IN THE STATE COURTS OF THE REPUBLIC OF SINGAPORE

[2025] SGDC 294

District Arrest Case No 919634 of 2024 and 4 others
District Arrest Case No 920171 of 2025 and 4 others
District Arrest Case No 919632 of 2024 and 4 others

Public Prosecutor

Against

(1) Huang Qin Zheng
(2) Liu Yuqi
(3) Yan Peijian

EX TEMPORE JUDGMENT

[Criminal Law] – [Statutory Offences] – [Organised Crime Act] – [Locally Linked Organised Crime Group]

[Criminal Law] – [Statutory Offences] – [Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act]

[Criminal Law] – [Statutory Offences] – [Computer Misuse Act]

[Criminal Law] – [Statutory Offences] – [Employment of Foreign Manpower Act]

[Criminal Procedure and Sentencing] – [Sentencing] – [Principles]

TABLE OF CONTENTS

Public Prosecutor
v
B1) Huang Qin Zheng
B2) Liu Yuqi
B3) Yan Peijian

[2025] SGDC 294

District Arrest Case No 919634 of 2024 and 4 others
District Arrest Case No 920171 of 2025 and 4 others
District Arrest Case No 919632 of 2024 and 4 others
District Judge Sharmila Sripathy-Shanaz

5 November 2025

District Judge Sharmila Sripathy-Shanaz:

Introduction

1 This case concerns an organised cybercrime syndicate operating from Singapore, whose members engaged in coordinated hacking operations, acquired criminal proceeds and sought to conceal their unlawful presence through false declarations to public institutions. The offences underscore the growing sophistication and transnational reach of organised crime in the digital age.

2 The accused persons, Mr Huang Qin Zheng ("**Huang**"), Mr Liu Yuqi ("**Liu**") and Mr Yan Peijian ("**Yan**") have each pleaded guilty to the following four offences:

(a) **Organised Crime Offence** - for being a member of a locally linked organised criminal group, the purpose of which was to obtain a financial benefit from the commission of offences under the Computer Misuse Act 1993 ("**the CMA**");[1]

(b) **CDSA Offence** – for acquiring cryptocurrency amounting to not less than 712,500 USDT each, which in whole directly represents their benefits from the commission of offences under the CMA;[2]

(c) **CMA Offence** – for retaining, on multiple occasions, computer programs with the intention of using them to commit offences under the CMA;[3] and

(d) **EFMA Offence** – for furnishing false employment-related information:

(i) Huang and Yan had provided false information to an Employment Inspector in the course of investigations conducted by the Ministry of Manpower;[4] and

(ii) Liu had made a false statement to the Controller of Work Passes in connection with an application to renew his work pass.[5]

---

[1] Huang, Liu and Yan's 3rd Charge, DAC-908962-2025, DAC-920172-2025 and DAC-908960-2025 respectively, framed under s 5(1) of the Organised Crime Act 2015 ("**OCA**")

[2] Huang, Liu and Yan's 2nd Charge, DAC-919634-2024, DAC-920171-2025 and DAC-919632-2024 respectively, framed under s 54(1)(c) and punishable under s 54(5) of the Corruption, Drug Trafficking and Other Serious Crimes (Confiscations of Benefits) Act 1992 ("**CDSA**")

[3] Huang, Liu and Yan's 4th Charge, DAC-908963-2025, DAC-920173-2025 and DAC-908961-2025 respectively, framed under s 10(1)(a)(i) of the CMA and amalgamated under s 124(4) and punishable under s 124(8)(a)(ii) of the Criminal Procedure Code 2010

[4] Huang and Yan's 5th Charge, MAC-904332-2025 and MAC-904331-2025 respectively, framed under s 22(1)(d) and punishable under s 22(1)(i) of the Employment of Foreign Manpower Act 1990 ("**EFMA**")

[5] Liu's 5th Charge, MAC-904324-2025 framed under s 22(1)(d) and punishable under s 22(1)(i) of the **EFMA**

3 Each accused has also consented to an additional charge of unauthorised access to computer materials, being taken into consideration. This offence was committed in the course of Huang, Liu and Yan acting on instructions to identify vulnerabilities and personal identifiable information on the websites of two companies (the "**Hacking Offence**").[6]

4 These *ex tempore* grounds set out the factors underpinning the sentences imposed for each of the offences and may be supplemented should the need arise.

