香港法律改革委员会

电脑网络罪行小组委员会

咨询文件

依赖电脑网络的罪行
及司法管辖权事宜

本咨询文件已上载互联网，网址为：<**http://www.hkreform.gov.hk**>。

2022 年 6 月

本咨询文件是由法律改革委员会（法改会）属下的电脑网络罪行小组委员会拟备，以供各界人士讨论及发表意见。本咨询文件的内容并不代表法改会或小组委员会的最终意见。

小组委员会欢迎各界人士就本咨询文件发表意见，并请于2022年10月19日或之前将有关的书面意见送达：

香港中环

下亚厘毕道18号

律政中心东座4楼

法律改革委员会

电脑网络罪行小组委员会秘书

电话：(852) 3918 4097

传真：(852) 3918 4096

电邮：hklrc@hkreform.gov.hk

法改会和小组委员会日后与其他人士讨论或发表报告书时，可能会提述和引用各界人士就本咨询文件所提交的意见。任何人士如要求将他提出的所有或部分意见保密，法改会当乐于接纳，惟请清楚表明，否则法改会将假设有关意见无须保密。

法改会在日后发表的报告书中，通常会载录就本咨询文件提交意见的人士的姓名。任何人士如不愿意接纳这项安排，请于书面意见中表明。

香港法律改革委员会

电脑网络罪行小组委员会

咨询文件

依赖电脑网络的罪行及司法管辖权事宜

目录

页

第 3 章　非法截取电脑数据

页

第 4 章　非法干扰电脑数据

第 5 章　非法干扰电脑系统

页

第 6 章　提供或管有用作犯罪的器材或数据

页

第 8 章　判刑

第 9 章　综合建议及咨询问题

界定用语

用语／简称	定义
《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）
CCP 制度	认证网络专业人员保证服务（Certified Cyber Professional assured service）
*郑嘉仪*案	*律政司司长 诉 郑嘉仪*（*Secretary for Justice v Cheng Ka Yee*）(2019) 22 HKCFAR 97, [2019] HKCFA 9
*朱峻玮*案	*香港特别行政区 诉 朱峻玮*（*HKSAR v Chu Tsun Wai*）(2019) 22 HKCFAR 30, [2019] HKCFA 3
《刑事司法管辖权条例》	《刑事司法管辖权条例》（第 461 章）
《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）
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”）
Ex parte United States	*R v Bow Street Metropolitan Stipendiary Magistrate, Ex parte United States (No 2)* [2000] 2 AC 216
《说明报告》	《布达佩斯公约说明报告》（Explanatory Report to the Budapest Convention）

香港	香港特别行政区
国际认可论坛	国际认可论坛（International Accreditation Forum）
《截取通讯及监察条例》	《截取通讯及监察条例》（第 589 章）
法释〔2011〕19 号	《最高人民法院、最高人民检察院关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》
《调查权力法令》	《2016 年调查权力法令》（Investigatory Powers Act 2016）（英格兰及威尔斯）
《示范法典委员会报告书》	示范刑事法典人员委员会（Model Criminal Code Officers Committee），《报告书》，第 4 章：《损坏及电脑罪行及对第 2 章：司法管辖权的修订》（2001 年）（*Report, Chapter 4, Damage and Computer Offences and Amendments to Chapter 2: Jurisdiction (2001)*）
《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》
《新西兰法令》	《1961 年刑事罪行法令》（Crimes Act 1961）（新西兰）
外交部驻港公署	中华人民共和国外交部驻香港特派员公署
中国	中华人民共和国
《中国刑法》	《中华人民共和国刑法》

《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*）
最高人民检察院指导性案例	中国最高人民检察院公布的指导性案例
第161条	《刑事罪行条例》（第200章）第161条
第27A条	《电讯条例》（第106章）第27A条
《电讯（截取及取览）法令》	《1979年电讯（截取及取览）法令》（联邦）（Telecommunications (Interception and Access) Act 1979 (Cth)）（澳大利亚）
英国	联合王国
联合国毒罪办	联合国毒品和犯罪问题办公室（United Nations Office on Drugs and Crime, "UNODC"）
美国	美利坚合众国
黄得强案	*香港特别行政区 诉 黄得强*（*HKSAR v Wong Tak Keung*）(2015) 18 HKCFAR 62, FACC 8/2014
《无线电讯法令》	《2006年无线电讯法令》（Wireless Telegraphy Act 2006）（英格兰及威尔斯）

导言

引言

1. 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。

2. 香港特别行政区政府于2000年召开电脑相关罪行跨部门工作小组，进行了香港特别行政区（"**香港**"）迄今为止最近期的电脑网络罪行官方研究。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。在这背景下，终审法院首席法官联同律政司司长于2019年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电脑网络罪行小组委员会探讨法律现况和提出建议。

3. 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，并在香港公布实施。香港维护国家安全的责任，再次确认有需要改革香港的电脑网络罪行法律，[1] 小组委员会研究电脑网络罪行这课题时已将此考虑在内。

研究范围

4. 2019年1月，电脑网络罪行小组委员会就电脑网络罪行课题展开研究，研究范围如下：

> "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；

[1] 除了《国安法》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。

(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

5. 小组委员会由梁镇宇先生担任主席，成员如下：

梁镇宇先生 ***（主席）***	德同国际有限法律责任合伙资深顾问律师
方永佳先生 （任期由2018年12月13日至2020年9月13日）	前香港海关版权及商标调查（行动）课监督
何沈洁玲女士 （任期由2018年12月13日至2020年12月20日）	前香港上海汇丰银行有限公司亚太区复元风险管理主管
徐诗妍女士 （任期由2019年8月12日起）	保安局首席助理秘书长
陈政龙先生，SC	资深大律师
陈淑仪女士	律政司助理刑事检控专员
曾裕彤先生 （任期由2018年12月13日至2019年8月9日）	前保安局首席助理秘书长
汤炽忠先生	消费者委员会副总干事
黄佩琪女士，SC	资深大律师

黄蕙荃女士 （任期由2020年9月14日起）	香港海关版权及商标调查（行动）课监督
叶旭晖先生	香港互联网供应商协会主席
邹锦沛博士	香港大学计算机科学系副教授
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总监
郑松岩博士 （任期由2022年1月12日起）	中国银行（香港）有限公司首席信息官
郑丽琪女士 （任期由2022年5月3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）	前罗本信律师行合伙人
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
关煜群博士	亚太互联网中心首席执行官

6. 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。政府律师李灏棋先生也为小组委员会提供协助。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。

研究内容

7. 自讨论初期，我们便发现电脑网络罪行并无普遍接纳的归类方式。

8. 本咨询文件的第 1 章描述电脑网络罪行以往如何以不同方式归类。就本咨询文件而言，我们采用联合国毒品和犯罪问题办公室（United Nations Office on Drugs and Crime，“**联合国毒罪办**”）所使用的术语，把罪行分为“依赖电脑网络”（cyber-dependent）和“借助电脑网络”（cyber-enabled）两类性质。联合王国（“**英国**”）政府的以下阐释有助理解：[2]

(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”*；及

(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”*。

项目的三个划定部分

9. 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。具体而言：

(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，并尝试应对数码时代的宏观挑战，包括数据主权（亦称为电脑网络、数码或技术主权），而第二部分的范围须待适当时候再作讨论。数据主权的要旨，在于地方应能够就其数码基础建设及科技应用作出自主行动和决策。数据主权亦与确保数码基础建设安全的工作，以及地方在与它领土和公民有关的数码通讯事宜方面的权限息息相关；[3] 及

(c) 第三部分会处理证据事宜及执法（程序）事宜。

---

2 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*）（英国政府，2016 年），第 3.2 段，登载于 https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021 （于 2022 年 5 月 3 日浏览）。

3 Julia Pohle & Thorsten Thiel, “Digital Sovereignty”, Internet Policy Review: Journal on internet regulation (2020), Vol 9, Issue 4，第 8 页。

小组委员会的研究方法

第一部分研究的五类依赖电脑网络的罪行

10. 本咨询文件关乎项目的第一部分。我们借鉴欧洲委员会（Council of Europe）的《电脑网络罪行公约》（Convention on Cybercrime，**《布达佩斯公约》**）及俄罗斯联邦（Russian Federation）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），[4] 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：

(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) 提供或管有用作犯罪的器材或数据。

比较研究

11. 我们参考(a)《布达佩斯公约》的规定及(b)香港和其他七个司法管辖区（即澳大利亚、加拿大、英格兰及威尔斯、中国内地、新西兰、新加坡和美利坚合众国（"**美国**"））的法例，[5] 检视上述罪行及相关的司法管辖权事宜。这些司法管辖区当中，有四个（即澳大利亚、加拿大、英格兰及威尔斯和美国）是《布达佩斯公约》的缔约方，另外四个（即香港、中国内地、新西兰和新加坡）则并非缔约方。

建议背后的指导原则

12. 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。

---

[4] 《布达佩斯公约》及《联合国合作打击网络犯罪公约》草案的详情载于第 1 章。

[5] 就澳大利亚、加拿大和美国而言，则指其联邦法例。

本咨询文件的格式

13. 本咨询文件由以下各章组成：

(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章先探讨项目第一部份所涵盖的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，即提供或管有用作犯罪的器材或数据。

(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章胪列我们的综合建议及咨询问题。

14. 在这次咨询工作中，小组委员会征询公众对以下问题的意见：经考虑现有法例下适用于电脑网络罪行的各项订罪条文及其他相关条文，有关刑事法律是否需要改革；如认为需要的话，则采用何种改革方案为佳。我们旨在尽可能让最多的公众人士参与是次咨询工作，并热切期待能听到社会各界不同声音。我们希望本咨询文件有助促进和便利公众讨论当中所提出的议题，并欢迎各界就此等议题发表意见、评论和建议，这将大力协助小组委员会达致研究范围定下的目标。

第 1 章　电脑网络罪行的归类

引言

1.1　正如联合国毒罪办在其编写的《网络犯罪综合研究》（Comprehensive Study on Cybercrime）所评析：

> “……互联网和个人计算机设备的普遍存在意味着计算机系统或数据能够辅助——至少在发达国家——几乎所有犯罪行为。”[1]

1.2　换言之，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。此外，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。即使是同一笔者，在不同情况或刊物所采用的归类及名称亦未必一致。

在联合国层面的归类

1.3　在第十届联合国预防犯罪和罪犯待遇大会（the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders）期间，举办了一次涉及电脑网络的犯罪问题讲习班。当时，电脑网络罪行划分为两类，各自的定义如下：

> “(a)　狭义上的电脑犯罪（‘计算机犯罪’）：任何以电子操作为手段进行的针对计算机系统的安全及其所处理数据的非法行为；
>
> (b)　广义上的电脑犯罪（‘涉及计算机的犯罪’）：任何以计算机系统或网络为手段进行的或与其有关的非法行为，包括利用计算机系统或网络非法占有、提供或分发信息等项犯罪。”[2]

1.4　联合国毒罪办在 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、借助电*

1　联合国毒罪办，《网络犯罪综合研究》（2013 年 2 月），第 18 页，登载于 https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Chinese.pdf。

2　联合国，“涉及计算机网络的犯罪——涉及计算机网络的犯罪问题讲习班背景文件”（A/CONF.187/10，2000 年 2 月 3 日），第 14 段，登载于 https://www.un.org/chinese/events/10thCrimeCong/187_10.html。

脑网络的罪行，以及网上性剥削和性虐待儿童这种特定罪行类型”。[3] 如导言所述，我们会在本咨询文件使用“依赖电脑网络的罪行”和“借助电脑网络的罪行”这两个词语。

1.5 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。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

1.6 《布达佩斯公约》于2001年11月23日开放予各国签署，并于2004年7月1日生效。[4] 《布达佩斯公约》由一份于2006年3月1日生效的《附加议定书》（Additional Protocol）作为补充，[5] 似乎是首份规管电脑网络空间的跨国协议。[6] 截至2020年3月16日，已有65个国家批准或加入《布达佩斯公约》。[7]

1.7 《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。[8] 《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“实质重于形式”）：

---

3 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/global-programme-cybercrime.html（于2022年5月3日浏览）。

4 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2022年5月3日浏览）。

5 全称为《电脑网络罪行公约关于宣告利用电脑系统犯下的种族主义或仇外行为为犯罪行为的附加议定书》（“Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems”）。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2022年5月3日浏览）。

6 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2022年5月3日浏览）。

7 欧洲委员会，“Colombia joined the Budapest Convention on Cybercrime”（2020年3月16日），登载于 https://www.coe.int/en/web/cybercrime/-/colombia-joined-the-budapest-convention-on-cybercrime（于2022年5月3日浏览）。

8 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）（**《说明报告》**），第33段，登载于 https://rm.coe.int/16800cce5b（于2022年5月3日浏览）。

(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。

《电脑罪行及电脑相关罪行示范法》

1.8 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）[9]（**《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。[10]

1.9 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。[11]

其他司法管辖区法律的相符程度

1.10 如导言所述，本咨询文件对七个司法管辖区的法律进行比较研究，即澳大利亚、加拿大、英格兰及威尔斯、中国内地、新西兰、新加坡和美国。对于该等法律与《布达佩斯公约》所订规定的一致程度，下文阐述相关的历史背景：

(a) 在加拿大，最高法院于1980年对 *R v McLaughlin*[12] 所作的决定，促使当局改革《刑事法典》（Criminal Code）以应对误

---

9 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2022年5月3日浏览）。

10 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。

11 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2022年5月3日浏览）。

12 [1980] 2 SCR 331.

用电脑的问题。[13]《1985 年刑事法修订法令》（Criminal Law Amendment Act 1985）和《1996 年刑事法改善法令》（Criminal Law Improvement Act 1996）先后在《刑事法典》加入第 342.1 条[14] 和第 430(1.1)条[15] 等多项电脑网络罪行条文。1997 年 4 月，各方就后来的《布达佩斯公约》展开磋商，[16] 加拿大于 2001 年签署《布达佩斯公约》。

(b) 在美国，《电脑欺诈及滥用法案》（Computer Fraud and Abuse Act）是应对电脑网络罪行的主要联邦法例，该法案于 1986 年制定，并编纂于《美国法典》第 18 篇第 1030 条（18 USC 1030）。《美国法典》第 18 篇第 1030 条的修订历程（1986 至 2008 年间共修订九次）显示，尽管美国于 2001 年成为《布达佩斯公约》的签署国，该公约并没有构成任何直接影响。[17]

(c) 英格兰及威尔斯法律委员会（Law Commission of England and Wales）于 1989 年建议[18] 制定新法例，最终获通过成为《1990 年误用电脑法令》（Computer Misuse Act 1990，**《英格兰误用电脑法令》**）。《英格兰误用电脑法令》曾修订数次，但该法令的整体框架于 2001 年英国签署《布达佩斯公约》之后仍大致维持不变。

(d) 新加坡《1993 年误用电脑法令》（Computer Misuse Act 1993，**《新加坡误用电脑法令》**）于 1993 年制定，当中的罪行条文主要以《英格兰误用电脑法令》为基础，但亦有若干差异。[19]

---

13 Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd edition, 2015)，第 52 至 53 页。

14 最初编为第 301.2(1)条，现已重新编号，该条的标题是*"在未获授权下使用电脑"*（*Unauthorized use of computer*）。

15 最初编为第 387(1.1)条，现已重新编号，该条的标题是*"与电脑数据有关的损害"*（*Mischief in relation to computer data*）。

16 《说明报告》第 12 段。

17 此书有相关阐述：H Marshall Jarrett, Michael W Bailie, Ed Hagen and Scott Eltringham, *Prosecuting Computer Crimes* (Office of Legal Education, Executive Office for United States Attorneys, 2nd edition, 2010), 第 1 至 3 页, 登载于 https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf（于 2022 年 5 月 3 日浏览）。

18 法律委员会，*Criminal Law: Computer Misuse*（1989 年），法律委员会第 186 号，登载于 https://www.lawcom.gov.uk/project/criminal-law-computer-misuse/（于 2022 年 5 月 3 日浏览）。

19 Gregor Urbas, "An Overview of Cybercrime Legislation and Cases in Singapore" (ASLI Working Paper No 001, December 2008)，第 1 页，登载于 https://law.nus.edu.sg/asli/pdf/WPS001.pdf（于 2022 年 5 月 3 日浏览）。

(e) 在中国内地，《中华人民共和国刑法》（**《中国刑法》**）于1997年（亦即在《布达佩斯公约》2004年生效前）在第二百八十五及二百八十六条引入电脑网络罪行条文。[20] 2009年，第二百八十五条加入更多条文，以扩大电脑网络罪行的适用范围。[21]

(f) 按照新西兰法律委员会（Law Commission of New Zealand）于1999年的建议，[22] 新西兰《1961年刑事罪行法令》（Crimes Act 1961）于2003年加入规管电脑网络罪行的现有条文（第248至252条）。从法律委员会报告书所述的立法背景看来，《布达佩斯公约》对新西兰有关法例的草拟工作并没有重大影响，甚或毫无影响。

(g) 澳大利亚《刑事法典》（联邦）（Criminal Code (Cth)）中的电脑网络罪行条文，乃源于示范刑事法典人员委员会（Model Criminal Code Officers Committee）于2001年发表的报告书（**《示范法典委员会报告书》**）。[23] 一份就相关的《2001年电脑网络罪行法案》（Cybercrime Bill 2001）所发表的国会文件[24] 显示，《英格兰误用电脑法令》对《示范法典委员会报告书》的方针有*"明显影响"*，该报告书亦参照了当时的《布达佩斯公约》草案。尽管如此，而澳大利亚于2012年亦批准了《布达佩斯公约》，[25] 界定澳大利亚有关罪行的立法措辞自2001年制定以来，均与《英格兰误用电脑

---

20 《中国刑法》修订自1997年10月1日起实施。

21 《中国刑法》加入了第二百八十五条第二及三款。由于这些修订自2009年2月28日起施行，因此非法取览程式或数据罪亦一般适用于计算机信息系统，并订立了提供或管有用作犯罪的器材或数据罪。

22 新西兰法律委员会，*Computer Misuse*（1999年），第54号报告书，登载于https://www.lawcom.govt.nz/our-projects/computer-crime?id=814（于2022年5月3日浏览）。

23 示范刑事法典人员委员会，《报告书》，第4章：《损坏及电脑罪行及对第2章：司法管辖权的修订》（*Report, Chapter 4, Damage and Computer Offences and Amendments to Chapter 2: Jurisdiction*）（2001年1月）。该报告书的存档副本曾登载于律政部（Attorney-General's Department）网站，现时可通过"Wayback Machine"查阅（有关部分是第4章第4.2部），网址为https://web.archive.org/web/20060920231025/http://www.ag.gov.au/agd/WWW/rwpattach.nsf/viewasattachmentPersonal/(0AFA115E182148C186311CED66C0728D)~modelcode_ch4_Computer_offences_report.pdf/$file/modelcode_ch4_Computer_offences_report.pdf（于2022年5月3日浏览）。

24 Department of the Parliamentary Library, *Bills Digest No 48 2001-02* (2001)，登载于https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd0102/02bd048（于2022年5月3日浏览）。

25 按《2012年电脑网络罪行法例修订法令》（联邦）（Cybercrime Legislation Amendment Act 2012 (Cth)）的详题所述，这是*"为实施《欧洲委员会布达佩斯电脑网络罪行公约》和其他目的而订立的法令"*，见https://www.legislation.gov.au/Details/C2012A00120（于2022年5月3日浏览）。

法令》颇为不同，事实上与直接以《布达佩斯公约》为基础的《示范法》亦有相当差异。

联合国的最新动向

1.11 国际间对电脑网络罪行的规管情况正在急速变化。联合国有两个动向可能会产生影响，值得密切关注：

(a) 俄罗斯联邦于 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（**《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。[26]

(b) 然而，最近大会于 2019 年 12 月 27 日采纳的第 74/247 号决议[27] 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"。[28]

