting or deterioratingcomputer data or by restricting the access to such data

92 Article 323-1 of the French Criminal Code.

93 Art. 251(1) "the use of a computer system" of Macedonian Criminal Code.

94 German Criminal Code (Strafgesetzbuch), 2009 ("StGB"): Section 303b: Computer sabotage.

95 Article 635quinquies c.p.

96 Lithuanian Criminal Code, Article 197: Destruction or Replacement of Software, Disruption of the Operation of Computer Network, Data bank or Information System.

97 Section 28 of the Criminal Code of Montenegro "Criminal Acts against Safety of Computer Data", Article 350 - Obstructing Computer System.

98 Article 5, Law No. 109/2009.

99 Article 45 of Romania Law No. 161/2003.

Serbia[100]	entering, destroying, deleting, altering, damaging, concealing or otherwisemaking unusable computer datum or program or damaging or destroying acomputer or other equipment for electronic processing and transfer of data, withintent to prevent or considerably disrupt the procedure of electronic processing and transfer of data
Slovakia[101]	entering, transferring/transmitting, damaging, deleting, reducing quality, altering orrestraining/suppressing the computer data in order to obstruct/hinder thefunctionality/operation of a computer system
Ukraine[102]	violation of rules of exploitation of electronic machines (computers), automated systems, computer networks or networks of electrical communication or order or rules of information protection which is processed therein
UK[103]	unauthorised acts with intent to impair, or with recklessness as toimpairing, operation of a computer

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.[104] The CMA covered three distinct offences, namely, unauthorised access to computer material[105], unauthorised access with intent to commit other offence[106] and unauthorised modification of computer material.[107]

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 unauthorised modification of the contents of any computer. The question was whether the offence of

---

100 Articles 299 ("Computer sabotage") and 300 ("Creating and inserting of computer viruses") of CRRS.

101 Section 247 (1) d of the Criminal Code Act No. 300/2005 Coll.

102 Article 361(1) of the Criminal Code of Ukraine (with amendments of June 5, 2003) and Article 363.

103 Article 3(2/a, 6) of CMA 1990.

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

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

106 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.

107 Section 3: An offence is committed if any person does an act that causes unauthorised modification of the contents of any computer. The accused must have the intent to cause the modification and be aware the modification has not been authorised. There is no necessity for any unauthorised 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.

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.[108] 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 unauthorised access to a computer system, merely unauthorised "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,[109] the first reported criminal case in the U.K. concerning DoS attacks.

David Lennon, a UK teenager of 18 and a disgruntled employee,[110] overwhelmed an email server of his former employee by sending over five million messages. The massive volume of email disabled the office server.[111] 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 Kenneth Grant concluded that sending emails is an authorised 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 unauthorised 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).

---

[108] Shelley Hill, Driving a Trojan and Cart through the Computer Misuse Act (December 2003.January 2004), Computers & Law Vol. 5 31.

[109] [2005] EWCA Crim 2150.

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

[111] 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.

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,[112] 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 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.

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 Article 5 of the Budapest Convention and Article 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 unauthorised 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

---

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

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.

(V)

One of the fundamental premises of the Budapest convention is its use of technology-neutral language so that the substantive criminal law offences may be applied to both current and future technologies involved. Computer and internet technologies are evolving very fast with development of sophisticated new devices and programs. Any attempt to define certain unlawful activities involving computers and internet in very specific terms may fall short of successfully prosecuting a perpetrator in future. This very understanding led the drafters of the Convention to deploy technologically neutral language to secure a higher probability of successfully prosecuting currently non-existent future crimes. The Cybercrime Convention Committee (T-CY) is more optimistic in its language since it sees the use of technology-neutral language as 'to ensure that new forms of malware or crime would always be covered by the Convention.'[113]

However, the current status of ratification of the Convention is well outside the extent of effective and meaningful exploration of the treaty. As of January 1, 2014, the total number of ratifications to the Convention are 40 States[114], and 11 States have made their signatures but not followed up by ratifications[115]. Among the Member States of the Council of Europe, Russia has not signed the Convention. Several Member States such as Greece, Ireland, Poland, Sweden and Turkey have not followed up with a ratification.

At least three factors are preventing faster ratification of the treaty; firstly countries should have legislation compliant with Convention when depositing the instrument of ratification/accession[116]; secondly Convention has broad range of procedural provisions

---

[113] T-CY Guidance Note #6: Critical information infrastructure attacks, Cybercrime Convention Committee (T-CY), T-CY (2013)11E Rev, p. 3.

[114] Member States of the Council of Europe:Albania, Croatia, Hungary, Estonia, Lithuania, Slovenia, The former Yugoslav Republic of Macedonia, Romania, Cyprus, Denmark, Bulgaria, Bosnia and Herzegovina, Norway, France, Ukraine, Netherlands, Armenia, Iceland, Latvia, Finland, Italy, Slovakia, Serbia Germany, Moldova, Montenegro, Spain, Azerbaijan, Portugal, United Kingdom, Switzerland, Georgia, Austria, Belgium, Malta and Czech Republic.

Non-Member States of Council of Europe: United States of America, Japan, Australia and Dominican Republic.

[115] Andora, Greece, Ireland, Liechtenstein, Luxemburg, Monaco, Poland, Sweden, Turkey, Canada and South Africa.

[116] Acceding to Article 37, the Convention is open for accession by third countries. The accession process is as follows:

1. Once legislation has been adopted or is in advanced stage, government to send a letter to Secretary General of Council of Europe with a request to initiate consultation with parties to the Convention;
2. Secretariat of Council of Europe will carry out consultations and put question before Committee of Ministers;
3. If vote is positive, the country will be invited to accede;
4. The country is then free to decide when to accede, that is, deposit the instrument of accession.

that take time and parliamentary majorities to adopt and thirdly, cybercrime not always a priority of governments/parliaments.[117]

At least for the identifiable trends of legislative initiatives that are taking place all over the world, the impact of the Budapest Convention on DoS criminalization cannot be argued as linear. The most state parties to the Convention do not define DoS activities in strict and clear terms. Many have argued that the terminologies used in the Convention do not help the domestic legislators in formulating their own provisions. For example, Stein SchjolbergandSolange Ghernaouti-Helie observe:[118]

> [T]he Convention is based on criminal cyber conducts in the late 1990s. New methods of conducts in cyberspace with criminal intent must be covered by criminal law, such as phishing, botnets, spam, identity theft, crime in virtual worlds, terrorist use of Internet, and massive and coordinated cyber attacks against information infrastructures. Many countries have adopted or preparing for new laws covering some of those conducts. In addition, the terminology included in the Convention is a 1990s terminology, and is not necessarily suitable for the 2010s.

There is also a dominant argument that the Budapest Convention is a regional treaty and for most other global regions it still remains a European Convention and probably will remain so. This argument is amplified by the fact that only four countries outside Europe have become parties to the Convention - United States of America, Japan, Australia and Dominican Republic. And therefore, 4many countries treat the Convention as a reference, nothing more.[119]

---

[117] Alexander Seger, The Convention on Cybercrime: state of implementation, presentation, Octopus Interface Conference, Council of Europe, Strasbourg, 1-2 April 2008.

[118] Stein Schjolberg and Solange Ghernaouti-Helie, A Global Treaty on Cybersecurity and Cybercrime, AiTOslo 2011, p. ii.

[119] ITU Toolkit for Cybercrime Legislation, released in May 2009.