Public Prosecutor *v* James Raj s/o Arokiasamy
[2015] SGDC 36

Case Number : DAC 42809/2013 & Ors

Decision Date : 12 February 2015

Tribunal/Court : District Court

Coram : Jennifer Marie

Counsel Name(s) : DPPs G Kannan, Sanjiv Vaswani, Tang Shangjun & Rajiv Rai for Prosecution; For Defence Mr Ravi (till 30 Jan 2015); Accused in person

Parties : Public Prosecutor — James Raj s/o Arokiasamy

12 February 2015

Deputy Presiding Judge Jennifer Marie:

Introduction

1 The Accused is James Raj s/o Arokiasamy (James Raj), a 36 year old male Singaporean.

2 James Raj pleaded guilty to 39 charges under the Computer Misuse and Cyber-security Act Cap 50A ("CMCA") and one charge under Section 8(b) (ii) the Misuse of Drugs Act Cap 185 ("MDA"). He also consented to a further 119 charges under the CMCA and two charges under Section 8(b) (ii) of the MDA to be taken into consideration for the purposes of sentencing.

3 The hacking incidents perpetrated by James Raj can be broadly grouped into seven groups:

(a) Unauthorised access to a Fuji Xerox server, which contained customer data belonging to Standard Chartered Bank ("SCB")

DAC 13875 – 13925 of 2014 (51 counts);

Date of offences - 1 – 24 March 2013

(b) The hacking of the fan website (www.heyaosun.com) of one Sun Ho, pastor of City Harvest Church ("CHC");

DAC 13821 – 13863 of 2014 (43 counts);

Date of offences - 28 August – 2 September 2013

(c) The attempted hacking of three websites linked to CHC;

DAC 13864 – 13866 of 2014 (3 counts)

Date of offences - 15 October 2013

(d) The hacking of a Straits Times journalist's blog ("ST Blog");

DAC 10591 – 10594 of 2014 (4 counts)

Date of offences - 1 November 2013

(e) The hacking of the People's Action Party ("PAP") Community Foundation ("PCF") website;

DAC 10543 – 10547 of 2014 (5 counts)

Date of offences - 17 October 2013

(f) The hacking of the Ang Mo Kio Town Council website ("AMKTC");

DAC 10548 – 10590 of 2014 and DAC 43752 of 2013 (44 counts)

Date of offences – 27 & 28 October 2013

(g) The scanning and penetration testing of various government servers;

DAC 13867 – 13874 of 2014 (8 counts)

Date of offences – 18 October – 4 November 2013

Brief Facts

4 James Raj admitted the detailed and lengthy Statement of Facts tendered by the prosecution without qualification[note: 1]. I have reproduced brief extracts of the SOF here to give some overview of the case against James Raj.

Charges relating to the Hacking of the PCF Website (proceeded with DAC 10543, 10546 & 10547 of 2014)

5 On 18 Oct 2013 at about 11.06 am the police were informed that the PCF website had been hacked on 17 Oct 2013.

6 Investigations revealed that the PAP PCF server was accessed and modified without authorization on 17 October 2013. In brief, the hacker (James Raj) had uploaded a file named "pcf.html" onto the server. James Raj had also posted the URL of the 'hacked' webpage on online forums to draw attention to, and to take credit for, his actions.

7 The 'hacked' webpage depicted an image of a figure in a hooded jacket, accompanied by the word "HACKED". The hacker identified himself as "The Messiah" and expressed his displeasure at an incident at a PCF child care centre in which a 9-month old child had been accidentally scalded. The hacker threatened to "bury" PCF, in the event that PCF failed to conduct proper investigations into the incident.

Charges relating to the Hacking of the AMKTC Server (proceeded with DAC 10548, DAC 10553, 10554, 10555, 10556, 10557, 10558, 10559, 10590 of 2014 & DAC 43752 of 2013)

8 On 28 October 2013 at about 9.11 pm the police were informed that the AMKTC website had been hacked earlier that same day.

9 Investigations revealed that the AMKTC website had been hacked on 28 October 2013. In particular, two 'What's New' banners displayed on the main-page of the site had been modified and the amended the text of the first banner displayed the following message: "*I have been to various sites and seen how they take the initiative to secure their systems. You have a brain & you have money. You had a choice. Don't blame external factors (Anonymous) for this hack. The Messiah;)*". The second banner contained a purported resignation message by Member of Parliament for the Ang Mo Kio Constituency which stated as follows:

> "*MP Ang Hin Kee: I would like to tender my resignation as your minister of parliament. I am incapable and have failed all of you.*
>
> *URL: http://www.youtube.com/watch?v=mjyoQjYvjjU*"14

Charges relating to the Hacking of the ST Blog Webserver (proceeded with DAC 10591, 10592 & 10593 of 2014)

10 On 1 November 2013 at about 12.27pm, the Online Editor for Singapore Press Holdings (SPH), lodged a police report at Toa Payoh NPC informing the Police that the ST Blogs website (URL:blogs.straitstimes.com) had been hacked by a hacker who went by the moniker, "The Messiah".

