香港法律改革委员会

《依赖电脑网络的罪行及司法管辖权事宜》报告书

摘要

（本摘要为报告书内容的概要。报告书可于法律改革委员会（法改会）的网站下载，网址是：https://www.hkreform.gov.hk，其文本亦可向香港中环花园道 3 号冠君大厦 9 楼法改会秘书处索取。）

咨询过程

1. 法改会辖下的电脑网络罪行小组委员会（“**小组委员会**”）在 2022 年 7 月发表《依赖电脑网络的罪行及司法管辖权事宜》咨询文件（“**咨询文件**”），所研究的范围如下：

> “鉴于资讯科技、电脑和互联网方面发展迅速，加上其有被利用来从事犯罪活动的潜在可能，
>
> (a) 从刑事法角度找出这些迅速发展对保障个人权利和执法带来哪些挑战；
>
> (b) 检讨处理上文(a)段所指挑战的现有法例和其他相关措施；
>
> (c) 探讨其他司法管辖区的相关发展；及
>
> (d) 建议可作出哪些法律改革以应对上述事宜。”

2. 小组委员会在公众咨询期间收到 65 份意见书。我们十分感谢所有曾提出意见的**回应者**。回应者的名单载于报告书附件。

报告书的结构

3. 报告书关乎小组委员会的研究的第一部分，[1] 共有九个章节，处理 16 项最终建议：

(a) 第 1 章描述国际机构和举措如何将电脑网络罪行归类。欧洲委员会（Council of Europe）的《电脑网络罪行公约》（Convention on Cybercrime，**《布达佩斯公约》**）所处理的*"损害电脑数据及系统的机密性、完整性和可用性的罪行"*，[2] 大致上对应报告书的重心。

(b) 第 2 至 6 章分别处理五类依赖电脑网络的罪行，即：

(i) 非法取览程式或数据；

(ii) 非法截取电脑数据；

(iii) 非法干扰电脑数据；

(iv) 非法干扰电脑系统；及

(v) 提供或管有用作干犯电脑网络相关罪行的器材、程式或数据。

(c) 第 7 章处理香港法庭行使司法管辖权的准则。

(d) 第 8 章处理这些罪行的判刑事宜。

(e) 第 9 章总结我们的最终建议。

第 2 章：非法取览程式或数据（"取览罪"）

4. 咨询文件建议 1 提出，在未获授权下取览程式或数据应定为简易程序罪行，而作出这类取览并意图进行其他犯罪活动应构成加重罪行。有关条文应以英格兰及威尔斯《误用电脑法令》（Computer Misuse Act，**《英格兰误用电脑法令》**）第 1、2 及 17 条为蓝本。回应者普遍赞成建议 1，但部分回应者质疑纯粹在未获授权下取览（即"没有犯

---

1 由於小組委員會的研究範圍廣泛，我們的研究分為三個階段。研究的第二部分會涵蓋借助電腦網絡的罪行，該部範圍再作討論。第三部分會處理證據事宜及執法（程序）事宜。

2 該公約所處理的其他罪行類別，是電腦相關罪行（包括電腦相關偽造及欺詐）、內容相關罪行（包括兒童色情物品相關罪行，以及通過電腦系統散布種族主義和仇外材料的相關罪行），以及關於侵犯版權和相關權利的罪行。

罪意图”）应否构成罪责。其他回应者则提议厘清“合理辩解”免责辩护的涵盖范围。

取览罪的意念元素 [3]

5. 值得注意的是，就简易程序罪行及加重罪行的犯罪意念而言，控方均必须证明，被告人在作出未获授权的取览时，知悉该项取览未获授权，这与《英格兰误用电脑法令》第 1(1)条的规定一致。

6. 我们同意，鉴于电脑网络空间的设计和运作特点，在某些获广泛接受的情况下，网上用户均已默示给予取览程式或数据的授权，并且应继续容许在使用电脑网络空间时已普遍接受的情况下，无须就取用或取览事先寻求明示授权的惯常做法。另一些涉及默示授权的情况例子，包括但不限于以下情况：因设计缘故和实际需要而进行自动连接，并由此而发生取览程式或数据。[4]

7. 因此，我们仍然认为，把某人知悉有关取览未获授权定为取览罪的先决条件，是公允的做法。最终法庭会在考虑案件的整体情况后，裁定是否可从证据作出被告人知悉该项取览未获授权的必然推论。[5]

纯粹在未获授权下取览应属犯罪 [6]

8. 各回应者就取览罪的意念元素所提出的意见，关乎纯粹在未获授权下取览程式或数据应否被定罪这问题，咨询文件已对此作出讨论。[7]

9. 由于黑客的企图入侵所造成的不确定性及成本，《英格兰误用电脑法令》所订的纯粹在未获授权下取览罪当时所回应的，是人们需要保护电脑系统的完整及安全，使其免受未获授权人士攻击，不论这些人有何意图。个别案件中的取览是否获得默示授权，会视乎证据所显示的事实和情况而定。

10. 由于互联网如今渗透大部分公共和私人生活，因此更有需要确保电脑系统及网络完整，使其免受未获授权的取用或取览。简易程序罪行及加重罪行旨在共同发挥作用，以有效阻吓各种形式的未获授

---

3 報告書第 2.18 至 2.24 段。
4 報告書第 2.25 及 2.26 段。
5 請參閱報告書第 2.23 及 2.24 段的說明例子。
6 報告書第 2.25 至 2.31 段。
7 第 2.4、2.5、2.96 至 2.101 段。

权取览。故此，我们维持原先看法，认为纯粹在未获授权下取览程式或数据应构成罪行。

合理辩解一般免责辩护及特定的免责辩护 [8]

11. 我们认为，尝试在电脑网络罪行法例中诠释"合理辩解"，甚或提供一份例子清单，以阐明有关立法原意，均可能会无意中收窄合理辩解免责辩护的范围。

12. 虽然我们的结论是不应界定"合理辩解"，但我们建议应另外加入特定的免责辩护，以豁除我们认为显然不应属非法的各类行为。[9] 这样会消除公众对某些活动是否属合理辩解免责辩护范围的疑惑，从而使新法例更为清晰明确。

执法机关进行的合法活动 [10]

13. 部分回应者寻求澄清以下一点：执法机关在有手令或无手令的情况下为刑事调查目的而取览电脑程式或数据，会否获豁免刑事法律责任。由于取览罪并非旨在影响执法机关进行的任何合法活动，我们建议将"无合法权限"纳入为该罪行的元素。个别案件中是否有"合法权限"这问题关乎事实。警务人员如已为搜查流动电话或其他电子器材而取得裁判官所发出的搜查令，或有合理依据支持在无手令的情况下搜查这些器材，因而符合*岑永根 诉 警务处处长*[11]中订立的规定，便属有*"合法权限"*而取览程式或数据。此外，不论是否有合法权限，在迫切情况下取览程式或数据，本身便可能属于合理辩解免责辩护的范围。因此我们认为，如未能提供充分理由而在无手令的情况下取览程式或数据，即使是为了执法目的，也应构成取览罪，实属适当。

14. 因此，我们的**最终建议 1** 如下：

"我们建议：

(a) 无合法权限而在未获授权下取览程式或数据，应在新法例下定为简易程序罪行，而合理辩解可作为法定免责辩护。

---

8 報告書第 2.32 至 2.34 段。
9 見本摘要第 18 至 33 段。
10 報告書第 2.35 至 2.37 段。
11 [2020] 2 HKLRD 529, CACV 270/2017（判決日期：2020 年 4 月 2 日）。

(b) 这项建议罪行的犯罪意念是：

(i) 被告人意图获得对有关程式或数据的取览，或意图使他人能够获得该项取览；及

(ii) 被告人在取览有关程式或数据时，知悉该项意图作出的取览未获授权。

(c) 在未获授权下取览程式或数据，并意图进行其他犯罪活动，应构成新法例所订的加重罪行，并招致更高刑罚。

(d) 新法例的建议条文应以英格兰及威尔斯《误用电脑法令》第1、2及17条为蓝本。"

建议2之中的咨询问题

15. 咨询文件建议2邀请公众就以下问题提交意见书：在未获授权下取览，应否有任何特定的免责辩护或豁免。该问题由以下几部分组成：

"(a) 对于为网络安全目的而取览而言，如答案是应该的话，应有甚么条款？举例来说：

(i) 该免责辩护或豁免应否只适用于经认可专业团体或评审团体审定的人士？

(ii) 如(i)段的答案是应该的话，评审制度应如何运作……？

(iii) 反之，如不属意设立评审制度，则新订针对电脑网络罪行的特定法例应否订明指认的网络安全专业人员须符合某些规定，方可援引建议为网络安全目的提供的免责辩护或豁免？如应该的话，这些规定应是甚么？

(b) 该免责辩护或豁免应否适用于非保安专业人员（请参阅建议8(b)所述的例子）？"

16. 绝大多数回应者均支持订定特定的网络安全免责辩护，因为他们认为，白帽黑客及其他网络安全专业人员在侦测网络安全威胁及保安漏洞方面的工作，的确有其价值。另一方面，少数回应者则反对订定该项特定的免责辩护，不赞成免责辩护实际上带来一个"享有特权的界别"。他们认为，该项特定的免责辩护应适用于所有人，而非只适用于经由认可专业团体或认可团体认可的人士，不论这些人有何意图。