The Organised Crime Offence

General Deterrence is Paramount

5 The Organised Crime Act ("**OCA**") was enacted to combat the pernicious operations of organised criminal groups ("**OCGs**") which engage in serious criminal conduct and pose a grave threat to Singapore's safety and security. As explained during the Second Reading of the Organised Crime Bill, the laws seek to enhance Singapore's ability to disrupt such groups "at various levels of their hierarchy so as to prevent them from establishing a foothold to perpetrate serious crimes": *Singapore Parliamentary Debates, Official Report* (17 August 2015), vol 93 at p 45, Mr S Iswaran, Second Minister for Home Affairs.

6 Given this legislative objective of both pre-empting and dismantling organised criminal structures, general deterrence must assume primacy in sentencing. Offences under the OCA are not isolated or opportunistic acts of individual wrongdoing. Instead, they are manifestations of coordinated and concerted profit-driven criminal enterprises that often operate across borders.

[6] Huang, Liu and Yan's 1st Charge, DAC-917974-2024, DAC-920170-2025 and DAC-917975-2024 respectively, framed under s 3(1)(a) of the CMA

The harm lies not only in the predicate offences committed, but in the broader capacity of such groups to entrench criminal activity, with attendant ills that carry far-reaching ramifications for the very fabric of society.

7 Sentences must therefore convey a clear and unequivocal message that any form of participation in, or facilitation of, organised crime – whether by financing its operations, supplying technical expertise (as in this case), recruiting members, laundering its proceeds or providing logistical or administrative support – will attract stern punishment. Indeed, a strong deterrent sentence is necessary to signal Singapore's firm and uncompromising stance against the use of its territory as a base for syndicated criminal activity.

Harm and Culpability Assessed

8 An offence under s 5 of the OCA is punishable with a fine not exceeding $100,000, imprisonment for a term of up to five years', or both.

9 I find it appropriate to approach sentencing by reference to the harm-culpability matrix, which assesses the seriousness of the offence through this dual lens.

10 In assessing harm, it is necessary to consider both the nature and gravity of the illegal purpose pursued by the organised criminal group. In the present case, the syndicate's *purpose* was rooted in cybercrime – specifically, the systematic exploitation of computer systems through the infiltration of online gambling sites and SMS service platforms.[7] While the accused persons may not have successfully achieved the full gamut of objectives set for them by Xu,[8] the

[7] Statement of Facts ("**SOF**") at [11]

[8] Huang and Liu's Mitigation Plea ("**HL-MP**") at [17(b)-(c)] and Yan's Mitigation Plea ("**Y-MP**") at [18(b)-(c)]

Statement of Facts makes plain that they did successfully download other compromised data in the course of locating vulnerabilities for Xu.[9] This is concrete evidence of *actual harm* and demonstrates that the group's activities were not merely preparatory, but had in fact culminated (at least minimally) in unauthorised intrusions and collateral data exfiltration.

11 It is also undisputed that the offence bears clear transnational features[10] which is aggravating: *Logachev v Vladislav v Public Prosecutor* [2018] 4 SLR 609 at [55]. The syndicate was physically based in Singapore but sought to execute hacking operations targeting computer systems located overseas, *viz.* foreign online gambling websites[11] and an SMS service company based in China. Such conduct gives the offending behaviour a distinctly transnational character, as the criminal activities extended beyond Singapore's borders.

12 That the accused persons targeted foreign illegal gambling platforms, does not meaningfully mitigate the harm caused. The Defence's contention to the contrary[12] is misguided and risks normalising the dangerous notion that unauthorised access to computer systems may be justified by one's choice of victim. It bears emphasis that the harm engendered by such offences does not depend on the perceived legitimacy of the intended targets. The law does not countenance the hacking of unlawful enterprises any more than it condones attacks on legitimate ones. To do so would be to sanction vigilantism (though this consideration does not even arise on the present facts) and to ignore the broader societal harm caused by such cyber-intrusions, which undermine digital security and facilitate further criminal conduct. Neither is the harm diminished

[9] SOF at [15]

[10] HL-MP at [50] and [53(f)] and Y-MP at [51] and [54(f)]

[11] HL-MP at [14] and Y-MP at [15]