1.12 若日后在联合国的框架内订立关于电脑网络罪行的条约，该条约所采纳的归类及名称或许会逐渐成为权威。

---

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

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

28 第 3 段。2021 年 5 月，特设委员会在组织会议上选举主席团成员并讨论其进一步活动的纲要和方法。见 https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home（于 2022 年 5 月 3 日浏览）。然而，由于 2019 冠状病毒病大流行持续，该委员会的首次会议推迟至 2022 年 2 月 28 日至 3 月 11 日。见：联合国毒罪办，"First session of the Ad Hoc Committee"，登载于 https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-first-session.html（于 2022 年 5 月 3 日浏览）。

第 2 章　非法取览程式或数据

引言

2.1　我们会在本章探讨五大类依赖电脑网络的罪行中的第一类：非法取览电脑中的程式或数据。这类罪行须与非法截取电脑数据区分开来，后者会是下一章的讨论重点。概括而言，就非法取览电脑中的程式或数据而订立的罪行，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。

2.2　黑客入侵大概是该罪行最典型的例子。此外，至少在某些司法管辖区，[1] 任何获授权取用电脑的人（例如操作雇主电脑的雇员）在授权范围外行事，便可能犯罪。

2.3　我们在考虑非法取览程式或数据罪时，紧记电脑网络空间的性质独特。作为起点，在未获授权下取用电脑（或取览存于电脑内的程式或数据），可比喻为在现实世界中，陌生人在未获准许下进入某地方（例如某人的居所）的情境。

2.4　定夺现实世界中入侵的刑事法律责任较为简单直接，是因为实体空间的界线是有形的，这令在未获授权下进出的概念有相对明确的定义。举例来说，陌生人若"进出"他人的住所，便至少曾亲身踏足该住所，而且其作为显然有所不妥。此外，在现实世界中，受害人亦较容易阻止入侵者。

2.5　相反，电脑网络空间则是截然不同的情境。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

---

[1]　举例来说，香港、澳大利亚和美国（见第 2.9、2.23 至 2.26 及 2.83 至 2.88 段）。

联网，[2] 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。

香港的现行法律

《刑事罪行条例》（第 200 章）

第 161 条

2.6 《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**"）有以下规定：

"(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）；

(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

---

[2] 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。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 2022 年 5 月 3 日浏览）。

(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。”

第 161 条所订的犯罪行为

2.7 *律政司司长 诉 郑嘉仪*[3]（*Secretary for Justice v Cheng Ka Yee*，“***郑嘉仪案***”）是关于第 161 条的主导案例。终审法院按照第 161 条的文本、文意和目的来解释该条文，并对有关犯罪行为（“取用”，“obtain access”）有以下评析：

> “‘Obtain（获得）’一词……若用来描述某人使用自己的器材，显然格格不入，‘access（取用）’一词亦是如此……从语言的角度来看，一个人必然是本来没有取用某物，其后才‘获得’对该物的取用。”[4]

2.8 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”*。[5] 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 条不适用于下述情况：

(a) 任何人使用*自己的*电脑设立仿冒诈骗网站；及

(b) 任何人使用*自己的*智能电话拍摄裙底。[6]

取用的未获授权性质

2.9 虽然从表面上看，第 161 条并无规定有关取用须属未获授权，但法院似乎都将该条解释为包含这项要求。[7] 在这方面，涉及根本没有授权的案件相对上简单直接。在多个司法管辖区，争议点往往在犯罪者（例如雇员）在超逾授权范围下行事的案件中产生。*香港特*

---

3 (2019) 22 HKCFAR 97, [2019] HKCFA 9.

4 同上，第 38 段。

5 同上，第 48 段。

6 第 161 条并无界定何谓“电脑”。早于*郑嘉仪*案之前，在*律政司司长 诉 王嘉业* [2013] 4 HKLRD 588, HCMA 77/2013（判决日期：2013 年 4 月 29 日）这宗高等法院原讼法庭审理的裁判法院上诉案件，高等法院原讼法庭法官冯骅裁定，就根据第 161 条提出的检控而言，能够摄录短片等的智能电话构成“电脑”。冯骅法官并无采用《证据条例》(第 8 章)第 22A(12)条、《税务条例》（第 112 章）第 26A 条及《商业登记条例》（第 310 章）第 19 条对“电脑”所下的定义，即*“任何用作储存、处理或检索资料的器材”*，而是采用《牛津网上字典》对该词（computer）的定义：
“一个电子装置，可以接收某一特定形式的资讯，并可以按照预定但可变的程式指令执行一连串的运算，从而产生资讯或讯号形式的结果”。

7 见上文注脚 3，第 38 段。

别行政区　诉　秦瑞麟（*HKSAR v Tsun Shui Lun*）[8]是一宗相关的香港案例，高等法院首席法官陈兆恺对该案作出以下裁定：

> "就第 161 条所订罪行而言，本席认为在没有权限的情况下取用与在超逾权限范围下取用并无分别，亦不应存在分别。该条并没有区分这两种情况。"[9]

第 161 条所指"获益"的涵盖范围

2.10　在*香港特别行政区　诉　秦瑞麟*，首席法官陈兆恺进一步把第 161 条的"获益"一词解释为*"不限于在经济上或所有权上的利益，而是足以包括无形利益"*，并可能属*"短暂而非永久性质"*。[10]按照此广阔的诠释，有关罪行适用于任何人从某电脑取得自己先前无法取览的资料的情况。[11]举例来说，该案中的"获益"是某病人的医疗纪录，储存于犯罪者任职的医院的电脑系统。

《电讯条例》（第 106 章）

第 27A 条

2.11　与本章相关的另一条文是《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——
>
> (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；

8　[1999] 3 HKLRD 215, HCMA 723/1998（判决日期：1999 年 1 月 15 日），高等法院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。

9　[1999] 3 HKLRD 215，第 223 页 D 行（第 22 段）。

10　同上，第 223 页 G 行（第 24 段）。

11　同上，第 223 页 J 行（第 25 段）。

(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。"

比较第161条与第27A条

2.12 在*香港特别行政区 诉 秦瑞麟*，高等法院首席法官陈兆恺将第161条与第27A条比较如下：

"一方面，第161条的适用范围较《电讯条例》第27A条广阔，因为不论有关取用是否藉着电讯获得，均有可能犯第161条所订罪行。另一方面，第161条所订罪行须证明犯罪或不诚实的特定意图或目的，是较严重的罪行，这亦反映于该条文指明的最高刑罚。由此推论，并非对电脑的每类取用均构成第161条所订罪行。"[12]

2.13 正如首席法官陈兆恺所述，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*案被定性为*"'黑客入侵'罪行"*，*"明显是针对不属于犯罪者自己的电脑"*。[13]

---

12 同上，第222页B–C行。

13 见上文注脚3，第41段。

2.14 尽管有此定性，案例显示，控方倾向根据第 161 条而非第 27A 条检控黑客入侵事件。[14] *香港特别行政区 诉 谭曦伦及其他人*（*HKSAR v Tam Hei Lun & Ors*）[15] 是其中一例，案中的犯罪者使用名为 Back Orifice 的程式来取用其他互联网用户的电脑，并取得他们的登入名称和密码。涉及犯罪者使用另一部电脑进行黑客入侵的另一案例是*香港特别行政区 诉 谢文礼*（*HKSAR v Tse Man Lai*），[16] 案中的犯罪者两度用自己的电脑向"披露易"网站的伺服器发动攻击，并取得三个静态影像和录影片段。

显然难以证明第 27A 条所订罪行

2.15 根据第 161 条而非第 27A 条检控黑客入侵案件，可能是因为控方显然难以证明第 27A 条所订的犯罪意念。此犯罪意念涉及的两方面都以否定语句表达，即被告人：

(a) *"不相信自己已获……授权"*，使他获得有关种类的取用；及

(b) *"不相信若他曾申请适当的授权，则他本已获如此授权"*。

2.16 相比之下，视乎案情而定，有时候可能较容易按照第 161 条的规定证明被告人意图犯罪或不诚实。此外，正如上文指出，若被告人并非"藉着电讯"获得有关取用，则第 27A 条并不适用。

2.17 在第 161 条及第 27A 条均可援引的情况下，条文的选择可能事关重大，因为两者所订的最高刑罚各异：根据第 27A 条可处第 4 级罚款，[17] 而根据第 161 条循公诉程序定罪则可处监禁五年。

《布达佩斯公约》订定罪行的标准

2.18 与本章重点相对应的是《布达佩斯公约》[18] 第一节之下的第一篇第二条：

---

14 迄今为止，似乎并没有针对黑客入侵而援引第 27A 条的经汇报判决。以下文章探讨了 1996 年一宗根据第 27A 条成功提出的检控：Rynson W H Lau, Kwok-Yan Lam and Siu-Leung Cheung, "The Failure of Anti-Hacking Legislation: a Hong Kong Perspective" (Invited Paper in Proceedings of ACM Conference on Computer and Communications Security, March 1996)，第 62–67 页。然而，未能找到任何书面判决。

15 [2000] 3 HKC 745, HCMA 385/2000（判决日期：2000 年 10 月 9 日）。

16 [2013] 3 HKLRD 691（此案例目前应在*郑嘉仪*案的规限下予以解读），CACC 455/2012（判决日期：2013 年 6 月 18 日）。

17 根据《刑事诉讼程序条例》（第 221 章）附表 8，现为 25,000 元。

18 有关《布达佩斯公约》的背景资料，见导言第 11 段，以及第 1 章第 1.6 至 1.10 段。

"各缔约方均应采取必要的立法及其他措施，在其本土法律中将下列行为定为刑事罪行：在无权的情况下蓄意取用整个电脑系统或其任何部分。任何缔约方可规定，任何人有取得电脑数据的意图或其他不诚实意图而违反保安措施，或就连接至另一电脑系统的电脑系统违反保安措施，即属犯该罪行。"

2.19 《说明报告》对第二条的评注如下：

"44. '非法取用'涵盖损害电脑系统及数据安全……的危险威胁及攻击的基本罪行。组织及个人均享有以不受干扰及不受限制的方式管理、操作和控制其系统的权益，因此有需要就此获得保障。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……及秘密，以及免费使用有关系统，甚或鼓励黑客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。

……

46. '取用'涉及进入整个电脑系统或其任何部分（硬件、零件、已安装系统所储存的数据、目录、流量数据及内容相关数据），但并不包括纯粹向该系统发送电邮讯息或档案。'取用'包括进入另一电脑系统……或连接至同一网络上某电脑系统……。通讯方法……属无关重要。

47. 有关作为亦须在'无权'的情况下作出……如在有关系统或其任何部分的拥有人或其他权利持有人的授权下而取用……，不属犯罪……取用开放予公众自由取用的电脑系统，亦不属犯罪……

48. 运用特定的技术工具可能会引致第二条所指的取用，例如取览某网页……运用这类工具本身不属'无权'。如某公共网站维持存在，即意味着网站拥有人同意让任何其他网络用户取览该网站……

……

50. 各缔约方可采取宽泛的方针，按照第二条首句把纯粹的黑客入侵定为罪行；或者附加第二句列述的任何或所有规限元素：违反保安措施、取得电脑数据的特别意图、有理由施加罪责的其他不诚实意图，或规定犯该罪行须与远程连接至另一电脑系统的电脑系统有关。[19] 若采用最后一个元素，各缔约方便可豁除任何人实体取用一部独立运作的电脑（而并无使用另一电脑系统）的情况。他们可以把该罪行限于非法取用已连接网络的电脑系统……"[20]

其他司法管辖区的法定体制

澳大利亚

《刑事法典》（联邦）第 477.1 及 478.1 条

2.20 在澳大利亚，《刑事法典》（联邦）（Criminal Code (Cth)）第 478.1 条（*"在未获授权下取览或修改受限数据"*）规定如下：

"(1) 任何人在以下情况，即属犯罪：

(a) 该人导致在未获授权下取览或修改受限数据；及

(b) 该人意图导致该项取览或修改；及

(c) 该人知悉该项取览或修改未获授权。

---

19 《说明报告》第 23 及 24 段对"电脑系统"一词有以下论述：

"23. 《公约》所指的电脑系统是任何由硬件和软件组成，为自动处理数码数据而开发的器材。这种器材可能包括输入、输出和储存设施，可能独立运作或与其他相类器材连成网络。'自动'指无需直接的人为干预，'处理数据'指通过执行电脑程式来运算电脑系统内的数据。'电脑程式'是一组可由电脑执行，以达致预期产生的结果的指令。电脑可运行不同程式。电脑系统通常由不同器材组成，这些器材区分为处理器（亦称中央处理器）和周边设备。'周边设备'是任何通过与处理器互动而执行若干特定功能的器材，例如打印机、视像屏幕、光碟阅读器／烧录器或其他储存器材。

24. 网络是两个或以上电脑系统的相互连接。这些连接可以是地面连接（例如导线或电缆）、无线连接（例如无线电、红外线或卫星），或两种形式兼用。就地域而言，网络可能限于某个细小区域（局部区域网络）又或涵盖某个广大区域（宽广区域网络），而这些网络本身亦可能互连。互联网是由众多互连的网络组成的全球网络，全都采用相同的规约。其他类型的网络亦能在电脑系统之间传达电脑数据，不论这些网络是否连接至互联网。电脑系统连接至有关网络，可能是作为端点，或用作协助该网络上的通讯。至关重要的是数据能在网络上交换。"

20 《说明报告》第 44、46 至 48 及 50 段。

刑罚：监禁2年。

(3) 在本条中：

受限数据指符合以下说明的数据：

(a) 存于某电脑内；及

(b) 其取览受与该电脑任何功能相关的存取控制系统所限。”

2.21 此外，《刑事法典》（联邦）第477.1条（*“在未获授权下作出取览、修改或损害，并意图干犯严重罪行”*）实际上是在未获授权下取览电脑数据的加重罪行。该条文把三类错误行为定为不合法，在未获授权下取览电脑数据是其中之一：

“意图干犯联邦、各州或领地的严重罪行

(1) 任何人在以下情况，即属犯罪：

(a) 该人导致：

(i) 在未获授权下取览存于某电脑内的数据；或

(ii) 在未获授权下修改存于某电脑内的数据；或

(iii) 在未获授权下损害往来某电脑的电子通讯；及

(c) 该人知悉该项取览、修改或损害未获授权；及

(d) 该人意图藉该项取览、修改或损害而干犯或利便干犯任何违反联邦、各州或领地法律的严重罪行（不论是由该人干犯或由他人干犯）。

(3) 在就违反第(1)款的罪行而提出的检控中，无须证明被告人知悉有关罪行是：

(a) 违反联邦、各州或领地法律的罪行；或

(b) 严重罪行。

刑罚

(6) 任何人犯违反本条的罪行，一经定罪，可处不超过适用于严重罪行的刑罚。

不可能性

(7) 即使干犯有关严重罪行并不可能，任何人仍可被裁定犯违反本条的罪行。

企图犯罪不属犯罪

(8) 企图干犯违反本条的罪行，不属犯罪。

严重罪行的涵义

(9) 在本条中：

严重罪行指可处终身监禁或为期 5 年或以上监禁的罪行。"

企图取览但不成功

2.22 在本章探讨的法定条文中，第 477.1 条有其独特之处，当中第 477.1(8)条明文免除企图犯罪的刑事法律责任。第 477.1 条显然仅适用于企图并成功取览的情况。

取览的未获授权性质

2.23 《示范法典委员会报告书》构成《刑事法典》（联邦）所载电脑网络罪行条文的基础，该报告书对取览的未获授权性质有以下论述：

"任何个人就某目的获得授权，但为另一隐秘目的行事，应否属犯本部所订罪行？如果原有授权是以与犯罪者目的有关的欺骗手段取得，无疑应施加法律责任；但如果授权是在并无欺诈的情况下取得，而被告人误用该授权，则不能一定得出应施加法律责任的结论。这点显然具争议性……"[21]

---

[21] 《示范法典委员会报告书》，第 4 章：《损坏及电脑罪行及对第 2 章：司法管辖权的修订》（2001 年），第 141 页。

2.24 其后制定的《刑事法典》（联邦）第 476.2(1)及(2)条有以下规定：

> (a) *"如任何人取览存于某电脑内的数据……而该人无权导致该项取览……，则该人的该项取览……即属未获授权"*；但
>
> (b) *"该人导致的任何上述取览……，不会纯粹因为该人导致该项取览……时有隐秘目的而属未获授权"*。

2.25 新南威尔士上诉法院对 *Salter v DPP (NSW)*[22] 所作的决定，揭示应如何理解上述条文。在该案中，法院对《1900 年刑事罪行法令》（新南威尔士）（Crimes Act 1900 (NSW)）第 308B(2)条（《刑事法典》（联邦）第 476.2(2)条在州法例中的对等条文）有以下诠释：

> "第 308B(2)条旨在保障任何有合法权利取览特定数据，但可能是另有隐秘目的而取览该等数据的人员［在该案中是一名警务人员］。因此，即使另有隐秘目的，有关人员只要有合法目的便不会违反该法令……该款的目的是确保任何人在行使其权限而取用［电脑］系统时，不会'纯粹'因为另有某种隐秘目的而犯罪。"[23]

2.26 法院最终维持对犯罪者的定罪，因为*"她［纯粹］为私人目的而取览［有关数据］，这与她代表警方履行的职能毫无关连"*。[24]

加拿大

《1985 年刑事法典》第 326(1)(b)及 342.1(1)条

2.27 加拿大《1985 年刑事法典》（Criminal Code 1985）订有两项相关条文。第一项是第 326(1)(b)条（*"盗取电讯服务"*），根据该条：

> "任何人意图欺诈、恶意或在无表面权利[25] 的情况下……使用任何电讯设施或取得任何电讯服务，即属犯盗窃罪。"

2.28 第二项是第 342.1(1)条（*"在未获授权下使用电脑"*）：

---

22 [2011] NSWCA 190.

