香港法律改革委员会

报告书

依赖电脑网络的罪行及司法管辖权事宜

本报告书已上载互联网，网址为：**http://www.hkreform.gov.hk**。

2026 年 1 月

香港法律改革委员会（“法改会”）于 1980 年 1 月由当时的行政局任命成立，负责研究由律政司司长或终审法院首席法官转交该会的有关香港法律的课题，以进行改革。

法改会现时的成员如下：

主席：	**林定国资深大律师**	**GBS，JP** **律政司司长**
成员：	**张举能首席法官**	**大紫荆勋贤，终审法院首席法官**
	林文翰法官	**终审法院常任法官**
	林少忠先生	**法律草拟专员**
	陈淑薇女士	**GBS，JP**
	熊运信先生	**MH**
	蔡关颖琴女士	**BBS，MH，JP**
	陈泽铭先生	**JP**
	梁高美懿议员	**SBS，JP**
	陆飞鸿教授	
	庄迈豪教授	
	骆敏贤资深大律师	
	习超教授	

法改会的秘书长是**律政专员黄惠冲资深大律师，JP**，法改会的办事处地址为：

香港中环花园道三号
冠君大厦 9 楼
电话：3703 6518
传真：3702 0136
电邮：hklrc@hkreform.gov.hk
网址：http://www.hkreform.gov.hk

陈泽铭先生，JP 在 2025 年 12 月 31 日后卸任法律改革委员会（法改会）成员。法改会主席及秘书处感谢陈先生多年来对法改会工作的宝贵贡献及意见。

香港法律改革委员会

报告书

依赖电脑网络的罪行及司法管辖权事宜

目录

页

界定用语

用语／简称	定义
取览罪	非法取览程式或数据
《基本法》第二十三条立法	《维护国家安全条例》
《布达佩斯公约》	欧洲委员会（Council of Europe）的《电脑网络罪行公约》（Convention on Cybercrime）
《英格兰误用电脑法令》	《1990 年误用电脑法令》（Computer Misuse Act 1990）（英格兰及威尔斯）
《新加坡误用电脑法令》	《1993 年误用电脑法令》（Computer Misuse Act 1993）（新加坡）
《刑事罪行条例》	《刑事罪行条例》（第 200 章）
私隐专员	个人资料私隐专员
同意免责辩护	《刑事罪行条例》（第 200 章）第 64(2)(a)条所示的免责辩护[1]
分布式拒绝服务	分布式拒绝服务（Distributed denial of service，“DDOS”）
域名系统	域名系统（Domain name system，“DNS”）
《数位服务法案》	《数位服务法案》（Digital Services Act）
欧盟	欧洲联盟
大律师公会	香港大律师公会
女律师协会	香港女律师协会有限公司
香港特区	中华人民共和国香港特别行政区

[1] 见第 2.96 及 4.11 段。

女工商专联	香港女工商及专业人员联会
《截取通讯及监察条例》	《截取通讯及监察条例》(第 589 章)
干扰罪	非法干扰电脑数据及非法干扰电脑系统
互联网规程	互联网规程 (Internet protocol, "IP")
互联网服务提供者	互联网服务提供者 (Internet service provider, "ISP")
英格兰法律委员会	英格兰及威尔斯法律委员会 (Law Commission of England and Wales)
律师会	香港律师会
《精神健康条例》	《精神健康条例》(第 136 章)
《相互法律协助条例》	《刑事事宜相互法律协助条例》(第 525 章)
《裁判官条例》	《裁判官条例》(第 227 章)
《示范法》	《电脑罪行及电脑相关罪行示范法》(Model Law on Computer and Computer Related Crime)
《国安法》	《中华人民共和国香港特别行政区维护国家安全法》
国安公署	中央人民政府驻香港特别行政区维护国家安全公署
私隐专员公署	个人资料私隐专员公署
《私隐条例》	《个人资料(私隐)条例》(第 486 章)
《公安条例》	《公安条例》(第 245 章)

保护财产免责辩护	《刑事罪行条例》（第 200 章）第 64(2)(b)条所示的免责辩护[2]
《俄罗斯公约》	俄罗斯联邦于 2017 年 10 月 11 日向联合国提交的《联合国合作打击网络犯罪公约》草案（*Draft United Nations Convention on Cooperation in Combating Cybercrime*）
第 161 条	《刑事罪行条例》（第 200 章）第 161 条
第 64(2)条	《刑事罪行条例》（第 200 章）第 64(2)条
第 27A 条	《电讯条例》（第 106 章）第 27A 条
《储存通讯法案》	《储存通讯法案》（Stored Communications Act）
《盗窃罪条例》	《盗窃罪条例》（第 210 章）
《电讯条例》	《电讯条例》（第 106 章）
《联合国公约》	《联合国打击网络犯罪公约》（United Nations Convention against Cybercrime）
《儿童权利公约》	《联合国儿童权利公约》（United Nations Convention on the Rights of the Child）
美国	美利坚合众国

[2] 见第 2.96 及 4.11 段。

导言

引言

1. 法律改革委员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**"）。本报告书论述就该咨询文件收到的回应，并载列我们对这个课题的分析及最终建议。

背景

2. 对世上很多人而言，资讯科技、电脑和互联网已渗透日常生活各方面。正当我们享受科技进步带来的便利，不法之徒亦藉此从事非法勾当。关于刑事法应如何应对这些不当手段，全球各地似乎普遍认为特别针对电脑网络空间的法例可补足一般适用的法例。

3. 中华人民共和国香港特别行政区（"**香港特区**"）最近期的电脑网络罪行官方研究追溯至2000年，当时香港特区政府召开了电脑相关罪行跨部门工作小组。随着过去20年科技和社会发展一日千里，现正是再次检视这个课题的成熟时机。因此，于2019年初，终审法院首席法官联同律政司司长将电脑网络罪行这课题转介予香港法律改革委员会研究。法律改革委员会委任小组委员会探讨法律现况和提出建议。

4. 小组委员会就这课题展开讨论后，《中华人民共和国香港特别行政区维护国家安全法》（**《国安法》**）于2020年6月30日制定为全国性法律，并在香港特区公布实施。香港特区维护国家安全的责任，再次确认有需要改革香港特区的电脑网络罪行法律，[1] 我们研究电脑网络罪行这课题时已将此考虑在内。

研究范围

5. 2019年，小组委员会就电脑网络罪行课题展开研究，研究范围如下：

---

[1] 除了《中华人民共和国香港特别行政区维护国家安全法》第三条所载的总则外，第九条亦特别规定，对网络等涉及国家安全的事宜，香港特别行政区政府应当采取必要措施，加强管理。

"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。"

小组委员会的成员

6. 小组委员会由陈政龙资深大律师出任主席，成员如下：

陈政龙资深大律师 ***（由 2023 年 1 月 19 日起出任主席）***	资深大律师
梁镇宇先生 ***（由 2018 年 12 月 13 日至 2023 年 1 月 18 日出任主席）***	德同国际有限法律责任合伙资深顾问律师
陈淑仪女士 （任期由 2018 年 12 月 13 日至 2023 年 9 月 12 日）	律政司助理刑事检控专员
陈颖诗女士 （任期由 2025 年 3 月 25 日起）	保安局首席助理秘书长
郑松岩博士 （任期由 2022 年 1 月 12 日至 2024 年 2 月 25 日）	中国银行（香港）有限公司前首席信息官

郑丽琪女士 （任期由2022年5月3日至2024年2月25日）	香港警务处财富情报及调查科总警司 香港警务处网络安全及科技罪案调查科前总警司
张佩珊女士 （任期由2023年4月21日至2025年3月24日）	保安局前首席助理秘书长
邹锦沛博士	物流及供应链多元技术研发中心有限公司研究顾问 香港大学计算机科学系前副教授
徐诗妍女士 （任期由2019年8月12日至2023年4月16日）	保安局前首席助理秘书长
方永佳先生 （任期由2018年12月13日至2020年9月13日）	香港海关版权及商标调查（行动）课前监督
何沈洁玲女士 （任期由2018年12月13日至2020年12月20日）	香港上海汇丰银行有限公司亚太区复元风险管理前主管
何应富先生 （任期由2023年1月13日起）	消费者委员会副总干事
关煜群博士	亚太互联网中心首席执行官
林焯豪先生 （任期由2024年2月26日起）	香港警务处网络安全及科技罪案调查科总警司

罗绍佳先生 （任期由2018年12月13日至2020年7月13日）	罗本信律师行前合伙人
罗越荣博士 （任期由2018年12月13日至2022年4月12日）	香港警务处东九龙总区指挥官 香港警务处网络安全及科技罪案调查科前高级警司
梁育珩先生 （任期由2023年9月13日起）	律政司署理高级助理刑事检控专员
谭佩英女士 （任期由2024年5月21日至2025年7月31日）	香港海关版权及商标调查科高级监督 香港海关版权及商标调查（行动）课前监督
邓均林先生 （任期由2021年1月11日至2022年1月11日）	香港上海汇丰银行有限公司香港及澳门区营运韧性风险前总监
邓子扬先生 （任期由2023年1月9日起）	邓子扬顾嘉恩律师行合伙人
汤炽忠先生 （任期由2018年12月13日至2023年1月12日）	消费者委员会前副总干事
曾裕彤先生 （任期由2018年12月13日至2019年8月9日）	保安局前首席助理秘书长
王家俊先生 （任期由2025年8月1日起）	香港海关版权及商标调查（行动）课监督

黄佩琪资深大律师	资深大律师
黄蕙荃女士 （任期由 2020 年 9 月 14 日至 2024 年 5 月 8 日）	香港海关助理关长 香港海关版权及商标调查（行动）课前监督
黄咏恒女士 （任期由 2024 年 2 月 26 日至 2025 年 12 月 19 日）	香港上海汇丰银行有限公司前常务总监兼首席资讯科技总监
叶旭晖先生	香港互联网供应商协会主席

7. 小组委员会自成立以来，一直定期召开会议。法律改革委员会秘书处高级政府律师卓芷颖女士是小组委员会的秘书。[2]

项目的三个阶段

8. 由于小组委员会的研究范围广泛，加上国际间电脑网络罪行的规管情况瞬息万变，我们决定分阶段处理这课题所引起的事宜：

(a) 项目第一部分处理依赖电脑网络的罪行及司法管辖权事宜；

(b) 第二部分会涵盖借助电脑网络的罪行，该部范围适时再作讨论；及

(c) 第三部分会处理证据事宜及执法（程序）事宜。

第一部分研究的五类依赖电脑网络的罪行

9. 本报告书关乎项目的第一部分。我们借鉴欧洲委员会（Council of Europe）《电脑网络罪行公约》（Convention on Cybercrime，**《布达佩斯公约》**）及《联合国打击网络犯罪公约》（United Nations Convention against Cybercrime，**《联合国公约》**），[3] 集中研究以下五类依赖电脑网络的罪行。这些罪行是全球公认应对付的主要电脑网络罪行种类：

---

[2] 时任高级政府律师马文舜先生担任小组委员会的秘书至 2021 年 5 月，而高级政府律师李灏棋先生由 2024 年 9 月 2 日至 2025 年 9 月 17 日担任小组委员会的秘书。

[3] 欧洲委员会《电脑网络罪行公约》及《联合国打击网络犯罪公约》的详情载于第 1 章。

(a) 非法取览程式或数据；

(b) 非法截取电脑数据；

(c) 非法干扰电脑数据；

(d) 非法干扰电脑系统；及

(e) 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（包括为向他人提供该等器材、程式或数据而管有它们）。

建议背后的指导原则

10. 我们明白制订建议时需顾及各方持份者不同的权益及看法，亦理解当中的重要性。我们的指导原则，是同时平衡兼顾：

(a) 网民的权利和资讯科技业内人士的权益；及

(b) 保障公众在使用和操作电脑系统时免受骚扰或攻击的权益和权利。

咨询过程

11. 为期三个月的咨询期于2022年10月19日结束。总计收到的意见书共65份（部分于要求延期后收到），由简单的确认收到咨询文件，以至对咨询文件内小组委员会的建议及问题发表详细意见不等。

12. 提交意见书的回应者包括学者、政府决策局／部门、半官方机构、资讯科技相关团体、法律专业团体、商业团体、政党，以及公众人士（"**回应者**"）。回应者的名单载于本报告书附件。我们十分感谢所有曾对咨询文件提出意见的回应者，后述各章会概述他们所提交的意见书。

13. 小组委员会的代表除了出席电视及电台访问，解释咨询文件内的建议之外，亦参加了由香港大学计算机科学系于2022年9月14日举办的网上科技论坛（HKU-CS Online Tech Forum），以及由立法会科技创新界功能界别邱达根议员于2022年10月27日主持的答问环节。两个场合席上大多为资讯科技及电讯界别的持份者，为小组委员会提供适当机会接触网络安全从业员，并厘清咨询文件内某些建议。

14. 2022年11月7日（此为征询立法会后为小组委员会所能安排的最早会议时段），小组委员会成员出席立法会司法及法律事务委员会的会议，简介咨询文件内容，并听取团体代表意见。

本报告书的结构

15. 本报告书由九个章节组成，处理16项最终建议：

(a) 第1章交代背景，描述国际机构和举措如何将电脑网络罪行归类。

(b) 第2章先探讨五类依赖电脑网络罪行的第一类，即非法取览程式或数据。

(c) 第3章集中讨论第二类依赖电脑网络的罪行，即非法截取电脑数据。

(d) 第4章涵盖第三类依赖电脑网络的罪行，即非法干扰电脑数据。

(e) 第5章继而检视第四类依赖电脑网络的罪行，即非法干扰电脑系统。

(f) 第6章处理第五类依赖电脑网络的罪行，即提供用作干犯电脑网络相关罪行的器材、程式或数据，或管有用作干犯电脑网络相关罪行的器材、程式或数据。

(g) 第7章转谈香港法庭行使司法管辖权的准则。

(h) 第8章处理有关上述依赖电脑网络罪行的判刑事宜。

(i) 第9章总结我们的最终建议。

16. 回应者的名单（附件）载于本报告书末。

第 1 章　电脑网络罪行的归类

引言

1.1　正如小组委员会在咨询文件指出，[1] 电脑网络罪行既没有确切的清单，也无法巨细无遗地逐一胪列。文献列述了多种电脑网络罪行的归类方法，以及多组用于有关归类的术语。在联合国的层面，联合国毒品和犯罪问题办公室（United Nations Office on Drugs and Crime）在 2013 年展开的网络犯罪问题全球方案（Global Programme on Cybercrime），区分*"依赖电脑网络的罪行"*及*"借助电脑网络的罪行"*。[2] 联合王国政府的以下阐释有助理解：

(a) 依赖电脑网络的罪行指*"只能通过使用资讯及通讯科技器材进行的罪行，当中有关器材既是犯罪工具，亦是犯罪目标"*。[3] 依赖电脑网络的罪行的例子包括：黑客入侵、散播电脑病毒及分布式拒绝服务攻击。

(b) 借助电脑网络的罪行指*"通过使用电脑、电脑网络或其他形式的资讯及通讯科技，使犯罪规模或范围得以扩大的传统罪行"*。[4] 借助电脑网络的罪行的例子包括：在网上散布儿童色情物品、设立仿冒诈骗网站及网上"起底"（即在互联网未经授权而披露他人的私人资料或识别身分资料）。

在《布达佩斯公约》下的归类

《布达佩斯公约》订明的罪行

1.2　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》**）于 2001 年 11 月 23 日开放予各国

1　第 1.2 段。

2　联合国毒品和犯罪问题办公室（"**联合国毒罪办**"），*"网络犯罪问题全球方案"*，登载于 https://www.unodc.org/unodc/en/cybercrime/our-approach（于 2025 年 11 月 1 日浏览）。

3　内阁办公室国家安全及情报部（Cabinet Office, National security and intelligence）、英国财政部（HM Treasury）和国会议员夏文达（The Rt Hon Philip Hammond MP）：《2016–2021 年国家网络安全战略》（*National Cyber Security Strategy 2016-2021*）（联合王国政府，2016 年），第 3.2 段，登载于 https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021（于 2025 年 11 月 1 日浏览）。

4　同上。

签署，并于 2004 年 7 月 1 日生效。[5] 此后，《布达佩斯公约》由两项《附加议定书》（Additional Protocol）作为补充，内容分别关于宣告将利用电脑系统犯下的种族主义或仇外行为订为犯罪行为，[6] 以及关于加强合作和披露电子证据。[7]《布达佩斯公约》似乎是首份规管电脑网络空间的跨国协议。[8] 截至 2025 年 11 月 1 日，已有 81 个国家批准或加入《布达佩斯公约》。[9]

1.3 《布达佩斯公约》第一节（第二至十三条）旨在制定有关罪行的共同最低标准，藉以改善防止和制止电脑罪行或电脑相关罪行的方法。[10]《布达佩斯公约》规定各缔约国均须*"采取必要的立法和其他措施"*，在其本土法律中就以下主题订定刑事罪行（就遵从规定而言，显然是"重实质多于形式"）：

(a) 损害电脑数据及系统的机密性、完整性和可用性的罪行（包括非法取用电脑系统、非法截取非公开传送的电脑数据、非法干扰电脑数据、非法干扰电脑系统，以及为犯电脑网络罪行而误用器材或数据）；

(b) 电脑相关罪行（包括电脑相关伪造及电脑相关欺诈）；

(c) 内容相关罪行（包括儿童色情物品相关罪行，以及通过电脑系统散布种族主义和仇外材料的相关罪行）；及

(d) 关于侵犯版权和相关权利的罪行。

---

5 全文登载于欧洲委员会（Council of Europe）网站，网址为 https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185（于 2025 年 11 月 1 日浏览）。

6 第一项《附加议定书》于 2006 年 3 月 1 日生效，全文登载于欧洲委员会网站，网址为 https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=189（于 2025 年 11 月 1 日浏览）。

7 第二项《附加议定书》于 2022 年 5 月开放予各国签署，全文登载于欧洲委员会网站，网址为 https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224（于 2025 年 11 月 1 日浏览）。

8 除《布达佩斯公约》外，亦有其他区域举措。例子见：联合国毒罪办，*"International and regional instruments"*，登载于 https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/international-and-regional-instruments.html（于 2025 年 11 月 1 日浏览）。

9 欧洲委员会，签署及批准《电脑网络罪行公约》列表（ETS 第 185 号），登载于 https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185（于 2025 年 11 月 1 日浏览）。

10 欧洲委员会，《电脑网络罪行公约说明报告》（*Explanatory Report to the Convention on Cybercrime*）（ETS 第 185 号，2001 年 11 月 23 日），第 33 段，登载于 https://rm.coe.int/16800cce5b（于 2025 年 11 月 1 日浏览）。

《电脑罪行及电脑相关罪行示范法》

1.4 英联邦（Commonwealth of Nations）秘书处是欧洲委员会电脑网络罪行公约委员会（Cybercrime Convention Committee of the Council of Europe）的观察员。英联邦经参照《布达佩斯公约》，制定了《电脑罪行及电脑相关罪行示范法》（Model Law on Computer and Computer Related Crime）[11]（**《示范法》**）。《示范法》于2002年获采纳，而截至2017年7月，当局正考虑检讨该法。[12]

1.5 英联邦秘书处于2016年4月22日的新闻稿指出，已有22个英联邦国家采用《示范法》，作为其全国性电脑网络罪行法律的基础。[13]

联合国的最新动向

1.6 国际间对电脑网络罪行的规管情况正在急速变化。联合国以下动向可能具影响力，值得密切关注：

(a) 俄罗斯联邦（Russian Federation）于2017年10月11日向联合国提交《联合国合作打击网络犯罪公约》草案（Draft United Nations Convention on Cooperation in Combating Cybercrime，**《俄罗斯公约》**）。联合国大会的有关决议没有记录任何协定的后续行动。[14]

(b) 大会于2019年12月27日采纳的第74/247号决议[15]中决定：

> "……设立一个代表所有区域的不限成员名额特设政府间专家委员会，以拟订一项关于打击为犯罪目的使用信息和通信技术行为的全面国际公约，同时充分考虑到关于打击为犯罪目的使用信息和通信技术行为的现有国际文书和国家、区域和国际各级的现有努力，特别是全

---

11 全文登载于英联邦网站，网址为 http://thecommonwealth.org/sites/default/files/key_reform_pdfs/P15370_11_ROL_Model_Law_Computer_Related_Crime.pdf（于2025年11月1日浏览）。

12 2018年，在伦敦举行的英联邦政府首脑会议上签署了《英联邦网络宣言》（Commonwealth Cyber Declaration）。此后展开了一项计划，以便在英联邦各国落实《网络宣言》的承诺。

13 英联邦秘书处，*"Commonwealth model law promises co-ordinated cybercrime response"*（2016年4月22日），登载于 https://thecommonwealth.org/media/news/commonwealth-model-law-promises-co-ordinated-cybercrime-response（于2025年11月1日浏览）。

14 联合国大会，第72/196号决议（A/RES/72/196，2017年12月19日）。

15 联合国大会，第74/247号决议（A/RES/74/247，2019年12月27日）。

面研究网络犯罪问题不限成员名额政府间专家组的工作和成果”。[16]

(c) 经过上述特设委员会多年努力，《联合国打击网络犯罪公约》（**《联合国公约》**）于2024年12月24日由大会透过第79/243号决议采纳。[17]《联合国公约》于2025年10月25日在越南开放供各国签署，并会在纽约联合国总部继续开放供签署，直至2026年12月31日。在40个国家成为缔约方后，《联合国公约》便会生效，而缔约国会议将定期召开，审议该公约的实施情况，以期增强缔约国的能力和促进缔约国之间的合作，从而实现该公约的各项目标。[18]

1.7 《联合国公约》是首条全面针对电脑网络罪行的全球性条约，为各国提供一系列可采取的措施，以预防和打击电脑网络罪行，同时亦旨在加强国际合作，共享严重罪案的电子证据。[19]

1.8 读者会记得，在2022年发表的咨询文件中，有关建议借鉴了《布达佩斯公约》及《俄罗斯公约》的概念。[20] 就研究第一部分所载的依赖电脑网络罪行而言，该等罪行在《布达佩斯公约》及《联合国公约》下的归类基本上相同，只是后述公约采用不同术语，例如“信息通信技术”（一如在咨询文件中曾研究的《俄罗斯公约》）[21] 及“电子数据”，而非《布达佩斯公约》所分别采用的“电脑”及“电脑数据”。[22] 由此，继续沿用咨询文件所采纳的术语，以及在本报

---

16 第3段。2022年至2023年间，特设委员会召开六次会议，其闭幕会议于2024年1月29日至2月9日在纽约举行，并于2024年7月29日至8月9日重新召开闭幕会议，由该委员会批准《联合国打击网络犯罪公约》的决议草案。见：联合国毒罪办，*“Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes”*，登载于 https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home（于2025年11月1日浏览）。

17 联合国毒罪办，*“United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes”*，登载于 https://www.unodc.org/unodc/en/cybercrime/convention/home.html（于2025年11月1日浏览）。