[12] HL-MP at [18], [51(b)] and Y-MP at [19], [52(b)]

merely because the targets were foreign entities rather than Singapore based websites or companies. The attendant harm to Singapore arises from its use as the operational base for these illicit activities, thereby drawing transnational crime to our shores, which carries with it the potential to erode confidence in Singapore's reputation as a secure hub in the global digital ecosystem.[13]

13 These considerations are compounded by the nature of the group's operations. On the facts before the Court, while the syndicate comprised only five members[14] and did not exhibit a complex hierarchical structure, it was nonetheless well-organised, with a clear division of roles among its members.[15] It also functioned systematically, with operations ranging from the identification of vulnerabilities to the acquisition and deployment of hacking tools.[16] This level of organisation underscores the concerted and purposeful nature of the criminal enterprise, notwithstanding its modest size.

14 The assessment of culpability is informed by several key factors. First, the offences concern the *knowing* membership of an organised criminal group. A distinction must be drawn between an offender who knows that he is part of such a group and one who merely has reasonable grounds to believe that he is. It is an established principle of law that a person having 'reasonable grounds to believe', essentially has a "lesser degree of conviction than certainty but a higher one than speculation", whereas a person having actual knowledge is either certain or almost certain of the fact: see *Ang Jeanette v Public Prosecutor* [2011] 4 SLR 1 at [70] for the former proposition and *Tan Kiam Peng v Public Prosecutor* [2008] 1 SLR(R) 1 at [103] for the latter proposition. It is therefore

[13] Prosecution's Address on Sentence ("**AOS**") at [6(c)]

[14] The charges aver that the OCG comprised the accused persons, Chen Yiren and Xu Liangbiao

[15] SOF at [12] and [13]

[16] SOF at [14] to [16]

imperative for a sentencing court to recognise a corresponding distinction in culpability: *Huang Ying-Chun v Public Prosecutor* [2018] SGHC 279 at [74]. In the present case, the accused persons had knowingly lent themselves to the syndicate's operations, fully aware that its illicit purpose was to obtain "a financial benefit from the commission of offences under the Computer Misuse Act".[17]

15 Second, as to their respective roles within the organised criminal group, while Huang, Liu and Yan were not the masterminds of the operation, they formed the main engine of its cyber-offending activities.[18] Attempts by the Defence to downplay their roles grossly mischaracterises the evidence. The Statement of Facts makes plain that each accused was intimately involved in furthering the group's objectives.

16 Their respective roles were clearly delineated – Yan specialised in Linux-based systems, Huang focused on web systems and Liu concentrated on Windows-based systems.[19] Acting in concert, they approached their work methodically. They first gathered information on the domain and sub-domain names of target organisations and websites, and then used open-source tools to scan these networks for vulnerabilities. The identified vulnerabilities were then systematically categorised according to their severity, ease of exploitation and usefulness to the group's objectives. Once this groundwork was completed, they proceeded to exploit the weaknesses – either through direct data extraction or by deploying Remote Access Trojans.[20]

---

[17] Per Huang, Liu and Yan's 3rd Charge

[18] AOS at [7(a)]

[19] SOF at [13]

[20] SOF at [14]

17 The evidence also shows that Huang, Liu and Yan demonstrated a deliberate and sophisticated approach to concealing their intrusions. They exploited tools built into target computers' existing operating systems (such as the Network Policy Server) to establish remote connections, preferring these native tools over external malware because they were less likely to be detected.[21] When vulnerabilities were discovered, they would report them to Xu and, upon his instruction, download the compromised data which included personal information such as names, email addresses, phone numbers, IP addresses and site credentials.[22] To advance the group's objectives, they obtained malware from the internet, engaged with other hackers for technical advice, and sought out zero-day vulnerabilities in the network architectures of their targets. The group even went so far as to commission a developer to create a customised tool to aid their operations.[23]

18 These details collectively disclose that the accused persons were far from peripheral actors or passive, reluctant and nonchalant participants, as the Defence has sought to portray them. On the contrary, they formed the *operational core* of the organised crime group and were directly responsible for executing its cyber-offending activities. The Defence's contention that Huang, Liu and Yan lacked refined technical skills,[24] even if accepted, does not mitigate their culpability. It would be perverse to allow an offender to invoke his own *purported* incompetence as a basis to diminish his blameworthiness for deliberate and active participation in an organised cybercrime enterprise.