11 Investigations revealed that sometime in late October 2013, James Raj had produced and uploaded a video onto YouTube. This video contained a message purportedly from Anonymous. First, the narrator, garbed in a cloak and wearing a Guy Fawkes mask, acknowledged The Messiah as a member of Anonymous. Second, the narrator threatened that unleashing "aggressive cyber intrusions" on Government servers, if the Government did not rescind Singapore's proposed internet licensing regulatory framework for news websites. The narrator also called upon Singaporeans to join Anonymous' protest against the Singapore Government on 5 November 2013 by "dressing fully in black and red to paint your streets with the colours that represent the current Singaporeans' emotions."

12 The first article that was published at 4:32:49hrs on 1 November 2013 was entitled "Dear ST: You just got hacked for misleading the people!" ("first article"). The author introduced himself as "the Messiah" from Anonymous and:

> (a) Demanded an apology from Irene Tham within 48 hours for her 'misleading' article pertaining to the Anonymous YouTube video;
>
> (b) Demanded that the PAP commence investigations into the baby scalding incident at the PCF kindergarten;
>
> (c) Demanded that Attorney-General's Chambers and the High Court assist the mother of one "Dinesh Chandran" (an inmate who died in prison) by "giving her the closure that she needed";

(d) Issued a threat against Dr Esmee Koh (from the Animal Clinic) pertaining to the "murder" of a puppy named Tammy; and

(e) Clarified that the plans to attack the internet infrastructure of Singapore would only take place on 5 November 2013 if the proposed internet licensing framework was implemented.

13 The second article that was published at 4:56:50hrs on 1 November 2013 was entitled "Anonymous: We are legion The Story of the Hacktivists" ("second article"). The second article was an introduction to 'Anonymous' and their ethos.

Charges relating to the Hacking of the Heyaosun Webserver (proceeded with DAC 13821, 13825, 13828, 13829, 13830, 13846, 13847, 13851, 13863 of 2014)

14 On 2 September 2013, the site administrator of Heyaosun website reported to the police that the Heyaosun website had been defaced. The original homepage ("default.asp") had been replaced with a file of the same name, but with different content. The defaced webpage, which started and concluded with phrases from the Bible, ridiculed Sun Ho for her physical appearance and accused her of having hidden agendas in her charitable activities. The hacker (James Raj) also claimed to have downloaded databases, SMS messages, emails, users' personal information and other documents from the Heyaosun webserver. The hacker, who called himself "The Messiah", threatened to release all information if Sun Ho did not stop 'lying' or 'taking advantage' of her fans or followers.

15 Investigations also revealed that a database of personal particulars of the fans who had signed up on the website had been downloaded without authorisation.

Charges relating to the Attempted Access of CHC Website (proceeded with DAC 13864/2014)

16 On 8 Sep 2013 at about 11.21pm, the Operations Director of City Harvest Church ("CHC") lodged a police report at Central Police Division. He reported that after the defacement of www.heyaosun.com, there had been multiple attempts targeted at compromising other CHC websites.

Charges relating to the Scanning of Government Servers (proceeded with DAC 13867, 13870, 13871, 13872 & 13874 of 2014)

17 The YouTube video that was uploaded by James Raj in late October 2013, had threatened that Anonymous would launch a series of cyber intrusions against the Singapore Government's servers on 5 November 2013. Further investigations revealed that the James Raj had scanned various government websites/servers from 18 October 2013 to 4 November 2013, in order to identify security vulnerabilities. He had targeted the Prime Minister's Office, the Ministry of Communication and Information, Singapore Prisons Services, The Election's Department, amongst others.

Charges relating to the Hacking of Fuji Xerox Server (proceeded with DAC 13875, 13879, 13913, 13916, 13917, 13918, 13923 & 13924 of 2014)

18 In the course of investigations, 999 bank statements from Standard Chartered Bank ("SCB") were found in two zip files on James Raj's used laptop. The bank statements are of Private Banking clients of SCB.

19 Investigations also revealed that James Raj had scanned a computer with the IP address 203.117.237.100 which was identified to be a server maintained by Fuji Xerox Singapore Pte Ltd ("FX"), which provided printing services for SCB. The said bank statements were stored on this server, which was physically located in Singapore.

Charges Relating to Drug Consumption (proceeded with DAC 42809 of 2013)

20 James Raj was arrested by the CNB on 25 Nov 2011 on suspicion of having consumed a specified drug, an offence under section 8(b) (ii) of the MDA. He had absconded to Malaysia whilst on bail pending investigations. The scientific analysis of the urine samples taken from James Raj revealed that the urine samples contained 11-nor-delta-tetrahydrocannabinol-9-carboxylic acid which is a known metabolite of cannabis.