18 同上。2025年10月的签署仪式结束时有72个签署国，包括中国。各国在签署后会完成本土的内部程序，以履行该公约，并会于完成后向秘书长交存批准书、接受书或核准书，以正式成为该公约的缔约国。没有签署该公约的国家也可透过交存加入书而成为缔约方。作为进一步资讯提供，特设委员会将于2026年1月26至30日在维也纳召开会议，以拟备该公约缔约国会议议事规则草案。见 https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_session_on_RoP/main.html（于2025年11月1日浏览）。

19 见上文注脚17。

20 咨询文件导言第10段。

21 咨询文件第2.93至2.95段。

22 第2.42至2.46段会解释，我们认为在新订针对电脑网络罪行的特定法例中保留“电脑”一词属恰当。

告书下文提述《布达佩斯公约》，并不影响项目第一部分所提出的最终建议的理据。政府如落实本报告书的建议，当然可自由决定如何以最理想的方式在新订针对电脑网络罪行的特定法例表述相关概念。

第 2 章　非法取览程式或数据

引言

2.1　本章讨论关于咨询文件建议 1 至 3 的回应。建议 1 关乎第一类依赖电脑网络的罪行，即非法取览电脑中的程式或数据（“**取览罪**”）：

> “小组委员会建议：
>
> (a) 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。
>
> (b) 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。
>
> (c) 新法例的建议条文应以[英格兰及威尔斯《1990 年误用电脑法令》（Computer Misuse Act 1990，《**英格兰误用电脑法令**》）]第 1、2 及 17 条为蓝本。”

2.2　正如小组委员会在咨询文件解释，[1] 概括而言，取览罪一般旨在：

(a) 应对损害电脑系统安全的危险威胁及攻击；

(b) 从而保护人们以不受干扰及不受限制的方式管理、操作和控制其电脑系统的权利。

2.3　由于部分回应提述《刑事罪行条例》（第 200 章）第 161 条（*“有犯罪或不诚实意图而取用电脑”*）（“**第 161 条**”），这项条文又常被用来检控现行法律下的电脑罪行，因此宜在本章复述该条的内容：

> “(1) 任何人有下述意图或目的而取用电脑——
>
> (a) 意图犯罪（不论是在取用电脑的同时或在日后任何时间）；

---

[1] 第 2.1 段。

(b) 不诚实地意图欺骗(不论是在取用电脑的同时或在日后任何时间);

(c) 目的在于使其本人或他人不诚实地获益(不论是在取用电脑的同时或在日后任何时间);或

(d) 不诚实地意图导致他人蒙受损失(不论是在取用电脑的同时或在日后任何时间),

即属犯罪,一经循公诉程序定罪,可处监禁5年。

(2) 就第(1)款而言,获益(gain)及损失(loss)的适用范围须解释作不单扩及金钱或其他财产上的获益或损失,亦扩及属暂时性或永久性的任何该等获益或损失;而且——

(a) 获益(gain)包括保有已有之物的获益,以及取得未有之物的获益;及

(b) 损失(loss)包括没有取得可得之物的损失,以及失去已有之物的损失。"

2.4 在*律政司司长 诉 郑嘉仪*[2](*Secretary for Justice v Cheng Ka Yee*),终审法院裁定,*"根据恰当的诠释,当任何人使用自己的电脑,而其中不涉及取用另一人的电脑,该行为便不干犯第161(1)(c)条"*。[3] 按逻辑推断,亦可就第161(1)条的其他部分得出同一结论。因此,举例来说,第161条不适用于任何人使用自己的电脑设立仿冒诈骗网站的情况。

2.5 与考虑取览罪相关的另一条文是《电讯条例》(第106章)第27A条(*"藉电讯而在未获授权下取用电脑资料"*)("**第27A条**"):

"(1) 任何人藉着电讯,明知而致使电脑执行任何功能,从而在未获授权下取用该电脑所保有的任何程式或数据,即属犯罪,一经定罪,可处第4级罚款。

(2) 就第(1)款而言——

(a) 该人的意图不一定要针对——

---

2 (2019) 22 HKCFAR 97, FACC 22/2018(判决日期:2019年4月4日)。

3 同上,第48段。

(i) 任何个别程式或数据；

(ii) 任何个别种类的程式或数据；或

(iii) 任何个别电脑所保有的程式或数据；

(b) 任何人如无权控制对电脑所保有的程式或数据的有关种类的取用，且有下述情况，则他对电脑所保有的任何程式或数据的该类取用，即属未获授权——

(i) 他未获有此权利的人授权，使他获得对该电脑所保有的程式或数据的该类取用；

(ii) 他不相信自己已获如此授权；及

(iii) 他不相信若他曾申请适当的授权，则他本已获如此授权。

(3) 第(1)款的效力，并不损害关于检查、搜查或检取权力的任何法律。

(4) 尽管有《裁判官条例》（第227章）第26条的规定，关于本条所订罪行的法律程序，可在发生该罪行的3年内或检控人发现该罪行的6个月内（以最先届满的期间为准）任何时间提出。"

2.6 正如原讼法庭在*香港特别行政区 诉 秦瑞麟*（*HKSAR v Tsun Shui Lun*）[4] 裁定，第27A条适用的前提是犯罪者已"藉着电讯"获得有关取用。由此可见，除了目标电脑外，当中亦涉及使用电讯器材（例如另一部电脑）以获得有关取用。与此一致的是，第27A条在*郑嘉仪*被定性为*"'黑客入侵'罪行"，"明显是针对不属于犯罪者自己的电脑"*。[5]

对小组委员会建议1的回应

2.7 就建议1提出意见的回应者普遍同意，在未获授权下取览程式或数据应定为罪行。香港与内地法律专业联合会有限公司认为，

---

4 [1999] 3 HKLRD 215, HCMA 723/1998（判决日期：1999年1月15日），原讼法庭审理的裁判法院上诉案件，于*香港特别行政区 诉 欧阳家敏*（*HKSAR v Au Yeung Ka Man Yuniko*）[2018] HKCFA 23获引用和认同。

5 见上文注脚2，第41段。

第 161 条及第 27A 条有其*"明显"*局限，因为该等条文均不适用于任何人使用自己的电脑或其他非电讯器材干犯电脑网络罪行的情况。某政治团体及某商业机构也持同一看法，指出*"终审法院"*在*郑嘉仪*[6] *"大幅收窄了"*第 161 条的适用范围。

2.8 同样地，消费者委员会也总体上同意需要立法禁止纯粹在未获授权下取览程式或数据，前提是合理辩解可作为免责辩护，而且有特定的免责辩护或豁免涵盖在未获授权下为网络安全目的而取览。

2.9 然而，部分回应者关注取览罪的范围，并质疑"没有犯罪意图"而在未获授权下取览程式或数据（即纯粹在未获授权下取览）应否属犯罪。就建议 1 提出意见的其他回应者，则提议厘清"合理辩解"免责辩护的涵盖范围。下文会更详细地载列回应者就建议 1 提出的各项意见。

建议 1(a)所述的纯粹在未获授权下取览这项简易程序罪行的犯罪意念

2.10 部分回应者将建议 1 与第 161 条比较，认为建议 1 完全没有把*"恶意意图"*纳入考虑之列。多个资讯科技相关团体及个别人士均强调，把"犯罪 / 恶意意图"、"恶意"、"罔顾后果"及 / 或发生损坏列为取览罪的构成元素，实属重要。从有关意见书中的阐述来看，回应者所构想的"恶意"或"恶意意图"，似乎包括被告人参与*"犯罪活动或非法活动"*，或被告人如第 161 条所述般*"不诚实地意图获益、导致损失或欺骗"*。这些回应者有以下看法：

(a) 若不规定须怀有恶意，则合法行为也有可能被定罪。这些行为包括技术及保安方面的做法，例如云端计算、渗透测试，以及保安专业人员、白帽黑客及漏洞赏金计划参与者所采取的其他正常做法。

(b) 资讯科技专业人员及一般用户均可轻易接触大量数据（例如电话纪录、电脑日志纪录），当中许多更是无须提交密码即可取览。建议的（没有恶意或犯罪意图而）纯粹在未获授权下取览罪，*"忽视了取览作为的目的或意图"*。

---

[6] 见上文注脚 2。

合理辩解作为法定免责辩护

2.11 部分回应者（包括某商业团体）认为，建议 1 所述的"合理辩解"法定免责辩护的范围含糊不清、流于主观，亦有欠明确。多间资讯科技相关机构、商业团体及某政治团体共作出三项提议：

(a) 在"合理辩解"的定义内明文加入各种获豁免活动，例如*"网络安全操作"*、*"互联网服务提供者基于运作原因而进行的网络扫描"*及*"没有犯罪意图的合法业务运作"*；

(b) 在法例中提供一份非尽列的例子清单，列举会构成"合理辩解"的合法活动；及

(c) 就建议罪行订定特定的免责辩护，以涵盖合法的商业服务或行为，并应以概括方式拟定有关法定免责辩护或豁免，让合法的业务经营者有足够空间为自己辩白。

证明加重罪行

2.12 正如小组委员会在咨询文件解释，[7] 犯非法取览罪的人或会在取览有关程式或数据后进一步带来可能严重的伤害。举例来说，犯罪者可能会尝试在目标电脑安装间谍软件，或意图勒索受害人。单靠就建议的简易程序罪行立法，将不足以应对社会所面临的有关威胁。故此建议 1(b)提出，参照《英格兰误用电脑法令》第 2 条的拟定方式，[8] 订明在未获授权下取览，并意图进行其他犯罪活动，应构成新法例所订罪行的加重形式。

2.13 就加重罪行而言，香港女律师协会有限公司认为，要就*"未犯的潜在罪行"*证明意图*"颇为困难"*，故在严重罪行无法被确立为加重罪行时，当局或会极其依赖建议 1(a)所述的简易程序罪行来处理该等罪行。该会进一步请小组委员会在判刑方面考虑这点，即就简易程序罪行处以两年监禁是否具足够阻吓性。

---

7 第 2.107 段。

8 《英格兰误用电脑法令》第 2 条规定：

"(1) 任何人如犯上述第 1 条所订罪行（'在未获授权下取览罪'），并——

(a) 意图干犯本条所适用的罪行；或

(b) 意图利便干犯该等罪行（不论是由其本人干犯或由他人干犯），

即属犯本条所订罪行；而该人意图干犯或意图利便的罪行，在本条下文提述为其他罪行。

.....

(3) 就本条而言，不论其他罪行是与在未获授权下取览罪同时干犯或在日后任何时间干犯，属无关重要。

(4) 即使有关事实显示干犯其他罪行并不可能，任何人仍可被裁定犯本条所订罪行。"

罪行互相重迭

2.14 对于小组委员会建议保留第 161 条，直至新订的电脑网络罪行法例显然足以取而代之，两名回应者在第 161 条所订罪行与取览罪互相重迭的问题上意见分歧。

2.15 一方的看法是，罪行互相重迭*"相当可能会对公众造成混淆，亦令法律变得不必要地复杂模糊"*，并指出若对各项罪行的检控继续根据第 161 条而非根据新法例提出，则未必能达到小组委员会所期望的目的。

2.16 相反的看法是，罪行互相重迭大概只是看似令人担忧，但实际上不足为虑。有关论据引述如下：

> "……控方的检控常规，是'充分反映指称罪行的刑责，方式为既能兼顾检控效率亦能令法庭于社会与被告两者之间秉公行义'，且'在合理可行的情况下，控罪的数目应尽量减少'（《检控守则》第 8.1 段）……即使某人被控并被裁定犯了多项在刑责上可能互相重迭的罪行，法庭也必然须按照确立已久的整体量刑原则对被告人判刑。"

界定若干词语

2.17 部分商业团体、关注组及个别人士认为，应清晰界定或向公众解释若干概念（包括"在未获授权下"/"在获授权下"取用或取览、"取用或取览"、"电脑网络"及"数据"）的涵义。

我们的分析及回应

厘清犯罪意念

2.18 某些回应者认为*"没有犯罪意图"*而纯粹在未获授权下取览程式或数据不应属犯罪，他们似乎把建议的罪行视为严格法律责任罪行，或认为必须有从事犯罪活动的意图，方可构成在未获授权下取览罪。

2.19 在咨询文件的建议 1(c)，小组委员会建议取览罪应以《英格兰误用电脑法令》第 1、2 及 17 条为蓝本。应当强调的是，有关的英格兰罪行并非严格法律责任罪行，而是规定须证明犯罪意念。为清晰起见，宜在本报告书再次引述英格兰取览罪的相关条文。

2.20 《英格兰误用电脑法令》第 1 条（*"在未获授权下取览电脑资料"*）是英格兰取览罪的基本形式，该条规定如下：

"(1) 任何人在以下情况，即属犯罪——

(a) 该人致使某电脑执行任何功能，意图获得对存于任何电脑内的任何程式或数据的取览，或意图使他人能够获得该项取览；

(b) 该人意图获得该项取览，或意图使他人能够获得该项取览，但该项取览未获授权；及

(c) 该人在致使该电脑执行该功能时，知悉情况如此。

(2) 任何人犯本条所订罪行须具备的意图，不一定要针对——

(a) 任何特定程式或数据；

(b) 任何特定种类的程式或数据；或

(c) 存于任何特定电脑内的程式或数据。

....."

（底线后加）

2.21 《英格兰误用电脑法令》第 17(5)及(8)条解释取览的未获授权性质：

"(5) 在以下情况下，任何人取览存于某电脑内的任何程式或数据，不论取览属任何种类，即属未获授权取览——

(a) 该人本身无权控制对该程式或数据作出有关种类的取览；及

(b) 该人未获有此权利的人同意他对该程式或数据作出该类取览……

....."

(8) 在以下情况下，如某人就某电脑作出某作为，或导致就某电脑作出某作为，该作为即属未获授权——

(a) 该人本身不是对该电脑负有责任并有权决定可否作出该作为的人；及

(b) 该人未获任何上述的人同意该作为。

在本款中，'作为'包括一连串作为。"

2.22 故此，《英格兰误用电脑法令》第 1(1)条所订的简易程序罪行的犯罪意念包括以下两项：(i)被告人意图获得对任何程式或数据的取览（或意图使他人能够获得该项取览）；及(ii)被告人在犯罪行为发生时，知悉该项意图作出的取览未获授权。换言之，关于取览性质的犯罪意念是控方必须证明的所需元素，而且只有当犯罪行为（即取览的行为元素）及犯罪意念（即知悉取览的未获授权性质这项意念元素）同时存在，才能够产生取览罪。控方或法庭必须信纳，被告人在未获授权的取览作出时，知悉该项取览未获授权。

2.23 我们维持原先看法，即我们认为把某人知悉其取览未获授权定为取览罪的先决条件，是公允的做法。我们预料，法庭很可能会根据案件的环境证据，作出关于某人是否知悉未获授权的推论。[9] 就此而言，部分回应者的意见书所引述的一宗真实案例正可阐明这点：某乘客发现，航空公司发出的电子登机证存在保安漏洞，令他能透过修改有关划一资源定位址（URL）的最后两位字元，查阅其他乘客的资料。事件经调查后，发现被告人的互联网规约（"**IP**"）地址在未获授权下连接至另一乘客的网上预订页面。被告人根据第 27A 条被起诉。[10] 我们认为，虽然该航空公司没有采取足够的保安措施，以保护其他乘客的登机资料，但被告人乘客作为该公司有关电子系统的普通用户，并不应预期该公司已授权自己透过修改有关 URL，取览同机乘客的登机证。故此，有充分理由根据第 27A 条对他提出起诉。

2.24 我们在此补充一点，凡任何人指称自己不知悉某项取览的未获授权性质，便应在引致该项取览的整个事件过程中验证该项指称是否属实。举例来说，假设某法定机构的数据档案外泄，令数千名与该机构有事务往来的人的资料被泄露，某君自称积极分子，维持某网站或社交媒体专页（并宣称以在香港推动透明问责为宗旨），将这宗资

---

9 咨询文件第 2.101 段。

10 案件编号是 WKS6208/2019。最终，被告人同意签保守行为一年，获控方不提证供起诉。见 https://www.hk01.com/article/347780（于 2025 年 11 月 1 日浏览）。

料外泄事故公诸于世。若某人因此发现了这宗资料外泄事故，继而取览在公众领域的外泄数据，法庭便会对引致被告人浏览实际载有外泄资料的网站的各项事实进行查讯。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以下必然推论：被告人在作出有关取览时，知悉该项取览未获授权。

纯粹在未获授权下取览应属犯罪

2.25 各回应者就取览罪的意念元素所提出的意见，也关乎纯粹在未获授权下取览程式或数据应否属犯罪这问题，咨询文件第 2 章已对此作透彻的讨论。[11] 小组委员会从一开始就理解到，电脑网络空间因为其本质，与具有形和明确界线的现实世界分属截然不同的领域：

> "……鉴于虚拟空间的设计和运作的固有特点，以及在虚拟空间的惯常做法，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。事实上，任何人若把器材连接至互联网或使用互联网服务，他某程度上已默许与其他网上用户作某（合理）程度的互动。举例来说，我们一般并不预期网上用户在向传送对象（即另一网上用户）发送电邮或展示网页广告前，须事先寻求后者的明示授权，尤其是当有关发送或展示并非恶意作出。另一例子是，搜寻器会在多个互联网规约地址扫描互联网，[12] 从而确定这些地址是否有网页伺服器，并为找到的网页建立索引。因此，在电脑网络空间这一领域，应在上述背景之下理解'在未获授权下'取用或取览这个概念。"[13]

2.26 换言之，基于我们在上文解释"在未获授权下"取用或取览这概念时所述的理由，将继续容许在日常生活中已普遍接受在进入电脑

---

11 第 2.4、2.5、2.96 至 2.101 段。

12 具体而言，搜寻器会经常测试连接埠 80 及 443，这两个连接埠一般都与取览网站相关。在电脑网络空间，连接埠是网络连接开始与结束的电脑虚拟点，均以软件为基础，并由电脑系统管理。连接埠 80 被指定用于"HTTP"（超文本传输规约），用作传送网页。连接埠 443 被指定用于"HTTPS"（保密超文本传输规约），用作安全地经由传输层保安（TLS）或保密插口层（SSL）传送网页。见 https://isc.sans.edu/forums/diary/Cyber+Security+Awareness+Month+Day+25+Port+80+and+443/7450（于 2025 年 11 月 1 日浏览）。鉴于对连接埠 80 及 443 的明确指定，法律不应禁止连接至这些连接埠，以作其指明所用的指定用途。另外，搜寻器一般会使用网络爬虫软件，有系统地浏览网页，以搜集网页的相关资料。这过程可为有关资料建立索引，并让用户在进行搜寻查询时得以检索这些资料。见 Alexander S Gillis, "What is a web crawler?", 登载于 https://www.techtarget.com/whatis/definition/crawler（于 2025 年 11 月 1 日浏览）。

13 咨询文件第 2.5 段。

网络空间时的惯常做法或行业常规，亦即无须就小组委员会已举例说明（而我们亦同意）的取用或取览程度，事先寻求明示授权。[14] 建议 1 正是在这基础上提出纯粹在未获授权下取览程式或数据应构成罪行。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。[15] 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[16] 和实际需要[17] 而进行自动连接，并由此而产生取览程式或数据。

2.27 在此亦宜复述欧洲委员会（Council of Europe）的《电脑网络罪行公约说明报告》（Explanatory Report to the Convention on Cybercrime）中的评注，当中论述纯粹在未获授权下取用电脑／取览程式或数据所造成的后果：

> "44. 原则上，纯粹在未获授权下入侵……本身应属非法。有关行为可能会对系统和数据的合法使用者造成阻碍，亦可能导致涉及高昂重建费用的更改或摧毁。这类入侵行为或会使人得以取览机密数据（包括密码、关于目标系统的资料）及秘密，以及免费使用有关系统，甚或鼓励黑客干犯更具危害性的电脑相关罪行，例如电脑相关欺诈或电脑相关伪造。
>
> 45. 最有效防止在未获授权下取用的方法，当然是推行和制订有效的保安措施。不过，全面的应对方案亦须包括威胁施加和采用刑事法律措施。以刑事法例禁止在未获授权下取用，能够及早为有关系统和数据本身提供额外保护，免受上述各种危险。"

---

14 同上。

15 咨询文件第 2.100 段。

16 例如，当智能电话的用户在购物商场开机并启动其 Wi-Fi 功能时，即使该用户没有选择把自己的电话连接至商场的 Wi-Fi 热点，该器材也会自动侦测商场所提供的可用 Wi-Fi 热点，而商场的网络亦同样会侦测到该用户的电话。另一个例子是，当用户把自己的个人电脑连接至某公共 Wi-Fi 接驳点并将电脑设定为可搜寻时，连接至同一 Wi-Fi 接驳点的任何其他电脑或电子器材均能够侦测到该用户的个人电脑。在上述每个例子，有关用户的器材（前者）均是通过以下方式而被另一器材（后者）接达：后者向前者发出通讯请求，前者继而发出回应。

17 以下例子可用作说明：(i)点对点档案分享；及(ii)分散区块链技术。点对点档案分享让用户无需借助中央伺服器，便能互相分享数据及电子档案。某用户在个人电脑运行点对点软件时，该软件会向其他可供接达的节点（即其他连接至互联网的电脑）发出数据，而这些节点可能会发出回复，然后在两个节点之间建立连线。同样地，分散区块链经常会使用点对点网络来搜寻节点。在这种情况下，各节点（例如能够连接互联网的电脑或智能电话）会向有关网络作出广播以示其存在，并听候来自其他节点的信息。某节点在收到来自新节点的信息时，便可建立连线并交换信息。见 Radovan Stevanovic, *"Blockchain from Scratch: Understanding Network Communication in Blockchains"*（2023 年 1 月 3 日）。

（底线后加）

2.28　我们曾进一步研究《英格兰误用电脑法令》的外在立法材料，当中阐明订立取览罪的基本形式（即纯粹在未获授权下取览）的目的。由于黑客的企图入侵所造成的不确定性及成本，英格兰及威尔斯法律委员会（Law Commission of England and Wales，“**英格兰法律委员会**”）把通过在未获授权下进入而进行的黑客入侵，视为*“系统用户有正当理由高度关注的事情”*。[18] 据英格兰法律委员会解释：

> “……由于任何企图进入者或许均已透过密码获得重要级别的权限，其级别之高，有时更让他们可从有关系统中删除自己的活动纪录，因此须极为严肃看待一切在未获授权下成功取览的情况。故此，在以下两方面产生庞大费用：(i)采取保安措施抵御未获授权进入系统，并采取同等重要的预防措施，监察企图进入系统的情况；以及(ii)调查事实上确有发生未获授权进入系统的一切事件，不论案情如何轻微……我们信纳……相关成本庞大。”[19]

（底线后加）

2.29　因此，纯粹在未获授权下取览罪当时所回应的一点，是*“人们需要保护电脑系统的完整及安全，使其免受寻求进入这些系统的未获授权人士攻击，不论这些人有何意图或动机”*，[20] 而英格兰法律委员会建议分别订立《英格兰误用电脑法令》第 1 及 2 条的简易程序罪行及加重罪行，*“藉此阻吓黑客入侵”*。[21] 这两项罪行旨在共同发挥作用，以有效阻吓各种形式的未获授权取览。[22]