---

[21] SOF at [14]

[22] SOF at [15]

[23] SOF at [16]

[24] HL-MP at [17] and Y-MP at [18]

19 Third, the sustained nature of Huang, Liu and Yan's involvement further underscores their culpability. Having been members of the organised crime group for a protracted period of some 16 months, their participation cannot be characterised as fleeting or incidental. It matters not that the accused persons may have returned to China for brief periods during this time.[25] By pleading guilty to the charge, they accept that they remained members of the group from May 2023 to 9 September 2024. This extended duration of involvement reflects both commitment and persistence in advancing the group's criminal objectives and demonstrates that their participation was neither transient nor reluctant.

20 Fourth, it is not beyond reasonable contemplation that the accused persons' continued participation was driven by personal gain. Although the overarching purpose of the group was to enrich its leader, Xu,[26] each accused derived tangible benefits from his involvement. They resided in paid accommodation arranged for them (costing approximately $33,000 per month), had their daily needs catered for, received a sizeable sum of $52,412 for day-to-day expenses and were even paid a monthly salary of $2,000 from early 2024 to maintain the guise and appearance that they were legitimately and gainfully employed in Singapore.[27] Even on the limited facts before the Court, these were plainly not individuals acting out of altruism or magnanimity, but participants whose continued involvement clearly served their own interests. Offences committed for personal enrichment, will rarely be treated with much sympathy in sentencing: *Teo Chu Ha v Public Prosecutor* [2023] SGHC 130 at [165], citing *Zhao Zhipeng v Public Prosecutor* [2008] 4 SLR(R) 879 at [37].

[25] HL-MP at [60] and Y-MP at [61]

[26] SOF at [12]

[27] SOF at [19]

The Sentence Imposed

21 Drawing the threads together, I find that the harm occasioned by the offence is moderate and the offenders' culpability is medium. An indicative starting point of 24 months' imprisonment is appropriate.

22 The accused persons' plea of guilt, indicated at Stage 1 of the Sentencing Advisory Panel's *Guidelines on Reduction in Sentences for Guilty Pleas* ("**PG Guidelines**"), warrants a reduction of 30% - the maximum permitted at this stage. The resulting final sentence is therefore 16 months' imprisonment.

23 I would highlight that the sentence reflects the harm and culpability as presently established on the evidence. Had there been tangible evidence of the financial benefit accruing to the organised criminal group from the accused persons' participation, or of the degree of cyber-infiltration that was achieved, the harm occasioned by the offence would be greater, and a correspondingly higher sentence would be warranted.

24 For completeness, I do not find the sentence imposed to be inconsistent with existing sentencing practice. While the predicate offence in the present case is less serious than that in *Public Prosecutor v Hermanto Bin Abdul Talib* [2021] SGDC 205 ("***Hermanto***") – where the offender, who occupied a leadership role, was sentenced to 20 months' imprisonment – the present case is aggravated by a significantly longer period of offending and the presence of a transnational element, neither of which featured in *Hermanto*. Similarly, the cases of *Public Prosecutor v See Chye Huat* [2024] SGDC 229 and *Public Prosecutor v Lai Yen San* [2019] SGDC 39 – where the offenders were sentenced to 18 months' and 8 months' imprisonment respectively – are distinguishable, most notably due to the substantially longer offending period in the present case. As the Defence itself acknowledges, any comparison

between these cases would be "pointless", given their markedly different factual matrices.[28]

25 The fact remains that no two cases are ever alike, and the value of a particular sentencing precedent necessarily depends on the degree of factual similarity between the cases: *Toh Suat Leng Jennifer v Public Prosecutor* [2022] SGHC 146 at [34]. Ultimately, the principle of individualised justice requires that the sentence reflects the unique offence and offender-specific factors that are engaged. That is what I have done here.

The CDSA Offence

26 I turn next to the CDSA charge. The prescribed punishment for this offence is a fine not exceeding $500,000, imprisonment for a term not exceeding 10 years, or both.