17. 明显大多数回应者均同意应设立认可制度。这结果与回应者普遍认为适宜为在未获授权下取览订定特定免责辩护的意见相符。部分回应者同意，设立一个认可团体让网络安全专业获得适当认可，会为香港带来长远裨益。

为经认可的网络安全从业员提供特定的免责辩护 [12]

18. 我们认为，为资讯科技行业内某界定类别的人士订定特定免责辩护，是合理而务实的做法。我们建议，经认可的网络安全从业员如为真正的网络安全目的而行事，应有特定的免责辩护或豁免。然而，在顾及整体情况后，被告人的目的和行为必须是合理的。

经认可或持牌网络安全从业员

19. 鉴于为网络安全目的而取览程式或数据的入侵程度，以及网络安全目的这宽广概念，我们认为应只有持牌或经认可的从业员（即应具备一定水平的专业技能和正直品格者），才可为网络安全目的而作出取览。

20. 应设有一套独立的制度，以对网络安全从业员进行认可，并监督他们的纪律事宜。我们同意回应者所言，认可制度可以不同方式落实。其中一种方式是指定由某法定主管当局进行认可；另一种方式则是，任何人如是声誉良好的资讯科技专业团体或国际资讯科技协会的成员，即会获得认可。

21. 视乎所采用的模式，认可制度对网络安全业界和电脑网络空间用户的影响，并不限于网络安全专业人员的供应和收费。如何落实认可制度的细节问题，本质上属政府的政策事宜，故这些细节问题（包括对网络安全专业人员的认可要求、从业员须遵行的备存纪录责任、

12 報告書第 2.63 至 2.74 段。

认可团体是由资讯科技行业还是其他主管当局管理，以及应如何为认可制度提供资金）适宜留待政府决定。[13]

真正的网络安全目的

22. “真正的网络安全目的”这额外规定，意味着被告人的认可资格或身分不应具决定性。我们的有关建议拟达到以下效果：举例来说，经认可的网络安全从业员如并非为真正的网络安全目的而取览自己子女电话内的数据，则只能援引“为保障儿童利益而取览”作为免责辩护，这会在下文第 24 至 27 段讨论。

在顾及整体情况后，被告人的行为必须是合理的

23. 我们亦建议在该项特定免责辩护加入“合理性”要求，从而提供稳妥和一致的规范，以界定一名明理的人所能接受的行为。若认可团体公布任何道德守则，法庭当然可参考该守则，以评定被告人的行为是否合理。

取览罪的其他特定的免责辩护

为保障儿童利益而取览[14]

24. 在咨询期间，有人提出关于家长应否获准取用子女电脑的意见。我们认为，把“为保护 16 岁以下儿童而取览”明文豁除于取览罪之外，会是明智之举。虽然这项特定免责辩护可能会削弱 16 岁以下儿童的私隐权，但鉴于这些儿童的互联网渗透率甚高，我们认为订有此免责辩护会符合保障他们利益的原则。

25. 为提供最大保障，这项建议的免责辩护是否成立，视乎寻求作出有关取览的人的主观目的而定，而非视乎该人与有关儿童的关系而定。

26. 为避免这项免责辩护被滥用，取览作为应限于在顾及案件的整体情况后为保障儿童利益而合理所需者。我们已指明这项免责辩护的以下两个制定方案：

---

13 為方便政府考慮認可制度，我們已在報告書第 2.67 至 2.70 段對認可建議及它可能造成的影響提出看法。

14 報告書第 2.75 至 2.91 段。

(a) 涵盖范围较广的免责辩护：为保障儿童利益而取览程式或数据；及

(b) 涵盖范围较窄的免责辩护：为防止儿童受到身体、情绪或心理伤害而取览程式或数据。

27. 我们已在报告书分析这两个方案的优劣利弊。[15] 小组委员会稍微占多的成员属意采用涵盖范围较广的方案一。由于政府若决定落实我们这项建议，可进一步征询公众意见，因此这议题最好由政府在考虑社会意见后再作定夺。

28. 由于精神上无能力的成年人可能容易遭受剥削，因此我们进一步建议，这项在未获授权下取览程式或数据的特定免责辩护应延伸至保护易受伤害人士，即《精神健康条例》（第 136 章）所界定的精神紊乱的人[16] 及弱智人士。[17]

为真正的研究目的而取览 [18]

29. 多个资讯科技相关团体均提议，取览程式或数据如是为了在受控环境中进行研究、分析或测试自己拥有的器材或目标，应获得豁免。

30. 我们同意，由于这些研究或许能得出有用的分析或资讯，[19] 因此提供“为研究目的而取览程式或数据”这项特定免责辩护，属合理之举。我们认为，就各项儿童色情物品罪行所订的免责辩护[20] 可用作蓝本，把上述建议的免责辩护制定为“为真正的教育、科学或研究目的而取览程式或数据”。为免被滥用，该免责辩护应订有以下要求：取览须属合理，而该取览不得超过为达到有关目的而所需者。这项“合理性”要求作为客观准则，用以裁定被告人的取览是否适度或合理。

---

15 第 2.85 至 2.87 段。

16 根據《精神健康條例》第 2 條，*“精神紊亂的人”*指 *“任何患有精神紊亂的人”*。

17 根據《精神健康條例》第 2 條，*“弱智人士”*指 *“弱智的人或看來屬弱智的人”*。

18 報告書第 2.92 至 2.94 段。

19 例如研究人員或網絡安全從業員確定在香港未受保護的電腦數目。

20 《防止兒童色情物品條例》（第 579 章）第 4(2)(a)及(3)(a)條。

《刑事罪行条例》第 64(2)条所订、关于非法干扰电脑数据罪及非法干扰电脑系统罪（“干扰罪”）的免责辩护 [21]

31. 由于干扰电脑数据及／或干扰电脑系统通常只在取览程式或数据后发生，因此我们认为，《刑事罪行条例》第 64(2)条（“**第 64(2)条**”）所订的同意免责辩护及保护财产免责辩护[22]（两者均适用于干扰罪），[23] 应同样适用于取览罪。

32. 鉴于同意免责辩护及保护财产免责辩护均适用于干扰罪，我们认为，取览罪的免责辩护应采用统一的处理方式。将第 64(2)条所订的免责辩护改列于电脑网络罪行法例时，我们建议提高援引有关免责辩护的门槛，在上述两项免责辩护加入客观验证标准：

(a) 就同意免责辩护而言，被告人必须合理地相信自己已获同意或会获同意取览有关程式或数据；及

(b) 就保护财产免责辩护而言，被告人必须合理地相信有关财产需即时保护。

33. 上述调整会使同意免责辩护及保护财产免责辩护，与我们就取览罪所建议的其他特定免责辩护看齐，即所有免责辩护均一致采用“合理性”要求。

34. 因此，我们提出**最终建议 2** 如下：

> “就建议的非法取览程式或数据罪而言，我们建议除合理辩解可作为法定免责辩护外：
>
> (a) 在未获授权下为网络安全目的而取览，应有特定的免责辩护，但须符合以下条件：

---

21 報告書第 2.95 至 2.102 段。

22 根據《刑事罪行條例》（第 200 章）第 64(2)條，任何被告人被控以刑事損壞罪，在下述情況下均須被視為有合法辯解：

(a) 如指稱構成該罪行的作為作出時，被告人相信，他相信有權同意有關財產的摧毀或損壞的人已予同意，或相信該人如知道有關財產的摧毀或損壞及有關情形亦會予以同意（“**同意免責辯護**”）；或

(b) 如被告人摧毀或損壞有關財產或威脅會如此做，或（在被控以第 62 條所訂罪行時）意圖使用或導致或准許使用某些物品以摧毀或損壞有關財產，而他如此做是為了保護財產（不論屬於其本人或另一人），且於指稱構成該罪行的作為作出時，被告人相信——

(i) 該財產需即時保護；及

(ii) 在顧及一切有關情況後，所採用或打算採用的保護方法是或會是合理的（“**保護財產免責辯護**”）。

23 見本摘要第 62 至 64 段。

(i) 被告人必须是经认可的网络安全从业员(认可制度的细节本质上属政策事项,最好留待政府考虑);

(ii) 被告人必须为真正的网络安全目的而行事;及

(iii) 在顾及整体情况后,被告人的行为必须是合理的。

(b) 在未获授权下为保障16岁以下儿童及易受伤害人士(即《精神健康条例》(第136章)所界定的精神紊乱的人或弱智人士)的利益而取览,应有特定的免责辩护:

(i) 这项免责辩护建基于取览儿童或易受伤害人士的程式或数据的人的主观目的(即为了保障有关儿童或易受伤害人士的利益),而非该人与有关儿童或易受伤害人士的关系。

(ii) 在顾及整体情况后,被告人对程式或数据的取览必须是合理的。

(c) 在未获授权下为教育、科学或研究目的而取览,应有特定的免责辩护。在顾及整体情况后,被告人对程式或数据的取览必须是合理的。

(d) 《刑事罪行条例》(第200章)第64(2)条所订的关于非法干扰电脑数据罪及非法干扰电脑系统罪的免责辩护,也应可就非法取览程式或数据罪而提出。

(i) 第64(2)条所订的两项免责辩护涵盖以下情况:

(1) 被告人在取览程式或数据时,相信其作为已获同意或会获同意;或

(2) 被告人在取览程式或数据时,相信有关财产需即时保护,并相信在顾及整体情况后,所采用的保护方法是合理的。

(ii) 被告人不论是提出同意免责辩护或保护财产免责辩护，均必须合理地相信该免责辩护所订的有关事宜。"