23 同上，第 19 及 25 段（首席法官麦克莱伦（McClellan CJ））。

24 同上，第 24 段（首席法官麦克莱伦）。

25 "表面权利（colour of right）"一词指*"真诚地相信某事实状况，而该状况若实际存在，便会在法律上构成所作行为的理由或辩解"*（上诉法院法官马丁（Martin JA）在 *R v DeMarco* (1973) 13 CCC (2d) 369 第 372 页的判词，于 *R v Simpson* [2015] 2 SCR 827 获引用和认同）。

"任何人意图欺诈并在无表面权利的情况下作出以下作为，即属犯可公诉罪行，可处为期不超过10年的监禁，或属犯可循简易程序定罪而惩处的罪行：

(a) 直接或间接取得任何电脑服务；

(b) 藉电磁、声音、机械或其他器材直接或间接截取某电脑系统的任何功能，或导致藉电磁、声音、机械或其他器材直接或间接截取某电脑系统的任何功能；

(c) 直接或间接使用某电脑系统，或导致直接或间接使用某电脑系统，意图干犯(a)或(b)段所订罪行，或就电脑数据或某电脑系统干犯第430条所订罪行；或

(d) 使用、管有、非法传送或准许他人取览某电脑密码，而该密码会使某人能够干犯(a)、(b)或(c)段所订罪行。"

犯罪行为

2.29 这两项条文界定犯罪行为时，均提述被告人"使用"电讯设施或电脑系统等。某些学者认为"使用"一词较"取用或取览"为佳。举例来说，某评论员曾对两词作出以下比较：

"科技汇流、非对称数码用户线路（asymmetric digital subscriber line，英文简称ADSL）[26]及宽频的使用、无线互联网以及网络的不精确性均创造出一种环境，令'使用'电脑的说法比取用电脑更加准确。采用广阔的定义，有助避免关于何谓取用或取览而又往往带有武断成分的技术性争论，令人能够适当聚焦于余下的元素。这些元素会决定有关行为的刑责，有助避免涵盖过广。"[27]

2.30 但就现况来看，加拿大《刑事法典》并无界定何谓"使用"。该词到底是仅指实际上使用电脑系统，还是亦引伸指毫无实效地使用电脑系统（包括企图但不成功取用），可能有争议空间。

---

26 凭借这项技术，以往用来连接电话的铜线现在可支援连接互联网。

27 Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd edition, 2015)，第79页。这段见于作者对美国法律的论述，但他的评析亦适用于提述"使用"电脑系统的加拿大法律。

主要词语的法定定义

2.31 该法典也并无界定何谓"电脑"。然而，该法典第 342.1(2)条订有"电脑数据"、"电脑密码"、"电脑程式"、"电脑服务"、"电脑系统"及"功能"等词语的定义。

2.32 当中，该法典对"功能"所下的定义既广阔而又并非巨细无遗，"功能"包括*"逻辑、控制、算术运算、删除、储存及检索，以及往来某电脑系统或在某电脑系统内的通讯或电讯"*。这使"电脑系统"一词涵盖广泛，其法定定义载于下文：

> "***电脑系统***指任何符合以下说明的器材，或一组互连或相关的器材，而其中一部或多于一部器材：
>
> (a) 包含电脑程式或其他电脑数据，并且
>
> (b) 藉电脑程式而：
>
> (i) 执行逻辑和控制，以及
>
> (ii) 可执行任何其他功能"。

英格兰及威尔斯

《英格兰误用电脑法令》第 1 条

2.33 在英格兰及威尔斯，《英格兰误用电脑法令》第 1 条（*"在未获授权下取览电脑资料"*）有以下规定：

> "(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。

(3) 任何人犯本条所订罪行——

(a) 一经在英格兰及威尔斯循简易程序定罪，可处为期不超过 12 个月的监禁或不超过法定最高罚款，或两者兼处；

(b) [……]

(c) 一经循公诉程序定罪，可处为期不超过 2 年的监禁或罚款，或两者兼处。"

"电脑"的涵义

2.34 与澳大利亚及加拿大的法例一样，《英格兰误用电脑法令》没有界定何谓"电脑"。皇家检控署（Crown Prosecution Service）的网站载有以下论述：

> "[《英格兰误用电脑法令》]并无界定何谓电脑，因为在科技急速变迁的情况下，任何定义都会迅即过时。
>
> 因此，电脑的定义应交由法院决定，预期法院会采用该词当时的涵义。在 *DPP v McKeown*, *DPP v Jones*（[1997] 2 Cr App R 155, HL，第 163 页），贺辅明勋爵（Lord Hoffman）把电脑界定为'任何用作储存、处理和检索资料的器材。'"[28]

犯罪行为

2.35 第 1(1)(a)条所订的犯罪行为是致使某电脑执行任何功能。法律委员会（Law Commission）在其编写的报告书内（该报告书促成制定《英格兰误用电脑法令》），认为这种拟定方式较提述取用概念的拟定方式为佳，因为前者：

> "……涵盖任何有适当的犯罪意图而操控电脑的情况，而且……其所用词语日后并不会因科技发展而变得过时。

---

[28] 皇家检控署，"Legal Guidance, Computer Misuse Act"，登载于 https://www.cps.gov.uk/legal-guidance/computer-misuse-act（于 2022 年 5 月 3 日浏览）。

这种拟定方式排除了不涉及与电脑操作互动的纯实体取用及纯数据检视。"[29]（强调之处乃原文所有）

2.36 上述犯罪行为提述到"电脑"，而第 1(1)(a)条继而藉提述存于"任何电脑"内的任何程式或数据来界定犯罪意念。此法定措辞显然涵盖涉及两部电脑的情况，即犯罪者把一部电脑用作工具，另一部电脑则存有程式或数据。

2.37 此外，英格兰上诉法院在 *Attorney-General's Reference (No 1 of 1991)*[30] 裁定，上述条文中的"任何电脑"一词包括因被告人而执行任何功能的电脑。换言之，该条文亦适用于涉及单一电脑的情境。[31]

企图取览但不成功

2.38 事实上，《英格兰误用电脑法令》第 1(1)(a)条对犯罪行为所下定义之广，令纯粹启动电脑或尝试不同密码企图取览电脑中的程式或数据，表面上都足以构成犯罪行为[32]（不论该企图最终是否成功）。除了《布达佩斯公约》订定罪行的标准之外，[33] 纯粹在未获授权下取览（当中会涉及企图并成功取览）应属犯罪并未广获接纳。[34] 支持将企图但不成功取览定为罪行的理由，可说是更为薄弱。

2.39 英格兰案例 *R v Brown*[35] 牵涉到现已废除的《1984 年资料保护法令》（Data Protection Act 1984），虽然背景不同，但亦说明了类似的观

---

29 法律委员会，*Criminal Law: Computer Misuse*（1989 年），法律委员会第 186 号，第 3.26 段。

30 [1993] QB 94.

31 为作比较，如上文所述，《布达佩斯公约》的各缔约方可选择免除*"任何人实体取用一部独立运作的电脑（而并无使用另一电脑系统）的情况"*所涉的刑事法律责任（《说明报告》第 50 段）。

32 法律委员会，*Criminal Law: Computer Misuse*（1989 年），法律委员会第 186 号，第 3.20 及 3.26 段。

33 *"原则上，纯粹在未获授权下入侵……本身应属非法"*（《说明报告》第 44 段）。

34 《说明报告》在第 49 段提出这一点。
例如亦见 Neil MacEwan, "The Computer Misuse Act 1990: lessons from its past and predictions for its future" [2008] Crim LR 955，第 956 页：
"在［《英格兰误用电脑法令》］刚施行时，有人已质疑为何在未获授权下取览存于电脑内的机密资料应属犯罪，但如同一资料是存于卡片式索引内，在未获授权下取览该等资料却不属犯罪"。
在澳大利亚，《示范法典委员会报告书》第 135 页提到：
"纯粹在未获授权下取览并不会构成《［示范刑事］法典》所订罪行，这有别于多个司法管辖区的现有法律。然而，委员会建议把在未获授权下取览受限数据定为简易程序罪行。"
同样，美国联邦法律没有把纯粹在未获授权下取用定为罪行，见 Ian Walden, Computer Crimes and Digital Investigations (Oxford University Press, 2007)，第 3.240 段。
尽管有上文所述，但应注意在某些司法管辖区，例如香港、英格兰及威尔斯、新西兰和新加坡，纯粹在未获授权下取用或取览均构成罪行。

35 [1996] AC 543.

点。[36] 上议院在该案中以三比二的多数裁定，纯粹从电脑数据库提取资料（例如以屏幕显示或印本等形式），不足以构成该法令第 5(2)(b)条[37] 所指的"使用"；*"纯粹取览资料并不足够，还必需对资料作出某些事情"*。[38] 少数法官则持相反看法。

取览程式或数据，而非取用电脑

2.40 上议院在 *R v Bow Street Metropolitan Stipendiary Magistrate, Ex parte United States (No 2)*[39]（"***Ex parte United States***"）中裁定，高等法院分庭（Divisional Court）错误地把《英格兰误用电脑法令》第 1 条局限于对电脑系统的"黑客入侵"，而非将该条应用于针对使用电脑以获得对程式或数据的未获授权取览。[40] 《英格兰误用电脑法令》第 17(6)条的以下内容阐明了"程式或数据"与"电脑"之间的关系：

> "凡提述存于某电脑内的任何程式或数据，即包括提述存于当其时在该电脑内的任何抽取式储存媒体内的任何程式或数据；而电脑须视作包含存于任何上述媒体内的任何程式或数据。"

2.41 按照以上的阐述，举例来说，某人（"**甲方**"）如取走另一人的记忆棒并连接至自己的电脑，意图在未获授权下取览存于该记忆棒内的数据，似乎便犯了《英格兰误用电脑法令》第 1 条所订罪行。

2.42 在上述假设情境中，甲方的目标是存于该记忆棒内的数据。针对在未获授权下取览数据的法例，适合处理这类案件。在某些其他案件中，犯罪者针对的可能是某电脑或电脑系统。尽管在技术层面上，取用电脑也许必定牵涉到取览数据，但若有关犯罪者辩称在未获授权下取览数据（而非取用电脑或电脑系统）的控罪并不适当，也可能言之成理。

---

36 该案的被告人是一名警务人员，有权以所属警察总长的代理人身分，为警务工作这一登记目的而使用全国警察电脑数据库，而该名警察总长是《1984 年资料保护法令》所指的登记使用者。控方指称，被告人为警务工作以外的目的而使用该数据库内的个人资料。虽然有关案情是在《英格兰误用电脑法令》生效前发生，以致无法根据该法令对被告人提出控罪，但被告人代表律师在提出论点时曾提述该法令。若现在发生相同的案情，被告人很可能会根据《英格兰误用电脑法令》被检控。

37 *"载于［资料使用者］登记册的上述记项所涉及的任何人，不得……(b)为该记项所述一个或多于一个目的以外的目的，持有有关资料或使用自己持有的有关资料"*。

38 见上文注脚 35，第 548 页 D 行（上议院大法官哥夫（Lord Goff of Chieveley））。

39 [2000] 2 AC 216.

40 同上，第 226 页 E 行（霍豪斯勋爵（Lord Hobhouse of Woodborough））。

取览的未获授权性质

2.43 在这方面，《英格兰误用电脑法令》第 17(5)条有以下规定：

> "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……"

2.44 在 *DPP v Bignell*，[41] 英格兰高等法院分庭根据其对第 17(5)条的诠释，接纳*"凡任何人获授权获得对任何程式或数据的取览，则该人如按获授权的级别而取用有关电脑，并不属犯［《英格兰误用电脑法令》］第 1 条所订罪行"*，[42] 即使是为未获授权的目的而取用亦然。这项裁定引发了诸多批评。

2.45 其后，上议院在 *Ex parte United States*[43] 否定 *DPP v Bignell* 对第 17(5)条所作的上述诠释。上议院颁布判词，其中指出第 17(5)条并无引入按不同级别取用有关电脑的概念。[44] 因此，按*"获授权的级别"*而取用之说是*"毫不相干的想法"*。[45] 上议院对第 17(5)条的作用有以下概述：

> "该条纯粹指明可取得权限的两种方式：有关人士本身是有权授权的人，或者已获有权授权的人授权。该条亦阐明此权限不仅须关乎有关数据或程式，亦须关乎所获取览的实际类别。"[46]

2.46 上议院依据 *Ex parte United States* 的案情作出以下裁定：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。第 17(5)条并不能协助有关雇员。

---

41 [1998] 1 Cr App R 1.
42 同上，第 13 页（阿斯蒂尔法官（Astill J））。
43 [2000] 2 AC 216.
44 同上，第 225 页 C–F 行（霍豪斯勋爵）。
45 同上，第 226 页 E 行（霍豪斯勋爵）。
46 同上，第 224 页 C–D 行（霍豪斯勋爵）。

2.47　藉《2006 年警察及司法法令》（Police and Justice Act 2006）加入《英格兰误用电脑法令》的第 17(8)条亦与授权问题相关：

> "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。"

犯罪意念

2.48　《英格兰误用电脑法令》第 1(1)条所订的犯罪意念包括：

> (a) 犯罪者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；及
>
> (b) 犯罪者在犯罪行为发生时，知悉该项意图作出的取览未获授权。

2.49　该条提述犯罪者的意图及知悉的事，似乎意味着采用主观测试。这些思想状态是否涉及任何客观元素，以及牵涉何种举证责任等问题，均与刑事法律所有范畴相关。举例来说，载于下文的英格兰及威尔斯《1967 年刑事司法法令》（Criminal Justice Act 1967）第 8 条普遍适用：

> "法庭或陪审团在裁定某人有否犯某罪行时——
>
> (a) 在法律上并非一定需要仅因他的行动的结果是该等行动的自然和颇有可能的后果，而推断他意图造成或预见该结果；但
>
> (b) 须藉参考所有的证据，从该等证据作出在有关情况下看来是恰当的推论，从而决定他当时是否意图造成或预见该结果。"[47]

---

[47] 香港的对等条文是《刑事诉讼程序条例》（第 221 章）第 65A(1)条。唯一的分别在于该条提述该人的"作为或不作为"，而英格兰及威尔斯的法例则提述该人的"行动"。

加重罪行

2.50　任何人如犯《英格兰误用电脑法令》第 1 条所订罪行，并意图干犯（或意图利便干犯）第 2(2)条所指明的罪行，即会构成第 2 条所订的加重罪行（*"在未获授权下取览，并意图干犯或意图利便干犯其他罪行"*），其最高刑罚较重：

"(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。

(2) 本条适用于以下罪行——

(a) 刑罚为法律所固定的罪行；或

(b) 任何年满 21 岁（就英格兰及威尔斯而言，则为年满 18 岁）且无定罪纪录的人，可处为期 5 年监禁的罪行（或在英格兰及威尔斯，假若没有《1980 年裁判法院法令》〔Magistrates' Courts Act 1980〕第 33 条所施加的限制，则可被如此判刑的罪行）。

(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。

(5) 任何人犯本条所订罪行——

(a) 一经在英格兰及威尔斯循简易程序定罪，可处为期不超过 12 个月的监禁或不超过法定最高罚款，或两者兼处；

(b) [……]

(c) 一经循公诉程序定罪，可处为期不超过5年的监禁或罚款，或两者兼处。”

《2003年通讯法令》第125条

2.51 为完整起见，下文载列一项与加拿大《1985年刑事法典》第326(1)(b)条（于上文引用）相若的英格兰及威尔斯条文，即《2003年通讯法令》（Communications Act 2003）第125条（*“不诚实地取得电子通讯服务”*）：

“(1) 任何人——

(a) 不诚实地取得某电子通讯服务，而

(b) 作出上述作为的意图，是逃避缴付适用于提供该服务的收费，

即属犯罪。

(2) [……]

(3) 任何人犯本条所订罪行——

(a) 一经循简易程序定罪，可处为期不超过6个月的监禁或不超过法定最高罚款，或两者兼处；

(b) 一经循公诉程序定罪，可处为期不超过5年的监禁或罚款，或两者兼处。”

中国内地

2.52 首先，我们宜说明在中华人民共和国（“**中国**”）内地全部五类依赖电脑网络的罪行的共通元素。

犯罪意念

2.53 关乎《中国刑法》所订罪行（包括五类依赖电脑网络的罪行）的犯罪意念的一般原则，于《中国刑法》第十四至十六条列明。该等条文规定，犯罪者如：(i)故意犯罪，或(ii)在法律有规定的情况下过失犯罪，须负刑事责任：

"第十四条　明知自己的行为会发生危害社会的结果，并且希望或者放任这种结果发生，因而构成犯罪的，是故意犯罪。

故意犯罪，应当负刑事责任。

第十五条　应当预见自己的行为可能发生危害社会的结果，因为疏忽大意而没有预见，或者已经预见而轻信能够避免，以致发生这种结果的，是过失犯罪。

过失犯罪，法律有规定的才负刑事责任。

第十六条　行为在客观上虽然造成了损害结果，但是不是出于故意或者过失，而是由于不能抗拒或者不能预见的原因所引起的，不是犯罪。"

（底线后加）

2.54　由于《中国刑法》第二百八十五及二百八十六条没有对过失犯罪作出明确规定，因此看来在中国内地，五类依赖电脑网络的罪行的犯罪意念包括第十四条所界定的意图，以及第二百八十五及二百八十六条所指明的下述其他意念元素（如有的话）。

"违反国家规定"

2.55　《中国刑法》第二百八十五及二百八十六条中的所有相关罪行均规定，犯罪者须作出"违反国家规定"的作为。按照《中国刑法》第九十六条的解释，"违反国家规定"是指：

"违反全国人民代表大会及其常务委员会制定的法律和决定，国务院制定的行政法规、规定的行政措施、发布的决定和命令。"

2.56　中国内地的官方资料来源，没有详尽无遗地列明全部相关的国家规定。本咨询文件重点列述看来最为相关的国家规定。

2.57　根据《中国网络安全法》第二十七条：

"任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事侵入网络、干扰网络正常功能及

防护措施、窃取网络数据等危害网络安全活动的程序、工具；明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。”

（底线后加）

2.58 根据《中国计算机信息系统安全保护条例》第七条：

“任何组织或者个人，不得利用计算机信息系统从事危害国家利益、集体利益和公民合法利益的活动，不得危害计算机信息系统的安全。”

（底线后加）

2.59 《计算机信息网络国际联网安全保护管理办法》第六条亦有以下规定：

“任何单位和个人不得从事下列危害计算机信息网络安全的活动：

（一）未经允许，进入计算机信息网络或者使用计算机信息网络资源的；

（二）未经允许，对计算机信息网络功能进行删除、修改或者增加的；

（三）未经允许，对计算机信息网络中存储、处理或者传输的数据和应用程序进行删除、修改或者增加的；

（四）故意制作、传播计算机病毒等破坏性程序的；

（五）其他危害计算机信息网络安全的。”

（底线后加）

《中国刑法》第二百八十五条

2.60 《中国刑法》第二百八十五条第一款有以下规定：

“违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。”

（底线后加）

2.61 《中国刑法》第二百八十五条第二款进一步述明：

> "违反国家规定，侵入前款规定以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，或者对该计算机信息系统实施非法控制，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。"

（底线后加）

"计算机"的涵义

2.62 按2011年8月公布的《最高人民法院、最高人民检察院关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》（"**法释〔2011〕19号**"）所指示，"计算机信息系统"一词是指具备自动处理数据功能的系统，包括计算机、网络设备、通信设备、自动化控制设备等。

犯罪行为

2.63 根据第二百八十五条第一款，纯粹在未获授权下进入指明类型[48]的计算机信息系统会构成罪行。就其他类型的计算机信息系统而言，第二百八十五条第二款规定，除了纯粹在未获授权下进入外，犯罪者还须获取该计算机信息系统中存储或处理的数据，才会招致刑事责任。

进入的未获授权性质

2.64 根据中国最高人民检察院公布的第九批指导性案例[49]的第36号案例，第二百八十五条第一款中的"侵入"一词，是指违背被害人意愿、非法进入计算机信息系统的行为。其表现形式既包括采用技术手段破坏系统防护进入计算机信息系统，也包括未取得授权擅自进入计算机信息系统，还包括超出授权范围进入计算机信息系统。[50]

---

48 见上文第2.60段。

49 根据《最高人民检察院关于案例指导工作的规定》第十五条，各级人民检察院可以引述相关指导性案例进行释法说理，但不得代替法律或者司法解释作为直接依据。

50 最高人民检察院公布的第九批指导性案例第36号（卫梦龙、龚旭、薛东东非法获取计算机信息系统数据案），该案的指导意义指出："*非法获取计算机信息系统数据罪中的'侵入'，*

新西兰

新西兰《1961 年刑事罪行法令》第 249 及 252 条

2.65 新西兰《1961 年刑事罪行法令》（Crimes Act 1961，**《新西兰法令》**）订有三项与本章相关的罪行，其最高刑罚轻重有别。在这些罪行中，第 252 条（*"在未获授权下取用电脑系统"*）所订罪行的最高刑罚最轻：

> "(1) 任何人知悉自己未获授权取用任何电脑系统，或罔顾自己是否已获授权取用任何电脑系统，而在未获授权下蓄意直接或间接取用该电脑系统，可处为期不超过 2 年的监禁。
>
> (2) 为免生疑问，任何人如获授权取用某电脑系统，为某目的获准取用，而为其他目的而取用该电脑系统，则第(1)款并不适用。"

2.66 其他两项罪行载于《新西兰法令》第 249 条（*"为不诚实目的而取用电脑系统"*）：

> "(1) 任何人直接或间接取用任何电脑系统，并藉此不诚实地或以欺骗手段在无声称拥有权利的情况下——
>
> (a) 取得任何财产、特权、服务、金钱利益、得益或有值代价；或
>
> (b) 导致其他人蒙受损失，
>
> 可处为期不超过 7 年的监禁。
>
> (2) 任何人直接或间接取用任何电脑系统，意图不诚实地或以欺骗手段在无声称拥有权利的情况下——
>
> (a) 取得任何财产、特权、服务、金钱利益、得益或有值代价；或
>
> (b) 导致其他人蒙受损失，

是指违背被害人意愿、非法进入计算机信息系统的行为。其表现形式既包括采用技术手段破坏系统防护进入计算机信息系统，也包括未取得被害人授权擅自进入计算机信息系统，还包括超出被害人授权范围进入计算机信息系统。"

可处为期不超过5年的监禁。

(3) 在本条中，**欺骗手段**的涵义与第240(2)条中该词的涵义相同。"[51]