27 The overriding sentencing consideration is general deterrence: *Public Prosecutor v Su Jianfeng* [2024] SGDC 188 ("***Su Jianfeng***") at [17]. The value of the property acquired is a key indicator of harm, and in this regard, I cannot ignore the fact that the offences concern cryptocurrency of substantial value, *viz.* 712,500 USDT. The presence of a transnational element is additionally aggravating as the property acquired by the accused persons comprised benefits derived from criminal conduct with transnational links (*supra* at [11]).[29]

[28] HL-MP at [82] and Y-MP at [83]

[29] The Defence accepts that but for the OCA offence, Xu would not have remitted the USDT to the accused persons. It also accepts that the "OCG had transnational links": HL-MP at [53(f)], [93(b)] and Y-MP at [54(f)], [94(b)]

28 I accept that the accused persons neither dictated the quantum of the criminal proceeds they ultimately received,[30] nor utilised the cryptocurrency upon receipt.[31] However, it bears emphasis that the absence of an aggravating factor is not, by itself, mitigating: *Edwin s/o Suse Nathen v Public Prosecutor* [2013] 4 SLR 1139 at [24] to [25]. The aforementioned matters are thus, at best, neutral for the purpose of sentencing here.

29 It must be borne in mind that the present offence concerns the *acquisition* of ill-gotten proceeds derived from criminal conduct. While acts to conceal, disguise or otherwise deal with such property *may* aggravate the underlying offence – particularly where they reflect an intention to evade detection, demonstrate sophistication or facilitate further illicit activity for example – the *absence* of such acts cannot properly be regarded as mitigating. In any event, it does not escape attention that the accused persons were arrested within four days of acquiring the property, which would plainly have curtailed their ability to deal further with it. Further, even if the accused persons did not determine the quantum of the proceeds they received, the sum they acquired clearly reflected their value to Xu and the organised criminal group.

30 Balanced against the foregoing considerations, are Huang, Liu and Yan's plea of guilt and their voluntary surrender of the full sum of cryptocurrency acquired,[32] both of which I accept as demonstrating genuine contrition. The latter, in particular, significantly attenuates the harm occasioned by the offence, and I accord substantial weight to it in sentencing.

---

[30] AOS at [13(a)]

[31] AOS at [13(b)]

[32] HL-MP at [101] and Y-MP at [102]

31 Having regard to all the circumstances, and taking the sentence imposed in *Su Jianfeng*[33] as a yardstick, I find that a sentence of 12 months' imprisonment in the present case is condign.

The CMA Offence

32 The sentence to be imposed for the CMA Offence calls for separate consideration. Being amalgamated, the offence is punishable with a fine not exceeding $20,000, imprisonment for a term not exceeding six years, or both. A holistic appreciation of the harm and culpability associated with the entire course of conduct is necessary: *Prakash s/o Mathivanan v Public Prosecutor* [2025] SGHC 167 at [39].

The Need for Deterrent Sentencing

33 The scale and complexity of cybercrime has increased markedly in recent years, fuelled by rapid technological advancement and the "evolving tactics of cybercriminals" who now employ a wide array of tools and methods to execute elaborate attacks. Massive data breaches and system intrusions have become alarmingly commonplace, imposing significant costs on individuals, businesses and society at large. Section 10 of the CMA was enacted to criminalise acts involving items designed primarily for the commission of computer crimes, commonly referred to as 'hacking tools'. These may include physical devices, software, passwords and access codes intended to facilitate unauthorised access to computer systems: *Singapore Parliamentary Debates, Official Report* (3 April 2017), vol 94, Mr Desmond Lee, Senior Minister of State for Home Affairs.

[33] A sentence of 14 months' imprisonment was imposed for a similar charge involving $550,903, even though the total quantum of ill-gotten proceeds across the charges taken into consideration, amounted to a significant S$17,000,000

34 The provision was introduced to pre-empt and deter cybercriminal activity at its inception, by criminalising the acquisition or retention of such tools with the requisite criminal intent, even before any substantive intrusion or harm occurs. In doing so, the law seeks to address the potential cascading harm that may arise from the possession of such tools. The legislative intent thus underscores the preventive and deterrent purpose of the provision, recognising that the ready availability of hacking tools poses an inherent threat to the integrity and security of computer systems. In light of this broad legislative purpose, general deterrence must feature as the dominant sentencing consideration for this class of offences.

Harm and Culpability Assessed

35 In the present case, the malware accumulated by the accused persons between May 2023 and 9 September 2024 was not only substantial in quantity, but also sophisticated, comprising Java deserialisation exploits, webshells, payload writers and at least 175 remote access trojans ("**RATs**"), no fewer than 14 of which were associated with *'plugX'*, a particularly sophisticated RAT.[34]

The Sentence Imposed

36 Having regard to the nature and volume of the malware retained, the intended end use of these hacking tools to further the objectives of an organised criminal group, as well as the prescribed punishment for the offence, I find that a sentence of 6 months' imprisonment is warranted and accords with the legislative purpose underlying s 10 of the CMA, which, as earlier canvassed, seeks to deter the proliferation of tools capable of facilitating cyberattacks.