延长循简易程序检控五类依赖电脑网络罪行的时效期 [24]

35. 《裁判官条例》（第 227 章）第 26 条订定提出检控的一般时效期为六个月。由于六个月或不足以调查电脑网络罪行案件，[25] 因此咨询文件建议 3 提出，新订的电脑网络罪行法例应把时效期延长至两年。

36. 大多数回应者均支持建议 3，而少数回应者则属意维持六个月的期限，以鼓励执法机关保持警惕。我们希望澄清一点，建议 3 仅旨在延长时效期，以确保即使由于本身涉及的难题，以致有关指称罪行的调查按理不能在预设的六个月期限内完成，随后提出检控的时限也不会届满，而非因为我们不相信执法机关能在公平情况下尽速处理电脑网络罪行案件。

37. 因此，我们建议保留咨询文件建议 3 作为**最终建议 3**：

"我们建议，尽管有《裁判官条例》（第 227 章）第 26 条的规定，适用于循简易程序就任何建议罪行提出检控的时效期，应为发现就该罪行定罪而须予以证明的任何作为或不作为或其他事情（包括一项或多项作为或不作为所产生的任何后果）后的两年。"

第 3 章：非法截取电脑数据

38. 明显大多数回应者均支持咨询文件建议 4，该建议提出，为不诚实或犯罪目的而在未获授权下截取、披露或使用电脑数据应定为罪行。然而，部分资讯科技团体忧虑，建议的截取罪会对网络安全从业员所进行涉及截取的合法作为（例如网络入侵侦测、渗透测试，以及为找出攻击或分析网络通讯而进行的网络监察）带来潜在不确定性。

---

24 報告書第 2.106 至 2.110 段。

25 正如諮詢文件所解釋，受害人可能在電腦網絡罪行案件發生後兩或三個月才向警方報案，而更甚者，六個月在事件被揭發時經已屆滿。警方從互聯網服務提供者取得日誌紀錄，可能需要幾個月。分析這些日誌紀錄可能再需要幾個月，還須顧及達至檢控決定所需的額外時間。

"为不诚实或犯罪目的"这项规定适当 [26]

39. 正如咨询文件所述，[27] 我们强调，我们完全知悉现代网络器材的运作方式难免牵涉截取，而网络安全公司在正常业务中亦可能会以各种方式截取数据。这解释了咨询文件为何建议把*"为不诚实或犯罪目的"*而截取列为规定之一。这项意念元素旨在订立较高的门槛，避免所订罪行的范围不合理地广泛，以免日常使用电脑网络科技时正常进行的数据截取会被定罪。

40. 我们亦承认，若干临界情况的行为或会出现一些不确定性。在该等情况下，某人是否犯截取罪会视乎案件的特定情况而定，包括被告人截取的目的和牵涉的数据。[28]

41. 采用*"为不诚实目的"*这标准的好处在于法庭可以考虑众多因素，以决定截取行为是否属于可接受的界限内。权衡之下，我们的结论是，*"为不诚实或犯罪目的"*这个犯罪意念门槛属适当，能够避免令无恶意进行截取的人无意间误堕法网。

在未获授权下披露或使用数据 [29]

42. 咨询文件建议 4 拟禁止在未获授权下披露或使用"截取的数据"，原因在于其后披露或使用截取的数据，可能会引起私隐方面的关注及其他潜在问题。[30] 经再三检视后，若罪行是基于为不诚实或犯罪目的而在未获授权下披露或使用"任何数据"（不限于截取的数据），则未免过于广泛，因为这项罪行实质上会适用于我们日常数码生活中接触到的各类数据。

43. 鉴于在未获授权下披露或使用电脑数据这项一般罪行[31] 影响甚广，为审慎起见，我们应先在研究的第二部分[32] 深入探讨这

---

26 報告書第 3.30 至 3.36 段。

27 第 3.97 段。

28 相關例子見報告書第 3.34 及 3.35 段。

29 報告書第 3.25 至 3.29 段。

30 例如在電子商貿交易中，倘若信用卡資料在傳送至賣方期間被截取作不當用途，持有人可能會蒙受財務損失。見諮詢文件第 3.92 及 3.94 段。

31 在未獲授權下披露或使用電腦數據的罪行，只要涉及個人資料，就更當屬個人資料私隱專員公署（"**私隱專員公署**"）檢視的範疇。最近一次在 2021 年的立法修訂工作中（即制定《2021 年個人資料（私隱）（修訂）條例》），私隱專員公署特別聚焦於"起底"罪行，務求遏止在未獲同意下披露個人資料（見該修訂條例的詳題）。"起底"罪行的犯罪意念非常局限於特定範圍。

32 第二部分的範圍適時再作討論，該部分會涵蓋借助電腦網絡的罪行，即通過使用電腦、電腦網絡或其他形式的資訊及通訊科技，使犯罪規模或範圍得以擴大的傳統罪行。見報告書導言第 8 段。

议题，然后才就应否建议订立这方面的新罪行（以及如应该的话，如何订立）发表任何确定意见。例如，可进一步斟酌该项罪行应否局限于截取的数据，因为有人或会认为，某人如*"为不诚实或犯罪目的"*而披露或使用电脑数据，该项行为本身便应构成罪责，不论有关数据是在获授权下截取而获得，或是在未获授权下截取（或以任何其他方式）而获得。

44. 基于上述理由，我们提出**最终建议 4** 如下：

"我们建议：

(a) 为不诚实或犯罪目的而在未获授权下截取电脑数据，应在新法例下定为罪行。

(b) 建议的罪行应：

(i) 保障一般通讯，而并非只保障私人通讯；

(ii) 一般适用于数据（不论有关数据是否元数据）；及

(iii) 适用于截取在传送人一端前往传送对象一端途中的数据，即传送中的数据及在传送期间暂时静止的数据。

(c) 除上述另有规定外，建议的条文应以《电脑罪行及电脑相关罪行示范法》（Model Law on Computer and Computer Related Crime）第 8 条为蓝本，包括犯罪意念（即"蓄意"截取）。

(d) 关于在未获授权下披露或使用电脑数据（不论该数据是以截取或其他方式取得），我们应先在研究的第二部分更详尽探讨它所带来的影响，然后才就应否建议订立任何这方面的新罪行（以及如应该的话，如何订立）发表任何确定意见。"

该罪行的免责辩护 [33]

45. 咨询文件建议 5 邀请公众就以下问题提交意见书，有关意见在某程度上互相重迭：

---

[33] 報告書第 3.54 至 3.64 段。

"(a) 任何专业如需在合法业务的通常运作过程中截取数据和使用截取的数据，应否有免责辩护或豁免？如答案是应该的话，该免责辩护或豁免应涵盖哪类专业，并应有甚么条款（例如应否对使用截取的数据有任何限制）？

(b) 提供 Wi-Fi 热点或电脑供顾客或雇员使用的真正业务（咖啡店、酒店、购物商场、雇主等）应否获准截取和使用传送中的数据，而无须负上任何刑事法律责任？如答案是应该的话，哪类业务应受涵盖，并应有甚么条款（例如应否对使用截取的数据有任何限制）？"

46. 大多数回应者认为，任何专业如需在合法业务的通常运作过程中截取数据和使用截取的数据，均应享有免责辩护。他们提议，有关免责辩护应涵盖特定类别的专业或活动。[34] 至于真正业务应否获准截取和使用传送中的数据，而无须负上刑事法律责任，有关回应则意见不一。

47. 我们审慎衡量回应者的意见书及建议的非法截取电脑数据罪的元素后，认为无须为需在合法业务的通常运作过程中截取和使用电脑数据的人士，订定任何特定免责辩护或豁免，主要理由如下：

(a) 理论上，就已明确规定须证明*"不诚实或犯罪目的"*的罪行提供任何免责辩护，似乎不合逻辑；

(b) 在这前提下，某专业或真正业务如为不诚实或犯罪目的而截取电脑数据，则不应只是因为它经营某专业或业务，便获豁免刑事法律责任；

(c) 为日常工作经常需要使用和处理截取的数据的机构提供免责辩护，实际上便会向某些专业或业务（例如私家侦探社或传媒机构）给予截取数据的无限制授权；及

(d) 在针对电脑网络罪行的特定法例内为特定类别的专业或人士提供免责辩护，或会暗示法例内未有指明的其他专业

---

34 報告書第 3.54 段。回應者建議的六個類別是：(a)互聯網服務提供者；(b)日常工作經常需要使用和處理截取的數據的機構；(c)純粹為偵測安全威脅而截取其本身網絡的公司；(d) 執法機關就犯罪活動及國家安全事宜進行的調查；(e)為公眾利益或為日後法律程序搜證而真誠地進行的舉報活動；及(f)合理相信有損害其利益的活動正在進行的業務或機構。

或人士截取数据必然是不合法，继而令有关法律更为含糊，而非更为清晰。

48. 我们的结论是，任何业务如有意截取客户或消费者的数据，均可向后者索取截取数据的授权。倘若截取的数据用于获授权目的以外的其他目的，则会由法庭根据个别案件的证据，决定有关截取是否为不诚实或犯罪目的而进行。

49. 因此，我们提出**最终建议 5** 如下：

> "我们不建议为在通常运作过程中截取或使用电脑数据的专业或真正业务（例如咖啡店、酒店、购物商场、雇主）提供任何免责辩护或豁免。为不诚实或犯罪目的而截取电脑数据这项犯罪意念规定，已免除订定任何特定免责辩护或豁免的需要。"