2.30　由于《英格兰误用电脑法令》在数码时代来临前已经制定，当时互联网的使用较不普及，故我们曾考虑英格兰法律委员会的理据在现今状况下依然适用的程度。我们认为，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的完整性，使其免受未获授权的取用或取览。最近数码港及消费者委员会先后遭黑客入侵的新闻，正好显示在电脑网络空间这范畴上绝不能掉以轻心。[23]

18　英格兰法律委员会，*“Criminal Law – Computer Misuse”*（英格兰法律委员会第 186 号，1989 年），第 1.29 段。

19　同上，第 1.37 段。

20　同上，第 1.37 段。

21　同上，第 1.37 段。

22　同上，第 3.2 段。

23　2023 年 8 月，据报某勒索软件组织先对数码港的电脑系统进行黑客入侵，再向它勒索。大量个人资料外泄，其后在暗网被公开，当中包括银行帐户资料、身分证号码及职员证资

2.31 鉴于上述理由，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。

合理辩解作为法定免责辩护——应否在"合理辩解"的定义内明文加入某些活动，以及应否在法例中提供一份非尽列的例子清单

2.32 正如终审法院在*香港特别行政区 诉 何来*（*HKSAR v Ho Loy*）[24]所解释，"无合理辩解"（不论作为免责辩护，还是控方须证明的元素）是法规中常见的用语，而某辩解是否合理须视乎个别案件的具体事实和情况而定。[25] 我们认为，尝试在电脑网络罪行法例中诠释"合理辩解"，或尝试阐明有关立法原意（例如拟定一份"合理辩解"的例子清单），均可能会收窄合理辩解免责辩护的范围。倘若被告人在案中的作为或行为偏离法例中的例子所述，便会面临法庭对其作出不利裁决的风险。因此，为了让"合理辩解"的范围尽可能广阔，我们建议不应界定该词。

2.33 另外，我们留意到就概念而言，"合理辩解"是被告人无须承担法律责任的辩白理由，而非支持其行为的理由。故此，"合理辩解"这概念，本来就与不应视为违法的合法目的并不契合。正因如此，我们认为不宜把各种合法活动归入合理辩解免责辩护的范围，反而较适宜把这些活动订明为法定免责辩护，即表明有关活动并不构成罪行。

2.34 故此，我们建议应在合理辩解免责辩护之外提供特定的免责辩护，以豁除我们认为显然不属非法的行为。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，而在我们建议的特定免责辩护并不适用时，合理辩解免责辩护或可作为后备选择。这种处理方法亦清晰明确，可释除对法例有含糊之处的疑虑。在本章的后半部分，我们会详细阐释建议的各项特定免责辩护。[26]

执法机关取览程式或数据

2.35 部分回应者（包括政府相关机构及商业团体）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

料。两星期后，消费者委员会亦遭黑客入侵，被盗取的内容包括员工及空缺申请人的资料。见《南华早报》社评，*"Hong Kong's Cyberport hack sends reminder to be alert"*（2023 年 9 月 16 日），以及《星岛日报》*"消委会：遭黑客入侵 7 小时 盗取员工、月刊户等资料 被要求交 50 万美元赎金"*（2023 年 9 月 22 日）。

24 (2016) 19 HKCFAR 110, FACC 7/2015（判决日期：2016 年 3 月 23 日）。

25 同上，第 127 页（第 37 段）。

26 下文第 2.63 至 2.102 段。

脑程式或数据（例如疑犯的流动电话所储存的电脑程式或数据），以及业务经营者为执法目的而取览上述程式或数据（例如资料当事人的个人资料），会否获豁免刑事法律责任。

2.36　我们留意到，*岑永根 诉 警务处处长*（*Sham Wing Kan v Commissioner of Police*）[27] 就执法机关搜查被捕人身上流动电话的数码内容，订下清晰指引。正如上诉法庭裁定，裁判官可根据《警队条例》（第 232 章）第 50(7)条发出手令，[28] 授权搜查流动电话或其他电子器材的数码内容。[29] 对于没有手令的搜查，该搜查的范围和目的须因有关逮捕而附带引起。警务人员须有合理依据支持即时进行没有手令的搜查对以下目的而言属必要：(i)调查相关人士怀疑涉及的罪行，包括获取及保存与罪行有关的资料或证据；或(ii)保护个人安全。[30] 此外，有关人员应按上述准则，将对数码内容的仔细审查范围限于相关项目，并对该项没有手令的搜查的目的和范围，作出充分书面记录。[31]

2.37　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"*纳入为取览罪的元素。个别案件中是否有*"合法权限"*这问题关乎客观事实。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*案中订立的规定，便属有*"合法权限"*而取览程式或数据。若没有搜查令或合理依据，则有关情况会类似于执法机关以胁迫或欺骗等手段非法取证。在该等情况下，有关证据的可接纳性可能受到质疑，执法机关的负责人员亦可能面对刑事调查，若有充分证据并符合公众利益，更可能须面对刑事检控。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。

27　[2020] 2 HKLRD 529, CACV 270/2017（判决日期：2020 年 4 月 2 日）。

28　《警队条例》（第 232 章）第 50(7)条订明，裁判官如觉得有合理因由怀疑在任何地方内，有任何物品或实产是相当可能对调查任何人所犯或合理地怀疑任何人已经或即将或意图犯的罪行有价值的（不论就其本身或连同任何其他东西），则该裁判官可向任何警务人员发出手令，赋权给他搜查及接管该等物品或实产。

29　见上文注脚 27，第 34、163、166 及 218(a)段。

30　见上文注脚 27，第 187 及 218(b)段。

31　见上文注脚 27，第 188、199、218(c)及(d)段。

适宜订立加重罪行

2.38 对于有回应者指出加重罪行"*太难证明*"，[32] 我们相信本港法庭会从个别案件的情况作出推论，并能据此就被告人的思想状态作出裁定，因为这正是它们日常必须作出的判断。此外，根据《检控守则》，"*控方必须在法律上有充分证据支持检控*"，[33] 而验证标准是"*根据这些证据，是否有合理机会达致定罪*"。[34] 故此，控方相当可能只会在下述情况下就加重罪行提出检控：有人实际上干犯有关较严重的罪行；或案件中有充分或具说服力的环境证据，可据此推论被告人意图干犯其他罪行或（如未有人干犯加重罪行）意图利便干犯其他罪行。控方亦可能就初步罪行（即企图干犯加重罪行）提出检控。基于这些原因，加重罪行虽然在观感上看似难以证明，但事实上或许并非如此。

2.39 然而，倘若控方如上述回应者所指，在确立加重罪行时遇到实际困难，我们并不排除控方可能会改控建议 1(a)所建议订立的简易程序罪行。这亦说明了为何需要保留纯粹在未获授权下取览这项简易程序罪行。

2.40 须注意的另一重点是，无论如何，控方时刻有责任就众多可循简易程序审讯的可公诉罪行（不论它们是由成文法规订立还是根据普通法订立）选定审讯法庭。控方须考虑的主要因素包括：指称罪行的严重程度、整体案情，以及定罪后可能判处的刑罚。[35] 因此，尽管有关加重罪行是可公诉罪行，但如根据案情有此需要，控方仍可选择在裁判法院循简易程序审讯该罪行。

罪行互相重迭

2.41 毫无疑问，每项作为均可能被多于一项法定条文或法定罪行所涵盖。由于非法作为可在不同情况下发生，我们认为法律中有重迭之处属可接受。在建议的依赖电脑网络的罪行仍未订立时，就先揣测控方日后会如何处理电脑网络罪行案件，似乎并无实质意义。如议论针对电脑网络罪行的特定法例与第 161 条相比的优劣利弊，而没有参考任何刑事案件的事实背景，上述揣测就显得更无意义。

---

32 上文第 2.13 段。

33 香港特别行政区律政司，《检控守则》（2013 年），第 5.4 段。

34 同上，第 5.5 段。

35 同上，第 8.4 段。其他因素包括：可能有争议的事宜、须予裁定的争议事宜是否涉及社会的标准及／或价值观、法律程序对公众的重要性，以及任何加重或减轻刑罚的因素。

应否界定“取用或取览”、“在获授权下／在未获授权下”取用或取览、“电脑网络”及“数据”

2.42 正如咨询文件所解释，[36] 小组委员会曾考虑应否参考俄罗斯联邦（Russian Federation）拟备的《联合国合作打击网络犯罪公约》草案（Draft United Nations Convention on Cooperation in Combating Cybercrime，**《俄罗斯公约》**），为“电脑”赋予法定定义。该公约把“资讯及通讯科技器材”界定为*“任何用于或设计用于自动处理和储存电子资料的硬件组件的集合体（组合体）”*。[37] 小组委员会留意到原讼法庭对*律政司司长 诉 王嘉业*[38] 的判决的以下摘录，并认为法庭有关观点也适用于建议的依赖电脑网络的罪行：

> “69. ……立法会对《刑事罪行条例》第 161 条之‘电脑’一词不作出定义，是因为科技发展迅速，‘电脑’的定义广阔和演变，不能尽录。
>
> ……
>
> 73. ……诠释涉及科学及技术的条文时，应视之为‘一直发言’，按照法例的语言，给与广义的诠释，应用于立法后演变的情况，除非超越了法例语言的自然释义，或后果是荒谬或明显不公义的。”[39]

2.43 我们赞同小组委员会的看法。随着物联网兴起，未来可能会有越来越多器材成为罪犯的攻击目标，即使是“资讯及通讯科技器材”这一概括定义，也可能落后于资讯科技势如破竹的发展与演进。我们理解到若然欠缺定义，可能会令人无法立即清楚分辨某种采用较新颖技术的器材是否构成“电脑”。不过我们亦紧记，不管法定定义的表达是如何清晰（例如《俄罗斯公约》对“资讯及通讯科技器材”或《联合国公约》对“信息通信技术系统”所下的定义），[40] 法定定义在实际应用上也不无困难，这是因为被告人或会极力提出各种技术性论点，辩称有关“器材”在法律上并不构成立法机关原意中的“电脑”，随着加入有关法定定义后时间日久，尤其会出现这种情况。我们固然可以信任

---

36 第 2.93 至 2.95 段。

37 第四条第(o)款。

38 [2013] 4 HKLRD 588, HCMA 77/2013（判决日期：2013 年 4 月 29 日）。

39 同上，第 601 页（高等法院原讼法庭法官冯骅）。

40 《联合国公约》则力求界定甚么会视为“信息通信技术系统”。根据该公约第二条第（一）项，“信息通信技术系统”指*“任何设备或任何一组相互连接或相关的设备，其中一个或多个设备按照某一程序收集、存储并自动处理电子数据”*。有关《联合国公约》的详情，见第 1.6 至 1.8 段。

法庭会在法例文本容许的情况下，因应科技进步而灵活地解释在针对电脑网络罪行的特定法例所加入的任何定义，以尽量体现真正的立法原意，但这样也无法排除上述困难。

2.44 正如某商业团体在提交的意见书中正确地指出，“取用或取览”及“截取”等电脑相关作为均可随着科技发展而不断演变。取览电脑程式或数据的崭新方法可能不时涌现。故此，较为适当的做法是不硬性界定何谓“取用或取览”，而是赋予“取用或取览”其通常涵义，以使建议的罪行达到应对损害电脑系统安全的威胁及攻击这目的。

2.45 我们亦倾向认为，是否获得授权的问题与事实密切相关，应由法庭按照个别案件的情况裁定，而且对“在未获授权下”作出具体定义，可能会使某些获普遍接受或惯常的互联网做法变成违法行为，而由于有关网上用户已默示给予取览程式或数据的授权，这些做法是我们的建议所拟容许的（见上文第 2.25 及 2.26 段）。

2.46 基于上述理由，我们仍然认为较可取的做法是不界定“取用或取览”、“在获授权下／在未获授权下取用或取览”、“电脑”及“电脑系统”等词语。无论如何，若我们的建议得到政府落实，法律草拟专员可在立法阶段进一步探讨这议题。

有关建议 1 的结论

2.47 基于上述各项理由，我们的结论是建议 1 可予保留，并可进一步厘清如下：

最终建议 1

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。

(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。

对小组委员会建议 2 的回应

2.48 我们接着探讨咨询文件建议 2 之中的咨询问题，这项建议由以下几部分组成：

> "小组委员会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：
>
> (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，例如有关评审的准则是甚么？经审定人士应否有持续进修的规定？香港应否设立（譬如根据新订的电脑网络罪行法例设立或以行政方式设立）一个评审团体，并由该团体备存一份网络安全专业人员名单，而比方说如经审定人士未能符合持续进修规定，便可将该人从该名单内除名或不准该人将其审定资格续期？评审团体以外的哪些人（如有的话）也应获准查阅该名单？

(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）？"

支持为网络安全业界提供特定免责辩护的回应者的意见

2.49 绝大多数回应者均支持建议2，当中包括法律专业团体、大专院校、资讯科技相关团体、商业团体及政府机构。他们提出的主要理由如下：

(a) 许多回应者均表示，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所进行的工作，的确有其价值。他们认为，广泛类别的人士均可受惠于白帽黑客的工作。举例来说，网络安全专家的工作可揭示电子服务或产品的潜在保安漏洞或安全缺陷，促进网上消费体验的安全和公平性。

(b) 白帽黑客入侵若进行得当并受到妥善监管，会令香港受惠，不但可加强本港的网络安全，亦推动本港网络安全业界的强劲和稳健发展，从而建立香港作为网络安全专业服务枢纽的信誉。

(c) 为在未获授权下取览订定免责辩护或豁免，对推动善意的安全研究和促进把新科技引入香港，均至关重要。

反对为网络安全业界提供特定免责辩护的回应者的意见

2.50 少数回应者（包括三个资讯科技相关团体及一名个别人士）则反对为网络安全业内人士提供特定免责辩护。某资讯科技相关机构指出，若专为这些经认可人士订定免责辩护，实际上便会带来一个*"享有特权的界别"*，当中的行事者不论有何意图，均可获豁免刑事法律责任，因此特定的免责辩护或豁免应适用于所有人，而非只适用于经由认可专业团体或认可团体认可的人士。

2.51 另一方面，另一资讯科技界机构则表示，各机构在委托他人提供网络安全服务（例如网络扫描）时，通常会订立书面合约，当中界定网络安全服务提供者的取览范围。故此，可能无须为在未获授权下取览订定特定的免责辩护或豁免。

应否推行认可制度？

2.52 明显大多数回应者均同意应设立认可制度，当中包括政府部门、资讯科技相关团体及商业机构。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或豁免的意见相符。

支持设立认可制度的回应者的意见

2.53 赞成设立认可制度的回应者（包括消费者委员会）指出，认可制度的好处在于能为网络安全专业人员提供认证机制，若届时需确定法定免责辩护或豁免是否适用，便能以此轻易识别出这些专业人员。消费者委员会在其回应中有以下提议：

> "……应考虑设立一套设有发牌或认可准则（例如'适当人选'规定及持续进修规定）的法定制度。鉴于认可情况如小组委员会所言不断演变，认可团体或发牌机构可因应这些变化，发布各种指引、通告及实务守则。就认可制度的行政和运作事宜，应全面征询网络安全业界的意见。"

2.54 与此同时，多个资讯科技相关团体也同意，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。

2.55 回应者提出了多种认可网络安全从业员的方式。除上述消费者委员会提议的法定制度外，香港女律师协会有限公司（"**女律师协会**"）认为，可用行政方式在认可团体的规章中列载认可准则，并认为这样会较易修订认可准则，以紧贴任何技术要求的变化。另外，

少数资讯科技相关团体则认为可设立网络安全从业员注册制度，让他们在进行渗透测试前自行注册。

2.56 香港律师会的以下意见也值得一提：香港应否设有认可制度，应属政府的政策事项。该专业团体指出，需要敲定认可制度的某些运作细节：

> "政府应全面征询各持份者和业界的意见……宜考虑例如以下的各种（并非尽列无遗的）问题：若设立一个认可团体，该团体发出的证书可否作为这项控罪的免责辩护？如可以的话，其免责程度有多大？该免责辩护又如何施行？这种基于认证的免责辩护，是否与被告人有权提出的其他免责辩护分开看待？另一方面，即使有认可团体发出的证书，执法机关是否仍可不受其限，调查指称在未获授权下作出的取览？"

2.57 在认可制度的细节方面，我们收到回应者的有用意见。某资讯科技相关团体认为，将予设立的负责监督认可或注册事宜的机构，应有权在任何个人违反或未能达至有关专业的道德及专业标准的情况下，撤销该人的注册，但必须实行正当程序。

2.58 此外，一名有多年网络安全从业经验的个别人士表示，可备存一份网络安全专业人员资料名单，以记录有关人员的资历，而该名单应区分不同的网络安全专业工种。然而，这名回应者有以下告诫：

> "其中部分特殊资讯敏感工种，例如：电子取证调查人员（Forensics and Investigation），密码（解码／密码分析）学家（Cryptanalysis Expert），漏洞研究人员（Zero Day Vulnerability Researcher）等等……的名册查阅应当受到限制以保护这些人员的人身安全"。

2.59 最后，某商业团体表示，在香港推行的任何认可制度都不应过于复杂，以免窒碍资讯科技行业的发展。

反对设立认可制度的回应者的意见

2.60 尽管大多数对建议 2 作出回应的资讯科技相关团体均同意推行认可制度，其中两个团体反对这项建议，理由如下：

(a) 无论是科技或是网络安全专业，两者都瞬息万变。服务提供者、软件公司及网络安全团体均不时提供经认可的网络

安全课程。认可制度无法迅速适应变化，以法规为基础的尤其如此。

(b) 若设立认可制度，很可能会对招聘合资格人才投身香港的资讯科技行业构成挑战。网络安全专业人员匮乏，或会无意中限制本港网民所得到的保障。

(c) 开放源码软件日渐增多，非保安专业人员用户都能加以修改或改良，造福社群。若订有认可方面的规定，可能会限制电脑爱好者在识别潜在网络安全威胁方面的参与度。

我们的分析及回应

2.61 由于建议 2 的咨询问题关乎在未获授权下为网络安全目的而取览这项免责辩护或豁免，因此我们会先讨论取览罪的网络安全免责辩护，然后再探讨其他特定免责辩护。

2.62 在咨询文件中，[41] 小组委员会已参考以下的学术文章说明何谓"网络安全"，在此复述有其用处：

> "网络安全又称为资讯科技安全，指为了保护电脑、网络及程式免受网络攻击或电脑网络罪行行为（例如病毒、恶意软件或勒索软件）损害而采取的各种步骤。"[42]

为经认可的网络安全从业员提供特定的免责辩护

2.63 在就建议 2 提交意见书的资讯科技团体之中，大多数均乐于接受设立认可制度的建议，理由是此举能提升资讯科技专业。我们相信，为资讯科技行业内某界定类别的人士订定特定免责辩护，会是合理而务实的做法。虽然部分回应者可能认为，特定免责辩护会将网络安全专业人员提升为享有特权的界别，但我们希望指出，该免责辩护实际上使网络安全专业人员和所有其他人均受制于一套新的规管制度，在该制度下，任何人必须先经认可，才能以可能涉及未获授权取览的方式从事网络安全服务。从这角度来看，该免责辩护事实上是对任何有意在未获授权下（包括在无法证明有默示授权的情况下）作出取览的人（包括资讯科技专业人员）施加责任。

---

41 第 2.111 段。

42 Marion and Twede, *Cybercrime: An Encyclopedia of Digital Crime* (ABC-CLIO, 2020)，第 92 页。

2.64 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。在顾及整体情况后，被告人的目的和行为必须是合理的，亦即施加客观标准。在下述各段，我们会阐释所作建议的各项元素背后的理念。

(i) 经认可或持牌网络安全从业员

2.65 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才可为网络安全目的而作出取览。这意味着援引上述免责辩护的人士，应同时具备一定水平的专业技能和正直品格。换言之，不是每名自称网络安全专业人员或从业员的人士，都可提出为网络安全目的而取览这项特定免责辩护。

2.66 由于大多数回应者均支持推行认可制度，因此对参与网络安全工作的资讯科技业内人士实行制度措施，既可更好地保障所有持份者（即网络安全专业、有意雇用网络安全专业服务的人，以至社会大众），亦能使法律更为明确。故此，我们认为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。透过设立认可制度，加上订定为网络安全目的而取览这项特定免责辩护，不但能提升资讯科技行业的专业性，亦会使网络安全专业人员免于承担取览罪的法律责任。

由政府决定认可制度的细节

2.67 尽管如此，我们也意识到本港的网络安全人才供应短缺，若推行认可制度，可能会造成招聘资讯科技界人才方面的困难，加剧业界竞争，由此推高网络安全服务的费用。

2.68 我们同意回应者所言，认可制度可透过不同方式落实。举例来说，可指定由某法定主管当局对网络安全专业人员进行认可。就此而言，较严格的认可制度很可能会影响网络安全专业人员的供应和收费。相反，或许也可采用较宽松的模式，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，即可获得认可。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会有所不同。

2.69 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、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。为方便政府考虑认可制度，我们已在本报告书对认可建议及它可能造成的影响提出看法。

2.70 我们预计，政府如倾向设立一个网络安全认可团体，但又无意就此成立一个专责机构的话，或可考虑订定一个架构，当中指定由一间或多间现有机构（属自我规管的专业团体及专业协会）履行与香港律师会、香港大律师公会及香港国际公证人协会相类似的职能。香港律师会、香港大律师公会及香港国际公证人协会受托履行法定责任，分别负责监督律师（及外地律师）、大律师及公证人的行为操守，以维持他们的水平。法律执业者若表现未达水平或有违反道德操守的行为，会面临纪律处分；同样地，网络安全专业人员若违反认可团体所公布的任何行为守则，也会面临纪律处分。

(ii) 真正的网络安全目的

2.71 我们认为被告人的认可资格或身分，不应是裁定为网络安全目的而取览这项特定免责辩护是否适用的决定性因素。经认可人士是为真正的网络安全目的而取览程式或数据，才是重点所在。女律师协会及另一商业团体所提出的意见，亦强调这点：

> "尽管我们同意，认可专业团体或认可团体给予的认可，为取览程式／数据的人有充分理由作出有关取览提供表面证据，但仍需要审视实际的作为，认可本身并不是充分的免责辩护。为成功确立有关豁免或免责辩护而需要证明的关键事项，是未获授权的取览是为网络安全目的而作出，而不是作出该项取览的人是经认可人士。"

2.72 "真正的网络安全目的"这规定，意味着经认可的网络安全从业员如为真正的网络安全目的而取览电脑程式或数据，便能以为网络安全目的而取览这项特定免责辩护作诉；但从业员如取览自己女儿电话内的数据，则不能提出相同的免责辩护，反而只能援引"为保障儿童利益而取览"作为免责辩护，这会在下文第 2.75 至 2.89 段讨论。

(iii) 在顾及整体情况后，被告人的行为必须是合理的

2.73 为进一步收紧为网络安全目的而取览这项免责辩护的范围，我们建议在该免责辩护加入"合理性"要求。我们相信，若以合理性作为指导原则，为网络安全目的而取览这项特定免责辩护所附带的条件便能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。