Antecedents

21 The prosecution tendered the antecedents of James Raj[note: 2] (marked Exhibit E) which is reproduced below:

S/N	Date of Conviction	Offence & Ordinance	Sentence	Court & Case No
1	24/09/2004	s.414 c.224 Assisting in Concealing / Disposing of Stolen Property r/w s.109 c.224 Abetment of an Offence	Imprisonment only, 3 months	Ct 16 DAC 34138/04
2	18/10/2007	s.8(B)(II) c.185 Consumption of a Specified Drug r/w s.34(2)(b) c.185 Subject to Treatment & Rehabilitation Drug Type: Cannabis	Drug Rehabilitation Centre Urine 6 months	
3	16/10/2008	s.8(B)(II) c. 185 Consumption of a Specified Drug r/w s. 34(2)(b) c. 185 Subject to Treatment & Rehabilitation Drug Type: Cannabis	DRC Extension 6 months (Date of review – 24/09/2008) Placed under Drug supervision 24 months Compl 1 yr SO 0 months (Date of review – 16/10/2009)	
4	23/03/1999 Commenced on: 23/03/1999	s.170 c. 224 Personating a Public Servant r/w s. 34 c.224 Common Intention	Probation 15 months Time Restriction from 2200 to 0600	Ct 12 DAC 33723/98

Prosecution's Address on Sentence

22 The prosecution submitted a written address on sentence, Exhibit P1 (as well as a skeletal summary; Exhibit P2) and this was augmented by a forceful cogent oral submission by the lead prosecutor, DPP G Kannan. The DPP urged the court to consider the public interest and the need for a deterrent sentence to be imposed in this case. He highlighted 13 aggravating factors for the CMCA offences (paras 26-70 Exhibit P1) as well as the aggravating factors for the MDA offences (paras 71-72 Exhibit P1).

23 The DPP submitted that there were no mitigating circumstances meriting a discount in sentence in this case. The DPP also averred that the current sentencing precedents are of limited value in light of the magnitude of the hacking offences perpetrated by James Raj.

24 The prosecution urged the imposition of a global sentence of 5-6 years imprisonment. In the table below, I have set out the sentencing range that the DPP had urged the court to consider as elicited from paras 108-109 of Exhibit P1.

Series	Offences	Proceeded Charges	Sentence range
ST Blog hack (DAC 10591, 10592 & 10593 of 2014)	Performing an act preparatory - s 3(1) r/w s 10(1) of the CMCA	1	3- 7 mths
	Unauthorised access – s 3(1) of the CMCA	1	4 – 12 mths
	Unauthorised modification - s5(1) of the CMCA	1	9 – 15 mths
AMKTC Hack (DAC 10548, DAC 10553, 10554, 10555, 10556, 10557, 10558, 10559, 10590 of 2014 & DAC 43752 of 2013	Performing an act preparatory – s 3(1) r/w s 10(1) of the CMCA	2	3 – 7 mths
	Unauthorised access – s 3(1) of the CMCA	6	4 – 12 mths
	Unauthorised modification - s 5(1) of the CMCA	2	9 – 15 mths
PCF Hack (DAC 10543, 10546 & 10547 of 2014)	Performing an act preparatory - s 3(1) r/w s 10(1) of the CMCA)	1	3 – 7 mths
	Attempted/Unauthorised access - s 3(1) of the CMCA	1	4 – 12 mths
	Unauthorised modification - s 5(1) of the CMCA	1	9 – 15 mths
Heyaosun hacking incident (DAC 13821, 13825, 13828, 13829, 13830, 13846, 13847, 13851, 13863 of 2014)	Performing an act preparatory – s 10(1) r/w s 3(1) of the CMCA	1	3 – 7 mths
	Unauthorised access – s 3(1) of the CMCA	6	4 – 12 mths
	Unauthorised modification - s 5(1) of the CMCA	2	9 – 15 mths
Scanning of CHC webservers (DAC 13864/2014)	Performing an act preparatory – s 3(1) r/w s 10(1) of the CMCA	1	2 – 7 mths

Scanning of government servers (DAC 13867, 13870, 13871, 13872 & 13874 of 2014)	Performing an act preparatory – s 3(1) r/w s 10(1) of the CMCA	5	5 – 12 mths
Hacking of Fuji Xerox webserver (DAC 13875, 13879, 13913, 13916, 13917, 13918, 13923 & 13924 of 2014)	Unauthorised access – s 3(1) of the CMCA	8	5 – 12 mths
Drug Consumption (DAC 42809 of 2013)	Consumption of a specified drug under s 8(b)(ii) MDA	1	12 mths

Plea in Mitigation

25 The defence submitted a written mitigation plea (Exhibit D1) and this was bolstered by Mr Ravi's oral address. He urged the court to consider that the acts of James Raj as "highly amateurish" and had not resulted in any physical damage or theft of intellectual property rights. He went on to state that the acts of James Raj helped to identify weaknesses in the networks which could have in time been destroyed by people with far more malicious intent. He further relied on *PP v Choo Luke Kuo* (2010) SGDC 538 and *PP v Leslie Liew Cheong Wee* (2012) SGDC 437 as well as the unreported cases of *Mohammad Azhar Tahir* and *Delson Moo* (paras 34-36 Exhibit D1).