第 4 章：非法干扰电脑数据

50. 极大多数回应者均支持咨询文件建议 6，该建议提出，《刑事罪行条例》第 59(1A)、60 及 64(2)条关于*"误用电脑"*的现行制度应改列于新法例，从而将无合法权限或合理辩解而蓄意干扰电脑数据定为罪行。

建议罪行的意念元素 [35]

51. 部分资讯科技相关团体认为，"恶意"应是建议罪行的所需元素。某法律专业团体则寻求澄清，为何"罔顾后果"这项意念规定属恰当或相关。

52. "恶意"是陈旧用语，过去曾造成诠释上的困难。[36] 另外，《刑事罪行条例》第 60 条所订的现行刑事损坏罪采纳"意图"及"罔顾后果"作为意念元素，而凭借第 59(1)(b)及(1A)条，该罪行引伸而适用于*"误用电脑"*。[37] 作为一般原则，在刑事法中，

---

35 報告書第 4.14 至 4.22 段。

36 英格蘭及威爾斯法律委員會（Law Commission of England and Wales）在檢討關於損壞財產的罪行時，發現難以處理"惡意"一詞，導致後來制定了《1971 年刑事損壞法令》（Criminal Damage Act 1971，香港的刑事損壞罪亦以該法令為藍本）。見英格蘭法律委員會，*Criminal Law Report on Offences of Damage to Property*（1970 年），英格蘭法律委員會第 29 號，第 44 段。

37 《刑事罪行條例》第 59(1A)條把*"誤用電腦"*界定為以下作為，當中(b)及(c)段與非法干擾電腦數據（相對於非法干擾電腦系統）最為相關：

"罔顾后果"这概念要求证明被告人察觉有关风险，而在被告人所知的情况下，承担该风险并不合理。[38] 不少刑事罪行已一并采纳"罔顾后果"与"意图"或"知悉"作为过失元素。

53. 就电脑网络罪行而言，"罔顾后果"这概念强调小心谨慎及负责任地使用电脑科技的重要性，即当事人必须保持警惕，注意其网上行为可能带来的后果（包括这些行为可能对他人造成的影响）。

54. 因此，我们建议就非法干扰电脑数据罪保留建议 6(b)(ii)的犯罪意念元素，即*"须怀有意图或罔顾后果，但无须怀有恶意"*。

加重罪行及危害国家安全的行为

55. 某回应者建议，除《刑事罪行条例》第 60(2)条所述元素外，*"任何意图危害国家安全的行为或活动，或罔顾国家安全是否会因而受到危害"*，亦应视为加重罪行。

56. 我们的分析详载于报告书第 4.23 至 4.31 段。概括而言，我们留意到，《中华人民共和国香港特别行政区维护国家安全法》（**《国安法》**）多项条文的范围似乎相当宽阔，足以包括非法干扰电脑数据（以及非法干扰电脑系统）的作为。当中，《国安法》第二十四（四）条清楚涵盖干扰及损坏互联网电子控制系统的作为。由于《国安法》构成我们法律制度不可或缺的部分，所以重要的一点，是针对电脑网络罪行的特定法例不得与《国安法》有任何抵触或冲突，即使并非有意亦然。

57. 《维护国家安全条例》（"**《基本法》第二十三条立法**"）在 2024 年 3 月制定。《基本法》第二十三条立法所订罪行包括以下罪行：意图危害国家安全（或罔顾是否会危害国家安全）而进行破坏活动，损坏或削弱公共基础设施（包括组成该设施的软件）；[39] 更具体的是，意图危害国家安全，而在没有合法权限下，就某电脑或电子系统作出某项作为。[40]

"(a) 導致電腦並非如其擁有人或其擁有人代表對其所設定的運作方式運作，即使如此誤用不會令該電腦的操作、該電腦內的程式或該電腦內的資料的可靠性減損亦然；
(b) 更改或刪抹電腦內或電腦儲存媒體內的程式或資料；
(c) 在電腦或電腦儲存媒體所收納的內容上增加程式或資料，
而造成導致(a)、(b)或(c)段所提述的任何類別誤用情形的任何作為，須視為導致該項誤用情形的作為。"

38 *Archbold Hong Kong 2025*，第 16 – 40 段，討論就刑事損壞罪作出判決的 *R v G* [2004] AC 341 及其後的法理發展。

39 《維護國家安全條例》第 49 條（危害國家安全的破壞活動）。

40 同上，第 50 條（就電腦或電子系統作出危害國家安全的作為）。

58. 考虑到《基本法》第二十三条现已藉本地立法的方式落实(包括引入特定罪行，涵盖电脑网络空间当中的国家安全风险)，我们认为，政府更具条件全面评估所有现存国家安全相关罪行是否足够，并考虑我们的建议，以研究应否建议任何可完善之处。

特定的免责辩护

为网络安全目的而干扰电脑数据 [41]

59. 由于干扰电脑数据(或电脑系统)通常会在取览程式或数据后发生，因此我们曾考虑，适用于第 2 章所讨论的取览罪的免责辩护，应否同样适用于干扰罪。合乎逻辑的结论是，为网络安全目的而干扰电脑数据这项免责辩护[42] 应同时适用于这两类罪行，而我们亦如此建议。

为保障儿童或易受伤害人士的利益而干扰电脑数据 [43]

60. 虽然家长、监护人或其他人士或会要求取览儿童或易受伤害人士的程式或数据，以保护该儿童或易受伤害人士免受网上危害，但据我们理解，这种取览并不涉及更改或干扰电脑数据(或电脑系统)。况且，准许某人取览任何程式或数据，绝不表示该人获授权更改或以其他方式干预有关数据。因此，我们认为，无须为保障儿童或易受伤害人士的利益而就干扰罪提供特定的免责辩护。

为真正的研究目的而干扰电脑数据 [44]

61. 若从事真正研究需要干扰电脑数据(或电脑系统)，我们认为是匪夷所思的。因此，无须提供特定的免责辩护，以豁免为真正的研究目的而进行的非法干扰电脑数据(或电脑系统)行为。

改列《刑事罪行条例》第 64(2)条的免责辩护 [45]

62. 咨询文件建议 6 建议采纳现时《刑事罪行条例》第 64(2)条所订的两项“合法辩解”。就干扰罪而言，由于回应者普遍欢迎采纳《刑事罪行条例》所设的现行制度，我们建议维持建议 6，但须在

---

41 報告書第 4.34 至 4.35 及 5.23 至 5.24 段。
42 見本摘要第 18 至 23 段。
43 報告書第 4.36 至 4.37 及 5.25 至 5.26 段。
44 報告書第 4.38 及 5.27 段。
45 報告書第 4.39 至 4.44 及 5.28 段。

同意免责辩护及保护财产免责辩护加入客观验证标准（和上文第 32 段所讨论的取览罪一样）。

63. 我们留意到现时《刑事罪行条例》第 64(2)(b)条之下的"合法辩解"仅限于保护财产，但不包括保护人命。我们曾考虑，就干扰罪而言，应否为保护生命及／或防止对他人造成身体伤害订定特定的免责辩护。我们相信，如有人为保护生命及／或防止身体伤害而干扰电脑数据（或电脑系统），建议 6 的"合理辩解"一般免责辩护能够应对这种情况，因此未必需要为此特定目的建议另一项免责辩护。我们赞成在这方面维持第 64(2)(b)条的现状。

64. 我们的**最终建议 6** 如下：

"我们建议：

(a) 无合法权限而蓄意干扰（损坏、删除、弄坏、更改或抑制）电脑数据，应在新法例下定为罪行，而合理辩解可作为法定免责辩护。

(b) 新法例应采用《刑事罪行条例》（第 200 章）所订以下特点：

(i) 第 59(1A)(a)、(b)及(c)条所订犯罪行为；

(ii) 第 60(1)条所订犯罪意念（该条规定须怀有意图或罔顾后果，而非怀有恶意）；

(iii) 第 64(2)条所示的两项免责辩护，但须因应上文(a)段所重新拟订的罪行，为恰当表达该两项免责辩护而作出所需改进，并同时保留任何获法律承认的其他合法辩解或免责辩护；及

(iv) 第 60(2)条所订加重罪行。

(c) 第 64(2)条所涵盖的两项免责辩护适用于以下情况：

(i) 被告人在干扰电脑数据时，相信其作为已获同意或会获同意；或

(ii) 被告人在干扰电脑数据时，相信有关财产需即时保护，并相信在顾及整体情况后，所采用的保护方法是合理的。

被告人不论是提出同意免责辩护或保护财产免责辩护，均必须合理地相信该免责辩护所订的有关事宜。

(d) 上述有关'误用电脑'的条文应与刑事损坏罪拆开，并纳入新法例内，同时删除《刑事罪行条例》（第200章）第59(1)(b)及(1A)条。

(e) 为网络安全目的而非法干扰电脑数据，应有特定的免责辩护，但须符合以下条件：

(i) 被告人必须是经认可的网络安全从业员（认可制度的细节本质上属政策事项，最好留待政府考虑）；

(ii) 被告人必须为真正的网络安全目的而行事；及

(iii) 在顾及整体情况后，被告人的行为必须是合理的。"

第5章：非法干扰电脑系统

65. 现时香港法律处理非法干扰电脑数据及非法干扰电脑系统的方式，是将两者视为*"误用电脑"*（即刑事损坏的一种形式）。因此，咨询文件建议7建议，关于非法干扰电脑数据及非法干扰电脑系统的条文，应采用一致的措辞。