"合理性"问题与事实极为密切相关。举例来说，如电脑拥有人或数据拥有人不授权经认可的网络安全从业员（可能是该拥有人的前雇员或已知的竞争对手）取览该拥有人的程式或数据，但该从业员仍然作出取览，则必须就该从业员所作的取览提出令人信服的解释或理由，才能令法庭信纳该项取览符合"合理性"要求，从而确立建议的网络安全免责辩护。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。

2.74 这项"合理性"要求也旨在使为网络安全目的而取览这项特定免责辩护，与非法干扰电脑数据及非法干扰电脑系统这两项建议罪行的免责辩护看齐（本报告书第 4 及 5 章会讨论后述两项罪行）。

取览罪的其他特定的免责辩护

为保障儿童利益而取览

2.75 在咨询文件发表后，小组委员会成员出席多次传媒访问，期间有人问及家长如查看子女电话内的内容，会否干犯建议的罪行。若没有订立关于家长监护的特定免责辩护，被控以建议罪行的家长便只能援引合理辩解这项一般免责辩护。

2.76 在收到的意见书中，本地慈善组织"母亲的抉择"强调儿童在上网时特别容易遇到的危害。这名回应者提到香港大学进行的一项研究，引述年青人遭受多种网络虐待的情况：香港有四成青少年在非情愿的情况下收到网上性裸露内容，每 10 名青少年就有 1 人曾受到网络性骚扰，每 5 名青少年就有 1 人遭受网络欺凌。

2.77 这名回应者因此认为，小组委员会应考虑提出立法建议，以*"防止儿童从互联网、数码及串流媒体取览含有不当、侮辱性或有害内容的资讯"*。该回应者再作出以下简短的评析，认同家长要监督儿童使用互联网的情况：

> "我们了解到，对于网络安全及保安这课题，为儿童提供支援的网络（包括家长、个别人士及专业人员）只具备有限的知识和技能。我们建议，与处于风险的易受伤害儿童有接触的所有持份者，均应作好装备并获赋权力，以预防、应对和举报网上风险。预防、应对和举报网上的保护儿童问题，对保障社会上易受伤害人士的安全和福祉至关重要"。

2.78 同样地，法律援助署也提议应订有一些豁免，让家长能为了保障子女利益（例如在发生网络欺凌的情况下）而取用他们的电脑。

2.79 根据在 1997 年后继续适用于香港的《联合国儿童权利公约》（**《儿童权利公约》**）第十六条，儿童享有一般私隐权，[43] 但我们相信，由于儿童容易因为电脑网络空间上的各种危险而受到伤害，家长确实有充分理由采取行动来保护子女的福祉。在人们频繁进行网上活动和接通互联网的现今世界，对育有子女的家长而言，切实可行的行动可能包括取用子女的流动电话或电脑，以找出（比如说）哪些人透过社交平台或通讯应用程式与他们接触。

2.80 在这方面值得注意的是，以推广保障及尊重个人资料私隐为使命的个人资料私隐专员公署（"**私隐专员公署**"），也发布了为家长及教师而设的多项建议，让他们能教导其照顾的儿童在网上保护自己，[44] 其中一项建议就是善用家长监护功能。私隐专员公署指出，有些网上平台或系统提供家长监护功能，让家长监察或配置适当设定，以免儿童（尤其是年幼儿童）接触不良内容或人士。此外，私隐专员公署亦认为，家长及教师*"应警戒儿童，网上通讯有可能会为人身安全带来危机及造成财物损失"*。[45]

我们的分析

2.81 总结而言，有一点似乎很清楚：家长监护是香港社会所接受的惯常做法，家长在互联网使用方面的指导角色亦得到大众认同。我们认为，为了达到保护儿童的目的，新订的电脑网络罪行法例把"为保障某年龄以下儿童的利益而取览"明文豁除于取览罪之外，会是明智之举。我们理解到，这项特定免责辩护可能会削弱儿童的私隐权，但鉴于年幼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儿童利益的原则。

---

43 见香港特别行政区政府政制及内地事务局于 2009 年 3 月发布的小册子，第 3 页。《儿童权利公约》第十六条第一款有以下规定：*"儿童的隐私……或通信不受任意或非法干涉……"*。

44 个人资料私隐专员公署，《儿童网上私隐——给家长及老师的建议》（2015 年），登载于 https://www.pcpd.org.hk/tc_chi/resources_centre/publications/files/leaflet_childrenonlineprivacy_c.pdf（于 2025 年 11 月 1 日浏览）。

45 同上。

儿童的年龄

2.82 根据本港法例，16 岁以下的人，在香港法律上一般不能对性接触给予同意。[46] 由于《儿童权利公约》第一条把"儿童"界定为 18 岁以下的任何人，因此我们曾考虑就电脑网络罪行而言，是否需要把这项特定免责辩护的儿童年龄上限定为 18 岁。我们认为，相较于对个人身体的自主权，私隐权属较次要的权利。由于本港法例确定了 16 岁以下的人对自己的身体并没有自主权（即 16 岁以下的人不能对性接触给予有效的同意），因此就电脑网络罪行而言，似乎没有充分理由为取览罪的这项特定免责辩护订定不同的年龄上限。总结而言，我们认为把年龄上限定为 16 岁既能够提供足够保障，亦与香港的其他现有法例大体上相符。

对程式或数据的取览应属合理

2.83 我们认为，如果把对程式或数据的取览，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，便可避免这项特定的免责辩护被滥用，这项合理性要求无异于为网络安全目的而取览的免责辩护。在取览的目的和程度均受限制的情况下，法庭会有更大空间审视证据，以裁定某项取览是否超乎适度。法庭最终会在考虑个别案件的所有相关因素后评估被告人的行为，以确保被告人没有逾越对儿童行使管教方面所应有的行为界限。

有关免责辩护的范围

2.84 我们已详细考虑这项建议的免责辩护的两个制定方案。方案一的涵盖范围较广，适用于为保障儿童利益而取览程式或数据；方案二的涵盖范围则较窄，只限于为防止儿童受到身体、情绪或心理伤害而取览程式或数据。

(i) 为保障儿童利益而取览程式或数据

2.85 支持订定这种较广阔免责辩护的主要论据，是家长可能在多种情况下有意取览儿童的程式或数据（例如为了确定儿童是否曾取览网上的色情或暴力资讯），较广阔的免责辩护能够将这些情况涵盖

---

[46] 例如，根据《刑事罪行条例》第 122(2)条，年龄在 16 岁以下的人，在法律上是不能给予同意，使某项作为不构成猥亵侵犯的。就性交而言，根据《刑事罪行条例》第 124(1)条，与年龄在 16 岁以下的女童非法性交，即属犯罪。此外，《刑事罪行条例》第 146(1)条亦订明，与或向年龄在 16 岁以下的儿童作出严重猥亵作为，或煽惑年龄在 16 岁以下的儿童与另一人或向另一人作出此种作为，即属犯罪。根据第 146(2)条，即使被控人证明该儿童同意作出该项严重猥亵作为，亦不得以此作为免责辩护。

在内。若订定具限制性的免责辩护，则可能令家长感到被剥夺父母权利，因为电脑网络罪行法例会禁止他们做某些在教养子女的过程中原本可做的事情。由于订有取览须属合理的要求，赞成订定这种较广阔免责辩护的人相信，法庭不但会考虑到家长主观相信有必要为保障儿童利益而作出取览，也会客观评估家长的行为，以裁定有关取览是否有理可据。这样能限制对儿童的程式或数据的取览范围，从而防止家长过度侵犯儿童的私隐权。

(ii) 为防止儿童受到身体、情绪或心理伤害而取览程式或数据

2.86 另一方面，我们也理解到，鉴于其他实际考虑因素，范围较窄的免责辩护可能较为合宜。广阔的免责辩护或会对亲子关系造成不良影响，有损家庭和睦。就父母已经离婚的情况而言，相对狭隘的免责辩护也许能防止其中一方操控子女，使他们投诉寻求对自己行使父母责任或管教的另一方。此外，私隐权亦正获得前所未有的重视。为了对儿童的私隐给予更多尊重，作为折衷做法，便不得不削弱或约束其他对立权利（例如透过取览子女的电脑程式或数据来行使父母管教的权利）。

2.87 最终，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，即为保障儿童利益而取览程式或数据。由于政府若决定落实小组委员会这项建议，可进一步征询公众意见，加上新订的电脑网络罪行法例的内容会由立法机关作最终决定，因此我们认为，这议题最好由政府在考虑社会意见后再作定夺。

有关免责辩护不应取决于取览者与取览对象的关系

2.88 为了体现这项免责辩护背后保障儿童利益的理念，我们进一步建议这项免责辩护是否成立，应视乎寻求取览儿童的程式或数据的人的主观目的而定。事与愿违的是，实际上儿童并不一定能在安全稳妥的环境中得到适切保护。家长或监护人忽略履行或没有履行自己保护或照顾儿童福祉的责任，并不鲜见。我们亦想象到，即使某儿童得到家长或监护人的适切照顾，现实中仍可能出现多种情况，需要陌生人介入来保障该儿童的利益。举例来说，若有人发现某儿童境况堪忧（例如儿童迷路），容许该人取览有关儿童的电话或电子器材内的程式或数据而无须负上刑事法律责任，似乎是合理的做法。

2.89 上述的考虑因素正好证明，支持在未获授权下取览儿童的程式或数据的充分理据，在于某人为达至保障儿童利益此真实目的而在未获授权下取览有关程式或数据，而非该人与该儿童的关系。如这项免责辩护并不取决于儿童与取览者的关系，便可为儿童利益提供最大保障。我们认为，"为保障而合理所需"这项凌驾性规定能够避免滥用。

把有关免责辩护延伸至保护易受伤害人士

2.90 由于精神上无能力的成年人可能容易遭受剥削，因此我们认为，上述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。至于应如何界定易受伤害人士，我们认为宜参考《精神健康条例》（第 136 章）（**《精神健康条例》**）对*"精神紊乱的人"*[47] 及*"弱智人士"*[48] 所作的清晰定义。根据《精神健康条例》第 2 条：

(a) *"精神紊乱"*界定为*"精神病"*，*"属智力及社交能力的显著减损的心智发育停顿或不完全的状态，而该状态是与有关的人的异常侵略性或极不负责任的行为有关连的"*，*"精神病理障碍"*，[49] 或*"不属弱智的任何其他精神失常或精神上无能力"*，而*"精神紊乱"*当用作形容词时亦须据此解释；及

(b) *"弱智"*指*"低于平均的一般智能并带有适应行为上的缺陷"*，而*"弱智"*当用作形容词时亦须据此解释。第 2 条进一步把*"低于平均的一般智能"*界定为*"按照魏克斯勒儿童智力测量表或按照任何标准化智力测验中的同等智力测量表是 70 或低于 70 的智商"*。

2.91 如有需要，法庭在个别案件中裁定是否已在所需的举证标准下证明前段所引定义的构成元素时，会借助从注册医生或精神科医生等所获得的专家证据。故此我们建议，上述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障易受伤害人士（即《精神健康条例》所界定的精神紊乱的人或弱智人士）的利益。[50] 这项建议也进一步巩固我们上文得出的结论，即有关免责辩护不应取决于取览者与取览

---

47 根据《精神健康条例》第 2 条，*"精神紊乱的人"*指*"任何患有精神紊乱的人"*。

48 根据《精神健康条例》第 2 条，*"弱智人士"*指*"弱智的人或看来属弱智的人"*。

49 *"精神病理障碍"*界定为*"长期的性格失常或性格上无能力（不论是否兼有显著的智力减损），导致有关的人有异常侵略性或极不负责任的行为"*。

50 这与法改会在 2019 年 12 月发表的《检讨实质的性罪行》报告书的最终建议 35 相符。该项建议提出，新订的涉及精神缺损人士的罪行，应适用于精神紊乱的人或弱智人士（如《精神健康条例》所界定者），而其精神紊乱或弱智（视属何情况而定）的性质或程度令他或她没有能力保护自己免受性剥削。

对象的关系。一如保护儿童的情况，“为保障而合理所需”这项规定亦同样适用。

为真正的研究目的而取览

2.92 对咨询文件作出回应的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。

2.93 我们同意，除了为网络安全目的而取览这项免责辩护外，“为研究目的而取览程式或数据”（例如研究人员或网络安全从业员为了确定在香港未受保护的电脑数目而作出取览）也应订为免责辩护或豁免。由于这些研究或许能得出有用的分析或资讯，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，《防止儿童色情物品条例》（第 579 章）第 4(2)(a)及(3)(a)条就各项关于儿童色情物品的罪行所订的免责辩护可用作蓝本，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”。

2.94 为免这项研究免责辩护被滥用，我们建议，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教育、科学或研究目的而所需者。这项“合理性”要求会作为客观准则，用以裁定被告人的取览是否适度或合理。

《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的免责辩护

2.95 现行《刑事罪行条例》第 64(2)条所订的两项免责辩护，均适用于咨询文件建议 6 及 7 所述的非法干扰电脑数据罪及非法干扰电脑系统罪（“**干扰罪**”），这会在本报告书第 4 及 5 章讨论。由于第 64(2)条目前适用于刑事损坏罪，而上述两项干扰罪又建议以该罪行为蓝本，因此宜先简述第 64(2)条所订的两项免责辩护。

2.96 第 64(2)条由两部分组成。任何被告人被控以刑事损坏罪，在下述情况下均须被视为有合法辩解：

(a) 如指称构成该罪行的作为作出时，被告人相信，他相信有权同意有关财产的摧毁或损坏的人已予同意，或相信该人如知道有关财产的摧毁或损坏及有关情形亦会予以同意（“**同意免责辩护**”）；或

(b) 如被告人摧毁或损坏有关财产或威胁会如此做，或（在被控以第 62 条所订罪行时）意图使用或导致或准许使用某些物品以摧毁或损坏有关财产，而他如此做是为了保护财产（不论属于其本人或另一人），且于指称构成该罪行的作为作出时，被告人相信——

(i) 该财产需即时保护；及

(ii) 在顾及一切有关情况后，所采用或打算采用的保护方法是或会是合理的（"**保护财产免责辩护**"）。

2.97 由于干扰电脑数据及／或干扰电脑系统通常只会在取览程式或数据后发生，因此我们认为，《刑事罪行条例》所订的同意免责辩护及保护财产免责辩护，应同样适用于取览罪。

第 64(2)(a)条所订的同意免责辩护

2.98 为了阐释这项免责辩护，我们现假设以下情境：被告人在登入另一人的电脑后更改了当中的数据（例如病毒），并相信该另一人会对有关更改予以同意。若这名被告人因可提出同意免责辩护而无须负上非法干扰电脑数据的法律责任，但却被裁定犯取览罪的话，这样的推论显然有悖逻辑。故此我们认为，取览罪及干扰罪的免责辩护应采用统一的处理方式。有关免责辩护条文的详细草拟工作可在立法阶段处理。

第 64(2)(b)条所订的保护财产免责辩护

2.99 同样地，由于可就干扰罪提出保护财产免责辩护，故我们认为被告人也应可就取览罪以相同的免责辩护理由作诉。

加入合理性要求，订明被告人须合理地相信有关事情

2.100 根据现行第 64(2)(a)条，被告人相信存有同意是完全主观的。《刑事罪行条例》第 64(3)条订明，*"只要是诚实地相信有关事情，则是否有充分理由支持，不具关键性"*。故此，只要法庭接纳被告人是真确相信有关事情，有关免责辩护便会适用，被告人所相信的事情无须有合理依据支持。

2.101 将第 64(2)条所订的免责辩护改列于新法例时，我们建议提高有关免责辩护的门槛，在同意免责辩护及保护财产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。

2.102 换言之，我们建议在针对电脑网络罪行的特定法例加入取览罪，而《刑事罪行条例》第64(3)条不适用于该罪行。上述调整会使同意免责辩护及保护财产免责辩护，与我们在上文就取览罪所建议的其他特定免责辩护看齐，即所有免责辩护均采用"合理性"要求，以确保一致。我们相信这种处理方法可避免各项免责辩护被滥用，并体现我们的指导原则：一方面平衡兼顾网民的权利和资讯科技业内人士的权益，另一方面亦保障公众在使用电脑系统时免受骚扰或攻击的权益和权利。

非保安专业人员取览程式或数据

2.103 咨询文件的建议2(b)及8(b)分别邀请公众对以下问题提出意见：非保安专业人员取览程式或数据及干扰电脑系统，应否有任何免责辩护或合法辩解。有关非保安专业人员的例子包括：由机械人进行网页抓取（web scraping）或由互联网资讯收集工具（例如搜寻器）启动网络爬虫（web crawlers），从而在未获授权下从伺服器收集数据；以及为找出保安漏洞或确保应用程式界面（Application Programming Interface）安全和完整而扫描服务供应商的系统。[51]

2.104 正如我们将在本报告书第5章解释，[52] 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，原因是人们在使用电脑网络空间时普遍接受的做法，如它们是以电脑用户通常接受的规模进行的，均会根据默示授权的原则而获准。同样道理，我们认为无须就取览罪为非保安专业人员建议订定特定的免责辩护。

有关建议2的结论

2.105 总结上述讨论，我们建议就取览罪订定各免责辩护如下：

---

51 见咨询文件建议8(b)。

52 第5.29至5.33段。

最终建议 2

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：

(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。

对小组委员会建议 3 的回应

简易程序案件的时效期

2.106 建议 3 处理适用于循简易程序就咨询文件所建议的五类依赖电脑网络罪行提出检控的时效期：

> "小组委员会建议，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。"

2.107 根据《裁判官条例》（第 227 章）（**《裁判官条例》**）第 26 条，简易程序罪行的时效期一般为所涉事项发生后起计的六个月，但如有关法例另有规定则除外。

2.108　大多数回应者均支持建议3。某商会表示，电脑网络罪行案件往往相当复杂，控方需耗用较多资源和时间来决定应否继续检控某宗案件。不过该商会也告诫，两年的时效期应视为用作应付较复杂案件的安全网，而不应视为通常所需的时间。然而，数名回应者不赞成把时效期从六个月"延迟"至两年，理由是六个月的期限可鼓励执法机关加快处理电脑网络罪行案件，因而能更好地保障公众利益。

2.109　正如小组委员会在咨询文件解释，[53]《裁判官条例》所订的预设时效期或不足以调查电脑网络罪行案件。受害人可能在案件发生后两至三个月才向警方报案，而更甚者，六个月的时效期在事件被揭发时已届满。警方从互联网服务提供者取得日志纪录，可能再需要两至三个月。分析这些日志纪录可能又另需两至三个月，还须顾及达至检控决定所需的额外时间。

2.110　我们希望澄清一点，建议3仅旨在把时效期延长至两年，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。因此，我们建议保留建议3。

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。

53　第2.122段。

第 3 章　非法截取电脑数据

引言

3.1　本章讨论关于咨询文件建议 4 及 5 的回应。建议 4 建议订立第二类依赖电脑网络的罪行，即非法截取电脑数据：

> "小组委员会建议：
>
> (a) 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）〔（**《示范法》**）〕第 8 条为蓝本，包括犯罪意念（即"蓄意"截取）。"

3.2　正如咨询文件所解释，[1] 在所有经研究司法管辖区的相关法规当中，就作为香港的参考对象而言，按下文所述修改的《示范法》第 8 条（*"非法截取数据等"*）与小组委员会的构思最为相近：

> "任何人如为不诚实或犯罪目的而在无合法辩解或权限的情况下，蓄意以技术截取：
>
> (a) 任何往来某电脑系统或在某电脑系统内的传送；或

[1] 第 3.111 及 3.112 段。

(b) 来自某电脑系统并载有电脑数据的电磁发射；[2]

即属犯罪，一经定罪，可处为期不超过〔刑期〕的监禁或不超过〔金额〕的罚款，或两者兼处。”

3.3 概括而言，非法截取电脑数据罪旨在：[3]

(a) 把类似传统窃听和记录电话对话，而并非依照法律权限（例如在执法时）进行的电脑数据截取定为不合法；及

(b) 从而保障人们的数据通讯私隐权。

3.4 在现今世界，即使无需特别设备或先进资讯科技知识，截取电脑数据也可以随处发生。[4] 例如，某人恶意设置虚假 Wi-Fi 热点，以获取受害人已连接的器材所传送的数据，可谓易如反掌。更精密的截取数据方式，则可能涉及设置“后门程式”[5] 或安装间谍软件。

香港的现行法律

3.5 由于部分回应者的意见书就现有法律的不足之处提出意见，因此我们宜先扼要重述现行法定机制的主要特点，然后再处理这些回应。

《截取通讯及监察条例》（第 589 章）

3.6 正如小组委员会在咨询文件解释，[6]《截取通讯及监察条例》着眼于规管执法机构（即公职人员）何时和如何可合法侵犯某人的私人通讯权利，例如藉着就拟进行的截取通讯或拟进行的秘密监察取得“订明授权”而侵犯该权利。[7] 另外，《截取通讯及监察条例》只规管截取在传送过程中的通讯。[8]

---

2 《示范法》中“电脑数据”的定义似乎与我们的建议一致，即建议的罪行应一般适用于数据（包括元数据），而非只限于构成私人通讯的数据：
“‘电脑数据’指任何对事实、资料或概念的表述，而该表述的形式适合电脑系统处理，电脑数据包括适合用于致使电脑系统执行功能的程式”。

3 咨询文件第 3.1 段。

4 数据经不同器材传送期间会留下足迹，这些器材甚至会保留数据的复本。控制任何这些器材的人或许能够分析传送的数据。

5 后门程式是*“获授权用户及未获授权用户能藉以绕过正常保安措施，从而按高用户级别取用或取览某电脑系统、网络或应用软件的任何方法。”*见 https://www.malwarebytes.com/backdoor（于 2025 年 11 月 1 日浏览）。

6 第 3.7 及 3.9 段。

7 《截取通讯及监察条例》（第 589 章）第 2 条。

8 见《截取通讯及监察条例》第 2(1)条对“截取作为”的定义。

《电讯条例》（第 106 章）第 27(b)条

3.7 在执法情况以外，则有《电讯条例》第 27 条下述规定：

> "任何人损坏、移走或以任何方式干扰电讯装置，而意图是——
>
> (a) 阻止或妨碍任何讯息的传送或传递；或
>
> (b) 截取或找出任何讯息的内容，
>
> 即属犯罪，一经循简易程序定罪，可处第 4 级罚款及监禁 2 年。"

3.8 正如小组委员会在咨询文件指出，[9] 第 27(b)条并非针对截取电脑数据的特定条文。该条文预设电讯背景，并不完全适用于电脑网络空间。此外，根据第 27(b)条，拟截取的目标只限于*"任何讯息的内容"*，这句显然并不涵盖元数据（即提供其他数据相关资料的数据）。

对小组委员会建议 4 的概括回应

支持建议 4 的回应者的意见

3.9 在明确表达立场的回应者当中，明显大多数均支持建议 4。表示赞同的回应者包括法律专业团体、资讯科技相关团体、大专院校、商业团体及政府部门。

3.10 小组委员会收到的正面回应当中，个人资料私隐专员公署（"**私隐专员公署**"）表示，订立为不诚实或犯罪目的而在未获授权下截取电脑数据这项罪行，会*"有助遏止愈趋常见的资料外泄事故"*。基于这项截取罪的政策原意是*"保障人们的数据通讯私隐权"*，私隐专员公署支持引入这项罪行。