26 The defence urged the court to impose a lenient custodial sentence as James Raj is genuinely remorseful for the consequences of his actions borne out of naivety. He urged the court to impose 12 months imprisonment on the consumption of a specified drug charge, an offence under s 8(b)(ii) of the MDA; a cumulative sentence of 3 years for the CMCA offences and urged the court to impose a global sentence of 4 years imprisonment.

Reply by Prosecutor

27 Whilst the DPP agreed that there was no physical damage to the infrastructure or a breach of Intellectual Property rights, he submitted that the lack of aggravating factors is not a mitigating factor.

28 The characterization of the conduct of James Raj as merely "pentesting"and being amateurish is completely at odds with the assertion by the James Raj himself. See Annex D to the SOF Exhibit B-page 5- (reproduced below). This was not a case where James Raj had an innocuous knowledge about the cyber space. In fact about a decade ago James Raj had already started to be immersed in this

Posted: 29 July 2013

My friends,

About a decade ago when I was a ruthless dominating script body on IRC, I signed up on a forum called asianbookie.com. This forum was and still is one of the largest Asian handicap gambling forum on the internet. It reaches on to such a wide geographical location of gamblers.

What else??? Time to blast asianbookie.com down mofo!!! I blasted him in ways he never thought was possible (Goooood times). This lasted for a week or so till they gave up their arrogance and came begging to stop. Did I

stop? Nope. I demanded money (Remember I told u I was a malicious cunt) but we eventuall6y settled on some other financial arrangement that suited both parties.

29 The DPP also submitted that the cases cited by the defence in support of a more lenient sentence were neither relevant nor helpful as they involved different sets of facts and circumstances. *Leslie Liew's* case involved a single victim and there were 5 offences committed over 3 days. It was not a sophisticated offence and there were no difficulty in detecting the transgression whilst *Delson Moo's* case involved 3 charges of unauthorised interception, offences under Section 6 CMCA. There was no actual intrusion but the Accused *Delson* in that case only created an appearance of intrusion. Similarly in the other cases cited by the defence involving unauthorised access, these cases involved single victims and were not sophisticated.

30 On 30 Jan 2015, on the resumed date of hearing for sentencing, the Accused James Raj after having discharged his counsel Mr M Ravi, tendered an additional written mitigation plea (Exhibit D2). He pleaded for leniency and urged the court not to consider him as a malicious hacker as he had not used his skills for "more selfish reasons" and had not caused financial losses for personal gain. He urged the court to show mercy and leniency as this will earn his "humble gratitude and rebuild my faith in our system; leading me back [to] the right path."

Sentencing Considerations

(A) Prescribed Punishment

31 The prescribed punishment for an offence under section s3(1) read with section 10(1) of CMCA Cap 50A is as follows:-

> 3.-(1) Subject to subsection (2), any person who knowingly causes a computer to perform any function for the purpose of securing access without authority to any program or data held in any computer shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 2 years or to both …

The prescribed punishment for an offence under section s5 (1) of CMCA Cap 50A

> 5.-(1) Subject to subsection (2), any person who does any act which he knows will cause an unauthorised modification of the contents of any computer shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both ……

The prescribed punishment for an offence under section s 8(b)(ii) of MDA Cap 188

> No Minimun
>
> Maximum: 10 years imprisonment or $20,000/-, or both,

(B) Relevant sentencing principles

32 The conventional considerations, or "classical principles" of sentencing, may be divided into four broad categories: deterrence, retribution, prevention and rehabilitation: *R v James Henry Sargeant* (1974) 60 Cr App R 74 at 77. See also *Law Aik Ming v PP* (2007) 2SLR 823.

33 The principles of deterrence- both general and specific, in my view should be of prime focus in determining the appropriate sentence to be imposed in this case. At the outset I note that both the prosecution and defence agree that the threshold for a custodial sentence has been crossed in this case, and rightly so.

Specific deterrence

34 Specific deterrence is usually appropriate in instances where the crime is premeditated: *Tan Fook Sum* v PP (1999) 1SLR1022. This is because deterrence probably works best where there is a *conscious* choice to commit crimes and specific deterrence operates through the discouraging effects felt when an offender experiences and endures the punishment of a particular offence. See *Law Aik Ming v PP* supra

General Deterrence and Public Interest

35 General deterrence is derived from the overarching concept of "public interest". In *Angliss Singapore Pte Ltd v PP 4SLR 653*, Rajah J (as he then was), had stated that public interest in sentencing is tantamount to the court's view of how public security can be enhanced by imposing an appropriate sentence. A sentencing judge should apply his mind to whether the sentence is necessary and justified by the public's interest in deterring and preventing particular criminal conduct: *Angliss* ([16] *supra*) at [17].