66. 由于非法干扰电脑系统罪与非法干扰电脑数据罪息息相关，建议7同样得到绝大多数回应者支持，他们对建议7的回应与对建议6的大致相似。我们重申上文第51至63段的分析，并提出**最终建议7**如下：

"我们建议：

(a) 关于非法干扰电脑数据及非法干扰电脑系统的建议条文，应采用一致的措辞。

(b) 《刑事罪行条例》（第200章）第59(1A)及60条足以禁止非法干扰电脑系统，也应纳入新法例内。

(c) 新法例在适当厘清'误用电脑'一词（例如将'损害任何电脑的操作'的概念纳入该词）的同时，应保留现有法律的广度，不宜过于局限。

(d) 举例来说，建议的非法干扰电脑系统罪应适用于蓄意或罔顾后果地作出以下行为的人：

(i) 攻击电脑系统（不论成功与否——刑事法律责任不应取决于干扰成功与否）；

(ii) 在生产软件时，在软件编入缺损程式；及

(iii) 在未获授权下更改电脑系统，并知悉该项更改可能导致合法使用者不能取用或正常使用有关系统。"

67. 咨询文件建议8主要就以下活动应否足以视为建议的非法干扰电脑系统罪的合法辩解，征询公众意见：

(a) 扫描（或以类似的形式测试）他人的电脑；

(b) 非保安专业人员的行动，例如由机械人进行网页抓取（web scraping）（即利用电脑自动程式〔bots〕从网站提取内容及数据的过程），或由互联网资讯收集工具（例如搜寻器）启动网络爬虫（web crawlers）（即为建立索引而有系统地浏览网页的电脑自动程式），在未获授权下从伺服器收集数据。

建议8(a)：特定的免责辩护[46]

68. 由于两项干扰罪息息相关，我们同样建议，就非法干扰电脑系统罪而言，为网络安全目的而干扰电脑系统应可作为免责辩护。我们在上文第59至63段列出为非法干扰电脑数据罪提供特定免责辩护的理据，该等理据同样适用于非法干扰电脑系统罪。

---

46 報告書第5.23至5.28段。

建议 8(b)：无须为非保安专业人员建议免责辩护 [47]

69. 有些活动不一定会达致网络安全目的，但本身却存在于电脑网络空间的运作之中，或是电脑器材或系统之间的互动之中。电脑网络空间内有不少我们认为是数码生活中不可或缺，因而可以接受的合法活动，但是要把这些活动详尽无遗地全数列出，是不可能的，尤其是鉴于科技发展步伐之快，情况更是如此。我们同意咨询文件所述，认为当某人选择连接互联网，便应视为默示同意任何在使用电脑网络空间时可合理预期会发生的互动。我们应避免无意中使一些广为接受的互联网做法变成违法行为，而由于互联网或电脑系统的正常运作所需，这些做法应予准许。再者，其他国家虽然制定了非法干扰电脑系统罪及取览罪，但这些国家的电脑网络罪行法例并没有为非保安专业人员（如操作搜寻器）提供任何特定的免责辩护。

70. 故此，我们认为无须就电脑网络空间日常运作中所遇到的非保安代理提供特定的免责辩护，因为有关情况应能够与电脑网络攻击区分开来。[48]

71. 我们的**最终建议 8** 如下：

> "(a) 为网络安全目的而非法干扰电脑系统，应有特定的免责辩护，但须符合以下条件：
>
> (i) 被告人必须是经认可的网络安全从业员（认可制度的细节本质上属政策事项，最好留待政府考虑）；
>
> (ii) 被告人必须为真正的网络安全目的而行事；及
>
> (iii) 在顾及整体情况后，被告人的行为必须是合理的。
>
> (b) 就建议的非法干扰电脑系统罪而言，无须为非保安专业人员提供任何特定的免责辩护（例如由机械人进行网页抓取或由互联网资讯收集工具启动网络爬虫，从而藉着连接指定的协定埠，在未获授权下从伺服器收集数据），理由是根据默示授权的

---

47 報告書第 5.29 至 5.33 段。

48 例如在一分鐘內向某特定郵箱發送 10,000 封電郵，使郵箱及相應伺服器不勝負荷。

原则，构成互联网或电脑系统正常运作一部分的活动应继续获准。”

第 6 章：提供或管有用作干犯电脑网络相关罪行的器材、程式或数据

72. 咨询文件建议 9 建议订立一项独立的罪行，即提供或管有用作犯罪的器材或数据，这建议在市民大众之间引发不少争论。多名回应者关注到基本罪行的广度，为释除这些疑虑，我们已全盘检讨建议 9，并建议作出以下修订：

在罪行加入“程式”，即“器材、程式及数据”[49]

73. 建议罪行的目的在于打擊电脑网络罪行，我们认为将“程式”加入为建议罪行的标的之一，是适当的做法。这立场亦与《布达佩斯公约》订定罪行的标准相符。[50]

将罪行的适用范围限于使用器材、程式或数据以干犯电脑网络相关罪行（而非一般任何罪行）[51]

74. 假如器材、程式或数据的非法用途并不局限于干犯电脑网络罪行，则建议 9 在现实世界的适用范围便会无远弗届。[52] 此外，在咨询文件所讨论的其他司法管辖区，电脑网络罪行法例均一致将建议罪行的范围限制于干犯依赖电脑网络的罪行。如任何人使用器材、程式或数据，以干犯并非电脑网络罪行的其他一般罪行，该项构成罪责的行为可根据香港各项法定罪行及普通法罪行来处理。

75. 因此我们建议，建议的罪行应只适用于以下情况：透过提供器材、程式或数据（或为提供该器材、程式或数据而管有它）而干犯罪行，而该罪行属于电脑网络相关罪行，即第 2 至第 5 章所讨论的另外四类依赖电脑网络的罪行其中之一。[53]

---

49 報告書第 6.24 至 6.25 段。

50 《布達佩斯公約》第六條規定，各締約方應採取措施將以下行為定為刑事罪行：“*生產、出售、為使用而獲取、輸入、分發或以其他方式提供經設計或改裝以主要用作干犯第二至五條所訂任何〔依賴電腦網絡的〕罪行的器材（包括電腦程式）。*”（底線後加）

51 報告書第 6.26 至 6.36 段。

52 例如任何人撰寫電郵，試圖勒索受害人，但最終決定不送出電郵，只保留草稿，該人也屬於管有可用作干犯“罪行”的數據，因而觸犯諮詢文件建議 9 的建議罪行。

53 即非法取覽程式或數據罪、非法截取電腦數據罪、非法干擾電腦數據罪及非法干擾電腦系統罪。在研究涵蓋借助電腦網絡的罪行的第二部分，我們會考慮還有哪些罪行（如有的話）亦應納入“電腦網絡相關罪行”的清單內，並載於針對電腦網絡罪行的特定法例的附表。

重写罪行关于管有的部分 [54]

76. 我们认同，人们可能会在各种情况下管有恶意程式或数据，但并无意图使用该程式或数据以干犯电脑网络相关罪行。[55] 为避免造成过度刑事化的情况，我们建议将建议 9(a)关于管有的部分的范围限于*"为向他人提供被制造或改装以用作干犯电脑网络相关罪行的器材、程式或数据而管有它"*。根据这项形式较为狭隘的管有罪，某人如在不构成罪责的情况下管有被制造或改装以用作干犯电脑网络相关罪行的器材、程式或数据，便不会纯粹因管有该器材、程式或数据而招致刑事法律责任；但某人如管有有关器材、程式或数据供自用，以干犯电脑网络相关罪行，则会触犯有关罪行。

在罪行加入额外的犯罪意念规定 [56]

就器材、程式或数据的性质的所知所信等

77. 任何人未必可准确知悉或了解某器材、程式或数据的主要用途。[57] 如程式的有害性质并非可轻易识别，又或该有害程式并非广为人知，情况更是如此。我们认为，如某人误解该器材、程式或数据的性质，或不知悉该器材、程式或数据主要用作犯罪用途，该人便不应因建议的罪行而须负上法律责任。因此我们建议，控方必须证明被告人知悉、相信或声称某器材、程式或数据主要用作（以客观方式界定）干犯电脑网络相关罪行。

保留"提供"这项基本罪行

78. 就为"提供"而管有而言，我们必须先考虑建议的罪行是否应规定被告人须"知悉"他人或"意图"由他人将有关器材、程式或数据用作犯罪（即被告人必须知悉该器材、程式或数据实际拟作的用途）。订立这项规定，实际上等同摒弃咨询文件所建议的基本罪行，并导致某些有害器材、程式或数据的供应者成为漏网之鱼，原因是供应者可纯粹在暗网提供该等器材、程式或数据，而不顾或不知买家意图如何使用它们。建议的罪行旨在遏制供应和管有可在电脑网络空间作非法用途的器材或数据，为免破坏这个目标，我们认为应保留这项基本罪行，但须按上文第 76 及 77 段的建议作出修改。

---

54 報告書第 6.37 至 6.40 段。

55 例如某人在電腦執行防毒掃描時，可能從中得知自己管有惡意程式或數據，但防毒掃描未必能夠為一般電腦使用者提供很多關於該程式或數據的性質或影響的資料。

56 報告書第 6.41 至 6.51 段。

57 例如某人可能以為程式無害而下載。

替代精神意念元素：有合理理由相信某器材、程式或数据的主要用途构成罪责[58]