3.11 香港与内地法律专业联合会有限公司亦支持建议的罪行，并且同意上文第 3.8 段小组委员会对《电讯条例》第 27 条的局限所作出的分析。该会更提到，违反《电讯条例》第 27 条的最高刑罚颇轻，只是第 4 级罚款（25,000 元）[10] 及监禁 2 年。

---

9 第 3.14 段。

10 《刑事诉讼程序条例》（第 221 章）附表 8。

3.12 其他回应者——资讯科技相关团体及个别人士——亦赞成引入在未获授权下截取电脑数据罪，但强调加入"犯罪目的"或"犯罪意图"作为罪行构成元素这点至为重要。

反对建议 4 的回应者的意见

3.13 只有一个资讯科技相关团体反对扩大电脑罪行的范围。该回应者忧虑建议的截取罪会对网络安全从业员进行的合法作为（例如，网络入侵侦测及渗透测试可能涉及截取电脑数据）带来潜在不确定性，并认为即使被告人享有免责辩护，控方仍须负证明被告人意图的举证责任。

对小组委员会建议 4 的详细回应

截取罪的范围

3.14 关于咨询文件建议 4(a)，私隐专员公署表示，"披露"和"使用"电脑数据显然构成不同的刑事作为，与"截取"有所区别。私隐专员公署继而作出以下提议：

> "如政策原意是立法禁止披露或使用由先前截取作为而获得的电脑数据，我们提议应在法例内清楚述明，否则新订罪行的管辖范围可能涵盖披露或使用并非由截取而获得的电脑数据。"

截取罪与《个人资料（私隐）条例》（第 486 章）（《私隐条例》）现有的"起底"罪行是否互相重迭

3.15 私隐专员公署亦提述《私隐条例》第 64(1)[11]、(3A)[12] 及(3C)[13]条，该等条文订立有关"起底"的刑事罪行。私隐专员公署指出，

---

11 《私隐条例》第 64(1)条规定，*"任何人披露未经资料使用者同意而取自该资料使用者的某资料当事人的任何个人资料，而该项披露是出于以下意图的，该人即属犯罪——*
(a) 获取金钱得益或其他财产得益，不论是为了令该人或另一人受惠而获取；或
(b) 导致该当事人蒙受金钱损失或其他财产损失。"（底线后加）

12 《私隐条例》第 64(3A)条规定，*"如任何人（披露者）在未获资料当事人的相关同意下，披露该当事人的个人资料，而——*
(a) 披露者的意图，是导致该当事人或其任何家人蒙受任何指明伤害；或
(b) 披露者罔顾是否会（或相当可能会）导致该当事人或其任何家人蒙受任何指明伤害，披露者即属犯罪。"（底线后加）
指明伤害指对某人的滋扰、骚扰、缠扰、威胁或恐吓、身体伤害或心理伤害；导致某人合理地担心其安全或福祉的伤害；或某人的财产受损（见第 64(6)条）。

13 《私隐条例》第 64(3C)条规定，*"如——*

建议的非法截取电脑数据罪与现有的"起底"罪行对犯罪意念的规定明显有别。不过，私隐专员公署认为，视乎个别案件的案情及证据，相关的个人资料披露可能同时构成建议的截取罪及《私隐条例》所订罪行。

"为不诚实或犯罪目的"这项元素是否充分或适当

3.16 香港女律师协会有限公司（"**女律师协会**"）赞成建议 4，并表达以下意见：

> "应考虑是否亦应把任何不当目的包括在内，例如是否有披露个人或保密资料，而有关披露可能既不构成罪行，亦不涉及'财务上不诚实'此涵义中的不诚实"。

3.17 不过，该回应者并无提出任何实质例子，以说明有何构成罪责的电脑数据截取可能不符合建议 4 所订的*"不诚实或犯罪目的"*这个门槛。

3.18 此外，某资讯科技相关团体关注到，防毒解决方案提供者及其他互联网保安公司等科技保安公司或会监察网络，以找出攻击讯号或分析网络通讯。该回应者解释，这些活动的性质或会显示出截取电脑数据的特征，但这些活动不一定针对任何特定组织，并认为只有截取电脑数据的作为关乎向一个或多个特定目标发动攻击，才应属犯罪。

3.19 另一方面，另一个资讯科技相关团体认为，*"不诚实或犯罪目的"*这项规定足以保障网上服务提供者的正常运作，并同意所需犯罪意念应如建议 4(a)所述，即为*"不诚实或犯罪目的"*而截取。

行使执法权力的公职人员的刑事法律责任

3.20 对于公职人员（例如执法机关成员）在超逾其权限范围的情况下截取或取览电脑数据须负上的法律责任，某政府部门要求厘清小组委员会在这方面的立场。该回应者提出：

(a) 任何人（披露者）在未获资料当事人的相关同意下，披露该当事人的个人资料，而——

(i) 披露者的意图，是导致该当事人或其任何家人蒙受任何指明伤害；或

(ii) 披露者罔顾是否会（或相当可能会）导致该当事人或其任何家人蒙受任何指明伤害；及

(b) 该项披露导致该当事人或其任何家人蒙受任何指明伤害，

披露者即属犯罪。"（底线后加）

"在某些情况下，或会有公职人员真诚行事，却不慎超逾其获授执法权力的权限……在这些情况下，公职人员无须负刑事法律责任，才是符合重大公众利益的做法，否则公职人员或会倾向采取过分规避风险的执法态度……"

"超逾权限"的截取

3.21 两个专业团体（即女律师协会及香港女工商及专业人员联会〔"**女工商专联**"〕）提议，在未获授权下截取，应包括超逾权限的截取作为。就此，女律师协会特别建议采纳美利坚合众国（"**美国**"）《储存通讯法案》（Stored Communications Act）所载有关"超逾"授权范围的概念。

3.22 正如咨询文件所提及，[14] 《储存通讯法案》的主要条文是《美国法典》第 18 篇第 2701(a)条：

"除本条(c)款另有规定外，任何人如——

(1) 在未获授权下蓄意取用藉以提供电子通讯服务的设施；或

(2) 蓄意超逾授权范围而取用该设施；

从而在有线或电子通讯以电子方式储存于有关系统内期间，取得或更改该等通讯，或阻止对该等通讯的获授权取览，则须按照本条(b)款的规定惩处。"

（底线后加）

截取罪应否只保障私人通讯

3.23 关于建议 4(b)(i)，某资讯科技相关团体表示，建议的截取罪应只保障私人通讯。该团体认为，*"以电脑网络世界而言，一般通讯属过于广泛"*，建议的罪行拟为公众提供的保障*"或会不必要地扰乱正当通讯"*。

---

[14] 第 3.87 段。

应否界定何谓“截取”

3.24 正如第 2 章提到，[15] 部分商业团体认为应清晰界定或向公众解释若干概念（包括“截取”及“取用或取览”）的涵义。他们忧虑随着科技发展，这些概念或会有所重迭和不断演变。

我们的分析及回应

重订截取罪的焦点

3.25 在咨询文件中，[16] 小组委员会解释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（例如在电子商贸交易中，倘若信用卡资料在传送至卖方期间被截取作不当用途，持有人可能会蒙受财务损失）。

3.26 正如上文第 3.14 段所述，私隐专员公署就建议的非法截取电脑数据罪的涵盖范围提出疑问。就此，我们审慎检视该项罪行的应用情况。我们认为，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。

3.27 此外，在未获授权下披露或使用电脑数据的罪行，只要涉及个人资料，就更当属私隐专员公署检视的范畴。我们注意到，最近一次在 2021 年的立法修订工作中，[17] 私隐专员公署特别聚焦于“起底”罪行，务求遏止在未获同意下披露个人资料。[18] 《私隐条例》第 64(3A)[19] 及(3C)[20] 条的罪行，均规定须有意图导致指明伤害，或

---

15 上文第 2.17 段。

16 第 3.92 及 3.94 段。

17 透过制定《2021 年个人资料（私隐）（修订）条例》（2021 年第 32 号条例），在《个人资料（私隐）条例》（第 486 章）加入有关“起底”的条文。

18 见《2021 年个人资料（私隐）（修订）条例》的详题。

19 《私隐条例》第 64(3A)条规定，*“如任何人（披露者）在未获资料当事人的相关同意下，披露该当事人的个人资料，而——*

(a) 披露者的意图，是导致该当事人或其任何家人蒙受任何指明伤害；或

(b) 披露者罔顾是否会（或相当可能会）导致该当事人或其任何家人蒙受任何指明伤害，

披露者即属犯罪。”（底线后加）

指明伤害指对某人的滋扰、骚扰、缠扰、威胁或恐吓、身体伤害或心理伤害；导致某人合理地担心其安全或福祉的伤害；或某人的财产受损（见第 64(6)条）。

根据第 64(3B)条，最高刑罚为第 6 级罚款（即 100,000 元）及监禁两年。

20 《私隐条例》第 64(3C)条规定，*“如——*

罔顾是否会导致指明伤害。正如私隐专员公署在意见书内适切指出，"起底"罪行的犯罪意念非常局限于特定范围。

3.28 鉴于在未获授权下披露或使用电脑数据这项一般罪行影响甚广，为审慎起见，我们应先在研究的第二部分[21]深入探讨这议题，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。另外，该项罪行与《私隐条例》"起底"罪行之间的相互影响，或许亦值得再加考虑。

3.29 对于私隐专员公署认为在未获授权下披露或使用电脑数据罪与"起底"罪行或有重迭，考虑到我们建议的方案，这是我们现阶段的回应。不过，我们顺带补充，建议的截取罪针对在未获授权下"截取"一般电脑数据，虽然须证明有不诚实或犯罪目的，但该截取罪并非基于导致伤害。就此而言，截取罪与《私隐条例》的"起底"罪行可清楚区分开来。

"为不诚实或犯罪目的"这项规定适当

3.30 我们认为，某目的是否"不当"，可以是个视乎诠释而定的主观问题。相反，要判断某目的是否*"不诚实或犯罪"*，则存在客观标准。例如，*R v Ghosh* 厘定了不诚实验证标准，[22] 而该案仍然是香港遵循的主导案例。[23] 至于"犯罪目的"，在大多数案件中，某作为是否属犯罪，相对上清楚分明。此外，"犯罪目的"亦是订立已久的法定概念。

(a) 任何人（披露者）在未获资料当事人的相关同意下，披露该当事人的个人资料，而——

(i) 披露者的意图，是导致该当事人或其任何家人蒙受任何指明伤害；或

(ii) 披露者罔顾是否会（或相当可能会）导致该当事人或其任何家人蒙受任何指明伤害；及

(b) 该项披露导致该当事人或其任何家人蒙受任何指明伤害，

披露者即属犯罪。"（底线后加）

根据第 64(3D)条，最高刑罚为罚款 1,000,000 元及监禁五年。

21 第二部分的范围适时再作讨论，该部分会涵盖借助电脑网络的罪行，即通过使用电脑、电脑网络或其他形式的资讯及通讯科技，使犯罪规模或范围得以扩大的传统罪行。见导言第 8 段。

22 [1982] QB 1053。根据 *Ghosh* 案的验证标准，陪审团必须首先根据明理且诚实的人的一般标准，决定有关行为是否不诚实。假如有关行为属于不诚实，则陪审团必须进而考虑，被告人本人是否必定已认知其行为按该等标准衡量属于不诚实。

23 就不诚实验证标准而言，*Ghosh* 案的验证标准现时仍然是香港的有效法律，但因应英国最高法院就一宗民事申索案件（即 *Ivey v Genting Casinos (UK) Ltd (trading as Crockfords Club)* [2018]

3.31　我们应强调，在咨询文件内，[24] 小组委员会已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。正如小组委员会所概述，以下现象即使可能牵涉在未获授权下进行截取，亦不大可能被视为不妥：[25]

(a)　网络分析已成为网络系统一项标准特点。分析所得的统计资料可显示是否有人滥用网络、用户登入某网站的次数等等。这些资料可具管理用途，例如提醒网络管理员在域名系统层面封锁某网站。

(b)　在日常运作中，互联网服务提供者会因为各种原因透过其设备管有某些传送中的数据，而这些运作在技术上需获取元数据。

3.32　这正正解释小组委员会为何建议把*"为不诚实或犯罪目的"*而截取列为建议的截取罪的要求之一，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。*"为不诚实或犯罪目的"*这项元素旨在订立较高的犯罪意念门槛，避免把在未获授权下进行截取过度刑事化，或避免所订罪行的范围不合理地广泛。凭借*"为不诚实或犯罪目的"*这项规定，网络安全公司防范网络攻击的活动便会排除在建议的罪行的涵盖范围以外。

3.33　我们应补充，随着科技日新月异，如要新订的电脑网络罪行法例精准描述数据截取会被视为合法的各种确切情况，既不切实际，亦毫不恰当。我们认为，新订的电脑网络罪行法例只要能够清楚述明，建议的罪行只禁止为不诚实或犯罪目的而在未获授权下截取电脑数据，便已充分足够。

3.34　我们亦承认，如要把*"为不诚实或犯罪目的"*这项意念元素应用于若干临界情况的行为（例如私家侦探及狗仔队可能作出的数据截取作为），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。除了截取的目的之外，例如倘若被告人知道所截取的数据涉及私人通讯，法庭则可能会在考虑一般明理的人的标准后，裁定该项截取作为属不诚实。

AC 391, [2017] 3 WLR 1212）作出决定之后，英格兰及威尔斯上诉法院在 *R v Barton* [2021] QB 685, [2020] 3 WLR 1333 内确认的法理发展，香港法庭或须待有机会时对 *Ghosh* 案的验证标准加以考虑。见 *Archbold Hong Kong 2025*，第 22–20 段。

24　第 3.97 段。

25　同上。

3.35 不过，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，以决定被告人的截取行为是否属于可接受的界限内。例如，倘若一名电脑科学学生在购物商场截取数据，指称仅为某类研究目的进行数据截取（例如确定使用某个电话型号的人数），但截取的数据却包含信用卡资料或电话号码，而他未能提出一些属实或可能属实的清白解释说明为何收集过多数据，则法庭很可能会裁定他是*"为不诚实或犯罪目的"*而进行截取。

3.36 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。

行使执法权力的公职人员的刑事法律责任

3.37 正如我们刚才已在上文数段解释，建议的截取罪附带相对较高的意念门槛，即为不诚实或犯罪目的而在未获授权下截取电脑数据。倘若一名公职人员真诚行事，只是不慎超逾其权限，我们相信，除非香港法庭因应英格兰及威尔斯的法理发展[26]而对 *Ghosh* 案的不诚实验证标准再作考虑，否则该名公职人员不大可能会被裁定犯建议的罪行。在任何情况下，只要公职人员没有*"为不诚实或犯罪目的"*而截取数据，便不会构成截取罪。

3.38 另一方面，公职人员如*"为不诚实或犯罪目的"*而截取数据，便应该如其他人一样，被判犯了非法截取电脑数据罪。因此，我们认为无须在针对电脑网络罪行的特定法例内，就公职人员履行执法职务订定特定豁免。

在未获授权下截取，包括"超逾权限"的截取

3.39 "未获授权"这个概念体现于我们建议的首四项依赖电脑网络的罪行，即第 2 章讨论的非法取览程式或数据罪（"**取览罪**"）、建议的非法截取电脑数据罪，以及我们会于第 4 及 5 章讨论的非法干扰电脑数据罪及非法干扰电脑系统罪（"**干扰罪**"）。

---

[26] 如上文注脚 22 解释，根据 *Ghosh* 案的验证标准，陪审团必须：(i)根据明理且诚实的人的一般标准，决定有关行为是否不诚实；及假如有关行为属于不诚实，(ii)则考虑被告人本人是否必定已认知其行为按该等标准衡量属于不诚实。有人忧虑，*Ghosh* 案的验证标准的第二部分取决于被告人对社会标准的理解，因此道德准则薄弱的人只要坚称自己不知悉社会上对诚实的标准，便可逃避法律责任。在 *R v Barton and Booth* [2021] QB 685 第 729 页，英格兰上诉法院确认，在 *Ivey v Genting Casinos (UK) Ltd* [2018] AC 391, [2017] 3 WLR 1212 确立的验证标准将会是用于所有刑事案件的不诚实验证标准，即一旦确定被告人就事实所知或所信的实际思想状态，则其行为是否不诚实这个问题，会应用一般合乎体统的人的客观标准而裁定，而不是按被告人对该等标准的理解。香港法庭会否偏离 *R v Ghosh* 的不诚实验证标准，仍有待观察。

3.40　在最终建议1，我们建议取览罪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及2条为蓝本。《英格兰误用电脑法令》第1(1)及17(5)条已载于本报告书第2章，[27] 现再次引述以便读者参阅。第1(1)条规定：

"任何人在以下情况，即属犯罪——

(a) 该人致使某电脑执行任何功能，意图获得对存于任何电脑内的任何程式或数据的取览，或意图使他人能够获得该项取览；

(b) 该人意图获得该项取览，或意图使他人能够获得该项取览，但该项取览未获授权；及

(c) 该人在致使该电脑执行该功能时，知悉情况如此。"

（底线后加）

3.41　《英格兰误用电脑法令》第17(5)条规定如下：

"在以下情况下，任何人取览存于某电脑内的任何程式或数据，不论取览属任何种类，即属未获授权取览——

(a) 该人本身无权控制对该程式或数据作出有关种类的取览；及

(b) 该人未获有此权利的人同意他对该程式或数据作出该类取览……"

（底线后加）

[27] 上文第2.20及2.21段。

3.42 正如小组委员会在咨询文件解释，[28] 上议院在 *R v Bow Street Metropolitan Stipendiary Magistrate, Ex parte United States* [29] 裁定，第 17(5)条并无引入按不同级别取用有关电脑的概念，而任何获有限度授权取览电脑内数据的雇员，如在超逾该授权范围下行事，便可能犯《英格兰误用电脑法令》第 1 条所订罪行。换言之，"未获授权"一词涵盖某人在超逾权限范围下行事的情况，意味着以《英格兰误用电脑法令》为蓝本的取览罪拟适用于以下情况：(i)被告人在没有权限的情况下行事；或(ii)被告人在超逾权限范围下行事。

3.43 为保持一致，就"未获授权"这个概念而言，建议的截取罪及干扰罪应采用同一范围。倘若政府决定落实最终建议 4，法律草拟专员可考虑有关罪行条文应否明文述明"未获授权"包括*"在超逾权限范围下行事"*（如咨询文件讨论的美国《电脑欺诈及滥用法案》〔Computer Fraud and Abuse Act〕第 1030(a)条所述明），[30] 以确保建议的截取罪涵盖范围清楚明白。

截取罪不只适用于"私人通讯"，而是适用于一般"通讯"及"数据"，并包括元数据等

3.44 此处宜回顾《布达佩斯公约》第三条关于订定非法截取电脑数据罪的标准。正如咨询文件引述公约的《说明报告》所述：[31]

> "有关罪行适用于'非公开'传送电脑数据。'非公开'一词规限传送（通讯）过程的性质，而非所传送数据的性质。所传达的数据可能属公开资料，但有关各方希望将通讯保密。或者在服务获缴款前，数据可能因

---

28 第 2.45 及 2.46 段。

29 [2000] 2 AC 216.

30 第 2.81 段。《电脑欺诈及滥用法案》第 1030(a)条列出与取用有关而可根据第 1030(c)条规定予以惩处的作为，包括某人：

"(1) 知悉在未获授权下取用某电脑或知悉超逾获授权的取用范围，并已藉该行为而取得已裁断为……须获得保护以免被未获授权披露的资料……或任何受限数据……而且有理由相信该等资料……可用作损害美国［等］，而故意把该等资料传达［等］给任何无权收取该等资料的人［等］；

(2) 在未获授权下蓄意取用某电脑或超逾获授权的取用范围，并藉此——

(A) 取得载于某财务机构的财务纪录的资料［等］；

(B) 从美国任何部门或机关取得资料；或

(C) 从任何受保护电脑取得资料；

……

(4) 意图蓄意欺诈并知悉在未获授权下取用某受保护电脑或超逾获授权的取用范围，并藉该行为而促成故意欺诈并取得任何有价值的物品……"。（底线后加）

31 第 3.18 段。

商业目的而保密（例如是收费电视的情况）。因此，‘非公开’一词本身并不排除公共网络上的通讯……”

（底线后加）

3.45 换言之，《布达佩斯公约》第三条并无规定有关电脑数据须为私人数据。[32] 有关数据可以是公开数据或私人数据。

3.46 我们亦紧记，新西兰对《2012 年搜查及监察法令》（Search and Surveillance Act 2012）的检讨，曾识别出其法定机制仅限于涵盖截取“私人通讯”而引起的问题。新西兰的法律委员会（Law Commission）与司法部（Ministry of Justice）于 2016 年联合发表议事文件，强调不宜聚焦于通讯各方的期望，因为这存在循环论证成分，*“一直引来大量批评”*。[33] 鉴于上文所述，新西兰于 2017 年发布的报告书建议，“私人通讯”的定义应以“通讯”取代。[34]

3.47 此外，必须留意根据咨询文件建议 4(b)，建议的截取罪适用于所有“数据”，不论是元数据、传送中的数据，还是在传送期间暂时静止的数据，以免审讯中需要传唤极为技术性的证据。[35]

3.48 总括而言，我们认为建议的截取罪不应只保障“私人通讯”，而是应同时保障一般“通讯”及“数据”，并应包括元数据等。

不界定“截取”

3.49 正如某商业团体指出，“取用或取览”及“截取”等电脑相关作为会随着科技发展而不断演变。截取电脑数据的崭新方法可能不时涌现，并超乎我们的想象。若界定何谓“截取”，可能会损害有关法律应对新环境的弹性。

---

32 咨询文件第 3.100 段。

33 新西兰法律委员会及司法部，*Review of the Search and Surveillance Act 2012*（第 40 号议事文件，2016 年），第 4.11 段。

34 新西兰法律委员会及司法部，*Review of the Search and Surveillance Act 2012*（第 141 号报告书，2017 年），建议 24。另见咨询文件第 3.101(b)段。

35 正如咨询文件所讨论（见第 3.19 至 3.24、3.108 及 3.109 段），只要有关数据是在传送人一端前往传送对象一端的途中，截取数据便应属犯罪。因此，截取罪适用于整个传送过程中的通讯，不论数据是暂时静止还是正在传递中。订立这项罪行的方法之一，是加入类似于澳大利亚《1979 年电讯（截取及取览）法令》（Telecommunications (Interception and Access) Act 1979）第 5F 条的推定条文。该条规定，通讯：(a)在传送人*“发送或传送该通讯的那刻起，视为开始经过电讯系统”*；及(b)*“视为继续经过该系统，直至……传送对象可取览该通讯为止”*（见咨询文件第 3.22 段）。这会使控方无须援引极为技术性的证据，以证明有关罪行元素。