[34] SOF at [25] to [26]

37 The sentence applies uniformly across the accused persons, notwithstanding that the charges against them pertain to a different number of occasions on which the offence was committed. This reflects the reality that Huang, Liu and Yan had acted collectively on Xu's instructions, and the malware possessed by each, was unified by a common criminal objective. It is therefore appropriate to approach sentencing by reference to the overall culpability and harm engendered by the collective offence, rather than the individual acts of each accused in isolation.[35]

The EFMA Offence

38 I turn next to the offence under s 22(1)(d) of the EFMA, which concerns the furnishing of false employment-related information by the accused persons. The offence is punishable with a fine not exceeding $20,000, imprisonment for a term not exceeding two years, or both. Sentencing is guided by the principles espoused in *Chiew Kok Chai v Public Prosecutor* [2019] SGHC 169 ("***Chiew Kok Chai***") and *Koh Yong Chiah v Public Prosecutor* [2016] SGHC at 253. Though the latter concerns a framework established in relation to offences under s 182 of the Penal Code, it is similar in policy rationale, being likewise directed at the making of false statements to public authorities.

39 In the present case, the provision of false information by Huang and Yan arose in the course of investigations conducted by the Ministry of Manpower into the circumstances surrounding their entry into, and continued presence, in Singapore.[36] The parties are *ad idem* that the custodial threshold is crossed.[37] I agree. Having regard to the materiality of the falsehood, which sought to frustrate official investigations and conceal Yan and Huang's prolonged

[35] A position similarly advocated by the Prosecution, AOS at [22]

[36] SOF at [31]

[37] AOS at [26], HL-MP at [124] and Y-MP at [123]

illegitimate presence in Singapore, and the fact that it was maintained for about a month,[38] I find that a sentence of 1 weeks' imprisonment is appropriate.

40 By contrast, Liu's false statement to the Controller of Work Passes was made in connection with an application to renew his work pass. The falsity was material to the decision to approve the renewal[39] and was motivated by an intention to remain in Singapore to continue engaging in organised crime. The offence falls within Band 1 of the framework in *Chiew Kok Chai*, and warrants a starting point of 6 weeks' imprisonment. This is further moderated to reflect Liu's plea of guilt, indicated at Stage 1 of the PG Guidelines. Applying a 30% reduction, the resulting final sentence is 4 weeks' imprisonment.

The Aggregate Sentence

41 Finally, I order the sentences for the Organised Crime, CDSA and EFMA offences to run consecutively, as they engage different legal interests and it is, in my judgment, necessary to reflect the added criminality stemming from separate and unrelated offending. The aggregate sentences imposed on each of the accused persons is thus as follows:

(a) Huang and Yan: 28 months and 1 weeks' imprisonment

(b) Liu: 28 months and 4 weeks' imprisonment

42 On balance, I am satisfied that the sentences imposed are proportionate and not excessive. The sentences are backdated to 9 September 2024, being the date of the accused persons' arrest.[40]

[38] SOF at [35] and [40]

[39] SOF at [43] to [44]

[40] SOF at [47]

Concluding Remarks

43 As observed at the outset, the offences before the Court span multiple domains – syndicated cybercrime, the acquisition of criminal proceeds and false declarations to public authorities – each engaging distinct public interests and revealing the complex and multifaceted threats posed by organised criminal networks. The sentences imposed collectively reflect the heightened need for general deterrence, both to safeguard and preserve Singapore's integrity as a trusted and secure digital hub, and to send a clear and unequivocal message that those who seek to establish or conduct transnational criminal operations within our borders, will face firm sanction.

Sharmila Sripathy-Shanaz
District Judge

DPP Hon Yi, DPP Cheah Wenjie and DPP Shaun Lim
(Attorney General's Chambers)
for the Public Prosecutor;

Lee Teck Leng (Legal Clinic LLC)
for the accused B1 and B2;

Ong Kai Min, Kelvin (Contigo Law LLC)
for the accused B3.