2.67 应注意的是，第249(1)及(2)条均采用类似的措辞。两者的主要分别在于：

(a) 前者规定被告人须已取得财产、特权等或已导致损失；而

(b) 后者只规定被告人须已意图取得财产、特权等而行事或已意图导致损失而行事。

正因为有上述分别，第249(1)及(2)条所订两项罪行的最高刑罚各异。

"电脑系统"和"电脑"的涵义

2.68 根据《新西兰法令》第248条，"电脑系统"一词：

"(a) 指——

(i) 一部电脑；或

(ii) 两部或以上互连的电脑；或

(iii) 电脑之间的任何通讯链路，或通往远程终端机或另一器材的任何通讯链路；或

(iv) 两部或以上互连的电脑，并与电脑之间的任何通讯链路相结合，或与通往远程终端机或任何其他器材的任何通讯链路相结合；并

(b) 包括(a)段所述项目的任何部分，以及所有相关的输入、输出、处理、储存、软件或通讯设施及已储存数据。"

---

[51] 第240(2)条对欺骗手段的定义如下：

"(a) 属口头或书面形式或藉行为作出的虚假申述，而作出该申述的人意图欺骗其他人并——

(i) 知悉该申述在要项上属虚假；或

(ii) 罔顾该申述是否在要项上属虚假；或

(b) 在有责任披露某要项的情况下，意图欺骗任何人而不披露该要项；或

(c) 意图欺骗任何人而使用的欺诈手段、手法或计谋。"

2.69 《新西兰法令》并无界定何谓电脑。这种做法固然使法律不会因科技进步而变得不合时宜，但在某些案件中，被告人有罪与否可能取决于其所用的器材在法律上是否构成电脑。[52] 这个争议点与被告人的行为在事实和道德上应否受刑事制裁的问题相去甚远。

2.70 *Pacific Software Technology Ltd v Perry Group Ltd*[53] 是一宗涉及这个争议点的新西兰案例，当中关乎电脑程式的版权争议。新西兰上诉法院的以下论述，刻划出数码电脑及电脑程式的特点：

> "数码电脑以五项功能元素为基础：(i)输入；(ii)由记忆体系统储存该输入；(iii)从记忆体接收数据并发出必要算术指令的控制单元；(iv)执行控制命令的算术运算；及(v)输出容量。
>
> 电脑程式只是一组向电脑发出的指令。大多数程式均接受并处理使用者所提供的数据。程式编制员采用的基本程序称为算法（即机械式计算程序），是程式的核心所在。只有运用程式编制员的人类创造力，才能开发出这些算法。因此，程式并不可能包含任何从未被人考虑的算法。电脑的优势仅仅是能够比人类更快和更准确地执行这些算法。"[54]

取用的未获授权性质

2.71 第252(1)条明确规定取用须属未获授权，而且犯罪者须对此知情或罔顾实情，才会产生刑事法律责任。然而，第252(2)条继而订明，*"任何人如获授权取用某电脑系统，为某目的获准取用，而为其他目的而取用该电脑系统"*，则第252(1)条并不适用。

2.72 新西兰上诉法院在 *Watchorn v R*[55] 确认，*"第252(2)条的效力，是把雇员为未获授权的目的而取用的情况豁除于该条的适用范围之外。"*[56] 换言之，有关取用并不构成第252条所订罪行。这似乎较澳大利亚的情况宽松。如上文所论述，根据澳大利亚的条文，任何人如

---

52 在香港，这种情况见于*律政司司长 诉 王嘉业* [2013] 4 HKLRD 588, HCMA 77/2013（判决日期：2013年4月29日），上文讨论第161条时已引述该案。

53 [2004] 1 NZLR 164.

54 同上，第168页，第25及26段。

55 [2014] NZCA 493.

56 同上，第79段。同时，判案书注脚33暗示，第252(2)条把雇员豁除的做法可能并不符合原意。

为隐秘目的而取览电脑数据，则只有在该人亦有合法目的之情况下，才可免除刑事法律责任。

2.73 新西兰的情况看来亦较 *Ex parte United States* 所阐述的《英格兰误用电脑法令》宽松。如上文所述，上议院在该案中拒绝接纳源自 *DPP v Bignell* 的下述观点：任何获授权取览程式或数据的人，如按获授权的级别而取用有关电脑，并不属违反《英格兰误用电脑法令》第 1 条，即使是为未获授权的目的而取用亦然。

对第 249 条的解释

2.74 《新西兰法令》第 249 条并无提述授权这概念。

2.75 在 *Watchorn v R*,[57] 新西兰上诉法院对《新西兰法令》第 249(1)条所订罪行的元素有以下论述：

> "我们认为，把第 249(1)条说成规定须有取得得益的不诚实目的并不正确。虽然第 249 条的标题是'为不诚实目的而取用电脑系统'，但这并不能准确概述第 249(1)条所订立的罪行。第 249(1)条的构成元素并不包括不诚实目的。控方须证明的是，被告人曾取用电脑系统，并藉此不诚实地或以欺骗手段在无声称拥有权利的情况下取得得益。
>
> [依据有关案情] ……控方无须证明 [被告人] 是为甚么目的而 [从其雇主的电脑系统] 下载 [某些数据]。控方反而须证明被告人已取得得益，并且是不诚实地在无声称拥有权利的情况下取得该得益。"[58]

2.76 新西兰上诉法院亦裁定，虽然有关电脑数据按照先前的案例并不属第 249(1)(a)条所指的"财产"，[59] 但同一条文中的"得益"涵盖 *"任何使有关人士受益的东西"*，并且不限于经济利益。[60] 因此，可合理争辩的是，被告人 *"管有、控制并因此而有机会使用已下载的档案，构成第 249(1)(a)条所指的'得益'。"*[61]

---

57 见上文注脚 55。
58 同上，第 26 及 42 段。
59 同上，第 22 段。
60 同上，第 81 段。
61 同上，第 83 段。

新加坡

《新加坡误用电脑法令》第 3 及 4 条

2.77 如导言所指出,《新加坡误用电脑法令》所订罪行主要以《英格兰误用电脑法令》为基础。正如《英格兰误用电脑法令》以第 1 条把在未获授权下取览电脑资料定为不合法,再以第 2 条订定加重罪行一样,《新加坡误用电脑法令》也采用两层式的做法。《新加坡误用电脑法令》第 3 条(*"在未获授权下取览电脑资料"*)的内容如下:

> "(1) 除第(2)款另有规定外,任何人故意致使某电脑执行任何功能,目的是为了在没有权限的情况下获得对存于任何电脑内的任何程式或数据的取览,即属犯罪,一经定罪——
>
> (a) 可处不超过$5,000 的罚款或为期不超过 2 年的监禁,或两者兼处;及
>
> (b) 如属第二次或其后每次定罪,则可处不超过$10,000 的罚款或为期不超过 3 年的监禁,或两者兼处。
>
> (2) 如因本条所订罪行而导致任何损坏,被裁定犯该罪行的人可处不超过$50,000 的罚款或为期不超过 7 年的监禁,或两者兼处。
>
> (3) 就本条而言,如有关作为并非针对——
>
> (a) 任何特定程式或数据;
>
> (b) 任何种类的程式或数据;或
>
> (c) 存于任何特定电脑内的程式或数据,
>
> 均属无关重要。"

2.78 《新加坡误用电脑法令》第 4 条(*"意图犯罪或意图利便犯罪而取览"*)订立了以下加重罪行:

> "(1) 任何人如意图干犯本条所适用的罪行而致使某电脑执行任何功能,目的是为了获得对存于任何电脑内的任何程式或数据的取览,即属犯罪。

(2) 本条适用于任何涉及财产、欺诈、不诚实或导致身体受伤害，且一经定罪可处为期不少于2年监禁的罪行。

(3) 任何人犯本条所订罪行，一经定罪，可处不超过$50,000的罚款或为期不超过10年的监禁，或两者兼处。

(4) 就本条而言——

(a) 第(1)款所提述的取览是否已获授权；

(b) 不论本条所适用的罪行是在获得上述取览时干犯或在任何其他时间干犯，

均属无关重要。”

“电脑”的法定定义

2.79 尽管《新加坡误用电脑法令》第3及4条与《英格兰误用电脑法令》中的对等条文有相似之处，值得注意的是，《英格兰误用电脑法令》并无界定何谓“电脑”，而《新加坡误用电脑法令》第2(1)条则将“电脑”定义为：

“执行逻辑、算术运算或储存功能的任何电子、磁性、光学、电子化学或其他数据处理器材，或一组互连或相关的该等器材，亦包括任何与该器材或该组互连或相关的该等器材直接有关或共同操作的数据储存设施或通讯设施，但不包括——

(a) 自动打字机或排字机；

(b) 便携式手提计算机；

(c) 不可编程或不包含任何数据储存设施的相类器材；或

(d) 部长藉宪报公告订明的其他器材”。

2.80 上述定义中的许多部分均与《美国法典》第 18 篇第 1030(e)(1)条（18 USC 1030(e)(1)）[62] 的法定措辞相似。某评论员曾作出以下恰当的评析：排除打字机、排字机、计算机等的做法*"立即显示出该条文的制定年代，亦完全反映采用特定的技术性措辞所带来的危险"*。[63] 就电脑网络罪行这类课题而言，有特别充分的理据支持法例采用科技中立的措辞。

美国

《电脑欺诈及滥用法案》（Computer Fraud and Abuse Act）（《美国法典》第 18 篇第 1030 条）

2.81 在美国，任何人如作出与《美国法典》第 18 篇第 1030(a)条所述各种情境有关的作为，可按第 1030(c)条的规定予以惩处。在这些情境中，与本章相关的情境是某人：

> "(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；
>
> (3) 在未获授权取用美国某部门或机关的任何非公用电脑的情况下，蓄意取用该部门或机关的上述电脑……

---

62 *"在用于本条时……'电脑'一词指执行逻辑、算术运算或储存功能的任何电子、磁性、光学、电子化学或其他高速数据处理器材，亦包括任何与该器材直接有关或共同操作的数据储存设施或通讯设施，但该词不包括自动打字机或排字机、便携式手提计算机或其他相类的器材"*。

63 Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd edition, 2015)，第 65 页。

(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……

(5) (A) 故意导致向某受保护电脑传送程式、资料、代码或指令，并因着该行为而在未获授权下蓄意导致该电脑损坏；

(B) 在未获授权下蓄意取用某受保护电脑，并因着该行为而罔顾后果地导致损坏；或

(C) 在未获授权下蓄意取用某受保护电脑，并因着该行为而导致损坏及损失。"[64]

企图取用但不成功

2.82 根据第 1030(b)条，*"任何人如串谋犯或企图犯本条(a)款所订罪行，须按本条(c)款的规定予以惩处。"*这项条文与澳大利亚《刑事法典》（联邦）第 477.1(8)条恰恰相反。如上文所述，第 477.1(8)条免除企图犯罪的刑事法律责任。

取用的未获授权性质

2.83 《美国法典》第 18 篇第 1030 条的结构和格式，与香港的法例和上文所探讨的司法管辖区的法例有颇大差别。如美国的法理有值得香港借鉴之处，其中一处是当地法院对《美国法典》第 18 篇第 1030(a)条所提述的*"在未获授权下"*取用电脑，以及以*"超逾获授权的取用范围"*的方式取用这两者的区别，进行了详尽的分析。

2.84 尤其是，虽然《美国法典》第 18 篇第 1030(e)(6)条说明，*"'超逾获授权的取用范围'一词指在获授权下取用某电脑，并藉该项取用而取得或更改该电脑中的资料，但取用者无权如此取得或更改该等资料"*，不同巡回区的多宗案例都关乎*"在未获授权下"*及*"超逾获授权的取用范围"*这两个用语的涵义。

2.85 举例来说，联邦上诉法院第二巡回法庭（Court of Appeals for the Second Circuit）在 *United States v Valle*[65] 指出，下述的关键争议点*"引起了姐妹巡回区之间的严重分歧"*：

---

64 《美国法典》第 18 篇第 1030(a)(1)–(5)条。

65 807 F 3d 508 (2d Cir 2015)，2015 年 12 月 3 日。

> "……如任何人为不当目的而取用电脑，以取得或更改该人在其他情况下获授权取览的资料，是否属'超逾获授权的取用范围'而取用电脑；还是只有该人取得或更改自己未获授权为任何目的而取览的资料，而该等资料位于该人在其他情况下获授权取用的电脑时，方属'超逾获授权的取用范围'。"

该法院断定这两种解释均可接受，因此*"须按规定运用从宽原则，并采用后一种解释"*。

2.86 *United States v Valle*[66]与联邦上诉法院第九巡回法庭（Court of Appeals for the Ninth Circuit）全体法官[67]于2012年对*United States v Nosal*[68]所作的裁决相符一致，该项裁决掀起了热烈的学术辩论。审理*United States v Nosal*[69]的同一法庭在其后一项以大比数所作的裁决中，就*"在未获授权下"*一词作出对被告人较为不利的解释，[70]这增添了法律的不确定性。在这其后裁决中，大比数的法官实际上裁定只有电脑系统的拥有人方可授权某人取用该系统，而少数法官则认为系统拥有人或合法的帐户持有人均可授权。

2.87 不久之后，在*Facebook, Inc v Power Ventures, Inc*，[71]由与先前不同的法官所组成的联邦上诉法院第九巡回法庭采纳*United States v Nosal*[72]中第二项裁决的方针，并述明*"在分析《电脑欺诈及滥用法案》[（即《美国法典》第18篇第1030条）]所指的授权时应依循的两项一般规则"*：

> "首先，若被告人不获准许取用电脑，或该准许已被明确撤销，被告人即可能触犯《电脑欺诈及滥用法案》。一

---

66 同上。

67 《联邦上诉程序规则》（Federal Rules of Appellate Procedure）第35(a)条订明：
"多数并未丧失资格的常任现职巡回法官，可命令任何上诉或其他法律程序由上诉法院的全体法官进行聆讯或重新聆讯。除非有下述情况，否则由全体法官进行聆讯或重新聆讯并不可取，而且通常不会被命令进行：
(1) 有必要由全体法官考虑，以确保或维持法院裁决的统一性；或
(2) 有关法律程序牵涉某个极为重要的问题。"
根据《美国法典》第28篇第46(c)条，*"全体法官组成的法庭须由所有常任现职巡回法官组成，或由……订明人数的法官组成……"*。

68 676 F 3d 854 (9th Cir 2012)，意见书于2012年4月10日送交存档。

69 844 F 3d 1024 (9th Cir 2016)，意见书于2016年7月5日送交存档，并于2016年12月8日修订。

70 同上。

71 844 F 3d 1058 (9th Cir 2016)，意见书于2016年7月12日送交存档，并于2016年12月9日修订。

72 见上文注脚69。

旦准许被撤销，即使施展科技手段或征募第三方协助取用，也不会免除法律责任。第二，单单违反网站使用条款，并不足以确立《电脑欺诈及滥用法案》之下的法律责任。”

2.88 2017 年 10 月 10 日，最高法院在 *United States v Nosal* 和 *Facebook, Inc v Power Ventures, Inc* 拒绝作出移审令[73]（即拒绝聆讯拟进行的上诉），并无借此机会阐明有关的解释方式。

小组委员会的看法

宜制定针对电脑网络罪行的特定法例

2.89 目前，香港法例并无任何适用于电脑网络罪行的特定条例。不同罪行在各条例中订立，当中部分条例亦不合时宜。相比之下，上文论述的其他司法管辖区大多数有针对电脑网络罪行的特定法例，或以其部分成文法专门处理电脑网络罪行。我们认为这些司法管辖区的做法有其可取之处，因为这种做法有助确保在此领域内（例如在主要概念的定义方面）做到协调统一、周全完备和贯彻一致。

2.90 故此，我们建议制定一项针对电脑网络罪行的特定法例，当中包括本章和后面各章所建议的罪行，藉以全盘改革现行法律。尽管如此，我们也紧记第 161 条等现有条文在打击电脑网络罪行方面发挥着重要作用。虽然法律应尽量避免罪行互相重迭，但我们建议保留现有条文，直至新法例显然足以取而代之。

主要词语的定义

2.91 据我们所观察，现今不少器材都装有微处理器，并具备作特定用途的处理能力。《牛津英文字典》（Oxford English Dictionary）目前对“电脑”（computer）的定义已反映现今的科技状况，内容如下：

> “一项电子装置（或一项由多个装置组成的系统），用于储存、操控和传达资料，执行复杂的计算，或控制或调节其他装置或机器，并可接收资料（数据）及按照可变的程式指令（程式或软件）处理该等资料；尤指一项供人在家中或工作场所使用的小型自给式电子装置或系

[73] 美国最高法院，*Journal of the Supreme Court of the United States* (Oct Term 2017)，第 149 页，登载于 https://www.supremecourt.gov/orders/journal/Jnl17.pdf（于 2022 年 5 月 3 日浏览）。

> 统，尤其用作处理文字、图像、音乐和录像，接达和使用互联网，（例如以电邮等方式）与他人通讯，以及玩游戏。"[74]
>
> （底线后加）

2.92 1984年，《证据条例》（第8章）加入"电脑"的法律定义。就在刑事法律程序中接纳文件证据而言，"电脑"被界定为*"任何用作储存、处理或检索资料的装置"*。[75] 前述宽广的字典定义（或上文所引述条例中法定定义的字面解读）涵盖不同器材，其中一些例子包括：具备加密功能的记忆棒、模糊逻辑电饭煲、智能照明系统、网络摄影机和智能电视。

2.93 我们亦留意到《俄罗斯公约》所采用的其他术语，当中分别对"资讯及通讯科技"和"资讯及通讯科技器材"下定义。"资讯及通讯科技"指*"为产生、转换、传送、利用和储存资料而互连的方法、流程、硬件和软件的集合"*。[76] 同样地，"资讯及通讯科技器材"指*"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）"*。[77] 我们认为，尽管数码科技不断演进，但与"资讯及通讯科技器材"相比，"电脑"一词的概念仍然清晰，不仅为大众所通晓，我们的比较研究所引述各司法管辖区的法例亦广泛使用"电脑"一词。

2.94 我们进一步考虑了应否参考《俄罗斯公约》所采用的"资讯及通讯科技器材"的涵义，为"电脑"赋予法定定义。就此而言，我们注意到高等法院原讼法庭对*律政司司长 诉 王嘉业*[78] 的判决：

> "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

74 《牛津英文字典》（2022年3月）。
75 《证据条例》第22A(12)条。
76 第四条第(f)款。
77 第四条第(o)款。
78 [2013] 4 HKLRD 588, HCMA 77/2013（判决日期：2013年4月29日）。

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。"[79]

2.95 我们认为法院上述观点也适用于我们所建议的罪行。罪犯可能为不合法的目的而入侵任何具备处理能力的器材，例如为发动分布式拒绝服务攻击而组成僵尸网络。随着物联网兴起，未来数年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"所下的定义），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。我们固然可以信任法院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。在考虑和权衡所有因素后，我们认为不界定"电脑"和"电脑系统"等词语较为可取。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个议题。

把纯粹在未获授权下取用或取览定为不合法

2.96 我们基于下述法律和实际的考虑因素，仔细考虑新法例应否禁止纯粹在未获授权下取用或取览：

(a) 在香港，纯粹在未获授权下取用已属第 27A 条所订罪行，但该罪行仅适用于犯罪者*"藉着电讯"*取用的情况，而被定罪的人亦只须缴付罚款。某些其他司法管辖区（例如英格兰及威尔斯、新西兰）亦把纯粹在未获授权下取览及取用定为不合法，但所处的最高刑罚一般相对较轻。

(b) 《说明报告》表示，*"原则上，纯粹在未获授权下入侵"*电脑系统及数据*"本身应属非法。"*[80]

(c) 因着各种合法或可能不合法的理由，在未获授权下取用电脑／取览程式或数据的情况每分每秒都在互联网上发生，

---

[79] 同上，第 601 页（高等法院原讼法庭法官冯骅）。

[80] 《说明报告》第 44 段（于上文第 2.19 段引用）。

例如下文所详述的连接埠扫描。[81] 举例来说，取览网站者未必是人，机械人也可能会“爬行”未受保护的网站。此外，一般无专业知识的人或许难以得知自己的电脑是否曾被他人取用，不论该取用是否恶意作出。