36 For certain types of offences and offenders there will be a need for punishment to be "certain and unrelenting".

Reasons for Sentence

37 In this case, James Raj single handedly perpetrated what the prosecution has described as the largest, most prolific cyber-attacks against IT systems in Singapore. He systematically and unrelentingly over a couple of months pursued a course of conduct that has led to some 158 charges under the CMCA being preferred against him. A significant degree of resources has been expended by the authorities and the affected entities to investigate verify and rectify these acts.

38 The offences perpetrated by James Raj in addition to harming the immediate victims, also have the wider-felt impact of triggering unease and offending the sensibilities of the general public. A deterrent sentence is therefore necessary and appropriate to quell public disquiet and the unease engendered by such crimes: *Meeran bin Mydin* (1988) 2 SLR 522.

39 Given the current climate where international and domestic terrorist security threats are more prevalent than before, a threat to the IT systems; cyber-attacks in a country like Singapore that is highly networked, should be visited with exemplary sentences.

40 The views of the then SDJ in *PP v Mohammad Farhan bin Mohd Mustafa*, District Arrest Case No 1808 of 2004 where the accused was sentenced to three and a half years' imprisonment for a bomb hoax; are equally applicable for the offences before this court. The senior district judge had stated at [14] that "it [was] clear that the sentencing of [such] offences ... must be treated seriously and that a strong deterrent be sent to those whose idle minds might otherwise turn to creating false alarms".

41 The offences perpetrated by James Raj are easy to commit for persons who have the knowledge. But these offences are difficult to detect and could become rampant if not firmly dealt with. A clear signal must be unequivocally sent by the sentencing court that such behaviour will not be tolerated and will be viewed with grave and unrelenting disapprobation.

42 While a highly punitive sanction is necessary in this case for the purposes of specific and general deterrence as well as prevention, I recognize that it should also within reasonable limits be commensurate with the severity of the offence, both in terms of the harm caused and the culpability of the offender.

43 The question to be asked is will an increased sentence reduce the propensity of James Raj to risk further punishment by the commission of another offence. Given that the very propensity to re-offend is inextricably interlinked with the knowledge of James Raj, the court is of the view that there is a need to ensure that the sentence imposed will effectively deter him.

Aggravating Factors

44 The aggravating features indicated in prosecution's submission on sentence were supported by the facts of the case.

Escalation of Criminality

45 James Raj started his foray into cyber criminality by first scanning the Fuji Xerox server, which contained customer data belonging to Standard Chartered Bank ("SCB") sometime in March 2013. There was a lull for a couple of months and then on 2 Sep 2013 he hacked the website of Sun Ho and thereafter over a space of 2 months in quick succession he had hacked into more than 10 servers. It was alarming the escalation of his criminality; from penetrating a system insidiously to a very public act of threatening government systems.

Public Alarm and Fear – public interest

46 The very public manner the offences were perpetrated and James Raj's threatening taunts found in the video of the "The Messiah" that was posted on 31 Oct 2013 had caused public alarm and fear. The Prosecution played the video in Court: Annex I to SOF. Not only was the chilling effect brought home starkly but is also shed light on the person behind these acts - the audacious bravado of James Raj.

47 There was also the threat that the hacker would "go to war" with the Singapore government on 5 Nov 2013 to cause government "financial loss by aggressive cyber intrusions". The DPP submitted that this threat was taken seriously by the authorities- the Government IT Security Incident Response Team was set up to coordinate responses to a cyber-intrusion – alerting all government agencies of possible hacks to bring down government websites: Tab O Bundle of Authorities.

48 It was only fortuitous that the law enforcement officers who had expended so much resources, managed to crack the case and arrest James Raj on 4 Nov 2013. The prosecution had submitted that more than 2465 man hours had been expended by the Singapore Police Force in investigating these offences.

Criminal Intent / Motivated by Malice / Premeditation

49 The premeditated cyber-attacks reveal a pattern; a sinister motive to target not only government IT systems; the Prime Minister's Office, the Ministry of Communication and Information, Singapore Prisons Services, The Election's Department, PAP PCF, and AMKTC but also selected prominent newsworthy entities like SCB and a religious organization.

50 In the case of the SCB hack, a server containing confidential customer data of about 650 of SCB's Private Banking clients had been compromised. James Raj had maliciously left threatening, abusive, and taunting messages on the hacked sites. This sort of cyber-intrusions if left unchecked will seriously undermine public and international confidence in Singapore's IT systems and compromise Singapore's efforts to position itself as a global e-commerce hub.

Magnitude and Gravity of the Offences- Systematic attacks against IT systems in Singapore

51 James Raj had targeted and compromised the computer servers of no less than seven different entities. The manner the offences were committed show a high degree of premeditation, planning and sophistication as evidenced by the use of specialized software tools to scan servers for vulnerabilities and to exploit them, and in the steps taken to evade detection. His targeting IT systems in Singapore has the potential to cause enormous damage, both to the credibility of IT systems and the way in which our society now operates, and the apparent ease with which hackers, from the confines of their own homes, can damage important public institutions and individuals alike.