79. 虽然管有如电脑程式的被告人或许实际并不知悉该程式内含勒索软件或病毒（而可用作干犯电脑网络相关罪行），但情况可能相当可疑，足以令被告人有合理理由如此相信。[59] 蓄意提供用作干犯电脑网络罪行的器材、程式或数据，以及蓄意为提供任何上述物品而管有它们，均带有相当程度的刑责。遏止这种行为与建议罪行的更广泛目标相符，即防止有害器材、程式或数据被用作干犯电脑网络罪行。

80. 为加强法律的阻吓作用，我们建议，建议的罪行亦应涵盖*"有合理理由相信"*某器材、程式或数据主要用作干犯电脑网络相关罪行的人。

提供或管有恶意器材、程式或数据的部分[60]

81. 随着科技进步，程式或数据能够分散（例如在星际档案系统〔InterPlanetary File System〕等分散式档案系统，或区块链技术[61]）储存、取览及分享。犯罪者可能只持有整体数据的一部分，此举本身并非犯罪，但利用科技能够聚集储存于多个地点的数据，并向任何人提供综合的恶意数据。

82. 为使法例更具弹性，我们建议改进建议 9，指明对*"器材、程式或数据"*的提述会包括该器材、程式或数据的部分。这项修改根本上没有改变建议罪行的性质，因为要产生刑事法律责任，控方必须在毫无合理疑点下证明相同的犯罪意念元素，即有关的人(i)知悉自己管有某器材、程式或数据（或其任何部分）；及(ii)知悉、相信、有合理理由相信，或声称某器材、程式或数据（或其任何部分）主要用作干犯电脑网络相关罪行。

---

58 我們的論點詳載於報告書第 6.48 至 6.51 段。

59 例如陌生人將某程式交予被告人，要求被告人於指明日期的特定時間上載該程式至某電腦系統，以換取大額金錢報酬，但不作任何解釋。

60 報告書第 6.52 至 6.54 段。

61 區塊鏈是由電腦網絡節點共用的分散式數據庫或分類帳，最廣為人知的是它們在加密貨幣系統的關鍵作用，以維持安全而分散的交易紀錄，但其用途不限於加密貨幣。區塊鏈可用於任何行業的數據，使該些數據不可竄改。見 https://www.investopedia.com/terms/b/blockchain.asp（於 2025 年 11 月 1 日瀏覽）。

"合理辩解"作为法定免责辩护 [62]

83. 一如第 2 章所讨论的取览罪，我们认为无须提供一份例子清单，列举会属于建议罪行的"合理辩解"一般免责辩护范围内的合法活动。我们建议订立多项特定的免责辩护，该等免责辩护将于下文第 85 至 93 段讨论。

84. 根据咨询文件建议 9（稍经修改），我们提出**最终建议 9** 如下：

> "(a) 在新法例下，蓄意提供被制造或改装以用作干犯电脑网络相关罪行[63] 的器材、程式或数据（或其部分），或蓄意为提供该器材、程式或数据而管有它，不论它是有形物或无形物（例如勒索软件、病毒或其源码），应定为基本罪行，而合理辩解可作为法定免责辩护。
>
> (b) 建议罪行的犯罪行为，应涵盖供应（例如生产、提供、出售及输出有关器材、程式或数据）及需求（例如取得、管有、购买及输入有关器材、程式或数据）两方面。
>
> (c) 建议的罪行应适用于主要用作（以客观方式界定）干犯电脑网络相关罪行的器材、程式或数据（或其部分），不论该器材、程式或数据是否亦可能用作任何合法目的。
>
> (d) 建议罪行的犯罪意念规定为：
>
> (i) 某人知悉自己提供某器材、程式或数据（或其部分），或知悉自己为提供该器材、程式或数据（或其部分）而管有它；及
>
> (ii) 某人知悉、相信、有合理理由相信，或声称某器材、程式或数据（或其部分）主要用作干犯电脑网络相关罪行。
>
> (e) 某人如声称（不论该项声称是否属实）或误信某器材、程式或数据主要用作干犯电脑网络相关罪行，

---

62 報告書第 6.57 至 6.59 段。

63 即非法取覽程式或數據、非法截取電腦數據、非法干擾電腦數據及非法干擾電腦系統。

亦应属犯罪，犹如任何人即使就所贩运物质的性质构成罪责的信念原来出错，亦属干犯企图贩运危险药物罪一样。

(f) 在新法例下，蓄意提供被制造或改装以用作干犯电脑网络相关罪行的器材、程式或数据（或其部分），或蓄意为提供该器材、程式或数据而管有它，不论它是有形物或无形物（例如勒索软件、病毒或其源码），在以下情况下应构成加重罪行，而合理辩解可作为法定免责辩护：

(i) 该器材、程式或数据能够用作干犯电脑网络相关罪行，或犯罪者知悉、相信[64]或声称该器材、程式或数据能够用作干犯电脑网络相关罪行；及

(ii) 犯罪者意图任何人将该器材、程式或数据用作干犯电脑网络相关罪行。

(g) 在新法例下，蓄意管有器材、程式或数据（或其部分），在以下情况下应构成加重罪行，而合理辩解可作为法定免责辩护：

(i) 该器材、程式或数据能够用作干犯电脑网络相关罪行，或犯罪者知悉、相信[65]或声称该器材、程式或数据能够用作干犯电脑网络相关罪行；及

(ii) 犯罪者意图将该器材、程式或数据用作干犯电脑网络相关罪行。

(h) 除上述另有规定外，建议的条文应以英格兰及威尔斯《误用电脑法令》第 3A 条，以及新加坡《误用电脑法令》第 8 及 10 条为蓝本。”

64 包括某人有合理理由相信該器材、程式或數據能夠用作干犯電腦網絡相關罪行的情況。
65 同上。

特定的免责辩护

为网络安全目的提供有害器材、程式或数据（或为了为网络安全目的提供该器材、程式或数据而管有它）[66]

85. 一如取览罪及干扰罪，我们建议，为网络安全目的提供有害器材、程式或数据（或为了为网络安全目的提供该器材、程式或数据而管有它），应有特定的免责辩护。由于器材、程式或数据可由经认可的网络安全从业员以外的人管有或提供，[67] 我们建议，网络安全免责辩护应延伸至网络安全从业员以外，以涵盖获网络安全从业员事先批准或授权，为网络安全目的而管有或提供器材、程式或数据的人。

为教育、科学或研究目的提供有害器材、程式或数据（或为上述目的提供该器材、程式或数据而管有它）[68]

86. 我们同意回应者所言，建议的罪行应有为教育或研究目的而设的免责辩护，而且该免责辩护适用于电脑科学领域的教师及学生，以及为自行研究而取得或制造有害电脑程式（例如特洛依木马）的业余爱好者。我们理解到，从事电脑科学研究可出于善意或恶意，但法律应留有空间，以促进对有害器材、程式或数据的研究。为预防滥用，我们建议，援引这项免责辩护的人的行为必须是合理的，且不得超过为达到有关目的而所需者。

为互联网服务提供者提供免责辩护[69]

87. 互联网服务提供者为个人及机构提供互联网连接及相关服务（如网页寄存）。由于互联网服务提供者所分配的互联网规约地址可能寄存多个网站及 URL，互联网服务提供者要使被制造或改装以用作干犯电脑网络相关罪行的有害网站、程式或数据（如伪冒银行网站）不能被接达并非总是可行，因为此举可能扰乱向其他互联网使用者提供的服务。

88. 考虑到互联网服务提供者的处境，我们建议采用由欧洲联盟部长理事会通过的《数位服务法案》（Digital Services Act）第 4 条所订的纯导管免责辩护（mere conduit defence）为蓝本，并采纳如《版权条例》

---

66 報告書第 6.71 至 6.75 段。

67 例如在開發防毒軟件的公司，其技術人員、銷售員及其他非專業人員的僱員在履行職務期間也可能管有電腦病毒。

68 報告書第 6.76 至 6.79 段。

69 報告書第 6.82 至 6.87 段。

（第 528 章）第 65A(2)条中“服务提供者”那般广阔的定义，[70] 为互联网服务提供者提供免责辩护。互联网服务提供者作为服务提供者，如证明以下事项，即为免责辩护：

(a) 它并无启动传送有关器材、程式或数据（统称“**违法内容**”）；

(b) 它并无选定该项传送的接收人；及

(c) 它并无选定或修改该项传送所载的违法内容。

为储存及／或发布器材、程式或数据提供免责辩护 [71]

89. 在数码时代，寄存服务提供者、云端服务提供者及数据储存设施均提供各种各样的互联网服务。为使针对电脑网络罪行的特定法例臻于完善，我们建议以《数位服务法案》第 6 条[72] 为蓝本订立免责辩护，不同的“服务提供者”如服务包括“储存”及／或“发布”服务对象所提供的器材、程式或数据，均可受惠于这项免责辩护。这种处理方式会涵盖该等服务提供者，而无须将它们加以区别。

90. 上述服务提供者移除违法内容或使违法内容不能被接达，并非总是技术上可行，因为会造成连锁效应，影响其他使用者。因此我们建议，上述服务提供者如证明以下事项，即为免责辩护：

(a) 它知悉或有合理理由相信服务对象已提供违法内容后，已在合理地切实可行的范围内尽快移除该违法内容或使该违法内容不能被接达；或

---

70 《版權條例》（第 528 章）第 65A(2)條訂明“服務提供者”是*“藉電子設備或網絡（或同時藉兩者），提供任何聯線服務或為任何聯線服務操作設施的人”*。根據第 65A(2)(a)至(c)條，“聯線服務”包括：