3.50 因此，尽管现有的《截取通讯及监察条例》（第 589 章）[36] 及某些其他司法管辖区[37] 已界定“截取作为”，但我们认为，较为适当的做法是不在新订的电脑网络罪行法例中界定何谓“截取”，而是赋予“截取”其通常涵义，以使建议的罪行达到保障人们数据通讯私隐权这目的。

有关建议 4 的结论

3.51 我们的结论是建议 4 可予保留，但基于上文第 3.25 至 3.28 段所阐述的理由，有关*“披露或使用电脑数据”*的部分应予删除，以待作进一步研究。

最终建议 4

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）。

---

36 根据《截取通讯及监察条例》（第 589 章）第 2(1)条，“截取作为”的定义如下：
“截取作为(intercepting act)就任何通讯而言，指在该通讯藉邮政服务或藉电讯系统传送的过程中，由并非该通讯的传送人或传送对象的人查察该通讯的某些或所有内容”。

37 即英格兰及威尔斯（《2016 年调查权力法令》〔Investigatory Powers Act 2016〕第 4 条）、新西兰（《1961 年刑事罪行法令》〔Crimes Act 1961〕第 216A(1)条）及美利坚合众国（《搭线窃听法案》〔Wiretap Act〕第 2510(4)条）。

(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。

非法截取电脑数据罪的免责辩护：建议 5

3.52 咨询文件建议 5 邀请公众就以下问题提交意见书：

"(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）？"

对小组委员会建议 5 的回应

3.53 由于对建议 5(a)及(b)咨询问题的回应在某程度上密切相关及互相重迭，因此我们会一并分析。

建议 5(a)

支持豁免专业的回应者的意见

3.54 绝大多数回应者认为，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，均应享有免责辩护或豁免。该等回应者提议，有关免责辩护或豁免应涵盖以下类别的专业或活动：

(a) 互联网服务提供者；

(b) 日常工作经常需要使用和处理截取的数据的机构（建议这项豁免的资讯科技相关团体并无提出这类机构的具体例子）；

(c) 纯粹为侦测安全威胁而截取其本身网络的公司，不论是由该等公司自行截取，还是由其授权的安全顾问截取；

(d) 执法机关就犯罪活动及国家安全事宜进行的调查；

(e) 为公众利益或为日后法律程序搜证而真诚地进行的举报活动；及

(f) 合理相信有损害其利益的活动正在进行的业务或机构（女工商专联注明，这项免责辩护或豁免应以严谨及狭义的方式表达）。

反对豁免专业的回应者的意见

3.55 不过，部分来自资讯科技界别的回应者不赞成对任何专业在合法业务的通常运作过程中截取和使用数据的情况，一律提供免责辩护或豁免。他们指出：

(a) 第一，截取的数据不一定与进行截取的业务有关，这方面有不少灰色地带，很可能会引起争议；及

(b) 第二，免责辩护或豁免应适用于任何人，而非只适用于任何享有特权的特定界别。

建议 5(b)

支持豁免真正业务的回应者的意见

3.56 与建议 5(a)的情况类似，明显大多数的回应者均赞成真正业务应获准截取和使用传送中的数据，而无须负上刑事法律责任。该等回应者当中，私隐专员公署与小组委员会看法一致，认为倘若业务根据若干条款及条件提供 Wi-Fi 热点或电脑供人使用，而有关条款及条件保留权利截取和使用顾客或雇员的数据，则这类截取和使用数据的权限属于合约性质。[38] 私隐专员公署又指，如收集的数据涉及个人资料，则收集和使用这些个人资料会受到《私隐条例》的保障资料原则规管。

---

[38] 咨询文件第 3.118 段。

3.57 支持豁免真正业务的回应者就豁免条件作出建议。不同界别的回应者均认为，业务不得为不诚实或犯罪目的而截取和使用数据。女律师协会进一步提议，为了提供充分理据支持业务可截取和使用传送中的数据而无须负上刑事法律责任，这类截取的目的必须予以限制，而有关免责辩护或豁免亦可规定，进行截取的人与截取对象之间须存在特定关系（例如雇佣关系）。

3.58 关于建议 5 咨询问题内重点提出的购物商场例子，女律师协会指出：

> "似乎并无任何明显理由能解释为何顾客传送的数据应被截取。购物商场营运者 / 业主〔与〕整体顾客之间并无真正关系，因此这类法定许可会显得过于广泛。"

反对豁免真正业务的回应者的意见

3.59 另一方面，部分回应者对容许真正业务截取和使用传送中的数据有所保留。例如，消费者委员会提出以下观点：

> "当商场或商店提供免费 Wi-Fi 热点服务，消费者或会合理期望，有关服务性质上纯粹是为了招徕生意的增值服务。消费者未必会合理期望其数据会被截取和用于其他目的……
>
> ……尽管商场或商店或会列出使用条款，规定消费者须表示同意数据被截取，作为取用服务的条件，但消费者是否会花时间或精力妥为审阅该等条款，这却是个疑问……即使消费者给予同意，亦未必是在知情下同意。
>
> 不加区别地收集透过 Wi-Fi 热点传送的数据，在任何情况下也是过于广泛之举。有关收集可能会包括个人资料，甚或银行帐户资料及密码等敏感数据。不论数据是否经过编码处理，或该业务是否有意使用该等数据，消费者亦不大可能认为这样收集数据是公平的。"

3.60 最后，某资讯科技相关团体指出，业务为客户提供的 Wi-Fi 热点或电脑如被不当使用，可能会导致资料外泄，因此该回应者并不赞成为这类业务提供特定免责辩护或豁免。

我们的分析及回应

3.61　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。理论上，就已特意明确规定须证明*"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。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。

3.62　关于部分回应者认为特定类别的专业或业务应获提供免责辩护或豁免，我们有以下看法：

(a) 由于在正常业务过程中行事的互联网服务提供者已受保障，不会因并无犯罪意图的数据截取而负上法律责任，因此无须就建议的截取罪为他们提供任何免责辩护。

(b) 要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，但实际上又不向日常营运涉及数据截取的某些专业或业务（例如私家侦探社或传媒机构）给予截取数据的无限制授权，根本并不可行。

(c) 真正业务的确或会收集或截取电脑数据，主要作多种营销用途。然而，如证明在未获授权下截取确曾发生，并且是为不诚实目的（相对于以不诚实方式）而进行，即使该业务只是出于牟利动机，亦更有理由不应提供免责辩护。

(d) 非法取览程式或数据的作为[39] 或非法干扰电脑数据及/或电脑系统的作为，[40] 即使是为公众利益或为日后法律程序搜证而真诚地进行，亦没有获提供免责辩护。因此，我们难以理解为何应就建议的截取罪为举报者提供此等免责辩护。此外，不同人对甚么构成"真诚"或各有标准，咨询文件讨论的*香港特别行政区　诉　秦瑞麟*（*HKSAR v Tsun Shui Lun*）[41] 是一个好例子。案中任职医院雇员的被告人向传媒泄露一名主要官员的医疗报告，被控触犯《刑事罪行

39　有关非法取览程式或数据罪的免责辩护，在第 2 章第 2.63 至 2.102 段讨论。

40　有关非法干扰电脑数据罪及非法干扰电脑系统罪的免责辩护，分别在第 4 章第 4.32 至 4.44 段及第 5 章第 5.23 至 5.28 段讨论。

41　[1999] 3 HKLRD 215, HCMA 723/1998（判决日期：1999 年 1 月 15 日）。见咨询文件第 2.9 及 2.10 段。

条例》（第 200 章）第 161(1)(c)条，[42] 他争辩指自己以为公众有权知道真相。然而，原讼法庭裁定他针对定罪的上诉缺乏理据。[43]

(e) 最后但同样重要的是，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。

3.63 基于所有这些原因，我们倾向建议的截取罪无须提供免责辩护或豁免。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。

3.64 总括而言，有别于取览罪及干扰罪，建议的截取罪就截取电脑数据采用*"为不诚实或犯罪目的"*这个较高标准的犯罪意念，而这项犯罪意念本身已免除为有关罪行提供任何特定豁免或免责辩护的需要。

最终建议 5

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。

---

42 根据《刑事罪行条例》（第 200 章）第 161(1)(c)条，任何人取用电脑，*"目的在于使其本人或他人不诚实地获益"*（不论是在取用电脑的同时或在日后任何时间），即属犯罪，一经循公诉程序定罪，可处监禁 5 年。

43 见上文注脚 41，第 228 页。原讼法庭裁定，上诉人在超逾权限范围下取用医院的电脑系统，意图取得电脑内的保密资料，目的在于列印有关扫描报告的复本，并泄露予传媒，这属于《刑事罪行条例》第 161 条定义的获益。有关行为是不诚实行为，而被告人亦知悉事实如此。

第 4 章　非法干扰电脑数据

引言

4.1　本章讨论关于咨询文件建议 6 的回应。建议 6 建议订立第三类依赖电脑网络的罪行，即非法干扰电脑数据：

> “小组委员会建议：
>
> (a) 无合法权限或合理辩解而蓄意干扰（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。
>
> (b) 新法例应采用《刑事罪行条例》（第 200 章）所订的以下特点：
>
> (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（规定须怀有意图或罔顾后果，但无须怀有恶意）；
>
> (iii) 第 64(2)条所订两项合法辩解，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) 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。”

4.2　正如小组委员会在咨询文件解释，[1] 概括而言，干扰电脑数据罪旨在：

(a) 打击蓄意损坏、删除、更改电脑数据等行为；

(b) 从而保护电脑数据的完整性，确保有关数据能正常运作或使用。

---

[1] 第 4.1 段。

4.3 干扰数据罪可藉以下方式进行：

(a) 在没有权限的情况下取览储存于电脑的档案后，修改该档案。

(b) 藉电脑病毒（譬如是能够删除受感染电脑所储存的特定数据的电脑病毒）干扰数据。

4.4 由于干扰数据通常只会在某人初步入侵电脑系统时发生，因此非法干扰电脑数据罪与第2章所讨论的非法取览程式或数据罪（"**取览罪**"）息息相关。

对建议6的概括回应

4.5 绝大多数就建议6发表具体意见的回应者均支持该建议，这些回应者包括法律专业团体、资讯科技相关团体、大专院校、商业机构及政府部门。

4.6 个人资料私隐专员公署支持订立建议的非法干扰电脑数据罪，理由是此举有助遏止愈趋常见的资料外泄事故。

4.7 多个机构（包括香港与内地法律专业联合会有限公司、香港女律师协会有限公司、另一个专业协会及两个商业团体）同意，《刑事罪行条例》（第200章）下应对非法干扰电脑数据及电脑系统的现行制度（包括第59(1A)条*"误用电脑"*这概念）令人满意。这些回应者因此同意小组委员会的建议，将《刑事罪行条例》第59、60及64条的现有条文改列于新订的电脑网络罪行法例，以求贯彻一致。

香港的现行法律

4.8 正如小组委员会在咨询文件解释，[2] 现行的香港法律处理非法干扰电脑数据的主要方式，是把它视为刑事损坏的其中一种形式。根据《刑事罪行条例》第60(1)及(2)条（*"摧毁或损坏财产"*）：

"(1) 任何人无合法辩解而摧毁或损坏属于他人的财产，意图摧毁或损坏该财产或罔顾该财产是否会被摧毁或损坏，即属犯罪。

[2] 第4.4及4.5段。

(2) 任何人无合法辩解而摧毁或损坏任何财产（不论是属于其本人或他人的）——

(a) 意图摧毁或损坏任何财产或罔顾任何财产是否会被摧毁或损坏；及

(b) 意图藉摧毁或损坏财产以危害他人生命或罔顾他人生命是否会因而受到危害，

即属犯罪。”

4.9 与第 60(1)条相比，第 60(2)条所订罪行是有关罪行的加重形式。第 63 条（*“罪行的惩处”*）就这些罪行所订明的最高刑罚差别很大：

“(1) 任何人犯……第 60(2)条所订的罪行……，一经循公诉程序定罪，可处终身监禁。

(2) 任何人犯本部所订的其他罪行［即包括第 60(1)条］，一经循公诉程序定罪，可处监禁 10 年。”

《刑事罪行条例》在干扰电脑数据及电脑系统方面的应用

4.10 刑事损坏罪可处理非法干扰电脑数据（以及将于下一章讨论的非法干扰电脑系统），是因为《1993 年电脑罪行条例》（1993 年第 23 号）在《刑事罪行条例》加入以下条文：

(a) 第 59(1)(b)条将“财产”一词界定为包括*“电脑内或电脑储存媒体内的任何程式或资料，不论该程式或资料是否属实体性质的财产。”*

(b) 第 59(1A)条订明摧毁或损坏财产，就电脑而言，包括*“误用电脑”*。该词在第 59(1A)条界定为以下作为：

“(a) 导致电脑并非如其拥有人或其拥有人代表对其所设定的运作方式运作，即使如此误用不会令该电脑的操作、该电脑内的程式或该电脑内的资料的可靠性减损亦然；

(b) 更改或删抹电脑内或电脑储存媒体内的程式或资料；

(c) 在电脑或电脑储存媒体所收纳的内容上增加程式或资料，

而造成导致(a)、(b)或(c)段所提述的任何类别误用情形的任何作为，须视为导致该项误用情形的作为。”

第59(1A)条的三个部分当中，(b)及(c)部分与非法干扰电脑数据罪最为相关。

4.11 根据《刑事罪行条例》第64(2)条，任何人被控以刑事损坏罪，在下述情况下均须被视为有*“合法辩解”*：

“(a) 如指称构成该罪行的作为作出时，被控人相信，他相信有权同意有关财产的摧毁或损坏的人已予同意，或相信该人如知道有关财产的摧毁或损坏及有关情形亦会予以同意；或

(b) 如被控人摧毁或损坏有关财产或威胁会如此做，或（在被控以第62条所订罪行时）意图使用或导致或准许使用某些物品以摧毁或损坏有关财产，而他如此做是为了保护属于其本人或另一人的财产，或保护归属于或他相信归属于其本人或另一人的财产权利或财产权益，且于指称构成该罪行的作为作出时，他相信——

(i) 该财产、权利或权益即需保护；及

(ii) 在顾及一切有关情况后，所采用或打算采用的保护方法是或会是合理的。”

4.12 凭借第64(3)条，只要被告人是诚实地相信有关事情，则是否有充分理由支持，不具关键性。

对小组委员会建议6的详细回应

4.13 虽然极大多数回应者均支持订立建议的非法干扰电脑数据罪，但部分回应者亦就建议6所建议罪行的构成元素发表具体意见：

(a) 数个资讯科技相关团体留意到，建议的非法干扰电脑数据罪一经循公诉程序定罪，最高刑罚为监禁 14 年（见建议 16(c)）。鉴于刑罚甚重，这些团体认为"恶意"应是建议的干扰罪的所需元素。

(b) 香港律师会指出，不清楚为何"罔顾后果"的规定属恰当或相关。该回应者认为，如某人想到要干扰储存于某电脑的数据，必然有"意图"这样做。举例来说，该人会预先计划，获取所需工具（软件），把握机会取用该电脑，把数据拿到手，再加以更改或删除。香港律师会认为这些行动需要透过*"一连串故意行为"*来进行。

(c) 某政府部门建议，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。该回应者引用以下其他司法管辖区的例子，指出它们的法律条文明确提及损害国家安全：

(i) 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》**）订明，被告人的作为如导致国家安全严重损害，或产生导致该损害的重大风险，最高刑罚为终身监禁。[3] 被告人如就某电脑作出未获授权的作为，而该作为导致*"对任何国家的国家安全的损害"*，或产生导致该损害的重大风险，[4] 一经循公诉程序定罪，最高刑罚为监禁 14 年或罚款，或两者兼处。[5]

---

3 咨询文件第 4.41 段。第 3ZA(7)条的内容如下：

"如任何人——

……

(b) 因导致国家安全严重损害的作为而干犯［第 3ZA 条］所订罪行，或因产生导致该损害的重大风险的作为而干犯该罪行，

则该人一经循公诉程序定罪，可处终身监禁或罚款，或两者兼处。"（底线后加）

4 咨询文件第 4.41 段。第 3ZA 条相关条款的内容如下：

"(1) 任何人在以下情况，即属犯罪——

(a) 该人就某电脑作出任何未获授权的作为；

(b) 该人在作出该作为时，知悉该作为未获授权；

(c) 该作为导致关键性严重损害，或产生导致关键性严重损害的重大风险；及

(d) 该人意图藉作出该作为而导致关键性严重损害，或罔顾会否导致上述损害。

(2) 就本条而言，损害如属——

……

(d) 对任何国家的国家安全的损害，

即属'关键性'损害。"（底线后加）

5 《英格兰误用电脑法令》第 3ZA(6)条。

(ii) 新加坡《误用电脑法令》（Computer Misuse Act，**《新加坡误用电脑法令》**）第 11 条把最重的最高刑罚预留给涉及取用"受保护电脑"的案件。某电脑须视为"受保护电脑"，前提是干犯该罪行的人知悉或理应知悉有关电脑、程式或数据是在与*"新加坡的安全、防务或国际关系"*有直接关连的情况下使用的，或对*"新加坡的安全、防务或国际关系"*属必要的。[6]

我们的分析及回应

非法干扰电脑数据的罪行元素

恶意

4.14 我们希望指出，"恶意"是表达犯罪意念的陈旧用语，常见于较早期的法例。正如时任的上诉法院常任法官迪普洛克（Diplock LJ）在 *R v Mowatt* 所指出，[7] *"'非法及恶意'是 1861 年英国国会法律草拟人员的流行用词"*，[8] 旧法例《1861 年恶意损坏法令》（Malicious Damage Act 1861）正是于当年制定。

4.15 在刑事法中，"恶意"的涵义是有实际意图造成某种特定伤害，并事实上造成了该种伤害，或罔顾该种伤害是否应当发生（即被控人已预见可能会造成该种伤害，但仍然冒这风险行事），[9] "恶意"并不要求对受伤害的人怀有敌意。这项诠释解释了为何英格兰及威尔斯法律委员会（Law Commission of England and Wales）在检讨关于损坏财产的罪行时，发现难以处理"恶意"一词，导致后来制定了《1971 年刑事损坏法令》（Criminal Damage Act 1971，香港的刑事损坏罪亦以该法令为蓝本）：

> "因此，我们认为目前所需的相同元素应予保留，但同时应将该等元素表达得更加简洁清晰。我们尤其倾向避免使用'恶意地'一词，无非是由于其字眼会令人以为，这项意念元素有异于其他规定须怀有传统犯罪意念的

---

6 《新加坡误用电脑法令》第 11(2)(a)条。第 11 条载于咨询文件第 4.68 段。

7 [1968] 1 QB 421.

8 同上，第 425 页。

9 *Archbold Hong Kong 2025*，第 16−35 段，引用 *R v Cunningham* [1957] 2 QB 396；41 Cr App R 155 及其后发展（见下文进一步讨论）。亦见*香港特别行政区 诉 钟志辉*[2014] 3 HKLRD 538，第 26 段。

罪行所施加的意念元素。从 *R v Cunningham* 及 *R v Mowatt* 等案例可见，该词可能会造成诠释上的困难……"[10]

（底线后加）

4.16 考虑到上述问题，保留建议 6(b)(ii)的犯罪意念元素是恰当的，即*"须怀有意图或罔顾后果，但无须怀有恶意"*。

罔顾后果

4.17 正如在本章较前部分所见，[11] "意图"及"罔顾后果"是现有《刑事罪行条例》第 60(1)条就刑事损坏罪所订的替代犯罪意念元素，而凭借第 59(1)(b)及(1A)条，刑事损坏罪的现行法定框架适用于*"误用电脑"*。因此，建议 6 在建议采纳第 60 条的现行制度时，亦同样采纳"意图"及"罔顾后果"作为建议的非法干扰电脑数据罪的意念元素。

4.18 我们留意到，某些其他司法管辖区的电脑网络罪行法例亦一并采纳"罔顾后果"与"意图"作为意念元素。这些法例包括：

(a) 澳大利亚《刑事法典》（联邦）（Criminal Code (Cth)）第 477.2 条（*"在未获授权下修改数据，以导致损害"*）；[12]

(b) 《英格兰误用电脑法令》第 3 条（*"作出未获授权的作为，并意图损害或罔顾是否会损害电脑的操作等"*）[13] 及

---

10 英格兰法律委员会，*Criminal Law Report on Offences of Damage to Property*（1970 年），英格兰法律委员会第 29 号，第 44 段。

11 第 4.8 及 4.10 段。

12 咨询文件第 4.23 段。《刑事法典》（联邦）第 477.2(1)条规定，*"任何人在以下情况，即属犯罪：*

(a) 该人导致在未获授权下修改存于某电脑内的数据；及

(b) 该人知悉该项修改未获授权；及

(c) 该人罔顾该项修改是否损害或会否损害：

(i) 对存于任何电脑内的该等数据的取览，或对存于任何电脑内的任何其他数据的取览；或

(ii) 上述数据的可靠性、保安或操作。"（底线后加）

13 咨询文件第 4.38 段。《英格兰误用电脑法令》第 3(1)条规定，*"任何人在以下情况，即属犯罪——*

(a) 该人就某电脑作出任何未获授权的作为；

(b) 该人在作出该作为时，知悉该作为未获授权；及

(c) 下文第(2)款或第(3)款适用。"

第 3(2)条述明，*"如上述人士意图藉作出有关作为而……则本款适用。"*

第 3(3)条述明，*"如上述人士罔顾有关作为是否会造成上文第(2)款(a)至(d)段所述的任何事宜，则本款适用。"*（底线后加）

第 3ZA 条（*"作出未获授权的作为而导致严重损害或产生导致严重损害的风险"*）；[14] 及

(c) 新西兰《1961 年刑事罪行法令》（Crimes Act 1961）第 250(2) 条。[15]

4.19 在刑事法中，"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。[16] 这项对罔顾后果的诠释适用于整体刑事法，而非仅适用于电脑网络罪行。正因如此，被告人的作为在甚么情况下发生，本身并非充分理据，支持排除以罔顾后果为理由而引用建议的非法干扰电脑数据罪。

4.20 事实上，不少刑事罪行一并采纳"罔顾后果"与"意图"或"知悉"作为过失元素。以下是数个例子：

(a) 根据《刑事罪行条例》（第 200 章）第 118(3)条，任何人与女子非法性交，而该女子对此并不同意，他亦*"知道"*该女子并不同意性交，或*"罔顾"*该女子是否对此同意，即属强奸。在现实中，强奸罪的检控理由，通常是被告人罔顾受害人是否同意性交（例如受害人喝醉，无能力给予同意）；

(b) 如任何人藉作出任何*"欺骗"*（不论是*蓄意或罔顾后果地作出*）并意图诈骗而诱使另一人作出任何作为或有任何不作为，而导致该另一人以外的任何人获得利益，或该进行诱使的人以外的任何人蒙受不利或有相当程度的可能性会蒙受不利，即属犯欺诈罪；[17]