52 The fact that he had pleaded guilty to 39 charges under the Computer Misuse and Cyber-security Act Cap 50A (CMCA) and 1 charge under the MDA Cap 188 as well as admitted to another 121 charges reveals the extent of his criminality. Whilst he had decided to plead guilty, however based on the circumstances of this case the value of his guilty plea was substantially diminished: *Tan Kay Beng v PP* (2006) 4SLR 10 at [37]

The CMCA

53 The policy considerations underpinning the prevention of certain CMCA offences have been articulated during Parliamentary debates relating to the amendments to the Act. During the Second Reading of the Computer Misuse (Amendment) Bill on 30 June 1998 ("*Computer Misuse (Amendment) Bill*"), the Minister for Home Affairs, Mr Wong Kan Seng concluded,(see, *Singapore Parliamentary Debates, Official Report* (28 May 1993) vol 61 at col 400 of the *Computer Misuse (Amendment) Bill*:

> [T]his Bill is *intended to send a strong signal that computer crimes will be treated and dealt with seriously in Singapore*. As Singapore positions itself to be an intelligent island and a global centre for E-commerce, the legislative framework must keep pace with the developments to ensure the integrity of our computer systems against would-be cyber criminals and hackers. *With the Bill, banks, commercial institutions, foreign investors and businesses can rest assured that Singapore would be a good and safe place where E-commerce can flourish.* Singaporeans can also rest assured that the law provides adequate coverage for the safe operation of essential computer systems in Singapore.

54 Parliament's intention is loud and clear; it intended that offences prosecuted under the CMCA be treated seriously, and that deterrence functions as a necessary sentencing consideration in all such offences in order to protect the integrity of our computer systems and the security of financial and commercial institutions, foreign investors and locals alike.

Need for specific deterrence to prevent James Raj from re-offending

55 The DPP highlighted that in the case of the PCF hack, James Raj was able to determine the existence of the administrative page in 8 seconds, and was able to gain unauthorized access to the server's administrative page about 20 minutes later. From start to finish, the hacking and the defacement of the PCF webserver took only 7 hours. Quite clearly James Raj possesses the skills and the requisite know-how to re-offend with little ease, there is a need to ensure that the sentences will specifically deter him as well.

Offences Committed While on Bail

56 The CMCA offences were committed whilst James Raj was on bail and this is significant as it manifests a proclivity for offending behavior by James Raj. The prosecution had highlighted his evident lack of remorse as he was "entirely uncooperative with the police" and had resulted in the police expending significant resources and time to forensically piece together the evidence to implicate him.

Weight to be attached to the plea in mitigation

57 This is a case where the circumstances are such that any mitigating effect afforded by the guilty plea of James Raj is outweighed by the clear need for a deterrent sentence and the aggravating factors present: Chen Weixiong Jerriek v PP (2003) SGHC 103 [21].

58 I had also considered the additional plea of James Raj that was tendered in Court on 30 Jan 2015 (Exhibit D2) where he urged the court to show leniency and contended that he had not acted maliciously and that though over 600 bank details were discovered in his laptop there was "zero theft or financial loss". I accepted the submission by the prosecution that these cyber intrusions were neither amateurish nor committed as a result of naivety. The submission that James Raj was playing a vigilante sort of role, in my view was devoid of any merit. His intention was far from "pen testing" the systems, it was to instill fear and trepidation– an extract from the transcript of the Anonymous video posted by James Raj: Annex I reveals as much.

> " Now close your eyes and imagine a legion of Anonymous unleashed upon your tiny little island and infrastructures. It will be like dipping yourselves into a pool of piranhas. We have faced much larger and more secured corporations such as F.B.I & the N.S.A……?

Foreign precedents

59 Foreign authorities/precedents are helpful in clarifying the relevant *sentencing principles* in connection with a particular offence. In *Chia Kim Heng Frederick v PP* [1992] 1 SLR(R) 63 at [12] Yong Pung How CJ had declared:

> Because the approach towards sentencing is governed by the objective in inflicting punishment, which in turn reflects the social environment in a country, it would *not be appropriate for a court in Singapore to follow completely* the approach and practice followed by English courts in sentences for imprisonment...

60 *The precise quantum* relating to sentences imposed by foreign courts may not afford an appropriate guide or benchmark for sentencing by our courts in some instances. However, for crimes which have a global reach, in assessing the impact of such offences, it is useful to consider sentences and the approaches taken in other jurisdictions with similar legislation in deterring and preventing such offences.

61 The UK cases cited by the prosecution were helpful in providing broad guidelines as to the appropriate sentences to be imposed for each category of charges faced by James Raj. For example in two cases *cited in R v Mangham* (2013) 1 Cr App R(S) 11, namely *R v Lindesay* (2003) 1 Cr App R(S) 370, the Court had upheld a sentence of 9 months' imprisonment: that was imposed on an offender who had, in revenge for his dismissal, gained unauthorised entry into three websites and deleted certain data to cause inconvenience. There was no damage to the software or direct revenue loss. The appellant had pleaded guilty and had strong personal mitigation. And the case of *R v Baker* (2011) EWCA Crim 928, the sentence of 4 months' imprisonment on a person of good character was upheld. On 20 occasions, over a week in June, the appellant had used a remote dial-up connection from his home computer to gain unauthorised access to the Welsh Assembly computer system. The appellant had read a number of sensitive emails up to the restricted level. He had been dismissed and said he was searching for material relevant to that. In *R v Lewys Martin* (2014)1 Cr App R(S) 63, the CA had dismissed an appeal against a total sentence of two year's imprisonment in a case where the accused had pleaded guilty to 5 counts of unauthorised modification of computer material, 1 count of unauthorised access and three other offences under the UK Computer Misuse Act.