“(a) 傳送使用者所選擇的資料或材料，或為該資料或材料作出路由選擇，或為該資料或材料的數碼聯線通訊提供連接，而該等數碼聯線通訊，是在使用者指明的超過一個點之間或之中進行的；

(b) 寄存使用者能接達的資料或材料；及

(c) 在使用者能接達的系統或網絡儲存資料或材料。”

71 報告書第 6.88 至 6.92 段。

72 《數位服務法案》第 6(1)條內容如下：

“凡提供資訊社會服務，而該服務包含儲存服務對象所提供的資訊，有關的服務提供者無須為應服務對象要求而儲存的資訊承擔法律責任，前提是該提供者：

(a) 實際上並不知悉違法活動或違法內容，而就損害賠償申索而言，該提供者並不察覺明顯可見該違法活動或違法內容的事實或情況；或

(b) 知悉或察覺上述事宜後，已迅速行事移除該違法內容或使該違法內容不能被接達。”

(b) （如移除该违法内容或使该违法内容不能被接达，在技术上不可行或并不合理地切实可行）它已在合理地切实可行的范围内，就存在该违法内容尽快向执法机关备案。

以自动化科技提供器材、程式或数据的免责辩护 [73]

91. 由于现今科技发展使有害器材、程式或数据能够透过自动化程序（如区块链或电脑自动程式〔internet bot〕）来提供或发布，我们预计会出现以下情况：用来分发数据的自动化程序、工具或科技本身可能无害，但该程序、工具或科技被犯罪者以恶意器材、程式或数据（如病毒或恶意流动应用程式）玷污，而该区块链或电脑自动程式继而将恶意材料自动分发出去。

92. 凡某些违法内容纯粹藉某自动化程序、工具或科技而提供，则任何人如证明以下事项，即为免责辩护，我们认为是公平的：

(a) 他并无蓄意参与设计、制作或产生上述违法内容；及

(b) 他并无蓄意参与使上述违法内容成为该自动化程序一部分的过程。

93. 这项免责辩护会参照"自动化程序"以一般通用的方式拟定，而非述明任何特定科技，原因是随着科技继续演变，或会出现区块链及电脑自动程式的替代品。

94. 我们的**最终建议 10** 如下：

"我们建议，除合理辩解可作为法定免责辩护外，提供用作干犯电脑网络相关罪行的器材、程式或数据罪（或为提供用作干犯电脑网络相关罪行的器材、程式或数据而管有罪）应有以下特定的免责辩护：

(a) 为网络安全目的提供有关器材、程式或数据（或为了为网络安全目的提供该器材、程式或数据而管有它）：

(i) 这项免责辩护应只适用于为真正的网络安全目的而行事的经认可网络安全从业员（其资格会根据政府所设立的制度认可）；

---

73 報告書第 6.93 至 6.96 段。

(ii) 在顾及整体情况后，该网络安全从业员的目的和行为必须是合理的；及

(iii) 这项免责辩护应延伸至：

(1) 获网络安全从业员事先批准或授权，为网络安全目的而管有或提供该器材、程式或数据的人；及

(2) 协助网络安全从业员履行其专业职务的人。

(b) 为真正的教育、科学或研究目的提供有关器材、程式或数据（或为了为真正的教育、科学或研究目的提供该器材、程式或数据而管有它）。在顾及整体情况后，援引这项免责辩护的人的行为必须是合理的。

(c) 以欧洲联盟《数位服务法案》（Digital Services Act）第 4 条为蓝本，规定凡任何互联网服务提供者[74] 作为提供有关器材、程式或数据（或为提供该器材、程式或数据而管有它）的纯导管，则该提供者如证明以下事项，即为免责辩护：

(i) 它并无启动传送该器材、程式或数据（"**违法内容**"）；

(ii) 它并无选定该项传送的接收人；及

(iii) 它并无选定或修改该项传送所载的违法内容。

(d) 以《数位服务法案》第 6 条为蓝本，规定凡任何服务提供者[75] 的服务包括储存及／或发布服务对象所提供的器材、程式或数据，而该服务提供者察觉或有合理理由相信，服务对象已提供违法内容或已提供途径接达（不论以直接或间接方式）该违法

74 我們建議採納如《版權條例》（第 528 章）第 65A(2)條中"服務提供者"那般廣闊的定義，以涵蓋大大小小的服務提供者，以及設立網上空間（例如論壇或網站）以寄存或儲存程式或數據的個人。見本摘要第 88 段。

75 同上。

内容，则该服务提供者如证明以下事项，即为免责辩护：

(i) 它知悉或有合理理由相信上述事宜后，已在合理地切实可行的范围内尽快移除该违法内容或使该违法内容不能被接达；或

(ii) （如移除该违法内容或使该违法内容不能被接达，在技术上不可行或并不合理地切实可行）它已在合理地切实可行的范围内，就存在该违法内容尽快向执法机关备案。

(e) 凡违法内容纯粹藉某自动化程序、工具或科技而提供，则任何人如证明以下事项，即为免责辩护：

(i) 他并无蓄意参与设计、制作或产生该违法内容；及

(ii) 他并无蓄意参与使该违法内容成为该自动化程序一部分的过程。"

第 7 章：香港法庭行使司法管辖权的准则

电脑网络罪行的司法管辖权规则 [76]

95. 基于香港适宜依循国际惯例，而国际惯例是司法管辖区应在合理范围内，为其法律的任何域外应用订定条文，咨询文件建议 11 至 15 参照以下事实情况，就五类依赖电脑网络的罪行订明司法管辖权规则：

(a) 罪行的任何"主要元素"[77] 在香港发生，即使其他"主要元素"在其他地方发生；

(b) 犯罪者是"香港人"；

(c) 受害人是"香港人"；

(d) 目标电脑、程式或数据处于香港；及

---

76 報告書第 7.2 至 7.6 段。

77 如以術語表達，即如《刑事司法管轄權條例》（第 461 章）第 3(1)條所述明：*"就該罪行定罪而須予以證明的任何作為或不作為或其他事情（包括一項或多項作為或不作為所產生的任何後果）"*。

(e) 犯罪者的作为，已导致或可能导致对香港的严重损害（例如导致对香港的基础建设或公共机构的严重损害，或已威胁或可能威胁香港的安全）。

扩大事实情况(c)的范围：受害人是"香港人"[78]

96. 我们获得绝大多数回应者支持，将建议的电脑网络罪行法例适用于域外范围。至于上一段所述的事实情况(c)，咨询文件建议"香港人"的概念应包括香港永久性居民、通常居于香港的人或在香港经营业务的公司。

97. 因应某回应者的提议，我们深思香港法庭应为电脑网络罪行的受害人提供多大的保障范围。我们明白，各有原因而暂时在香港工作或逗留的人（例如外籍家庭佣工、游客及其他在香港短暂逗留的访客，在身处香港时遇上建议的依赖电脑网络的罪行），亦应受到香港法律保障。

98. 故此，我们建议将事实情况(c)改进如下：

> "受害人是香港永久性居民、通常居于香港的人，或于相关罪行发生时身处香港，又或是在香港经营业务的公司。"

对危害国家安全行为的司法管辖权[79]

99. 至于是否需要就依赖电脑网络的罪行订定针对危害国家安全行为的域外法律效力条文，而非只是针对威胁*"香港的安全"*的作为立法，我们的分析详载于报告书第 7.33 至 7.40 段。总括而言，《基本法》第二十三条立法已解决上述问题，该项立法清楚订明凡任何其他条例提述*"特区的安全"*（或意义相同的词句），[80] 须理解为包括法例所界定的"国家安全"。[81] 此外，当电脑网络罪行案件涉及《国安法》规定的任何罪行时，显而易见，一般原则是香港法庭可根据《国安法》第四十条[82] 对案件行使司法管辖权。最后，鉴于电脑网络罪行案件如危害国家安全，有关案件的司法管辖权因着《国安法》

---

78 報告書第 7.25 至 7.28 段。
79 報告書第 7.33 至 7.40 段。
80 第 8(2)條。
81 第 4 條。
82 第四十條訂明，*"香港特別行政區對〔《國安法》〕規定的犯罪案件行使管轄權，但〔《國安法》〕第五十五條規定的情形除外。"*

第五十五[83]及五十六条[84]的规定而并不完全归于香港法庭，我们认为并不适合在针对电脑网络罪行的特定法例中订立司法管辖权规则，订明香港法庭对有关案件行使司法管辖权。

证据事宜及程序事宜[85]

100. 部分回应者提出证据事宜及程序事宜，包括从其他司法管辖区搜集证据、保存取自云端环境的证据及该等证据是否可接纳呈堂，以及应否修订《刑事事宜相互法律协助条例》（第525章）（**《相互法律协助条例》**）下任何条文。由于我们的研究第三部分会处理执法及程序事宜，这些事宜为一大议题，我们会紧记回应者帮忙识别的问题。考虑到《相互法律协助条例》的相关修订，最终会取决于建议的电脑网络罪行法例的制定形式，而且或需与其他司法管辖区商讨，以促进跨司法管辖区的合作，我们若对《相互法律协助条例》的相应修订作出任何建议，实属言之尚早。有关修订最好留待政府适时按需要决定。