---

14 咨询文件第 4.41 段。《英格兰误用电脑法令》第 3ZA(1)条规定，*"任何人在以下情况，即属犯罪——*

(a) 该人就某电脑作出任何未获授权的作为；

(b) 该人在作出该作为时，知悉该作为未获授权；

(c) 该作为导致关键性严重损害，或产生导致关键性严重损害的重大风险；及

(d) 该人意图藉作出该作为而导致关键性严重损害，或罔顾会否导致上述损害。"（底线后加）

15 咨询文件第 4.50 段。《1961 年刑事罪行法令》第 250(2)条规定，*"任何人知悉自己未获授权或罔顾自己是否已获授权，而蓄意或罔顾后果地在未获授权下——*

(a) 损坏、删除、修改或以其他方式干扰或损害任何电脑系统内的任何数据或软件；或

(b) 导致任何电脑系统内的任何数据或软件被损坏、删除、修改或以其他方式受到干扰或损害；……

可处为期不超过 7 年的监禁。"（底线后加）

16 *Archbold Hong Kong 2025*，第 16−40 段，讨论就刑事损坏罪作出判决的 *R v G* [2004] AC 341 及其后的法理发展。

17 《盗窃罪条例》（第 210 章）第 16A 条。

(c) 以欺骗手段取得财产罪亦有类似的过失元素，该罪行是指任何人以欺骗手段（不论是*蓄意或是罔顾后果*）而不诚实地取得属于另一人的财产，意图永久地剥夺该另一人的财产；[18] 及

(d) 根据《证券及期货条例》（第 571 章）第 295(1)条，任何人如*"意图"*使某事情具有或相当可能具有造成在认可市场交易的证券或期货合约交投活跃的虚假或具误导性表象的效果，或*"罔顾"*某事情是否具有或相当可能具有造成该表象的效果，即属犯虚假交易的罪行。

4.21 此外，"罔顾后果"这概念强调人们应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）。

4.22 基于上文所解释的理由，我们建议保留"罔顾后果"这项元素，与"意图"一同作为非法干扰电脑数据罪的过失元素。

加重形式的干扰罪应否明确涵盖危害国家安全行为？

4.23 首先，值得我们仔细考虑的是，于 2020 年 6 月 30 日制定为全国性法律，并在香港公布实施的《中华人民共和国香港特别行政区维护国家安全法》（**《国安法》**），在多大程度上已涵盖建议的非法干扰电脑数据罪及／或非法干扰电脑系统罪。

4.24 《国安法》的罪行条文主要着重具体说明威胁国家安全的受禁活动、从事这些活动的人所怀目的及这些活动的影响。受禁活动的进行方式（例如在现实世界还是电脑网络空间进行），就《国安法》而言相对无关重要。

4.25 然而，《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。第二十四条述明：

> "为胁迫中央人民政府、香港特别行政区政府或者国际组织或者威吓公众以图实现政治主张，组织、策划、实施、参与实施或者威胁实施以下造成或者意图造成严重社会危害的恐怖活动之一的，即属犯罪：
>
> ……

[18] 同上，第 17 条。

（三）破坏交通工具、交通设施、电力设备、燃气设备或者其他易燃易爆设备；

（四）严重干扰、破坏水、电、燃气、交通、通讯、网络等公共服务和管理的电子控制系统；

（五）以其他危险方法严重危害公众健康或者安全。”

（底线后加）

4.26 我们已仔细考虑干扰电脑数据（以及干扰电脑系统）的加重罪行应否明确涵盖危害国家安全行为，与《国安法》有关的法律及实际考虑因素如下：

(a) 《国安法》地位超然，理应必然凌驾所有其他本地法例，包括我们所建议制定的针对电脑网络罪行的特定法例。倘若电脑网络罪行同时符合《国安法》所订罪行的元素，我们预料援引《国安法》应属执法机关、检控机关及法庭的首要考虑。

(b) 如《国安法》已涵盖非法干扰电脑数据罪及／或非法干扰电脑系统罪，加重形式的干扰罪又再特别提述危害国家安全行为，就可能会显得多余。尽管如此，我们留意到第二十四条所订罪行有非常特定的意图——被告人必须造成或意图造成严重社会危害，并怀有特定意图，为胁迫中央人民政府、香港特别行政区（“**香港特区**”）政府或者国际组织或者威吓公众以图实现政治主张。

(c) 《国安法》以概括的措辞表达。《国安法》的其他条文（即明确提述互联网电子控制系统的第二十四（四）条[19] 以外的条文）强调受禁活动的目的及影响，范围似乎相当广阔，足以涵盖非法干扰电脑数据（以及非法干扰电脑系统）的作为。例如：

(i) 第二十四（三）条没有提及被告人可藉甚么方式“破坏”该条所述的各项公用设施。由于第二十四（三）条着眼于受禁行为（即“破坏”），该条似乎适用于任何会导致破坏指明公用设施的作为，包括非法干扰与

[19] 上文第 4.25 段。

相关公用设施有关的电脑数据及/或电脑系统而造成破坏。

(ii)《国安法》第二十四（五）条是一项包含一切的条文，涵盖所有严重危害公众安全的危险活动，其重点规定在于有关方法的性质，即必须是危险方法。由于电脑网络罪行与现实世界的罪行均可符合这项规定，第二十四（五）条看来相当广阔，足以涵盖非法干扰电脑数据罪及非法干扰电脑系统罪（"**干扰罪**"）。

(d) 第二十四条所订罪行设有两层罚则。如被告人致人重伤、死亡或者使财产遭受重大损失，刑罚为无期徒刑或者十年以上有期徒刑。这项《国安法》所订的最高刑罚较重，与非法干扰电脑系统的加重罪行的最高刑罚相称，后者建议判处终身监禁。[20] 在其他情形下，较轻的刑罚（即三年以上十年以下有期徒刑）适用于第二十四条所订罪行。

4.27 尤其是因为《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。国家安全至关重要，我们预料在《国安法》下订立国家安全相关罪行时，已充分考虑该等罪行须以电脑网络中立的措辞来拟订，并据此解释，但如《国安法》的文本、文意和目的显示相反情况，则属例外。我们意识到，若然没有政府对国家安全实体法律整体立场的全面观点，则分析建议干扰罪的加重罪行会有欠完整。

4.28 2024年3月，立法会制定《维护国家安全条例》（"**《基本法》第二十三条立法**"），以全面落实《基本法》第二十三条、《全国人民代表大会关于建立健全香港特别行政区维护国家安全的法律制度和执行机制的决定》，以及《国安法》所规定的宪制责任及义务，并有效应对现今及日后可能出现的国家安全风险和威胁。[21]

4.29 《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）；[22] 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

---

20 最终建议16(c)(ii)。至于非法干扰电脑数据及电脑系统的基本罪行，建议刑罚为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。

21 《立法会參考资料摘要——维护国家安全条例草案》（2024年3月）。

22 《维护国家安全条例》第49条（危害国家安全的破坏活动）。

作为。[23] 就后一项罪行而言，政府于2024年1月发表的咨询文件解释背后理据如下：

> "本文件中所讨论的建议罪行，基本上并不取决于犯罪者实际上采用了哪种特定的方法或技术实施犯罪行为，因此应涵盖大部分透过电脑进行的危害国家安全的行为和活动。另一方面，由于电脑或电子系统科技非常普及且发展迅速，例如人工智能技术正广泛应用于社会上不同的领域，其蕴含的潜在国家安全风险不容忽视，特别是电脑或电子系统遭受入侵或干扰而引起的风险。为应对现时电脑或电子世界及未来可能出现的新技术所带来的国安风险，建议引入罪行，打击对电脑或电子系统作出危害国家安全的行为。"[24]

4.30 终审法院裁定，《国安法》第四十二（二）条[25] 提述的*"危害国家安全行为"*，是指任何根据其性质可构成违反《国安法》或香港特区法例中维护国家安全的罪行的行为。[26] 因此，《国安法》的特定程序规则（包括在保释、[27] 陪审团审讯、[28] 海外律师参与案件[29] 及判刑[30] 方面的规则），应用范围并不局限于《国安法》所订罪行。

---

23 同上，第50条（就电脑或电子系统作出危害国家安全的作为）。

24 香港特别行政区政府保安局，《维护国家安全：〈基本法〉第二十三条立法公众咨询文件》（2024年1月），第6.5段。

25 《国安法》第四十二条规定：
"对犯罪嫌疑人、被告人，除非法官有充足理由相信其不会继续实施危害国家安全行为的，不得准予保释。"

26 *香港特别行政区 诉 黎智英*（*HKSAR v Lai Chee Ying*）[2021] HKCFA 3，(2021) 24 HKCFAR 33（判决日期：2021年2月1日及9日），第53(c)(ii)及70(d)(ii)段。

27 同上，第53(a)及(b)段。终审法院指出，《国安法》第四十二（二）条*"订下的门槛要求严格得多"*，原因是有利于保释的假定已即时被排除——根据《国安法》，此条文开宗明义说不得准予保释，除非法官有充足理由相信被控人不会继续实施危害国家安全行为。终审法院亦注意到，国安法第四十二（二）条的主题内容，与《刑事诉讼程序条例》（第221章）第9G(1)(b)条的主题内容重迭：两者均以被控人可能在保释期间犯罪的风险为拒绝保释的基础。

28 《国安法》第四十六条规定：
"对高等法院原讼法庭进行的就危害国家安全犯罪案件提起的刑事检控程序，律政司长可基于保护国家秘密、案件具有涉外因素或者保障陪审员及其家人的人身安全等理由，发出证书指示相关诉讼毋须在有陪审团的情况下进行审理……。"

29 在*香港特别行政区 诉 黎智英*（*HKSAR v Lai Chee Ying*）[2023] HKCFI 1440（判决日期：2023年2月2日及29日），原讼法庭裁定在《基本法》第三十五条下并无"选择律师"的绝对权利。"选择律师"的权利只不过是指诉讼人可从可供选择的律师当中自由选择代表律师。任何人均无权坚持由在香港不具一般执业资格的律师作为代表（见第75及87段）。

30 在*香港特别行政区 诉 吕世瑜*（*HKSAR v Lui Sai Yu*）[2023] HKCFA 26（判决日期：2023年8月22日），终审法院裁定，《国安法》第二十一条就情节严重的案件订明*"五年以上……有期徒刑"*的罚则，属强制性规定。因此，下级法院不以上诉人认罪为由，全数扣减三分一刑期，做法是恰当的，因为扣减三分一刑期会导致最终刑期低于《国安法》第二十一条订明的较高幅度下限（见第66及76段）。

如某人干犯干扰罪的方式亦构成《国安法》或《基本法》第二十三条立法所订罪行，《国安法》所规定的程序规则即告适用。

4.31 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，从而考虑我们的建议，以研究应否建议任何可完善之处（假如政府日后决定接纳我们的建议，在针对电脑网络罪行的特定法例中引入新的干扰罪）。

特定的免责辩护

考虑适用于取览罪的免责辩护

4.32 正如本章开首所解释，[31] 取览程式或数据通常于干扰电脑数据前发生，因此非法干扰电脑数据罪与取览罪息息相关。有见及此，我们已并行探讨取览罪与非法干扰电脑数据罪（以及非法干扰电脑系统罪）的免责辩护，以确保我们所建议的法律是一致的。当然，随着科技进步，将来或可能无须取览任何程式或数据，已可干扰电脑数据（或电脑系统），但我们认为这点不应影响我们分析这两项罪行的接近程度，因为在一般情况下，取览程式或数据都会在干扰数据前发生。

4.33 在本报告书第 2 章，我们回应受咨询者对取览罪的"合理辩解"一般免责辩护所提出的意见时，[32] 已解释在电脑网络罪行法例加入特定的免责辩护有何好处。概括而言，这些特定的免责辩护可预防日后出现关于某项作为是否构成"合理辩解"的争议。毕竟，"合理辩解"这概念不易为外行人所理解，而且可作不同诠释。订立特定的免责辩护，能使公众有所依从，了解哪些行为属可接受，从而令法律更加清晰。

为网络安全目的而干扰电脑数据

4.34 在第 2 章，我们建议，就在未获授权下为网络安全目的而取览订定特定的免责辩护，其条件如下：[33]

(a) 该项免责辩护应只适用于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）。

---

31 第 4.4 段。

32 第 2.32 至 2.34 段。

33 第 2.63 至 2.74 段。

(b) 被告人必须为真正的网络安全目的而行事。

(c) 在顾及整体情况后，被告人的行为必须是合理的。

4.35 由于干扰电脑数据（或电脑系统）通常只会在取览程式或数据后发生，为非法干扰电脑数据罪（以及非法干扰电脑系统罪）提供类似的免责辩护，是合乎逻辑且连贯一致的做法。因此，我们建议，就建议的非法干扰电脑数据罪而言，为网络安全目的而干扰电脑数据应可作为免责辩护。

为保障儿童或易受伤害人士的利益而干扰电脑数据

4.36 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，按照常理，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。

4.37 因此，我们认为，与取览罪不同，无须为保障儿童或易受伤害人士的利益而就非法干扰电脑数据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

4.38 同样地，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，与取览罪不同，我们认为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

4.39 正如本章开首所概述，[34] 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”（于上文第 4.11 段引述）。

4.40 在本报告书第 2 章，[35] 我们已解释这两项“合法辩解”（分别称为同意免责辩护及保护财产免责辩护）也应适用于取览罪。

4.41 就非法干扰电脑数据罪（以及非法干扰电脑系统罪）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，我们认

---

34 第 4.1 段。

35 第 2.95 至 2.99 段。

为适宜维持建议 6，但须在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 2.101 段所讨论的取览罪一样）：

(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干扰有关电脑数据（或电脑系统）；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。

4.42 换言之，我们建议在针对电脑网络罪行的特定法例加入非法干扰电脑数据罪（以及非法干扰电脑系统罪），而《刑事罪行条例》第 64(3)条不适用于该等罪行。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非法干扰电脑数据罪（以及非法干扰电脑系统罪）所建议的其他特定免责辩护看齐，即所有免责辩护均采用"合理性"要求，以确保一致。与取览罪的免责辩护一样，我们相信这种处理方法可避免各项免责辩护被滥用，并体现我们的指导原则：一方面平衡兼顾网民的权利和资讯科技业内人士的权益，另一方面亦保障公众在使用电脑系统时免受骚扰或攻击的权益和权利。

4.43 经检视第 64(2)条，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。因此，我们曾考虑，就非法干扰电脑数据罪（以及非法干扰电脑系统罪）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。

4.44 我们倾向认为，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。我们相信，在保护生命这方面不设明文订定的特定免责辩护，或可留给法庭更大的回旋余地，处理人命攸关的情况。因此，我们赞成在这方面维持第 64(2)(b)条的现状。相同的原则及理据亦适用于第 2 章所讨论的取览罪。

有关建议 6 的结论

4.45 概括而言，我们的结论是建议 6 可予保留，但建议就非法干扰电脑数据罪而对第 64(2)条作出改进，并将为网络安全目的而干扰数据加入为免责辩护。

最终建议 6

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

引言

5.1　本章讨论关于咨询文件建议 7 及 8 的回应。建议 7 建议订立第四类依赖电脑网络的罪行，即非法干扰电脑系统：

> “小组委员会建议：
>
> (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) 在软件生产时，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系统。”

5.2　正如咨询文件所解释，[1] 概括而言，非法干扰电脑系统罪旨在：

(a) 禁止藉使用或干扰电脑数据，阻碍合法使用电脑系统；

(b) 从而确保电脑系统能正常运作。

---

[1] 第 5.1 段。

香港的现行法律

5.3 鉴于非法干扰电脑数据罪与非法干扰电脑系统罪（"**干扰罪**"）息息相关，本章会在第 4 章讨论的基础上再作探讨。正如第 4 章所述，[2] 根据《刑事罪行条例》（第 200 章）第 60 条，刑事损坏的其中一种形式是"误用电脑"。第 59(1A)条把该词界定为：

> "(a) 导致电脑并非如其拥有人或其拥有人代表对其所设定的运作方式运作，即使如此误用不会令该电脑的操作、该电脑内的程式或该电脑内的资料的可靠性减损亦然；
>
> (b) 更改或删抹电脑内或电脑储存媒体内的程式或资料；
>
> (c) 在电脑或电脑储存媒体所收纳的内容上增加程式或资料，
>
> 而造成导致(a)、(b)或(c)段所提述的任何类别误用情形的任何作为，须视为导致该项误用情形的作为。"

这三个部分中，第 59(1A)(a)条与建议的非法干扰电脑系统罪最为相关。

5.4 正如小组委员会在咨询文件解释，[3] 非法干扰电脑系统可能以分布式拒绝服务攻击这形式进行，其定义是：*"蓄意从多台独立电脑同时向某电脑网络发送大量数据，藉此瘫痪该电脑网络"*。[4] 分布式拒绝服务攻击通常藉一组被入侵的电脑发动，这组电脑称为"殭尸网络（botnet）"。如寄存有关网页的伺服器的容量不足，未能回应大量电脑同时发出的相同请求，该伺服器就可能没有反应、崩溃或发生其他故障。

---

2 第 4.10 段。

3 第 5.3 及 5.4 段。

4 https://www.cpaaustralia.com.au/tools-and-resources/cyber-security/cyber-threats-introduction（于 2025 年 11 月 1 日浏览）。

对小组委员会建议 7 的回应

5.5 由于建议的非法干扰电脑系统罪与非法干扰电脑数据罪息息相关，对建议 7 的回应与对建议 6 的大致相似，我们已在第 4 章讨论对建议 6 的回应。

5.6 绝大多数回应者表示支持建议 7，当中香港与内地法律专业联合会有限公司及香港女律师协会有限公司（"**女律师协会**"）同意《刑事罪行条例》的现行制度行之有效，而"误用电脑"这概念足以涵盖干扰电脑系统的作为。因此，女律师协会同意建议 7，认为关于非法干扰电脑系统及非法干扰电脑数据的条文，应采用一致的措辞。

罔顾后果作为建议罪行的犯罪意念元素之一

5.7 正如建议 6，多名就建议 7 提供意见的回应者，要求澄清是否会将"罔顾后果"纳入为建议的非法干扰电脑系统罪的意念元素之一。数个资讯科技相关机构提出，建议的罪行应只在有"犯罪意图"的情况下才产生，而且应摒弃建议 7 的"罔顾后果地"这项元素。

5.8 读者会记得咨询文件的建议 7(d)列出数个例子，说明建议的非法干扰电脑系统罪如何应用。这些例子包括在生产软件时，某人"蓄意"或"罔顾后果地"在软件编入缺损程式。[5] 两个资讯科技相关团体指出，缺损程式在电脑软件、电脑应用程式及器材十分常见。其中一个团体认为，程式开发人员推出尚未成熟的新发明，便可能导致缺损程式出现。由于测试受时间及资源所限，即使识别出保安问题，当中有些问题在程式推出前未获软件开发人员纠正，也不足为奇。该回应者询问，在这种情况下，软件开发人员会否须就建议的罪行负上法律责任。

5.9 与此同时，香港律师会认为，对罔顾后果地向电脑系统发送大量数据的行为施加刑事法律责任，需要更全面分析相关的法律依据。该专业团体引用的例子，是歌迷在网上争相抢购演唱会门票。

---

[5] 建议 7(d)(ii)。

我们的分析及回应

一致处理干扰数据及干扰系统

5.10 我们已在第4章分析以"罔顾后果"作为建议的非法干扰电脑数据罪的替代犯罪意念元素，由于干扰罪相当近似，有关分析亦同样适用于回应者就建议7所提出的意见。[6]

5.11 概括而言，"意图"及"罔顾后果"是现有《刑事罪行条例》第60(1)条刑事损坏罪的替代犯罪意念元素，而凭借第59(1)(b)及(1A)条，刑事损坏罪的现行法定框架适用于*"误用电脑"*。因此，建议7建议采纳第60条的现行制度，以一致处理非法干扰电脑系统及非法干扰电脑数据，亦同样采纳"意图"及"罔顾后果"作为建议的非法干扰电脑系统罪的意念元素。

5.12 我们重申在第4章提出的观点："罔顾后果"是常见且确立已久的刑事罪行过失元素。"罔顾后果"这概念要求证明被告人察觉某特定风险，而在被告人所知的情况下，承担该风险并不合理。[7] 这项对罔顾后果的诠释适用于整体刑事法，而非仅适用于电脑网络罪行。至于被告人在某特定情境下干扰有关电脑系统是否罔顾后果（例如在网上购买演唱会门票，或是开发机械人显微手术所用的软件，这两种情况可以大为不同），最终须由法庭根据个别案件的证据，并针对整体情况来进行评估及评定。因此，被告人的作为在甚么情况下发生，本身并非充分理据，支持排除以罔顾后果为理由而引用建议的罪行。

5.13 恰当理解上文所解释的"罔顾后果"概念后便会明白，程式开发人员大致知悉软件存在缺损程式或缺陷，这一点本身并不足以确立干扰罪所需的犯罪意念元素。"罔顾后果"的门槛及所代表的罪责，比纯粹不小心或一般疏忽为高。在开发软件的情境中，多项因素与法庭评定甚么行为会构成罔顾后果固然相关，例如软件开发人员在质素保证方面是否遵照业界标准。众所周知，在软件开发期间，难免会出现一些合理地预期的缺损程式或缺陷。因此，某人购买或以其他方式取得某程式或软件，可视为同意有关产品内一般会存有可能造成不便的瑕疵，甚至是可合理容忍的保安漏洞。正因如此，《刑事罪行条例》第64(2)条的同意免责辩护可能有机会适用，从而免除程式开发人员

---

6 我们的分析载列于第4.17至4.22段。

7 *Archbold Hong Kong 2025*，第16–40段。

负上非法干扰电脑系统罪的法律责任，而我们亦建议在新订的电脑网络罪行法例中为干扰罪纳入这项免责辩护。[8]

5.14 基于以上理由，我们建议保留"罔顾后果"这项元素，与"意图"一同作为非法干扰电脑系统罪的过失元素。总括而言，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，我们亦保留这项建议。

有关建议 7 的结论

5.15 基于上述所有理由，加上考虑到绝大多数回应者均支持订立非法干扰电脑系统罪（以及非法干扰电脑数据罪），我们的结论是建议 7 可予保留。

最终建议 7

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

[8] 上文第 4.39 段。我们亦建议，《刑事罪行条例》第 64(2)条所示的免责辩护应适用于第 2 章所讨论的非法取览程式或数据罪（见上文第 2.95 至 2.97 段）。

(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。**

对小组委员会建议 8 的回应

5.16 咨询文件建议 8(a)及(b)就以下议题征询意见：

"(a) 就建议的非法干扰电脑系统罪而言，如网络安全专业人员在目标电脑的拥有人并不知情或没有给予授权的情况下，在互联网扫描（或以类似的形式测试）某电脑系统，例如评估潜在的保安漏洞，应否属合法辩解？

(b) 就建议的非法干扰电脑系统罪而言，非保安专业人员应否有合法辩解，例如：

(i) 由机械人进行网页抓取（web scraping）或由互联网资讯收集工具（例如搜寻器）启动网络爬虫（web crawlers），从而藉着连接指定的协定埠（例如 RFC6335 所界定的连接埠），在未获授权下从伺服器收集数据；及／或