(d) 实际上，即使准许任何网上用户全面授权他人扫描该用户的程式或数据（由此无需就未获授权的扫描提供豁免），也未必有助于应对现实世界的情况。除了难以划定有关扫描的界线外，获如此授权的人亦可能会滥用上述权限，为了自己的利益（亦即为网络安全以外的目的）而使用所取览的程式或数据。在某些情况下，网上用户与操作人实际上亦可能无法在有关扫描发生前缔结合约关系。举例来说，要搜寻器开始在互联网“爬行”之前，先逐一与各网站以某种形式缔结令人满意的合约关系，并非切实可行。

2.97 小组委员会曾详尽讨论以下事项：(a)在未获授权下取用电脑／取览程式或数据，与现实世界中陌生人在未获准许下进入某地方（例如某人的居所）的情境到底有多类似，以及(b)纯粹在未获授权下取用或取览应否招致刑事后果。在现实世界中，如任何人在未获准许下进入他人的居所，并告知后者其门锁不够牢固，则不论入侵者在通过大门后是否立即止步，该进入本身已属错误。我们难以找到任何理由，支持在电脑网络空间准许某些在现实世界被禁止的行为。故此我们认为，纯粹在未获授权下取用电脑／取览程式或数据应属犯罪。

2.98 就上述在未获授权下取用或取览而言，有关取用或取览应在何时定为不合法可能会令人混淆（例如到底在取用或取览时便应定为不合法，还是在入侵者于取用或取览后作出其他错误作为时方定为不合法）。由于法律的明确性相当重要，故小组委员会大多数成员认为，纯粹在未获授权下取用电脑／取览程式或数据应定为简易程序罪行，该罪行并无规定恶意为罪行元素，而合理辩解可作为法定免责辩护。

取用或取览的未获授权性质

2.99 如上文所述，[82] 取用的未获授权性质是第 27A 条所订罪行的元素，但就第 161 条而言，取用须属未获授权只不过是法院对该条的解释。

---

81 连接埠是网络连接起始与结束的虚拟点，均以软件为基础，并由电脑系统管理。每项互联网服务均与某连接埠相关，例如网络接达是与连接埠 80 及 443 相关。亦见第 2.5 段注脚 2。

82 第 2.9 及 2.11 段。

2.100　我们认为，新法例应明文规定取用或取览须属未获授权，从而提供指引以消除不必要的争议。上述其他司法管辖区的法规展示了多种方式来描述取用或取览的未获授权性质，我们在审视这些法规后，认为 *Ex parte United States*[83] 所阐述的《英格兰误用电脑法令》第 17(5)及(8)条较为可取。就此而言，我们希望重申，基于我们在较早部分解释"在未获授权下"取用或取览这一概念时所述的理由，应继续容许在日常生活中已普遍接受在进入电脑网络空间时的惯常做法，亦即无须就我们已举例说明的取用或取览程度，事先寻求明示授权。[84] 我们正是在这基础上建议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。

2.101　我们进一步认为，把某人知悉其取用或取览未获授权定为我们所建议罪行的先决条件，是公允的做法。我们预料，法院很可能会根据环境证据，作出关于某人是否知悉未获授权的推论。按照常理，人们应知道进入某特定地方是否获得准许。就此而言，两种截然不同的比喻，分别是在营业时间内进入百货公司，以及在银行保险库大门敞开时走进去。我们确信，按常理判断的同一方针也适用于电脑网络空间，故此举例来说，即使某人的电脑器材或系统并不受密码或其他保安措施保护，我们认为也不应视该人为一律同意对有关程式或数据的任何取览，而且若有关取览超出了人们在一般使用电脑网络空间时通常可接受的限度，构成入侵（例如对他人的 WhatsApp 进行黑客入侵），便应产生在未获授权下取览的法律责任。

取览程式或数据

2.102　我们的比较研究显示，不同司法管辖区在这方面的取向各异。第 27A 条提述取用程式或数据，《英格兰误用电脑法令》第 1 条及《新加坡误用电脑法令》第 3 条提述取览程式或数据，而第 161 条以及《新西兰法令》第 249 及 252 条则分别提述取用电脑及电脑系统。

2.103　"电脑"的涵义正在迅速演变，但"程式"及"数据"两词既有相对明确的定义，亦一直无甚改变。"程式"是*"一连串编码指令和定义，在输入某电脑时会自动指示其操作，藉以执行某特定工作"*，[85] "数据"

83　见第 2.43 至 2.47 段。

84　见第 2.5 段。

85　《牛津英文字典》（2022 年 3 月）。

则指*"任何电脑对其进行运算并视为一个整体的数量、字符或符号"*。[86] 在非技术层面上，"数据"亦指*"数码形式的资料"*。[87] 我们倾向于提述取览程式或数据，因为这样较为清晰，亦可避免把有关罪行与任何实体器材不必要地联系起来。电脑只是一种工具或器材，当中储存的资料（主要是数据和程式）才属重要，亦是任何未获授权取用或取览的目标所在。我们认为，若提述取用电脑，看来会过于局限。

合理辩解可作为免责辩护

2.104 我们曾讨论应建议订定多项适用于特定情况的免责辩护、一项基于（比如说）取览有合理辩解的全面性免责辩护，还是应同时订定这两类免责辩护。

2.105 就第一种做法而言，要做到周全无缺并就每项度身订造的免责辩护制定准则，实非易事。举例来说，我们曾分析应否为特定类型的取览（如测试电脑系统是否有已知的保安漏洞，例如是具预设密码的网络摄影机或所运行作业系统未经修补的电脑）或者特定类别的人士（如经认可专业团体审定的网络安全从业员）提供免责辩护。要以切合文化及实况并在技术层面上不易引起事实争议的准则来制定免责辩护，对我们来说实属挑战。

2.106 我们的结论是，基于合理辩解的概括性免责辩护能更有效兼顾公众利益，应付未能预见的情况，并给予法院酌情权和弹性去决定被告人应否获判无罪。因此，我们建议采用这种做法。由于一切都视乎案件的证据和情况而定，似乎无须担心这类免责辩护会有被滥用的风险。以下例子正可阐明这一点：尽管被告人的网络安全从业员审定资格可能属重要因素，但被告人未必会因此而获宽免未获授权取览的罪责。

加重罪行

2.107 在决定建议订立上述的简易程序罪行时，我们意识到犯罪者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。

---

86 同上。
87 同上。

2.108　在借鉴上文所探讨的某些司法管辖区的法例后，我们建议，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。至于哪些其他犯罪活动会触发加重罪行，我们认为适宜以《英格兰误用电脑法令》第 2(2)条[88] 的拟定方式为起点。

香港法例的蓝本

2.109　我们建议，建议的条文应以《英格兰误用电脑法令》第 1、2 及 17 条为蓝本，并可适当参照其他司法管辖区法例的良好草拟方式。

建议 1

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《英格兰误用电脑法令》第 1、2 及 17 条为蓝本。

在未获授权下为网络安全目的而取览

2.110　读者或许注意到，我们在上文探讨应就建议罪行订定何种免责辩护时，曾多次提及网络安全从业员。这反映我们曾广泛讨论在未获授权下为网络安全目的而取览这一概念。

2.111　我们认为宜开宗明义先说明何谓"网络安全"。其他司法管辖区的科技公司和网络安全机构所下的各种定义[89] 的共通点，是以保护

88　于上文第 2.50 段引述。

89　举例来说，英国政府的国家网络安全中心（National Cyber Security Centre）把网络安全形容为*"个人及组织减低网络攻击风险的方式"*，并指网络安全的核心功能是保护*"所有人均使用的器材（智能电话、手提电脑、平板电脑和电脑），以及人们在上网和工作时均会取用的服务，使之免遭盗窃或损坏"*。同样地，美国政府的网络安全及基础设施安全局（Cybersecurity and Infrastructure Security Agency）把网络安全界定为*"保护网络、器材及数据免受未获授权的*

电脑系统免受数码攻击的做法，作为“网络安全”这个概念的根基。就本咨询文件而言，以下的学术文章勾划出“网络安全”的精髓：

> “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）损害而采取的各种程序。”[90]

2.112 有鉴于下述背景，我们考虑了在未获授权下为网络安全目的而取览所涉及的各个议题：

(a) 在环球层面，总会有人在电脑网络空间测试他人的电脑，而往往没有事先取得他人授权。用作测试电脑数据或系统的工具既容易获取，又得到广泛使用。

(b) 举例来说，这类测试的一种常见形式称为连接埠扫描。[91] 虽然连接埠扫描只会令被扫描的电脑产生日志纪录而不会造成不良影响，但若网络活动异常增加，有关电脑的系统管理员或拥有人可能会有所警觉，耗费时间和金钱来调查该电脑是否已被入侵。

(c) 从科技角度来看，连接埠扫描是否构成取用目标电脑，是颇具争议的问题。但就概念而言，以概括方式拟定的在未获授权下取览罪似乎可能适用于连接埠扫描。《英格兰误用电脑法令》第 1 条所订罪行便是一例，当中“取览”一词按第 17(2)条解释。

(d) 人们测试他人的电脑，可能是出于善意、商业目的或恶意。举例来说：

(i) 于 2017 年“WannaCry”事件期间，[92] 一些网络安全专家进行测试，并提醒相关电脑用户其电脑须安装修补程式以免遭受感染。这些专家的工作显然惠及社会。

---

*取用或取览或免被用作犯罪的技巧，以及确保资料机密、完整和可用的常规。”*分别见 https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security 及 https://www.cisa.gov/uscert/ncas/tips/ST04-001#:~:text=Cybersecurity%20is%20the%20art%20of,integrity%2C%20and%20availability%20of%20information（于 2022 年 5 月 3 日浏览）。

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

91 见上文注脚 81。

92 “WannaCry”是一款加密勒索软件，会透过网络扫描存在某种 Microsoft Windows 保安漏洞而未经修补的电脑，然后作出攻击。全球多处地方，包括香港的电脑用户均受到影响。例如见香港生产力促进局属下的香港电脑保安事故协调中心于 2017 年 5 月 13 日发布的新闻稿，登载于 https://www.hkcert.org/tc/press-center/hkcert-security-alert-watch-out-for-wannacry-ransomware（于 2022 年 5 月 3 日浏览）。

(ii) 某人进行连接埠扫描，可能是为了得知某电脑是否已安装最新的修补程式、某伺服器的哪个连接埠编号可供连接等。若识别到问题，该人或会就此收取高昂的修复费用。这些资料亦可能利便其他犯罪活动，例如以恶意软件感染有关电脑。

就连接埠扫描而言，单凭日志纪录无法洞悉某人进行扫描的背后意图。缺乏科技知识的电脑用户，甚至无从知晓自己的电脑已被扫描。

(e) 一些网络安全公司从不间断地扫描互联网，以确定网络摄影机、网页伺服器等是否有某些常见的保安漏洞。若识别到保安漏洞，这些公司或会主动提出作收费修复。他们的客户亦可订阅已识别保安漏洞的资料，这些漏洞所涉及的互联网规约地址可能是由客户本身使用，亦可能是由其他人使用。

(f) 网络安全是个不断变化的领域，评审情况亦一直演变。对网络安全从业员来说，活跃于香港以至国际的业界机构众多，没有机构获视为唯一权威。[93]

(g) 不少网络安全从业员均具备实际经验，但资格未经正式审定，至少在香港如是。若干年前，香港金融管理局在推行网络防卫计划以提高银行业抵御网络攻击的能力时，曾承认本港经审定的网络安全专业人员数目有限。[94]

(h) 在香港商界，预防性网络安全服务显然不太流行。企业往往在发生网络安全事故后，才会寻求协助以采取补救行动和加强它们的电脑系统。

(i) 香港固然可选择订立新罪行，藉以禁止各种未获授权的电脑测试，但即使订立该罪行，事实上也无法阻止他人从其他司法管辖区扫描在香港的电脑系统。

(j) 无论如何，罪犯一般使用自己的网络来扫描互联网以寻找保安漏洞，而并非依赖网络安全公司。禁止各种未获授权

---

93 香港网络安全团体的一些例子，包括专业资讯保安协会和资讯保安及法证公会。其他与本港资讯科技专业人员有关的团体包括：香港电脑学会、香港资讯科技商会、香港资讯科技联会和香港互联网供应商协会。

94 见时任香港金融管理局总裁于 2016 年 5 月 18 日发表的网络安全峰会主题演辞，第 8 段，登载于 https://www.hkma.gov.hk/chi/news-and-media/speeches/2016/05/20160518-2/。

的测试，只会对网络安全公司构成影响，却无法制止罪犯识别这些漏洞。

2.113 基于上述各点，对于应如何在获准许与不获准许的取览之间划定界线，似乎难免会意见纷纭。某些人可能认为，若各种未获授权的电脑测试不论因由，亦不论测试是否造成损坏，均可产生刑事法律责任，我们所建议的罪行便会过于广阔。

2.114 因此，我们曾考虑在未获授权下为网络安全目的而取览，在新法例下应否有免责辩护或豁免。应注意的是，举例而言，在保障资料方面的现有法律下，《个人资料（私隐）条例》（第 486 章）第 61 条[95] 就"新闻活动"订有豁免。考虑到即使未获授权取览是为了网络安全目的，亦有不同论据支持和反对禁止这类取览，要平衡兼顾这些互相矛盾的论据实有困难，因此我们不拟在现阶段确定立场，而是欢迎公众就下文建议 2(a)所载的咨询问题提出意见。

2.115 我们希望指出，若我们的法律应给予网络安全业界的专业人员免责辩护或豁免（待我们收到公众意见后才能决定这一点），便必须处理如何可确定或核实这类专业人员的身分这个基本问题。如上文所述，[96] 香港的网络安全从业员目前未经任何评审团体或专业团体正式认可，故此，可行方案之一是制订某种形式的评审制度，为网络安全专业人员提供认证机制，若届时有人须倚赖任何建议的免责辩护或豁免，便能以此轻易识别出这些专业人员。为方便公众提出有据可依

---

95 *"(1) 由——*
(a) 其业务或部分业务包含新闻活动的资料使用者持有；及
(b) 该使用者纯粹为该活动（及任何直接有关的活动）的目的而持有，
的个人资料，获豁免而——
(i) 不受第 6 保障资料原则及第 18(1)(b)及 38(i)条的条文所管限，除非及直至该资料已发表或播放（不论在何处或藉何方法）；
(ii) 不受第 36 及 38(b)条的条文所管限。
(2) 在以下情况，个人资料获豁免而不受第 3 保障资料原则的条文所管限——
(a) 该资料的使用包含向第(1)款所提述的资料使用者披露该资料；及
(b) 作出该项披露的人有合理理由相信（并合理地相信）发表及播放（不论在何处及藉何方法）该资料（不论是否实际有发表或播放该资料）是符合公众利益的。
(3) 在本条中——
新闻活动（*news activity*）*指任何新闻工作活动，并包括——*
(a) 为向公众发布的目的而进行——
(i) 新闻的搜集；
(ii) 关于新闻的文章或节目的制备或编纂；或
(iii) 对新闻或时事所作的评析；或
(b) 向公众发布——
(i) 属新闻的或关于新闻的文章或节目；或
(ii) 对新闻或时事所作的评析。"

96 第 2.112(f)及(g)段。

的意见，以助我们制订未来方向，随后各段概述了其他司法管辖区所采用的认证或以其他方式识别网络安全从业员的机制。

2.116 在英国，国家网络安全中心已制订"认证网络专业人员保证服务"（Certified Cyber Professional assured service，简称"**CCP 制度**"），务求建立由认可网络安全专业人员组成的社群。[97] 要根据 CCP 制度取得认证，申请人须持有某些资历或会员资格，以证明他们能广泛应用网络安全基础知识。其后，他们或会获授予在网络安全不同专门范畴执业的认可。[98] 在中国内地，中国网络安全审查技术与认证中心在《中国网络安全法》的批准范围内承担网络安全从业员的评审工作。[99] 我们亦注意到，新加坡网络安全局（Cyber Security Agency of Singapore）已推行一项计划，藉以培训网络安全专业人员并提升其技能，该等人员均须符合资讯及通讯科技方面有关资历及工作经验的正式规定。[100]

2.117 另一方面，我们理解到，并无制订评审或认证制度的司法管辖区或会依据国际标准（例如**国际认可论坛**（International Accreditation Forum）[101] 所订明的国际标准）来识别合资格的网络安全人员。

2.118 若公众属意法律应为网络安全从业员提供免责辩护或豁免，而香港应为此设立评审制度，我们便须考虑该制度实际上应如何运作。一些初步构思包括：评审团体可以属法定性质或行政性质，负责备存一份可供查阅的网络安全专业人员名单。我们邀请公众回应建议 2(a)(i)及(ii)所载的问题，就以下两方面发表意见：评审方式和方法（例如评审准则及可能订定的持续进修规定），以及评审制度的运作细节（例如若任何经审定人士未能符合持续进修规定，评审团体可否将该人除名或拒绝将其审定资格续期；以及评审团体以外的人应否获准查阅经审定人士名单）。

---

97 见 https://www.ncsc.gov.uk/information/certified-cyber-professional-assured-service（于 2022 年 5 月 3 日浏览）。国家网络安全中心是英国在网络安全领域的国家级技术机构。

98 同上。

99 见 https://www.isccc.gov.cn/zxjs/zxjs/index.shtml#intro（于 2022 年 5 月 3 日浏览）。中国网络安全审查技术与认证中心于 2006 年成立。《网络安全法》第十七条订明："*国家推进网络安全社会化服务体系建设，鼓励有关企业、机构开展网络安全认证、检测和风险评估等安全服务。*"

100 见新加坡网络安全局网站，网址为 https://www.csa.gov.sg/Programmes/CSAT（于 2022 年 5 月 3 日浏览）。

101 国际认可论坛是一个由评审团体及其他团体组成的全球组织，这些团体均着眼于不同领域（管理系统、产品、服务，以及最重要是人员）的合格评定。见 https://iaf.nu/en/about/（于 2022 年 5 月 3 日浏览）。据我们理解，国际认可论坛所认可的认证均获世界各地政府广泛接受。

2.119　但若社会各界认为，不断演变的评审情况[102]会对实施正式的评审架构造成阻碍，则我们倾向认为，针对电脑网络罪行的特定法例可订明任何人应符合某些规定，方可享有法律就在未获授权下为网络安全目的而取览所容许的免责辩护或豁免。一些基本规定可能关乎某人的培训资历、工作经验和正直品格，例如该人是否适合及适当人选。尽管如此，任何立法订明的准则要在实际上行之有效，似乎需要有一些可靠的方法来确定某特定网络安全从业员是否符合有关规定。我们欢迎公众就设立评审制度以外，任何能达到同样目的（即让人识别可享有所建议免责辩护或豁免的网络安全专业人员）的可行替代方案提出意见，相关问题载列于下文建议 2(a)(iii)。

2.120　最后，我们知道非保安专业人员亦可能作出非法取览程式或数据的作为。这类非法取览代表着入侵电脑系统的初期。正如我们将在第 5 章解释，在其后干扰有关电脑系统可能构成罪行，故我们邀请公众对非保安专业人员就该罪行应否有任何合法辩解这问题提出意见。[103] 鉴于第 2 及 5 章所建议的罪行息息相关，我们亦在这方面就非法取览程式或数据罪征询公众意见（见下文建议 2(b)）。

建议 2

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

102　第 2.112(f)段。
103　第 5 章建议 8(b)。

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）？[104]

简易程序案件的时效期

2.121 根据《裁判官条例》（第 227 章）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。第 27A(4)条[105] 便是一例，该条把时效期延长至*"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）"*。

2.122 我们理解到，《裁判官条例》（第 227 章）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的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经已届满。警方从互联网服务供应商取得日志纪录，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。

2.123 鉴于上文所述，我们建议把建议罪行的时效期延长至发现所涉事项后的两年，但维持其简易程序性质，即就该罪行更改《裁判官条例》（第 227 章）第 26 条。按照逻辑，如循简易程序就我们在本咨询文件所建议的任何罪行提出检控，经延长的同一时效期应亦适用。