62 The approaches and sentencing precedents will have to be balanced to reflect our society's distaste for this type of crime. Nevertheless, I note and accept that the cases cited support a deterrent custodial sentence of not an insubstantial length.

63 In this case the CMCA offences can be broadly categorised as follows – **Category 1** - *offences under s3(1) r/w s10 CMCA- performing acts preparatory*; **Category 2** - *offences under s 3 (1) CMCA - unauthorized access including scanning and penetration testing of government servers*[note: 3] and **Category 3** - *offences*

under s 5(1) CMCA involving unauthorized modification. The sentences in my view should range from **2 - 3months** for Category I ; **5-8 months** for Category 2 and **10** months for the more egregious Category 3 offences. As for the offence under the MDA the sentencing norm of **12 months imprisonment** is appropriate.

Deterrence tempered with proportionality

64 Whilst a strong deterrent sentence is called for in this case the need for specific deterrence always had to be circumscribed by the proportionality principle, and it is axiomatic that the court must abstain from gratuitous loading in its sentences see *Tan Kay Beng v PP* (2006) 4SLR 10 at [31].

65 Deterrence must always be *tempered by proportionality* in relation to the severity of the offence committed as well as by the moral and legal culpability of the offender. In a similar vein, Yong CJ in *Xia Qin Lai v PP* [1999] 3 SLR(R) 257at [29] stated:

> [T]he principle of deterrence (especially general deterrence) dictated that the length of the custodial sentence awarded had to be a not insubstantial one, in order to drive home the message to other like-minded persons that such offences will not be tolerated, *but not so much as to be unjust in the circumstances of the case*.

66 Therefore, a punitive sanction imposed in the name of deterrence should not contravene the principles of proportionality.

67 Having decided on the individual sentences, I next considered which of these sentences should run consecutively. The one transaction rule in my view did not apply in this case. The distinct offences in this case called for multiple punishments

Totality Principle

68 The second principle is the totality principle. In the case of *Mohamed Shouffee bin Adam v PP* (2014) SGHC 34, Chief Justice Sundaresh Menon stated that the totality principle was a principle of limitation and a manifestation of the requirement of proportionality that ran through the gamut of sentencing decisions. There were two limbs; first whether the aggregate sentence was substantially above the normal level of sentences for the most serious of the individual offences; and second whether its effect was to impose on the offender a crushing sentence not in keeping with his record and prospects.

69 It must be borne in mind that such a definition of the totality principle should not be rigidly and blindly applied to *all* cases. Rather, it must be invoked sensibly. The totality principle guides the court in sentencing an offender guilty of more than one offence, ensuring that the total sentence remains proportionate to the gravity of the context. There is a suggestion in *V Murugesan v PP (2006) 1 SLR (R) 388* that the aggregate sentence can be measured against the maximum sentence for the most serious of the offences the accused has been convicted of, *unless* the offender is a persistent offender or alternatively, if the maximum sentence seems *too short to reflect the gravity of the appellant's total conduct*. Where the circumstances warrant it, the totality principle must not be allowed to strait jacket the courts. See *ADF v PP* (2010) 1SLR 874 [925].

70 The court is obliged to impose a consecutive sentence in view of section 307 (1) of the Criminal Procedure Code Cap 68. The charges framed are distinct offences and the charges ordered to run consecutively, do not involve a single invasion of the same legally protected interest. James Raj had violated the interest of seven different entities and violated different legally protected interests.

71 In *Public Prosecutor v Tan Khoon Shan Terrance* [2012] SGHC 181 (*"Terrance Tan"*), the accused faced 617 charges under the Telecommunications Act (Cap 323, 2000 Rev Ed), which were committed over a period of slightly more than a month. The former Chief Justice Chan Sek Keong, stated as follows about sentencing offenders who faced a large number of charges:

> "(T)he correct approach for the court to adopt in sentencing the Respondent is not to consider the sentence for each charge and then to multiply it with the number of charges on which he was convicted. This approach is not appropriate as the totality of the sentence would then depend on how many charges the Public Prosecutor decides to have tried and the number to be taken into consideration for the purpose of sentencing. There is nothing to commend such an approach. Instead, a more suitable approach is for the court to determine on a global basis what the totality of the sentence should be so as to avoid imposing a "crushing" sentence on the offender.

72 In the present case, the damage inflicted on the integrity and reputation of a financial institution (SCB) and government entities, the premeditation and sophistication of the offences and the "audacious bravado" that led to the commission of the offences exacerbates the gravity of the offences.