(ii) 为以下目的，扫描服务供应商的系统（从而有可能令该系统被滥用或被拖垮）：

(1) 为保障他们自身安全，找出任何保安漏洞（例如他们在以私人身分提供信用卡资料进行交易前，找出信用卡交易的加密是否安全）；或

(2) 确保该服务供应商系统所提供的应用程式界面（Application Programming Interface）安全和完整？"

建议 8(a)

5.17 明显大多数的回应者均明确同意为网络安全专业人员扫描（或以类似的形式测试）电脑系统提供免责辩护。部分回应者则认为无须提供这项免责辩护，并指出网络安全专业人员如没有清晰草拟的合约，不大可能会提供安全扫描、评估或其他服务。

5.18 香港大律师公会表示：

> “由于网络安全专业人员及非保安专业人员可对电脑系统进行各种合法行为，以使用该系统内的选定资料或观察所得（如识别系统漏洞），要是试图详尽无遗地界定在建议的罪行下可构成‘合法辩解’的行为种类，并不可取……这种处理方法使法律具备必要的弹性，以便按每宗个案的情况来考虑被告专业人员的行为，使法庭得以在更多样的情境中考虑这项免责辩护。”

建议 8(b)

5.19 相类于建议 8(a)，明显大多数的回应者均支持为非保安专业人员提供免责辩护。

5.20 消费者委员会认为：

> “网页抓取和网络爬虫（web crawling）可在互联网上收集公开数据，在香港及世界各地甚为普遍。举例来说，谷歌（Google）使用网络爬虫为其搜寻器建立网页索引。全面禁止使用网页抓取和网络爬虫在互联网上收集公开资料，或会阻碍用作改善市场透明度、帮助消费者作出知情的消费选择，以及加强消费者保障的调查与研究（不论该调查与研究以商业、存档、新闻报道、学术或咨询为目的）。”

5.21 此外，消费者委员会在回应中述明，有关数据可能受版权、网站使用条款规限，或载有个人资料，在相应范围内收集及／或使用该等数据会受版权法、合约法及私隐法规管。如收集该等数据的方式或方法并不合法，有关行为可能会干犯建议的依赖电脑网络罪行。

5.22 再者，由于“网页抓取”可包括“数据抓取（data scraping）”（即某电脑程式从另一程式所产生的输出中提取数据），个人资料私隐专员公署指出，只有“经同意”或“合法”干扰电脑系统才应构成建议罪行的免责辩护，这是因为根据该署的执法经验：

> “数据抓取所收集的个人资料，有时会在资料当事人并不知情且没有给予同意的情况下在暗网出售，而抓取本身已构成资料外泄事故。为加强网络安全，我们认为未获授权的网页抓取（包括数据抓取）及对服务供应商

系统的未获授权扫描，均应受建议的罪行所涵盖，只有经同意或合法干扰电脑系统，方可构成免责辩护……”

我们的分析及回应

建议 8(a)：特定的免责辩护

为网络安全目的而干扰电脑系统

5.23 在第 4 章，[9] 我们建议，就建议的非法干扰电脑数据罪而言，为网络安全目的而干扰电脑数据应可作为免责辩护，其条件如下：

(a) 该项免责辩护应只适用于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）。

(b) 被告人必须为真正的网络安全目的而行事。

(c) 在顾及整体情况后，被告人的行为必须是合理的。

5.24 由于两项干扰罪息息相关，我们同样建议，就建议的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。因此，如符合上一段所述的条件，在互联网扫描（或以类似的形式测试）电脑系统并不属犯法。

为保障儿童或易受伤害人士的利益而干扰电脑系统

5.25 正如第 4 章所解释，[10] 我们认为无须为保障儿童或易受伤害人士的利益而就非法干扰电脑数据罪提供特定的免责辩护，理由如下：首先，取览程式或数据本身并不会导致电脑数据受到干扰；其次，容许某人取览程式或数据，并不表示该人获授权干预有关数据。

5.26 由于上述逻辑亦适用于干扰电脑系统的情况，我们认为无须为保障儿童或易受伤害人士的利益而就非法干扰电脑系统罪设置特定的免责辩护。

---

9 我们的分析载列于第 4.34 及 4.35 段。

10 第 4.36 及 4.37 段。

为真正的研究目的而干扰电脑系统

5.27 与干扰电脑数据一样，若从事真正研究需要干扰电脑系统，我们认为是匪夷所思的。因此，我们认为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系统行为。

改列《刑事罪行条例》第 64(2)条的免责辩护

5.28 我们重申上文第 4.39 至 4.44 段的分析。概括而言，将《刑事罪行条例》第 64(2)条的免责辩护改列于新订的电脑网络罪行法例时，我们建议就非法干扰电脑系统罪而对同意免责辩护及保护财产免责辩护作出以下改进：

(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干扰有关电脑系统；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。

建议 8(b)：无须为非保安专业人员建议免责辩护

5.29 除网络安全专业人员外，我们留意到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。正如咨询文件建议 8(b)所提及，这些活动的例子包括网页抓取（即利用电脑自动程式〔bots〕从网站提取内容及数据的过程）及网络爬虫（即为建立索引而有系统地浏览网页的电脑自动程式）。

5.30 受惠于专家意见，小组委员会进一步了解到，正常使用电脑系统必然会产生流量。举例来说，支援通讯平台（如 WhatsApp 及 Telegram）的应用程式界面会充当中介层，处理电脑系统之间的数据传输，从而使公司可向第三方开放其应用数据及功能。

5.31 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，尤其是当我们考虑到科技发展步伐之快，情况更是如此。因此，我们同意小组委员会在咨询文件表达的观点，即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。举例来说，我们一般并不预期网上用户在向传送对象（即另一网上用户）发送电邮或展示网页广告前，须事先寻求后者的明示授权，尤其是当有关发送或展示并非恶意作出。另一例子是，

搜寻器会使用称为网络爬虫的软件，定期探测互联网，以寻找网页并将它们添加至索引。[11]

5.32 关于建议为非保安专业人员提供非法干扰电脑系统罪及取览罪的免责辩护，我们有以下看法：

(1) 互联网通讯及使用电脑均需要电脑系统之间进行一定程度的互动。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。

(2) 其他国家虽然制定了非法干扰电脑系统罪及非法取览程式或数据罪，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。

5.33 鉴于上文所述，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，因为有关情况可作为事实和程度的问题来裁断，并应能够与电脑网络攻击（例如在一分钟内向某特定邮箱发送 10,000 封电邮，使邮箱及相应伺服器不胜负荷）区分开来。然而，若负责落实建议的决策局或法律草拟专员在立法阶段认为需要就此明文订定免责辩护，可在该阶段进一步探讨这议题。

最终建议 8

我们建议：

(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

11 咨询文件第 2.5 段。

(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

引言

6.1　本章讨论关于咨询文件建议 9 的回应。建议 9 涉及第五类（最后一类）依赖电脑网络的罪行，即提供或管有用作犯罪的器材或数据。

“小组委员会建议：

(a) 在新法例下，蓄意提供或管有器材或数据（不论是有形物或无形物，例如勒索软件、病毒或其源码），如制造或改装该器材或数据的目的是犯罪（即并非一定是电脑网络罪行），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或数据）及需求（例如取得、管有、购买及输入有关器材或数据）两方面。

(c) 建议的罪行应适用于：

(i) 主要用作（以客观方式界定，不论被告人的主观意图为何）犯罪的器材或数据，不论该器材或数据能否用作任何合法目的；及

(ii) 相信或声称有关器材或数据可用作犯罪的人，不论该人所信或所声称的是否属实。

(d) 在新法例下，蓄意提供或管有符合以下说明的器材或数据（不论是有形物或无形物，例如勒索软件、病毒或其源码）：

(i) 如该器材或数据能够用作犯罪，或犯罪者相信或声称该器材或数据能够用作犯罪；及

(ii) 犯罪者意图任何人将该器材或数据用作犯罪，

应构成加重罪行，而合理辩解可作为法定免责辩护。

(e) 建议的条文应以《英格兰误用电脑法令》第 3A 条，以及《新加坡误用电脑法令》第 8 及 10 条为蓝本。”

6.2 正如小组委员会在咨询文件解释，[1] 概括而言，就此主题而订立的罪行，旨在：

(a) 遏制生产、供应和管有可在电脑网络空间作非法用途的器材或数据；

(b) 藉以防止这类器材或数据被用作干犯电脑网络罪行。

6.3 如任何人实际使用器材或数据（例如对电脑进行黑客入侵），即会构成第 2 章所讨论的非法取览程式或数据罪（“**取览罪**”）的犯罪行为。本章着眼于一项独立的罪行，即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（如黑客器材），当中包括为提供该等器材、程式或数据而管有罪。

6.4 除黑客器材外，只可作有害用途的器材、程式及数据举例如下：[2]

(a) 存有勒索软件的记忆棒；

(b) 恶意软件；

(c) 病毒；

(d) 建立及管理殭尸网络的软件；及

(e) 收集软件（harvesting software），这类软件可扫描电脑来寻找特定物品（例如银行及信用卡凭证，以及其后可用作欺诈的其他数据）。

香港的现行法律

《刑事罪行条例》（第 200 章）第 62 条

6.5 正如咨询文件所解释，[3] 第 59(1A)条已订明在《刑事罪行条例》的第 VIII 部中，*“摧毁或损坏财产（to destroy or damage any property），*

---

1 第 6.1 段。
2 咨询文件第 6.2、6.10 及 6.91 段。
3 咨询文件第 6.6 段。

就电脑而言，包括误用电脑"。[4] 因此，第 VIII 部第 62 条（*"管有任何物品意图摧毁或损坏财产"*）所订的罪行，也适用于*"误用电脑"*：

> "任何人保管或控制任何物品，意图在无合法辩解的情况下使用或导致他人使用或准许他人使用该物品——
>
> (a) 以摧毁或损坏属于另一人的财产；或
>
> (b) 以摧毁或损坏该人本人或使用人的财产，而且知道所用方法相当可能会危害另一人的生命，
>
> 即属犯罪。"

6.6 然而，第 62 条有两个潜在主要问题，值得考虑法律改革：

(a) 第 62 条的英文文本用"anything"一词来描述受禁物。按照一般用语，该词并不限于有形物，且涵盖范围似乎比中文文本的对应词（"任何物品"）更广。然而，这个中文词语的惯常涵义会否明确引伸至某些无形物（例如恶意软件及有关利用漏洞〔exploit〕的专门知识），则是另一个问题。[5]

(b) 第 62 条与《刑事罪行条例》第 60 条所订的刑事损坏罪相关。对于其他条文所订罪行（例如《刑事罪行条例》第 161 条所订的*"有犯罪或不诚实意图而取用电脑"*罪），第 62 条并不适用。[6]

6.7 在上述背景下，小组委员会经考虑第 62 条及香港与其他司法管辖区的其他法例条文后，提出载于咨询文件的建议 9。

对小组委员会建议 9 的回应

6.8 与第 2 至第 5 章所介绍的另外四类依赖电脑网络的罪行相比，建议 9 在市民大众之间引发不少争论，支持与反对该建议的回应者几乎各占一半。众多回应者提出意见或观点，但没有明确表示支持或反对订立建议的罪行。

支持建议 9 的回应者的意见

---

4 《刑事罪行条例》（第 200 章）第 59(1A)(a)至(c)条中界定*"误用电脑"*。这概念与第 4 及第 5 章所讨论的非法干扰电脑数据罪及非法干扰电脑系统罪相关（见上文第 4.10 及 5.3 段）。

5 咨询文件第 6.9 及 6.10 段。

6 咨询文件第 6.16 段。

6.9 某商会认为《刑事罪行条例》第 62 条*"某程度上涵盖"*建议的罪行，该条禁止保管或控制任何物品，意图使用以摧毁或损坏财产，即干犯《刑事罪行条例》第 60 条所订的刑事损坏罪。该回应者同意小组委员会在咨询文件中的分析，指出第 62 条可能会豁除无形物（如电脑软件），无助于将该条应用于电脑网络空间。[7]

6.10 香港公司治理公会表明支持建议 9，并同意如建议 9(e)所提议，建议的罪行可用新加坡《1993 年误用电脑法令》（Computer Misuse Act 1993，**《新加坡误用电脑法令》**）第 8[8] 及 10[9] 条为蓝本。

反对建议 9 或对建议 9 另有意见的回应者的意见

6.11 多名回应者（特别是来自资讯科技界的回应者）反对订立建议 9(a)的基本罪行。他们的疑虑与其他机构（包括香港律师会及消费者委员会）的意见书互相呼应，这些意见书概括就建议的罪行提出观点。

建议罪行的基本形式性质广泛

6.12 回应者的意见书显示，主要关注点（不论意见书如何入手分析）均在于建议罪行的基本形式的广度。

管有有关器材或数据的人所怀意图

---

7 同上，第 6.9 至 6.15 段。

8 《新加坡误用电脑法令》第 8(1)条订明：

"任何人在没有权限的情况下，故意披露可取览存于任何电脑的任何程式或数据的任何密码、取用码或任何其他方法，而该人作出上述作为——

(a) 是为了不当地获益；

(b) 是为了达到任何非法目的；或

(c) 并知悉该作为相当可能会不当地导致任何人蒙受损失，

即属犯罪。"

9 《新加坡误用电脑法令》第 10 条订明：

"(1) 任何人在以下情况，即属犯罪——

(a) 该人取得或保留本条适用的任何物品——

(i) 并意图将该物品用作干犯或用作利便干犯第 3、4、5、6 或 7 条所订罪行；或

(ii) 以藉任何方式使该物品被供应或提供用作干犯或利便干犯任何该等罪行；或

(b) 该人以任何方式制造、供应、要约供应或提供本条适用的任何物品，意图使该物品用作干犯或用作利便干犯第 3、4、5、6 或 7 条所订罪行。

(2) 本条适用于以下物品：

(a) 经设计或改装以主要用作干犯第 3、4、5、6 或 7 条所订罪行的任何器材（包括电脑程式），或可用作干犯第 3、4、5、6 或 7 条所订罪行的任何器材（包括电脑程式）；

(b) 可藉以取用整台电脑或其任何部分的密码、取用码或类似数据。"

6.13 香港律师会认为，按照建议 9(a)至(e)而拟定的建议罪行：

> “极为广泛，而检控门槛甚低……根据有关建议，管有可能被改装以用作犯罪（并非一定是电脑网络罪行）的有形或无形数据，即属犯罪。任何人如相信有关数据可用作犯罪，便会犯法。”

6.14 该专业团体举出以下假设例子作说明：

> “……假如某方（甲方）交给另一方（乙方）一幅数码私人照片，显示某名人与第三方共度亲密时刻，乙方理论上可以入罪，原因是：(i)该照片可用来勒索该名人，以及(ii)乙方相信该照片可用作干犯勒索罪……上述情况可能造成广泛影响，比方说，例子中的乙方是私家侦探，甲方则是其委托人。委托人将数码照片交给私家侦探寻求意见，私家侦探却有机会因建议的罪行而被控告。这点令人忧虑——在这例子中，私家侦探只是为了正当做好自己的工作，才会接收数据，却面临被检控的风险。为何他要承受被检控的风险呢？”

6.15 多名来自资讯科技界的回应者认为，只有存在*“犯罪意图”*，而*“有关工具的唯一用途是用作犯罪目的，且有关刑事作为已确实作出”*，才应产生建议的罪行。这个建议实际上要求删除建议罪行的基本形式。

6.16 消费者委员会就建议的基本罪行阐述其关注事项，内容如下：

> “本会理解小组委员会的顾虑，假如被告人须有主观意图，便会需要证明被告人的主观思想状态，导致举证困难。然而，如无需证明犯罪意图，建议的基本罪行的范围则会过于广泛，以致消费者可能无意中犯法……建议的罪行将不考虑有关器材或数据能否作任何其他合法目的，亦不考虑管有人对使用该器材或数据的主观意图，这点亦令人担忧。举例来说，消费者为合法目的而管有器材，假如该器材的客观主要用途并不合法，则无论该消费者是否察觉这个主要用途，也可能会干犯建议的基本罪行。”

使用器材或数据以干犯罪行

6.17 消费者委员会及几个资讯科技团体认为，只有有关器材或工具用作干犯第2至第5章所考虑的另外四类依赖电脑网络的罪行[10]其中之一（而非用作干犯一般任何罪行）才应产生建议的罪行（不论是基本形式或加重形式）。

"合理辩解"作为免责辩护

6.18 根据咨询文件的建议9(a)，建议的罪行包括合理辩解这项法定免责辩护，原因是任何人或机构可因各种合法理由处理可用作犯罪的器材或数据。[11]

6.19 消费者委员会及另外数名来自商界及资讯科技界的回应者，均支持这项法定免责辩护的范围及适用情况应更为明确，理由是"合理辩解"并无定义，可有不同诠释。他们当中有些回应者提议在法例中制定一份非尽列的例子清单，列举属于"合理辩解"免责辩护范围的合法活动。

我们的分析及回应

背景

6.20 引入建议罪行的基本形式，源于小组委员会曾考虑《公安条例》（第245章）的管有攻击性武器罪。在咨询文件中，小组委员会指出：

(a) 就攻击性武器而言，《公安条例》区分以下物品：被制造以用作造成伤害的物品、被改装以用作造成伤害的物品，以及拟供用作上述用途的物品。在将*"攻击性武器"*的定义应用于枪、开山刀、蝴蝶刀、装有刺刀的雨伞，或削尖并装有尖钉的手杖等物品时，无须证明犯罪意图。纯粹在公众地方管有该等物品，便足以招致刑事法律责任；[12]及

(b) 兼具合法及非法用途的器材及数据相当常见。例如财务机构为安全起见，管有消磁器，并用它来清除旧硬碟的内容，如此这项工具是合法的。不过，如管有这项工具并意图将它用作非法目的（例如破坏），承担刑事法律责任则属合

---

10 即非法取览程式或数据（第2章）、非法截取电脑数据（第3章）、非法干扰电脑数据及非法干扰电脑系统（第4及第5章）。

11 咨询文件第6.87段。

12 同上，第6.71段。

理。[13]

6.21 基于上述考虑，咨询文件的建议 9 借镜《公安条例》的分类方法，把建议的罪行分为基本形式及加重形式。正如小组委员会所解释，[14] 在个别案件中，除了以某器材或数据是否被制造或改装以用作非法用途来将它们归类之外，还应以是否有犯罪意图作为另一区别因素，这是因为器材或数据的用途，可能随着电脑及互联网科技发展而改变，故单靠器材或数据是否被制造或改装用作非法用途来定夺刑事法律责任，并不理想。

全盘处理建议罪行及相关免责辩护

6.22 从公众咨询收取的意见，让我们有机会重新考虑建议 9。我们同意，将现实世界中“攻击性武器”的现有概念移至电脑网络世界并非直截了当的问题。与现实世界的攻击性武器（如铁莲花）相比，器材、程式或数据即使被主要用作犯罪目的，也较难为人注意，而任何人亦未必了解某器材、程式或数据属恶性。

6.23 我们在考虑建议 9 及 10 的建议罪行及相关免责辩护的广度时，已全盘研究所有相关事项。假如扩阔建议罪行中个别元素的范围，则可能需要调整该罪行的其他部分，又或提供适当的免责辩护或豁免，以确保该罪行不会过于宽泛。我们会在本章详细解释我们的最终建议。

在建议的罪行加入“程式”，即“器材、程式及数据”

6.24 这项修订源自香港警务处的提议，该处提出将建议的罪行与第 2 章所讨论的取览罪看齐（取览罪的刑事作为与“程式或数据”而非电脑有关联）。由于我们建议的罪行旨在同样禁止使用实体“器材”以干犯电脑网络罪行，[15] 我们认为“器材”应保留为建议罪行的标的之一。

6.25 尽管如此，建议罪行的目的在于打击电脑网络罪行，我们认为将“程式”加入为建议罪行可涵盖的标的之一，是适当的做法。这立场亦与欧洲委员会（Council of Europe）的《电脑网络罪行公约》

13 同上，第 6.70 段。
14 同上，第 6.72 段。
15 上文第 6.2 段。

（Convention on Cybercrime）第六条[16]订定罪行的标准相符，该条规定，各缔约方应采取措施将以下行为定为刑事罪行：

> “生产、出售、为使用而获取、输入、分发或以其他方式提供经设计或改装以主要用作干犯第二至五条所订任何〔依赖电脑网络的〕罪行的器材（包括电脑程式）。”

（底线后加）

将建议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

6.26 我们在反复思量后提议，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，即取览罪、非法截取电脑数据、非法干扰电脑数据及非法干扰电脑系统（最后两类罪行统称“**干扰罪**”）。

背景

6.27 我们理解，小组委员会在咨询文件提出建议 9，目标是订立一项全面性的罪行，以防范误用器材、程式或数据——任何人如取得或供应用作犯罪的器材、程式或数据，理论上应负法律责任。

原有建议 9 的影响

6.28 我们同意，禁止误用是重要的合理目的，但“器材”一词可作广阔的诠释，也是值得注意的问题。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 会使建议的罪行超出电脑网络世界，在现实世界的适用范围更是无远弗届。举例而言，如任何人撰写电邮，试图勒索受害人，但最终决定不送出电邮，只保留草稿，该人也属于管有可用作干犯“罪行”的数据，因而触犯小组委员会建议 9 的建议罪行。

其他司法管辖区的法例

6.29 我们还注意到，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。[17]

---

16 咨询文件第 6.20 段。

6.30 由于建议 9 是因应新西兰先有的法例[18]（即当时的《1961 年刑事罪行法令》〔Crimes Act 1961〕第 251(1)条）而制订，我们宜详加审视这项条文。第 251(1)条内容如下：

> "任何人（该人）如邀请他人从该人获取任何令另一人能够在未获授权下取用电脑系统的软件或其他资料，或向他人要约出售或要约供应或为向他人出售或供应而展示该软件或资料，或同意向他人出售或供应或向他人出售或供应该软件或资料，或为向他人出售或供应而管有该软件或资料，而：
>
> (a) 该人知悉该软件或资料的唯一或主要用途，是用作犯罪；或
>
> (b) 该人知悉该软件或资料会用作犯罪，或罔顾该软件或资料会否用作犯罪，并宣传该软件或资料对犯罪有用（不论该人是否也宣传该软件或资料对任何其他目的有用），
>
> 可处为期不超过 2 年的监禁。"
>
> （底线后加）

6.31 经过更仔细审视后，我们察觉到，该项由第 251 条所订的新西兰罪行的范围实际上受一项规定所限制，即有关软件或资料必须可令另一人能够在未获授权下取用电脑系统。因此，这项新西兰罪行并非广泛至足以涵盖一般纯粹可用来干犯*"任何罪行"*的软件或

---

17 咨询文件第 6.22 段（澳大利亚）、6.29 段（加拿大）、6.36 段（英格兰及威尔斯）、6.43 段（中国内地）及 6.58 段（新加坡）。

18 咨询文件第 6.74 段，小组委员会在该段表示：*"鉴于已有新西兰法例作为先例，我们属意新法例所禁止的器材及数据之非法用途，不应限于干犯电脑网络罪行，而应普及地关乎任何罪行"*。