---

104 建议 8(b)所述的例子是：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。

105 于上文第 2.11 段引述。

建议 3

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。

犯罪法人团体的高级人员的刑事法律责任

2.124 我们察觉到，法人团体可在其董事或其他相类高级人员同意或纵容下犯电脑网络罪行。故此，我们考虑了应否在新法例加入明文规定，使刑事法律责任可在某些情况下直接归于出任有关职位的人。[106]

2.125 现时，《刑事诉讼程序条例》（第 221 章）第 VI 部就公司的董事和其他高级人员的法律责任订有一般条文。[107] 我们认为，这项一般条文足以处理涉及电脑网络罪行的情况。此外，我们相信若我们有关订立在未获授权下取览程式或数据罪的建议获接纳，则可在进行立法程序时，才更具体地考虑有否需要就董事和担任管理职位的人的法律责任作出明文规定。[108] 因此，我们的结论是现阶段无需就这个议题作出具体建议。对于本咨询文件第 3 至 6 章所建议订立的其他罪行，我们也抱持同样的立场。

---

106 举例来说，《版权条例》（第 528 章）第 125(1)条订明：*"凡任何法人团体就任何作为而犯了本条例所订的罪行，而该罪行经证明是在该法人团体的任何董事、经理、秘书或其他相类高级人员或本意是以任何该等身分行事的任何人同意或纵容下犯的，或经证明是可归因于该法人团体的任何董事、经理、秘书或其他相类高级人员或本意是以任何该等身分行事的任何人本身的任何作为的，则上述的人及该法人团体均属犯该罪行。"*其他香港法例亦有许多相类似的条文。

107 《刑事诉讼程序条例》（第 221 章）第 101E 条订明：*"凡犯了任何条例内的罪项的人是一间公司，一经证明罪行是得到公司董事或与公司管理有关的其他高级人员同意、纵容，或得到宣称是以该董事或高级人员身分行事的人同意、纵容而犯的，则该董事或高级人员亦属犯了该项罪行。"*

108 《香港法律草拟文体及实务指引》（律政司，2012 年），第 6.2.12 段。

第 3 章　非法截取电脑数据

引言

3.1　我们会在本章探讨第二类依赖电脑网络的罪行，即非法截取电脑数据。概括而言，就此主题而订立的罪行，旨在更明确地：

(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；

(b) 从而保障人们的数据通讯私隐权。

3.2　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。[1] 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"[2] 或安装间谍软件。

香港的现行法律

《基本法》

3.3　一般而言，禁止非法取览罪及禁止非法截取罪分别关乎"静止数据"及"传递中的数据"。假若法律应保障前者的话，那么对后者亦应一视同仁。

3.4　此外，"传递中的数据"及"通讯"这两个概念密不可分，本章宜引述适用于一般通讯的《基本法》第二十七条及第三十条作为引子：

(a) *"香港居民享有言论……自由……。"*[3]

(b) *"香港居民的通讯自由和通讯秘密受法律的保护。除因公共安全和追查刑事犯罪的需要，由有关机关依照法律程序对通讯进行检查外，任何部门或个人不得以任何理由侵犯*

1　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。

2　后门程式是*"电脑系统的特点或缺陷，容许在未获授权下暗中取览数据。"*见：Oxford University Press, "Lexico.com"（2021 年），网址为 https://www.lexico.com/definition/back_door（于 2022 年 5 月 3 日浏览）。

3　第二十七条。

居民的通讯自由和通讯秘密。"[4]

《香港人权法案》

3.5 《香港人权法案》第十四条（*"对私生活、家庭、住宅、通信、名誉及信用的保护"*）及第十六（二）条（*"意见和发表的自由"*）[5]同样有关：

> (a) *"任何人之私生活……或通信，不得无理或非法侵扰……对于此种侵扰或破坏，人人有受法律保护之权利。"*[6]
>
> (b) *"人人有发表自由之权利；此种权利包括……寻求、接受及传播各种消息及思想之自由。"*[7]

《截取通讯及监察条例》（第 589 章）

条例目的

3.6 《截取通讯及监察条例》（第 589 章）（**《截取通讯及监察条例》**）补充上述《基本法》及《香港人权法案》的条文，该条例：

> "……就授权和规管执法机构为防止或侦查严重罪案和保障公共安全的目的而进行的截取通讯及秘密监察，订立法定机制。"[8]

3.7 《截取通讯及监察条例》着眼于规管执法机构（"**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。[9]

"传送过程中"的通讯

3.8 只有第一类行动（即截取通讯）与本章主旨有关。根据《截取通讯及监察条例》第 2(1)条：

> "'***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

---

4 第三十条。
5 《香港人权法案条例》（第 383 章）第 8 条。
6 第十四条。
7 第十六（二）条。
8 截取通讯及监察事务专员秘书处网站，网址为 https://www.sciocs.gov.hk/tc/ordinance.htm（于 2022 年 5 月 3 日浏览）。
9 《截取通讯及监察条例》第 2 条。

的传送人或传送对象的人查察该通讯的某些或所有内容；

‘***通讯***’（communication）指——

(a) 任何藉邮政服务传送的通讯；或

(b) 任何藉电讯系统传送的通讯”。

3.9 根据上述定义，《截取通讯及监察条例》只规管截取在*“传送过程中”*的通讯。第2(5)(b)条以下述措辞解释传送何时结束，换言之，就是《截取通讯及监察条例》不再适用于有关通讯之时：

> “就本条例而言……如藉电讯系统传送的通讯，已被该通讯的传送对象接收，或被该传送对象所管控或可取用的资讯系统或设施接收，则不论他有否实际阅读或听见该通讯的内容，该通讯不得视为是在传送过程中。”

“截取作为”的目标

3.10 如上文所述，“截取作为”的目标界定为*“通讯的某些或所有内容”*。根据《截取通讯及监察条例》第2(6)条：

> “……藉电讯系统传送的任何通讯的内容，包括联同该通讯一并产生的任何数据。”

3.11 这些数据似乎主要是元数据，即关于通讯本身的资料，而非通讯的内容或实质内容。连同电邮内容一并传送的电邮传送人和接收人的相关资料，便是电脑网络空间上元数据的例子。《截取通讯及监察条例》的实务守则阐述如下：

> “在通讯的传送过程中截获该等资料[10]亦同样视为截取，即使没有取用通讯的实际讯息亦是如此。然而，在传送

---

10 有关条例及实务守则分别提述“数据”及“资料”。虽然就本章而言，似乎无需区分两词，但两者技术上并不相同。国际标准化组织对“数据”的定义是*“为便于交流、解释或处理，对资讯的可再获解读的形式化表述”*，而对“资料”的定义则是*“关于客体（如事实、事件、事物、过程或思想，包括概念）的知识，而该知识在特定场合中具特定意义”*。见登载于以下网址的定义：
https://www.iso.org/obp/ui/#iso:std:iso:10782:-1:ed-1:v1:en（于2022年5月3日浏览）。

通讯后取得的纪录（例如通电纪录及电话帐单）并非截取作为。这类资料的纪录可藉搜查令取得。”[11]

《电讯条例》（第 106 章）

蓄意损坏电讯装置——第 27(b)条

3.12 《截取通讯及监察条例》只适用于公职人员。在执法情况以外，*任何人*均可能犯《电讯条例》（第 106 章）第 27 条所订的以下罪行：

> “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。”

可能适用于电脑网络空间

3.13 《电讯条例》于 1963 年生效，最初或者是参照二十世纪六十年代的电话而采用“电讯”及有关词句，但该等词句的定义广阔，而近数十载科技发展日新月异，[12] 按理电脑如今应可构成“电讯装置”。[13] 因此，如任何人损坏、移走或干扰这样的电脑，而意图是*“截取或找出任何讯息的内容”*，第 27(b)条便会适用。

并非针对电脑网络罪行的特定条文

3.14 纵然上述如此，第 27(b)条始终并非针对截取电脑数据的特定条文。该条文的措辞及定义预设电讯背景，并不完全适用于电脑网络空间。以下例子可说明这一点：

---

11 保安局局长，《依据〈截取通讯及监察条例〉（第 589 章）第 63 条而发出的实务守则》（2016 年 6 月），第 10 段。

12 例如透过采用称为非对称数码用户线路的技术，以往用来连接电话的铜线现在可支援连接互联网。

13 第 2(1)条将“电讯装置”界定为*“为电讯网络、电讯系统或电讯服务或与电讯网络、电讯系统或电讯服务相关而维持的器具或设备”*。
虽然加拿大最高法院在 *R v McLaughlin* [1980] 2 SCR 331 裁定，电脑系统不属当时《刑事法典》（Criminal Code）第 287 条所指的“电讯设施”，但该裁决建基于旧时的电脑科技及用途，应审慎评估该案如今是否具说服力的案例。

"***干扰***（interference）指由任何或任何组合的发射、辐射或感应所引起的无用能量对电讯网络、电讯系统或电讯装置的接收的影响，表现为性能下降、以及资讯（如没有上述无用能量则可从该电讯网络、电讯系统或电讯装置中提取出者）的误解或遗漏；

讯息（message）指藉电讯传送或接收的任何通讯，或交由电讯人员藉电讯传送的或交由电讯人员传递的任何通讯"。[14]

3.15 基于上述法定定义，假如某人具备所需意图而干扰电脑，因而根据第27(b)条被起诉，控方或需援引专家证据，以证明(a)有关电脑构成电讯装置，以及(b)被告人的行为构成该条文所定义的干扰。

3.16 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，因为《电讯条例》（第106章）中并没有与《截取通讯及监察条例》第2(6)条（于上文引述）对等的条文。尽管元数据可与"任何讯息的内容"同等重要，在有关通讯各方以外的人眼中亦可能具有价值，但元数据似乎不受第27(b)条保障。

《布达佩斯公约》订定罪行的标准

3.17 《布达佩斯公约》[15]第一节之下的第一篇第三条（引述如下）处理本章的主题事宜：

"各缔约方均应采取必要的立法及其他措施，在其本土法律中将下列行为定为刑事罪行：在无权的情况下蓄意以技术截取往来电脑系统或在电脑系统内的非公开传送电脑数据（包括由电脑系统发出载有该等电脑数据的电磁发射）。任何缔约方可规定，有关罪行须具不诚实意图，或须与连接至另一电脑系统的电脑系统有关。"

3.18 《说明报告》对第三条的评注如下：

"51. 本条旨在保障数据通讯的私隐权。有关罪行相当于传统窃听和记录人们口头电话对话的侵犯通讯私隐行为。《欧洲人权公约》（European Convention on Human Rights）第八条体现通讯私隐权，第三条所订罪行正是将这项原

---

14 《电讯条例》（第106章）第2(1)条。

15 有关《布达佩斯公约》的背景资料，见导言第11段，以及第1章第1.6至1.10段。

则应用于所有形式的电子数据传输（不论是藉电话、传真、电邮或档案传输）。

……

53. 以‘技术’截取，是指直接透过取览和使用电脑系统，或间接透过使用电子偷听或窃听器材，以监听、监测或监察通讯的内容和取得数据的内容。截取亦可能包含记录。技术包括装设在传输线及器材上用以收集和记录无线通讯的技术器材，可包括使用软件、密码及编码。使用技术这项规定是具限制性的要求，目的是避免造成过度刑事化的情况。

54. 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。构成‘非公开传送电脑数据’的雇员通讯，不论是否为了业务目的，亦会受第三条保障，使该通讯免遭他人在无权的情况下截取……

55. 以传送电脑数据形式进行的通讯，可在单一电脑系统内（例如由中央处理器传送至屏幕或打印机）进行，亦可在同一人拥有的两个电脑系统之间进行，或在两部互相通讯的电脑之间或电脑与人之间（例如透过键盘）进行。不过，缔约方仍可规定，通讯须在远程连接的电脑系统之间传送，作为额外罪行元素。

56. 应注意的是，虽然‘电脑系统’这个概念亦可包含无线电连接，但任何无线电传送如以相对公开和易于取用的方式进行，因而可被截取（例如被无线电业余爱好者截取），则即使无线电传送属‘非公开’传送，亦不代表缔约方有责任把截取这类无线电传送定为罪行。

……

58. 非法截取须是‘蓄意’和在‘无权’的情况下进行，方会招致刑事法律责任。例如，假若进行截取的人有权如此行事，或他是按照有关传送的参与者的指示或授权行

事（包括获授权的测试或参与者同意的保护行动），或假若调查机关为维护国家安全或侦查罪行而合法授权监察，有关作为便是有理可据的。由于使用‘小型文字档案（cookies）’等这类常见的商业做法不属在‘无权’的情况下进行截取，故这类做法本身亦不拟定为罪行。对于第三条所保障的非公开雇员通讯（见上文第 54 段），本土法律可订明合法截取这类通讯的理由。根据第三条，在这些情况下进行的截取会视为在‘有权’的情况下进行。

59. 在某些国家，截取可能与在未获授权下取用电脑系统罪关系密切。为确保有关法律的禁止事项和适用范围贯彻一致，如这些国家根据第二条，规定须具不诚实意图，或规定有关罪行须与连接至另一电脑系统的电脑系统有关，则亦可在本条就招致刑事法律责任订下类似的规限元素。这些元素应与有关罪行的其他元素（例如‘蓄意’和‘无权’）一并诠释和应用。”[16]

静止数据的两类特例

“静止数据”及“传递中的数据”

3.19 我们于上文评述，概括而言，禁止非法取览罪及禁止非法截取罪分别关乎“静止数据”及“传递中的数据”。两者概念截然不同，却又（如《说明报告》第 46 及 59 段[17] 所揭示）息息相关。

3.20 除了储存于电脑用户储存媒体内的数据这个明显例子外，数据还可能在两类情况下静止不动。我们会于下文先讨论这类静止数据，并以举例方式简略探讨若干司法管辖区的法例如何处理这类数据，随后再就非法截取电脑数据这个课题展开比较研究。

在传送期间暂时静止的数据

3.21 第一类特例之所以出现，是因为某些种类的互联网通讯所采用的技术。名为“存储转发”传递的机制，是指通讯可于前往目的地途中多次暂存在网络上。[18]

---

16 《说明报告》第 51、53 至 56、58 及 59 段。

17 分别于第 1 章及本章较前部分引述。

18 “存储转发”传递可与网上视像片段等串流媒体作对比。

3.22 问题是：当数据在传送期间有一刹那暂时静止，截取罪应否适用于该数据。对于这个问题，并非所有司法管辖区均有法例处理，但澳大利亚法律以《1979 年电讯（截取及取览）法令》（联邦）（Telecommunications (Interception and Access) Act 1979 (Cth)，**《电讯（截取及取览）法令》**）第 5F 条的推定条文给予肯定答案，该条文的内容如下：

> "就本法令而言，通讯：
>
> (a) 在发送该通讯的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，直至该通讯的传送对象可取览该通讯为止。"

3.23 根据这项条文，截取罪适用于整个传送过程中的通讯（不论在该通讯被指称截取时，构成该通讯的数据恰巧是暂时静止还是正在传递中）。

3.24 如没有这项条文，控方便可能需要极为技术性的证据，方可证明有关罪行的元素。例如，被控截取罪的人可能就其所取得的数据在关键时间是否正在传递中这个事实问题提出争议（因为倘若有关数据当时是暂时静止，原则上非法取览的控罪会较为恰当）。要在排除合理疑点的情况下证明这一点，未必直接简单。

储存于通讯系统的数据

3.25 第二类特例涉及到达通讯终点后，在通讯系统内静止并可供传送对象取览的数据。日常例子包括储存于手提电话用户语音留言信箱内的讯息，[19] 以及储存于网上电邮服务供应商伺服器内的电邮。这类数据显然不受《截取通讯及监察条例》规限，因为该条例不再适用于处于以下状况的通讯：

> "如……已被该通讯的传送对象接收，或被该传送对象所管控或可取用的资讯系统或设施接收，则不论他有否实际阅读或听见该通讯的内容"。[20]

3.26 在澳大利亚的相关概念是"储存通讯"，这概念在《电讯（截取及取览）法令》第 5 条界定为：

---

19 *R v Coulson (Andrew)* [2013] 2 Cr App R 32.

20 《截取通讯及监察条例》第 2(5)(b)条（于上文引述）。

"……符合以下说明的通讯：

(a) 并非正在经过电讯系统；及

(b) 由传送者操作和管有的设备所持有；及

(c) 在没有传送者的雇员的协助下，通讯各方以外的人不能在该设备上取览该通讯。"

3.27 从《布达佩斯公约》的罪行归类而言，处于这个状况的数据应属禁止非法取览（而非禁止非法截取）的焦点。然而，不同司法管辖区根据性质各异的法规（这些法规未必是专门针对电脑网络罪行的法例）把非法截取定为罪行。

3.28 例如，英格兰及威尔斯的《2016年调查权力法令》(Investigatory Powers Act 2016，**《调查权力法令》**）订明多项条文，当中包括合法截取通讯的情况和非法截取通讯的情况。就此而言，不论构成通讯的数据是静止不动还是在传递中，在概念上应差异无几。

3.29 由此，就《调查权力法令》而言，"截取"一词不一定与电脑网络罪行法例（即《英格兰误用电脑法令》）中的"取览"概念互作对比。由于《调查权力法令》中的"截取"一般可理解为取得构成通讯的数据，因此即使有关数据是静止不动，概念上亦无不协调之处。

3.30 上文为《调查权力法令》第4(4)[21]及(5)[22]条定下背景，该等条文的实际效果，是把第3(1)条所订的截取罪应用于在澳大利亚视为"储存通讯"的通讯。这个概念意义重大，因为：

"……随着网上电邮服务日渐普及，这代表取览的复本愈来愈可能是储存于传送者[23]的设备中，而非下载至接收人的电脑。"[24]

3.31 概念上，当通讯已获下载或储存于接收人的电脑（即不再留在任何通讯系统内），若有人非法取览构成该通讯的数据，便会受第2章所检视的非法取览程式或数据罪所规管。

---

21 *"在本条中，就藉电讯系统传送的通讯而言，'有关时间'指——*
(a) 该通讯传送期间的任何时间，及
(b) 该通讯于该系统内储存或由该系统储存期间的任何时间（不论是在该通讯传送之前或之后）。"

22 *"就本条而言，通讯的任何内容须视为已在有关时间提供予某人的情况，包括以下情况：在有关时间转发或记录该通讯的任何部分，以便在该时间后向某人提供该通讯的任何内容。"*

23 传送者是传送通讯服务的供应商，一般是电讯网络操作人。

24 Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd edition, 2015)，第187页。

其他司法管辖区的法定体制

澳大利亚

《刑事法典》（联邦）并不相关

3.32 在澳大利亚，《刑事法典》（联邦）（Criminal Code (Cth)）第10.7部处理电脑罪行。正如第2章所述，该部定为不合法的主要行为种类有：在未获授权下取览电脑数据、在未获授权下修改电脑数据，以及在未获授权下损害电子通讯。根据第476.1(1)条：

> "**损害往来某电脑的电子通讯**包括：
>
> (a) 阻止进行上述通讯；或
>
> (b) 在该电脑所使用的电子联网或网络上损害上述通讯；
>
> 但不包括纯粹截取上述通讯。"

3.33 上述但书显示《刑事法典》（联邦）与本章主旨并不相关。

《电讯（截取及取览）法令》所订的截取罪

3.34 《电讯（截取及取览）法令》的条文反而相关。根据第7(1)条，除非例外情况适用，否则：

> "任何人不得：
>
> (a) 截取；
>
> (b) 授权、容许或准许另一人截取；或
>
> (c) 作出任何作为或事情，使其本人或另一人能截取；
>
> 正在经过电讯系统的通讯。"