101. 基于以上原因，我们保留咨询文件建议11至15，并扩大事实情况(c)的范围，从而提出**最终建议11至15**如下：

> "<u>最终建议11</u>
>
> 我们建议，在以下情况下，就建议的非法取览程式或数据罪，香港的法庭应具有司法管辖权：
>
> (a) 就该罪行定罪而须予以证明的任何作为或不作为或其他事情（包括一项或多项作为或不作为所产生的任何后果）在香港发生，即使其他有关作为、不作为或事情在其他地方发生；
>
> (b) 受害人（目标电脑的拥有人、有关数据的拥有人或两者）是香港永久性居民、通常居于香港的人，或

---

83 第五十五條訂明，*"有以下情形之一的，經香港特別行政區政府或者駐香港特別行政區維護國家安全公署提出，並報中央人民政府批准，由駐香港特別行政區維護國家安全公署對〔《國安法》〕規定的危害國家安全犯罪案件行使管轄權：*
（一） 案件涉及外國或者境外勢力介入的複雜情況，香港特別行政區管轄確有困難的；
（二） 出現香港特別行政區政府無法有效執行〔《國安法》〕的嚴重情況的；
（三） 出現國家安全面臨重大現實威脅的情況的。"

84 第五十六條訂明，*"根據〔《國安法》〕第五十五條規定管轄有關危害國家安全犯罪案件時，由駐香港特別行政區維護國家安全公署負責立案偵查，最高人民檢察院指定有關檢察機關行使檢察權，最高人民法院指定有關法院行使審判權。"*

85 報告書第7.20至7.22、7.31及7.32段。

于该罪行发生时身处香港，又或是在香港经营业务的公司；

(c) 目标电脑、程式或数据处于香港；或

(d) 犯罪者的作为，已导致或可能导致对香港的严重损害（例如导致对香港的基础建设或公共机构的严重损害，或已威胁或可能威胁香港的安全），

惟须符合以下规定：如犯罪者因其在香港境外所作的作为而被控这项简易程序罪行，该作为本身或连同就这项香港罪行定罪而须予以证明的其他有关作为、不作为或事情，须在该作为作出的司法管辖区构成罪行。

<u>最终建议 12</u>

我们建议，在以下情况下，就建议的非法截取电脑数据罪，香港的法庭应具有司法管辖权：

(a) 就该罪行定罪而须予以证明的任何作为或不作为或其他事情（包括一项或多项作为或不作为所产生的任何后果）在香港发生，即使其他有关作为、不作为或事情在其他地方发生；

(b) 受害人是香港永久性居民、通常居于香港的人，或于该罪行发生时身处香港，又或是在香港经营业务的公司；

(c) 目标电脑、程式或数据处于香港；或

(d) 犯罪者的作为，已导致或可能导致对香港的严重损害（例如导致对香港的基础建设或公共机构的严重损害，或已威胁或可能威胁香港的安全）。

<u>最终建议 13</u>

我们建议，在以下情况下，就建议的非法干扰电脑数据罪（包括基本形式及加重形式），香港的法庭应具有司法管辖权：

(a) 就该罪行定罪而须予以证明的任何作为或不作为或其他事情（包括一项或多项作为或不作为所产生

的任何后果）在香港发生，即使其他有关作为、不作为或事情在其他地方发生；

(b) 受害人是香港永久性居民、通常居于香港的人，或于该罪行发生时身处香港，又或是在香港经营业务的公司；

(c) 目标程式或数据处于香港；或

(d) 犯罪者的作为，已导致或可能导致对香港的严重损害（例如导致对香港的基础建设或公共机构的严重损害，或已威胁或可能威胁香港的安全）。

<u>最终建议 14</u>

我们建议，在以下情况下，就建议的非法干扰电脑系统罪（包括基本形式及加重形式），香港的法庭应具有司法管辖权：

(a) 就该罪行定罪而须予以证明的任何作为或不作为或其他事情（包括一项或多项作为或不作为所产生的任何后果）在香港发生，即使其他有关作为、不作为或事情在其他地方发生；

(b) 受害人是香港永久性居民、通常居于香港的人，或于该罪行发生时身处香港，又或是在香港经营业务的公司；

(c) 目标电脑处于香港；或

(d) 犯罪者的作为，已导致或可能导致对香港的严重损害（例如导致对香港的基础建设或公共机构的严重损害，或已威胁或可能威胁香港的安全）。

<u>最终建议 15</u>

我们建议，在以下情况下，就建议的提供用作干犯电脑网络相关罪行的器材、程式或数据罪（或为提供用作干犯电脑网络相关罪行的器材、程式或数据而管有罪），香港的法庭应具有司法管辖权：

(a) 就该罪行定罪而须予以证明的任何作为或不作为或其他事情(包括一项或多项作为或不作为所产生的任何后果)在香港发生,即使其他有关作为、不作为或事情在其他地方发生(例如身处香港的人在暗网上提供用作干犯电脑网络相关罪行的器材、程式或数据);

(b) 犯罪者是香港永久性居民、通常居于香港的人,或在香港经营业务的公司;或

(c) 犯罪者的作为,已导致或可能导致对香港的严重损害(例如导致对香港的基础建设或公共机构的严重损害,或已威胁或可能威胁香港的安全)。"

第 8 章:判刑

102. 咨询文件建议 16 载列就五类依赖电脑网络的罪行所建议的最高刑罚。概括而言,回应者均支持引入一套较现有电脑相关罪行的罚则更重的罚则,因为此举将有助阻吓依赖电脑网络的罪行,而良好稳健的网络安全制度亦会促进香港的商业地位。

简易程序形式的取览罪 [86]

103. 因应某回应者的提议,我们已考虑就简易程序形式的取览罪处以最高两年监禁是否具足够阻吓性。总括而言,把最高刑罚订为两年监禁,便能彰显简易程序形式的取览罪的严重性:任何人一旦干犯该罪行,即使没有足够证据证明该人在未获授权下取览程式或数据后意图进行其他犯罪活动,法律旨在保护的有关目标系统的不可侵犯性或有关资料的机密性,也已经受到侵害。我们认为建议的最高刑罚是适当的,因为这样可给予判刑法院足够权力,判处能恰当地反映罪行重点的刑罚。

把干扰罪的加重罪行最高刑罚订为终身监禁的背后理念 [87]

104. 订明最高刑罚为终身监禁,仅旨在与现行《刑事罪行条例》第 63(1)条就刑事损坏的加重罪行所订的刑罚保持贯彻一致。若把第 63(1)条与《刑事罪行条例》第 60(2)(b)条[88] 一并阅读,便可确保

---

[86] 報告書第 8.9 至 8.13 段。

[87] 報告書第 8.14 至 8.18 段。

[88] 《刑事罪行條例》第 60(2)條規定:

所施加的刑罚足以处理涉及意图危害生命的财产损坏或摧毁的情况。由于干扰罪可能会危害数以千计的人的生命，[89] 因此有充分理由处以严厉的最高刑罚。事实上，视乎案情而定，非法干扰电脑数据及／或非法干扰电脑系统的行为可能已构成刑事损坏的加重罪行，该罪行现时的最高刑罚为终身监禁。新订的电脑网络罪行法例的用意，只是使这些已在《刑事罪行条例》设想的现有干扰罪在该法例中得以反映。

105. 经全盘检讨建议 16，我们信纳有关建议不但会发挥必要的阻吓作用，足以打击电脑网络罪行，亦不会过分偏离以下罪行的最高刑罚：(a)《盗窃罪条例》（第 210 章）所订的罪行，[90] 以及(b)其他司法管辖区的有关罪行。[91] 因此，我们保留咨询文件建议 16，作为**最终建议 16**：

"我们建议：

(a) 就建议的非法取览程式或数据罪而言，犯罪者应可处下述最高刑罚：

(i) 如属简易程序罪行，可处两年监禁；或

(ii) 如属加重罪行，一经循公诉程序定罪，可处 14 年监禁。

(b) 就建议的非法截取电脑数据罪而言，犯罪者一经循简易程序定罪，应可处两年监禁，一经循公诉程序定罪，应可处 14 年监禁。

(c) 就建议的非法干扰电脑数据罪及非法干扰电脑系统罪而言，犯罪者就每项罪行应可处下述最高刑罚：

"任何人無合法辯解而摧毀或損壞任何財產（不論是屬於其本人或他人的）——
(a) 意圖摧毀或損壞任何財產或罔顧任何財產是否會被摧毀或損壞；及
(b) 意圖藉摧毀或損壞財產以危害他人生命或罔顧他人生命是否會因而受到危害，即屬犯罪。"（底線後加）

89 例如干擾機場控制塔系統、鐵路信號系統、發電廠等所處理的電腦數據。

90 用作參考的具代表性罪行類別：《盜竊罪條例》（第 210 章）所訂的盜竊罪、欺詐罪、勒索罪、入屋犯法罪、嚴重入屋犯法罪及搶劫罪。

91 見諮詢文件的附錄，當中概述香港及其他司法管轄區的現行法律就建議的五類依賴電腦網絡的罪行所訂的最高刑罰。

(i) 如属基本罪行，一经循简易程序定罪，可处两年监禁，一经循公诉程序定罪，可处14年监禁；或

(ii) 如属加重罪行，可处终身监禁。

(d) 就建议的提供用作干犯电脑网络相关罪行的器材、程式或数据罪（或为向他人提供该等器材、程式或数据而管有罪）而言，犯罪者应可处下述最高刑罚：

(i) 如属基本罪行，一经循简易程序定罪，可处两年监禁，一经循公诉程序定罪，可处七年监禁；或

(ii) 如属加重罪行，一经循公诉程序定罪，可处14年监禁。”