73 Having considered the mitigation plea by the Defence and the Prosecution's address on sentence and having accorded due consideration for the totality principle and the need not to gratuitously overload the sentence, I am of the view the overall criminality of James Raj's conduct cannot be encompassed in two consecutive sentences.

74 The accused James Raj is sentenced as per the table below and I further order six of these charges to run consecutively. The total sentence of 56 months imprisonment, in my view, cannot be considered as crushing and the term of imprisonment adequately befits the gravity of the offences.

Series/date of offences	Offences	Proceeded Charges	Sentence/ charge	Sentences to Run Consecutively
ST Blog hack 1 Nov 2013 (DAC 10591, 10592 & 10593 of 2014)	Performing an act preparatory – s 3(1) r/w s 10(1) of the CMCA	1	2 mths	
	Unauthorised access – s 3(1) of the CMCA	1	5 mths	
	Unauthorised modification – s 5(1) of the CMCA	1	10 mths	**10months** **DAC 10593/2014**
AMKTC Hack 27-28 Oct 2013 (DAC 10548, 10553, 10554, 10555, 10556, 10557, 10558, 10559, 10590 of 2014 & DAC 43752 of 2013)	Performing an act preparatory – s 3(1) r/w s 10(1) of the CMCA	2 DAC 10548 & 10553/2014	3 mths	
	Unauthorised access – s 3(1) of the CMCA	6 DAC 10554, 10555, 10556, 10557, 10558& 10559/2014	5 mths	
	Unauthorised modification – s 5(1) of the CMCA	2 DAC 10590 /2014 & DAC 43752 /2013	10 mths	**10months** **DAC 43752/2014**
PCF Hack 17 Oct 2013 (DAC 10543, 10546 & 10547 of 2014)	Performing an act preparatory – s 3(1) r/w s 10(1) of the CMCA)	1 DAC 10543/ 2014	3 mths	
	Attempted/Unauthorised access – s 3(1) of the CMCA	1 DAC 10546/ 2014	5 mths	
	Unauthorised modification – s 5(1) of the CMCA	1 DAC 10547/ 2014	10 mths	
Heyaosun hacking incident 28 Aug – 2 Sep 2013 (DAC 13821, 13825, 13828, 13829, 13830, 13846, 13847, 13851, 13863 of 2014)	Performing an act preparatory – s 10(1) r/w s 3(1) of the CMCA	1 DAC 13821/ 2014	2 mths	
	Unauthorised access – s 3(1) of the CMCA	6 DAC 13828, 13829, 13830, 13846, 13847 &13851 /2014	5 mths	

	Unauthorised modification – s 5(1) of the CMCA	2 DAC 13825 &13863 /2014	10 mths	**10months** **DAC 13825/2014**
Scanning of CHC webservers 15 Oct 2013 (DAC 13864 of 2014)	Performing an act preparatory – s 3(1) r/w s 10(1) of the CMCA	1 DAC 13864/ 2014	2 mths	
Scanning of government servers 18 Oct – 4 Nov 2013 (DAC 13867, 13870, 13871, 13872 & 13874 of 2014)	Performing an act preparatory – s 3(1) r/w s 10(1) of the CMCA	5 DAC 13867, 13870, 13871, 13872 & 13874/2014	6 mths	**6months** **DAC 13870/2014**
Hacking of Fuji Xerox webserver 1 – 24 Mar 2013 (DAC 13875, 13879, 13913, 13916, 13917, 13918, 13923 & 13924 of 2014)	Unauthorised access – s 3(1) of the CMCA	8 DAC 13875, 13879, 13913, 13916, 13917, 13918, 13923 & 13924 / 2014	8 mths	**8 months** **DAC 13875/2014**
Drug Consumption 25 Nov 2011 (DAC 42809 of 2013)	Consumption of a specified drug under s 8(b)(ii) MDA	1 DAC 42809 / 2013	12 mths	**12 months** **DAC 42809/ 2013**

Total imprisonment -56 months with effect from the date when first produced in Court ie 5 November 2013.

Conclusion

75 Singapore is a major IT centre both regionally and globally. Cyber intrusions and threats pose considerable danger to the economy and the country. There is a need to send a strong signal to the Accused as well as like- minded persons that they should banish the thought of pursuing such criminal conduct. The courts will come down hard on such conduct unrelentingly but will also ensure that the sentence not only deters James Raj from committing such offences again but that it also induces him to turn from a criminal to an honest life. The public interest is indeed served, and best served, if James Raj is induced to turn away from criminal ways.

[note: 1]At the resumed hearing on 30 Jan 2015, after James Raj had discharged his counsel , Mr. M Ravi , James Raj was given an opportunity to review the SOF and he once again confirmed that he admitted it.

[note: 2]James Raj admitted the antecedent history.

[note: 3]I accepted that the offences relating to government web servers were graver as the potential to cause harm was far greater.

BACK TO TOP