3.35 第7(2)至(10)条接着详细列出例外情况。《电讯（截取及取览）法令》第105条订定，违反第7(1)条属可公诉罪行，最高可处两年监禁。

3.36 第7(1)条与第5F条一并施行。我们于上文考虑在传送期间暂时静止的数据时提到，第5F条实际上是把第7(1)条应用于整个传

送过程中的通讯（不论构成该通讯的数据恰巧是暂时静止还是在传递中）。

储存通讯

3.37 当通讯可供接收人取览，该通讯即属《电讯（截取及取览）法令》第 3 章所规管的"储存通讯"。[25] 我们在探讨储存于通讯系统的数据时，已在上文第 3.26 段讨论这个词语的法定定义。

元数据

3.38 除非任何例外情况适用，否则《电讯（截取及取览）法令》第 4 章一般禁止取览大体上是元数据的"电讯数据"：

> "电讯数据是关于电讯的资料，但电讯数据并不包括通讯的内容或实质内容……就互联网的应用而言，电讯数据包括使用时段所用的互联网规约（IP）地址、曾到访的网站，以及每节使用时段的开始和结束时间。"[26]

《电讯（截取及取览）法令》可能有其局限

3.39 与香港《电讯条例》（第 106 章）第 27(b)条一样，《电讯（截取及取览）法令》对"电讯"的提述亦可能限制其应用范围。有评论员认为：

> "有关在未获授权下截取通讯的罪行并非新事，在各个司法管辖区均可见。这些罪行一般由关于在公共电讯网络上截取电话通话的条文演变而来，这带来的种种挑战，不少与将这些罪行应用于数码通讯方面有关。"[27]

---

25 除非属订明例外情况，否则《电讯（截取及取览）法令》第 108 条禁止在储存通讯的传送人或传送对象不知情的情况下，取览该通讯。

26 澳大利亚联邦国会（Parliament of the Commonwealth of Australia）众议院（House of Representatives），《2007 年电讯（截取及取览）（修订）法案》摘要说明（Explanatory Memorandum for the Telecommunications (Interception and Access) Amendment Bill 2007），登载于 https://www.legislation.gov.au/Details/C2007B00124/Explanatory%20Memorandum/Text（于 2022 年 5 月 3 日浏览）。

27 Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd edition, 2015)，第 149 页。

加拿大

《1985 年刑事法典》第 342.1(1)(b)条

3.40 在第 2 章，我们提到加拿大《1985 年刑事法典》（Criminal Code 1985）第 342.1(1)条。该条文的四个部分中，(b)段与本章最为相关。根据(b)段，任何人意图欺诈并在无表面权利的情况下藉电磁、声音、机械或其他器材截取*"某电脑系统的任何功能"*，或导致藉电磁、声音、机械或其他器材截取*"某电脑系统的任何功能"*，即属犯罪，一经循公诉程序定罪，最高可处十年监禁。

3.41 我们在第 2 章亦可见《1985 年刑事法典》第 342.1(2)条对"功能"及"电脑系统"的宽广定义，特别是"功能"包括（但不限于）*"往来某电脑系统或在某电脑系统内的通讯或电讯"*。从表面看，第 342.1(1)(b)条所订罪行的犯罪行为可涵盖多种情况。

3.42 该罪行的犯罪意念（*"意图欺诈并在无表面权利的情况下"*）则相对明确。例如，单是知悉（自己截取或导致截取"某电脑系统的任何功能"）或罔顾后果，并不足以入罪。

《1985 年刑事法典》第 184(1)条

3.43 《1985 年刑事法典》第 VI 部第 184(1)条（*"侵犯私隐"*）订立另一项与本章相关的罪行：

> "任何人藉任何电磁、声音、机械或其他器材，故意截取[28]私人通讯，[29]即属
>
> (a) 犯可公诉罪行，可处为期不超过 5 年的监禁；或
>
> (b) 犯可循简易程序定罪而惩处的罪行。"

3.44 第 184(2)及(3)条接着列出若干豁除条文。例如，第 184(2)(c)条规定，第 184(1)条并不适用于：

---

[28] 《1985 年刑事法典》第 183 条对"截取"的定义包括*"监听、记录或获取通讯，或获取通讯的实质内容、涵义或大意"*。

[29] 《1985 年刑事法典》第 183 条将"私人通讯"界定为：
"由身处加拿大的发讯人作出或发讯人拟让身处加拿大的人接收的任何口头通讯或电讯，而该通讯或电讯在发讯人合理预期不会被他拟让其接收的人以外的任何人截取的情况下作出，私人通讯包括为了阻止有关通讯被发讯人拟让其接收的人以外的任何人以清楚易明的形式接收，而藉电子或其他方式处理的任何无线电电话通讯"。

"从事向公众提供电话、电报或其他通讯服务，并在以下情况下截取私人通讯的人：

(i) 该项截取对提供该服务而言属必需，

(ii) 该项截取在服务观察或抽样监察的过程中进行，而该服务观察或抽样监察对机械或服务质量控制检查而言属必需，或

(iii) 该项截取对保障该人与提供该服务直接有关的权利或财产而言属必需"。

比较第 342.1(1)(b)条与第 184(1)条

3.45 第 342.1(1)(b)条与第 184(1)条所订罪行的犯罪方式大致相同，它们均是"藉〔任何〕电磁、声音、机械或其他器材"进行截取。这两项条文分别订定的犯罪行为，显然均可涵盖针对电脑系统而进行的截取。检控当局只有在指称具有"意图欺诈并在无表面权利的情况下"这项所需的犯罪意念时，方可选择以第 342.1(1)(b)条属较具体的条文为理由，支持根据该条向针对电脑系统进行上述截取的人提出检控。

3.46 与此同时，如某人并非针对电脑系统而进行截取，即使该人意图欺诈并在无表面权利的情况下行事，亦只能根据第 184(1)条[30] 被检控，而不会根据第 342.1(1)(b)条[31] 被判处较重的最高刑罚。有人或会认为，是否涉及电脑系统这一因素，并非具充分说服力的理由解释这两项条文不同的最高刑罚。

英格兰及威尔斯

《调查权力法令》第 3(1)条

3.47 在英格兰及威尔斯，专门对付电脑网络罪行的法例（《英格兰误用电脑法令》）并无条文禁止截取电脑数据，反而《调查权力法

---

30 *"任何人藉任何电磁、声音、机械或其他器材，故意截取私人通讯，即属*
(a) 犯可公诉罪行，可处为期不超过 5 年的监禁；或
(b) 犯可循简易程序定罪而惩处的罪行。"

31 *"任何人意图欺诈并在无表面权利的情况下……(b)藉电磁、声音、机械或其他器材直接或间接截取某电脑系统的任何功能，或导致藉电磁、声音、机械或其他器材直接或间接截取某电脑系统的任何功能，即属犯可公诉罪行，可处为期不超过 10 年的监禁，或属犯可循简易程序定罪而惩处的罪行"。*

令》第 3(1)条（*"非法截取罪"*）才是相关的法规。该条之下共有七款，在此引述首两款已足够：

"(1) 如——

(a) 任何人蓄意在通讯[32]藉以下方式传送的过程中截取该通讯，

(i) 公共电讯系统，

(ii) 私人电讯系统，[33] 或

(iii) 公共邮政服务，

(b) 该项截取是在联合王国进行的，及

(c) 该人并无合法权限进行该项截取，

则该人即属犯罪。

(2) 但任何人如在通讯藉私人电讯系统传送的过程中截取该通讯，而该人——

(a) 是有权管控该系统的操作或使用的人，或

(b) 在上述的人明示或默示同意下进行该项截取，

则不属犯第(1)款所订罪行。"

3.48 《调查权力法令》第 4、5 及 6 条分别解释"截取"的涵义、在甚么情况下截取视为在英国进行，以及在甚么情况下某人有合法权限进行截取。

---

[32] 根据《调查权力法令》第 261(2)条：

"就电讯操作人、电讯服务或电讯系统而言，'通讯'包括——

(a) 任何类别的语言、音乐、声音、影像或数据所组成的任何事物，及

(b) 用于在人与人之间、人与物之间或物与物之间传递任何事物的讯号，或用于开动或控制任何器具的讯号。"

[33] 该法令第 261 条对"公共电讯系统"及"私人电讯系统"的定义并不特别精辟独到。不过，该法令显然预先假定电脑数据可藉电讯系统传送。例如，第 62(7)条将"互联网连接纪录"界定为：

"……为取览或驱动电脑档案或电脑程式而藉电讯系统传送通讯至某电讯服务时，可用于识别……该电讯服务的通讯数据……"。

储存通讯

3.49 正如我们在上文谈及如何处理储存于通讯系统的数据时提到，《调查权力法令》第 4(4)及(5)条实际上是把第 3(1)条所订的截取罪应用于在澳大利亚视为"储存通讯"的通讯。

元数据

3.50 有别于公共邮政服务，在关乎电讯系统的个案中，《调查权力法令》第 4(1)条（载于下文）实际上是把第 3(1)条所订罪行局限于截取通讯的"内容"：

> "就本法令而言，任何人在以下情况下并仅在以下情况下，方属在通讯藉电讯系统传送的过程中截取该通讯——
>
> (a) 该人就该系统作出有关作为，及
>
> (b) 该有关作为的效果，是在有关时间向该通讯的传送人或传送对象两者以外的人提供该通讯的任何内容。
>
> 就通讯而言，'内容'的涵义见第 261(6)条。"

3.51 《调查权力法令》第 261(6)条内容如下：

> "'内容'……指该通讯的任何元素，或该通讯所附带的任何数据，或逻辑上与该通讯相联的任何数据，而该元素或数据显露可合理认为是该通讯的涵义（如有的话）的任何事物，但——
>
> (a) 该通讯一事本身所产生的任何涵义，或与传送该通讯有关的任何数据所产生的任何涵义，均无须理会；及
>
> (b) 任何属系统数据[34]的事物，均不属内容。"

---

[34] 《调查权力法令》第 263(4)条将"系统数据"界定为：

"……使以下任何一项能运作或利便其运作的任何数据，或对于使以下任何一项能运作或利便其运作所关连的任何事物作出识别或说明的任何数据——

(a) 邮政服务；

(b) 电讯系统（包括组成该系统的任何器具）；

(c) 藉电讯系统提供的任何电讯服务；

(d) 有关系统（包括组成该系统的任何器具）；

(e) 藉有关系统提供的任何服务。"

3.52 简言之，通讯的“内容”似乎并不包括元数据。《调查权力法令》就元数据使用“通讯数据”一词，并在第 261(5)条对该词作出详尽定义，“通讯数据”主要涵盖第 261(3)及(4)条分别界定的“实体数据”及“事件数据”。根据《调查权力法令》第 11(1)条：

> “有关人士如无合法权限而故意或罔顾后果地从电讯操作人或邮政操作人取得通讯数据，即属犯罪。”

3.53 第 11(2)条将“有关人士”界定为在《调查权力法令》“*（第 3 部所指的）有关公共机构出任职位、职级或岗位的人*”，这显示第 11(1)条并不适用于由一般大众进行的截取，对“通讯数据”的保障因此有限。

《2006 年无线电讯法令》第 48(1)(a)条

3.54 另外，我们亦应提及《2006 年无线电讯法令》（Wireless Telegraphy Act 2006，**《无线电讯法令》**）第 48 条（*“截取和披露讯息”*）。根据第 48(1)(a)条，任何人在以下情况，即属犯罪：

> “……无合法权限而使用无线电讯器具，[35] 并意图取得与某讯息（不论该讯息是否藉无线电讯发送）的内容、传送人或收讯人有关的资料，而他本人或由他代表行事的人均并非该讯息的传送对象”。

3.55 有些行为似乎可同时根据《无线电讯法令》第 48(1)(a)条和《调查权力法令》第 3(1)条被检控。第 48(3A)条订定《调查权力法令》实际上凌驾《无线电讯法令》，从而确认了这观点：

> “如任何人的行为——
>
> (a) 构成《2016 年调查权力法令》第 3(1)条所订罪行（非法截取罪），或

---

[35] 《无线电讯法令》第 116(2)及 117(1)条将“无线电讯器具”界定为发射或接收以下（在订明频率范围内的）电磁能的器具，而所经途径并非由为此目的而建造或安排的物料提供：
(a) 用作传递讯息、声音或影像（不论实际上是否有人接收该等讯息、声音或影像），或用作操作或控制机械或器具的电磁能；或
(b) 在与厘定位置、方位或距离有关连的情况下使用，或为了获取有关某物件或某类物件是否存在或其位置或移动情况的资料而使用的电磁能。
根据上述定义，该词语似乎包括 Wi-Fi 路由器及可连接蓝芽或 NFC（近距离无线通讯）的智能电话等器材。

(b) 假若没有（该法令第 6 条所指的）合法权限，便会构成该法令第 3(1)条所订罪行，

则该人不会因该行为而犯本条所订罪行。”

中国内地

《中国刑法》第二百八十五条第二款

3.56 第二百八十五条第二款订定，如*“违反国家规定，侵入〔国家事务、国防建设、尖端科学技术领域的系统〕以外的计算机信息系统……，获取该计算机信息系统中存储、处理或者传输的数据”*，即属犯罪。

（底线后加）

截取目标

3.57 第二百八十五条第二款泛指被侵入的计算机信息系统所传输的数据，并无区分通讯内容及元数据。因此，第二百八十五条第二款似乎适用于元数据。

3.58 此外，由于第二百八十五条第二款同样保障计算机信息系统中存储和处理的数据，因此有关罪行亦适用于静止数据，例如是在传送期间暂时静止的数据，以及储存于通讯系统的数据。

新西兰

《新西兰法令》第 216B 条

3.59 相关的法例条文是《新西兰法令》第 216B 条（*“禁止使用截取器材”*）。该条文载于关于侵犯个人私隐罪行的《新西兰法令》第 9A 部，而非载于处理涉及电脑罪行的第 248 至 252 条之中。第 216B 条内容如下：

“(1) 除第(2)至(5)款另有规定外，任何人蓄意藉截取器材截取任何私人通讯，可处为期不超过 2 年的监禁。

(2) 如截取私人通讯的人——

(a) 是该私人通讯的其中一方；或

(b) 依据由以下法令向该人赋予的任何权限，或根据以下法令向该人赋予的任何权限，并按照该权限的条款进行截取——

(i) 《2012 年搜查及监察法令》（Search and Surveillance Act 2012）；或

(ii) 《2017 年情报及保安法令》（Intelligence and Security Act 2017）第 4 部；或

(iii) 《1987 年国际恐怖主义（紧急权力）法令》（International Terrorism (Emergency Powers) Act 1987），

则第(1)款并不适用。

(3) 〔废除〕

(4) 第(1)款不适用于根据《2004 年惩教法令》（Corrections Act 2004）第 113 条对囚犯通话进行的任何监测，亦不适用于根据该法令第 189B 条授权对私人通讯进行的任何截取。

(5) 在以下情况下，第(1)款不适用于从事向公众提供互联网或其他通讯服务的人所操作的任何截取器材对私人通讯进行的截取——

(a) 该项截取是由向公众提供该互联网或其他通讯服务的人的雇员，在执行该人职责的过程中进行；及

(b) 该项截取是为了维持该互联网或其他通讯服务而进行；及

(c) 该项截取就维持该互联网或其他通讯服务而言属必需；及

(d) 该项截取仅用于维持该互联网或其他通讯服务。

(6) 如根据第(5)款所取得的资料不再需用于维持有关互联网或其他通讯服务，则该等资料须即时销毁。

(7) 如任何人持有在协助执行根据《2012 年搜查及监察法令》发出的监察器材手令期间取得的任何资料，则该等资料须在该手令届满时——

(a) 即时销毁；或

(b) 交予执行该手令的机关。”

3.60 《新西兰法令》第 216C 至 216F 条继而订明相关事宜，例如禁止披露非法截取的私人通讯，以及禁止处理截取器材。

主要词语的法定定义

3.61 第 216A(1)条广泛界定第 216B 条所用的三项词语：

“就私人通讯而言，**截取**包括在——

(a) 该通讯进行期间；或

(b) 该通讯传送期间，

听见、监听、记录、监测、获取或接收该通讯。

截取器材——

(a) 指用于或可用于截取私人通讯的任何电子、机械、电磁、光学或光电工具、器具、设备或其他器材；但

(b) 不包括——

(i) 助听器或相类器材……；或

(ii) 获总督会同行政局豁免受本部条文规管的器材……

私人通讯——

(a) 指在可合理视为显示通讯任何一方意欲将该通讯局限于该通讯各方的情况下作出（不论是以口头或书面形式或其他形式作出）的通讯；但

(b) 如任何一方理应合理预期通讯可能会被某些未经任何一方明示或默示同意可截取该通讯的其他人截取，则不包括在这些情况下发生的通讯。”

3.62 “通讯”一词并无独立定义。无论如何，截取目标均是“进行中”或“传送中”的私人通讯。这显然不包括传送期间暂时静止的数据，以及在澳大利亚相当于“储存通讯”的数据。

截取罪的豁除条文

3.63 第 216B(2)至(5)条的豁除条文，主要与执法以及互联网或其他通讯服务供应商必需进行的截取有关。

3.64 有关第 216B(2)(a)条豁除条文（即截取私人通讯的人是该通讯的其中一方）的指引，见于第 216A(3)条：

“凡在本部提述私人通讯的其中一方，即提述——

(a) 该通讯的任何发讯人，以及发讯人拟让其接收该通讯的任何人；及

(b) 在该通讯的任何发讯人明示或默示同意下截取该通讯的人，或在发讯人拟让其接收该通讯的任何人明示或默示同意下截取该通讯的人。”

法律委员会与司法部的联合研究

3.65 新西兰的法律委员会（Law Commission）与司法部（Ministry of Justice）于 2016 年 11 月 8 日发表联合议事文件，[36] 当中提及多个有关《2012 年搜查及监察法令》内“截取”及“私人通讯”定义的问题，这些定义与《新西兰法令》第 216A(1)条中的定义几乎完全一样。

3.66 虽然《新西兰法令》第 216B 条的用字显示，该条文本拟适用于多种情况，包括针对电脑而进行的截取，但该议事文件提出以下各点：

“4.11 ……断定何谓‘私人’的测试，取决于通讯任何一方是否‘理应合理预期该通讯可能会被截取’……假若国家

---

[36] 法律委员会及司法部，*Review of the Search and Surveillance Act 2012 (IP40)*，登载于 https://www.lawcom.govt.nz/our-projects/search-surveillance-act-2012 （于 2022 年 5 月 3 日浏览）。见第 4 章。

截取通讯变得普遍平常，便几乎总可合理预期通讯可能会被截取。

……

4.19 另一类很可能不属'私人通讯'定义范围的通讯例子，是元数据或机器类型通讯。概括而言，元数据是关于电子活动的资料，与其内容无关。元数据包括进行各种形式的电子通讯时所产生的数据，例如电话通话或电邮的时间及日期、各方电邮地址或电话号码，以及收发通讯的单元塔或互联网规约地址。元数据亦可包括互联网使用者曾到访的网站。

4.20 元数据可显露与关系、位置、身分及活动有关的资料，这些资料可能是宝贵的调查工具。例如，元数据可让警方证明疑犯与犯罪组织成员通讯，或曾到访显示不良材料的网站。

4.21 然而，元数据似乎并不符合'私人通讯'的定义，因为该定义提述通讯各方及他们的意图，意味着有关通讯必须在两人或多于两人之间进行。"（斜体乃原文所有）

3.67 法律委员会与司法部在 2018 年 1 月 30 日发表的报告[37] 内提出多项建议，其中包括以下建议。下文提述的法令虽是《2012 年搜查及监察法令》，但就《新西兰法令》第 216B 条而言，这些建议似乎亦大致适用：

(a) 法令应修订为提述截取"技术"而非"器材"。有关定义应重新草拟，以涵盖使用电脑程式、器材和其他技术辅助工具。[38]

(b) "私人通讯"的定义应予废除。现时使用"私人通讯"一词之处应以"通讯"取代，因此需要修订"截取"及"截取器材"的定义。[39]

---

37 登载于新西兰法律委员会网站，网址为 https://www.lawcom.govt.nz/our-projects/search-surveillance-act-2012 （于 2022 年 5 月 3 日浏览）。

38 建议 14。

39 建议 24。读者会备悉《布达佩斯公约》规定禁止截取非公开传送的电脑数据。

(c) 法令应加入条文，将“通讯”界定为包括任何人或机器在任何媒介制造、发送、接收、处理或持有的符号、讯号、脉冲、文字、图像、声音、资料或数据。[40]

(d) 新西兰政府应考虑新西兰应否加入《布达佩斯公约》。[41]

3.68 法律委员会与司法部的报告有待新西兰政府回应。

新加坡

《新加坡误用电脑法令》第 6 条

3.69 《新加坡误用电脑法令》第 6 条（*“在未获授权下使用或截取电脑服务”*）规定如下：

> “(1) 除第(2)款另有规定外，任何人——
>
> (a) 为了直接或间接取得任何电脑服务，在没有权限的情况下，故意取用任何电脑；
>
> (b) 在没有权限的情况下，故意藉电磁、声音、机械或其他器材直接或间接截取某电脑的任何功能，或故意导致藉电磁、声音、机械或其他器材直接或间接截取某电脑的任何功能；或
>
> (c) 为了犯(a)或(b)段所订罪行，故意直接或间接使用电脑或任何其他器材，或故意导致直接或间接使用电脑或任何其他器材，
>
> 即属犯罪，一经定罪——
>
> (d) 可处不超过$10,000 的罚款或为期不超过 3 年的监禁，或两者兼处；及
>
> (e) 如属第二次或其后每次定罪，则可处不超过$20,000 的罚款或为期不超过 5 年的监禁，或两者兼处。

---

40 建议 25。
41 建议 44。

(2) 如因本条所订罪行而导致任何损坏，被裁定犯该罪行的人可处不超过$50,000 的罚款或为期不超过 7 年的监禁，或两者兼处。

(3) 就本条而言，未获授权的取用或截取并非针对——

(a) 任何特定程式或数据；

(b) 任何种类的程式或数据；或

(c) 存于任何特定电脑内的程式或数据，

均属无关重要。”

3.70 《新加坡误用电脑法令》第 6 条以加拿大《1985 年刑事法修订法令》（Criminal Law Amendment Act 1985）第 301.2(1)条为蓝本，第 301.2(1)条已成为于上文引述的《1985 年刑事法典》第 342.1(1)条。

3.71 《新加坡误用电脑法令》第 6(1)条的三个部分中，(b)部分对应本章的主题事宜。该部分对犯罪行为的拟定方式，特别是“藉电磁、声音、机械或其他器材”截取“某电脑的任何功能”，与《1985 年刑事法典》第 342.1(1)(b)条[42] 的相似之处显而易见。《新加坡误用电脑法令》第 2(1)条更逐字逐句采用加拿大《1985 年刑事法典》第 342.1(2)条对“功能”的宽广定义。

3.72 尽管新加坡与加拿大的法规有上述相类之处，它们亦有重大差异：

(a) 就犯罪意念而言，根据新加坡的条文，知悉便已足够。加拿大的条文则规定，犯罪者须“意图欺诈并在无表面权利的情况下”行事。

(b) 根据新加坡的条文，有关截取必须“在没有权限的情况下”进行。从加拿大的条文表面上看，这并非罪行元素，尽管按道理，该条文使用“在无表面权利的情况下”等字眼，这意味着只有在没有权限的情况下进行截取，方属违法。

---

[42] *“任何人意图欺诈并在无表面权利的情况下……藉电磁、声音、机械或其他器材直接或间接截取某电脑系统的任何功能，或导致藉电磁、声音、机械或其他器材直接或间接截取某电脑系统的任何功能，即属犯……罪……”*。

《1999 年电讯法令》第 61(b)条

3.73 另外，根据新加坡《1999 年电讯法令》（Telecommunications Act 1999）第 61 条（*"蓄意损坏用于电讯的装置或工业装置"*）：

> "任何人意图——
>
> (a) 为阻止或妨碍任何讯息的传送或传递；
>
> (b) 为截取或令其本人知悉任何讯息的内容；或
>
> (c) 为导致损害，
>
> 而损坏、移除、干预或触摸属于公共电讯持牌人而用于电讯的任何装置或工业装置（或其任何部分），或干扰公共电讯持牌人的无线电通讯服务或系统，[43] 即属犯罪。"

3.74 这条文的(b)部分可对照香港《电讯条例》（第 106 章）第 27(b)条。第 27(b)条提述某人的意图是"截取或找出任何讯息的内容"，显然并不涵盖截取与讯息有关的元数据。较后这一点似乎亦适用于新加坡《电讯法令》第 61(b)条。

比较加拿大法律与新加坡法律

3.75 如上文所述，[44] 加拿大《1985 年刑事法典》第 342.1(1)(b)及 184(1)条所订罪行似乎均适用于电脑网络空间，但只有后者涵盖并非针对电脑系统而进行的截取。由于两项罪行的犯罪意念有别（"意图欺诈并在无表面权利的情况下"相对"故意"），而且最高刑罚不一（监禁十年相对五年），两者不同的涵盖范围或会造成不公。

3.76 反之，《新加坡误用电脑法令》第 6(1)(b)条和《1999 年电讯法令》第 61(b)条所订罪行均没有规定犯罪意念标准与"意图欺诈"同样地高（条文分别只要求"故意"和"意图"）。若根据当中任何一条定罪，均可处不超过 10,000 新加坡元的罚款或为期不超过三年的监

---

43 根据该法令第 6 条：

"有关当局〔资讯通讯媒体发展局〕可在部长批准下，指定根据第 5 条获批出牌照作为公共电讯持牌人的任何人，根据本法令履行全部或任何关乎在新加坡经营和提供电讯系统及服务的职能（属发展局专有特权所管限范围内者）。"

44 第 3.45 至 3.46 段。

禁，或两者兼处。[45] 这两项条文将类似的行为定为不合法，并附带相同的最高刑罚，而这些刑罚与条文订定的相应犯罪意念大致相若。

3.77 就前两段所引的法规而言，新加坡法律似乎比加拿大法律较少不一致的问题。

美国

概览

3.78 以下学术观点对美国有关法例的看法颇为负面：

> "某著名评论员曾将美国的监察法例形容为'若非彻底难明费解，其错综复杂也是人所共知'，而法院亦指有关法例'繁复晦涩'、'含混不清且毫不明确'，是一场'举证恶梦'。截取法例随着《1986 年电子通讯私隐法案》（Electronic Communications Privacy Act 1986，《电子通讯私隐法案》）制定而经历重要改革，但由于这条法案早于互联网及万维网面世前拟订，故不少困难由此而生。因此，现有法律框架并不适合应对现代的通讯形式，'普遍视为落后过时'。"[46]

3.79 该著者亦指出，有关截取法例的复杂之处、辩论及改革，大多与执法部门进行监察的能力有关，而美国的案例及评注主要关乎美国宪法《第四条修正案》对免受不合理搜查和检取的保障。[47]

3.80 美国的相关法例现时由三部分组成，分别为规管截取通讯内容的《搭线窃听法案》（Wiretap Act）、[48] 规管取览储存通讯的《储存通讯法案》（Stored Communications Act），[49] 以及规管取览流量数据（一种元数据）的《通讯纪录器法案》（Pen Register Act）。[50]

《搭线窃听法案》内的《美国法典》第 18 篇第 2511(1)条

3.81 就本章而言，可集中研究《美国法典》第 18 篇第 2511(1)条：

---

45 《新加坡误用电脑法令》第 6(1)条及《1999 年电讯法令》第 85 条。

46 Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd edition, 2015)，第 155 页（书内引文省略）。

47 Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd edition, 2015)，第 150 页。

48 《电子通讯私隐法案》第 I 篇，编纂于《美国法典》第 18 篇第 2510 至 2523 条。

49 《电子通讯私隐法案》第 II 篇，编纂于《美国法典》第 18 篇第 2701 至 2713 条。

50 《电子通讯私隐法案》第 III 篇，编纂于《美国法典》第 18 篇第 3121 至 3127 条。

“除本章[51]另有特别规定外，任何人如——

(a) 蓄意截取、尝试截取或促致任何其他人截取或尝试截取任何有线、口头或电子通讯；

(b) 蓄意使用、尝试使用或促致任何其他人使用或尝试使用任何电子、机械或其他器材，以截取任何口头通讯……；

(c) 蓄意向任何其他人披露或尝试向任何其他人披露任何有线、口头或电子通讯的内容，并知悉或有理由知悉有关资料是在违反本款的情况下透过截取有线、口头或电子通讯而取得的；

(d) 蓄意使用或尝试使用任何有线、口头或电子通讯的内容，并知悉或有理由知悉有关资料是在违反本款的情况下透过截取有线、口头或电子通讯而取得的；或

(e) (i) 蓄意向任何其他人披露或尝试向任何其他人披露……截取的任何有线、口头或电子通讯的内容，

(ii) 并知悉或有理由知悉有关资料是在与刑事调查相关的情况下，透过截取上述通讯而取得的，

(iii) 并在与刑事调查相关的情况下取得或接收有关资料，及

(iv) 意图不正当地妨碍、阻挠或干扰妥为授权的刑事调查，

则须按照第(4)款的规定惩处，或按照第(5)款的规定被起诉。”

---

51 《美国法典》第 18 篇（罪行及刑事法律程序）第 I 部（罪行）第 119 章（有线及电子通讯截取和口头通讯截取）（Chapter 119 (Wire and Electronic Communications Interception and Interception of Oral Communications), Part I (Crimes), Title 18 (Crimes and Criminal Procedure), United States Code）。

有线、口头及电子通讯的涵义

3.82 第 2511(1)条把有线、口头及电子通讯区分开来。第 2510 条界定这些词语：

> "(1) '有线通讯'指任何符合以下说明的听觉传讯：该传讯之全部或部分是透过使用……通讯传送设施，借助导线、电缆或其他在来源点与接收点之间的类似接驳装置……而作出的；
>
> (2) '口头通讯'指某人说出的任何口头通讯，而该人在有理由预期该通讯不会被截取的情况下，展示出他如此预期，但该词不包括任何电子通讯；
>
> (12) '电子通讯'指符号、讯号、文字、图像、声音、数据或消息（不论任何性质）的任何传讯，而该传讯之全部或部分是透过影响州际贸易或对外贸易的导线、无线电、电磁、光电子或光学系统而传送的，但不包括——
>
> (A) 任何有线或口头通讯；
>
> (B) 任何透过只具音频系统的传呼器材作出的通讯；
>
> (C) 任何由追踪器材……发出的通讯；或
>
> (D) 金融机构在用作电子储存及资金转账的通讯系统中储存的电子资金转账资料"。

截取目标

3.83 第 2511(1)(a)条禁止截取"任何有线、口头或电子通讯"，而第 2511(1)(c)、(d)及(e)条则适用于在订明情况下披露和使用截取通讯的"内容"。尽管用字有所不同，但基于第 2510 条以下定义，第 2511(1)(a)条定为不合法的截取，其目标似乎亦只限于通讯的内容：

> "(4) '截取'指透过使用任何电子、机械或其他器材，听取或以其他方式获取任何有线、电子或口头通讯的内容；
>
> (8) '内容'用于任何有线、口头或电子通讯时，包括关于该通讯的实质内容、大意或涵义的任何资料"。

在传送期间暂时静止的数据

3.84 特别就"电子通讯"而言，该词语的法定定义中"传讯"及"传送"等文字显示该词语指传递中的通讯。然而，联邦上诉法院第一巡回法庭（Court of Appeals for the First Circuit）在 *United States v Councilman* 一案裁定，该词语*"包括通讯过程中固有的短暂电子储存"*。[52]

罪行的豁除条文

3.85 第 2511(1)条所订罪行不适用于因着第 2511(2)条而获豁除者。这些获豁除者主要是：

(a) 有线或电子通讯服务的供应商；

(b) 联邦通讯委员会（Federal Communications Commission）履行执法（监察）职责的人员、雇员或代理人；

(c) 进行获授权电子监察的美国人员、雇员或代理人；

(d) 有关通讯的其中一方；及

(e) 获有关通讯其中一方事先同意进行截取的人。

《储存通讯法案》（《美国法典》第 18 篇第 2701 至 2713 条）

3.86 简言之，《储存通讯法案》：

> "……保障服务供应商所存档案的内容及服务供应商所持的用户纪录（例如用户姓名、帐单纪录或互联网规约地址）的私隐。"[53]

3.87 《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

---

52 *United States v Councilman*, 418 F 3d 67 (1st Cir 2005)，第 85 页。

53 司法协助局（Bureau of Justice Assistance），"Electronic Communications Privacy Act of 1986 (ECPA)"，登载于：https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285（于 2022 年 5 月 3 日浏览）。

(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，则须按照本条第(b)款的规定惩处。”

3.88 《美国法典》第 18 篇第 2701(c)条所载的例外情况包括：

“(1) 提供有线或电子通讯服务的人或实体所授权的行为；

(2) 有关服务的使用者就其本人的通讯所授权的行为，或就以该使用者为对象的通讯所授权的行为；或

(3) 本篇第 2703、[54] 2704[55] 或 2518[56] 条所授权的行为。”

《通讯纪录器法案》（《美国法典》第 18 篇第 3121 至 3127 条）

3.89 有关法例将《通讯纪录器法案》内两个主要词语（即*“通讯纪录器”*及*“监测追踪装置”*）界定如下：

“(3) ‘通讯纪录器’一词指记录或解译从传送有线或电子通讯的仪器或设施传送的拨号、发讯路线、发讯对象或讯号资料的器材或过程，但该等资料不包括任何通讯的内容……；

(4) ‘监测追踪装置’一词指获取正输入的电子或其他脉冲资料的器材或过程，以识别来源号码或其他拨号、发讯路线、发讯对象及讯号资料，而该等资料合理地相当可能会识别某项有线或电子通讯的来源，但该等资料不包括任何通讯的内容”。[57]

3.90 《通讯纪录器法案》首先一律禁止使用通讯纪录器及监测追踪装置：

“除本条另有规定外，任何人如没有事先根据本篇第 3123 条或《1978 年外国情报监察法案》（Foreign Intelligence

---

54 *“规定须披露客户通讯或纪录”。*

55 *“备份保存”。*

56 *“截取有线、口头或电子通讯的程序”。*

57 《美国法典》第 18 篇第 3127 条。

Surveillance Act of 1978）（《美国法典》第 50 篇第 1801 条及其后段落）取得法庭命令，或没有事先从受行政协议（获司法部长断定并向国会证实符合第 2523 条者）所规管的海外政府取得命令，则不得安装或使用通讯纪录器或监测追踪装置。”[58]

3.91 下一条接着规定，代表美国政府的律师可向法庭申请授权或批准安装通讯纪录器或监测追踪装置，或申请授权或批准使用通讯纪录器或监测追踪装置。[59]

小组委员会的看法

把在未获授权下截取电脑数据定为不合法

3.92 我们于本章起首指出，既然静止数据应受保障，使其免遭非法取览，那么传递中的数据亦应受保障，使其免遭非法截取。两者不但会引起私隐方面的关注，[60] 亦可能会带来其他潜在问题，例如被截取的数据如遭利用，可能会造成财务损失。[61]

3.93 据我们理解，任何未经编码处理的电脑数据，如在开放连接的网络上传送，便可被外界截取。[62] 电脑数据即使被截取，仍相当可能继续传送。人类传送或接收该等数据所构成的通讯，未必会察觉通讯已被截取，有关截取作为可能只有经第三方才会曝光。

3.94 为保存通讯完整无损，我们认为应把在未获授权下截取电脑数据定为罪行，亦应禁止在未获授权下披露或使用截取的数据。由于现今使用不同器材均会经常牵涉传递中的数据（即可能遭他人在未获授权下截取的数据），我们希望建议的罪行有助并巩固器材之间的可靠连接。随着量子计算时代来临，所有数据或可通通保留，我们亦因此预期建议的罪行会变得更为重要。

3.95 我们对香港及多个其他司法管辖区现行法例所进行的研究显示，多项与非法截取电脑数据相关的法规并行共存，背后原因显然

---

58 《美国法典》第 18 篇第 3121(a)条。

59 《美国法典》第 18 篇第 3122(a)(1)条。

60 《个人资料（私隐）条例》（第 486 章）只适用于可识别在世的个人的身分的资料，而该条例所订的刑罚亦相对较轻。

61 例如，信用卡资料在传送至卖方期间，被截取作不当用途。

62 很多网上通讯采用称为 HTTPS（保密超文本传输规约）的规约，数据会在传送前先经过编码处理。虽然有人或可截取部分通讯，但该部分不会是纯文字，而且必须加以解密。

是有需要立法涵盖对各式通讯的截取，包括电脑网络空间内外的通讯。

3.96 根据小组委员会的职权范围，我们建议订立适用于电脑数据的截取罪，但同时保留立法规管现实世界中对应罪行的可能性，以留待政府从长计议。我们相信，建议的罪行会补足只适用于公职人员的《截取通讯及监察条例》。

为不诚实或犯罪目的而截取

3.97 现代网络器材的运作方式难免牵涉截取。有鉴于现时的科技，我们承认假如纯粹在未获授权下截取电脑数据便会招致刑责，则我们建议的罪行范围未免不合理地宽广。例如，即使以下现象可能牵涉在未获授权下进行截取，我们相信没有很多人会认为它们有不妥：

(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个网站。

(b) 在日常运作中，互联网服务供应商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。此外，某些种类的数据（例如有关域名系统查询的通讯）只属暂时性质，但其他种类的数据（例如域名系统纪录、登入数据及电邮事项）则不然。

3.98 我们就建议的罪行的犯罪意念提出多个可能性后，总结认为不应坚持须证明有犯*某项特定罪行*的意图，因为这样可能会令执法过于困难。

3.99 我们建议，在建议的罪行下，有关截取须"为不诚实或犯罪目的"而进行。

罪行适用范围不限于私人通讯

3.100 我们提到，《布达佩斯公约》第三条所订罪行适用于"非公开"传送电脑数据。[63] 如《说明报告》所述，"非公开"一词规限传送

[63] 第 3.17 段。

（通讯）过程的性质，而非所传送数据的性质。[64] 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。

3.101 我们亦留意到在新西兰，其法律委员会及司法部：

(a) 认为在决定通讯是否属私人通讯时，参照通讯任何一方是否“理应合理预期该通讯可能会被截取”的做法并不理想；[65] 及

(b) 提议以“通讯”取代《2012 年搜查及监察法令》中对“私人通讯”的提述。[66]

3.102 我们认为，尽管法律委员会及司法部的提议是建基于新西兰对“私人通讯”的法定定义，他们强调不宜聚焦于通讯各方的预期[67] 这一理据，对其他司法管辖区而言确是真知灼见。

3.103 基于以上考虑，我们赞成订立能保障一般通讯（而并非只保障私人通讯）的截取罪。

罪行涵盖包括元数据在内的所有数据

3.104 大体来说，通讯的元数据可与通讯的内容相对照。电脑网络空间内的元数据通常与规约层面或系统层面的事物有关。

3.105 然而，从技术角度而言，现实的情况更为复杂，尤其是互联网采用分层方式，某层的元数据可能是另一层的数据。例如，中继信息在网络层面属数据，但就电邮而言却是元数据。元数据并非定义明确的概念。

3.106 另外，虽然在某些司法管辖区内，截取罪似乎不适用于元数据，但原因可能是这些罪行在多年前引入，而当代的元数据概念尚未在电子或电脑通讯的背景下出现。

3.107 考虑到上述因素，我们建议，建议的罪行应一般适用于数据（不论有关数据是否元数据）。

---

64 《说明报告》第 54 段（于上文第 3.18 段引述）。

65 法律委员会及司法部，*Review of the Search and Surveillance Act 2012 (IP40)*，第 4.11 段（于上文第 3.67 段引述）。

66 第 3.67(b)段。

67 如第 3.82 段所述，美国对“口头通讯”的法定定义亦提述通讯方预期的事宜。

罪行适用于整个传送过程中的数据

3.108　关于在传送期间暂时静止的数据，我们已于上文[68]讨论有关问题。

3.109　为简易起见，我们建议只要有关数据是在传送人一端前往传送对象一端的途中，截取有关数据便应属犯罪。订立这项罪行的方法之一，是加入类似于上文第 3.22 段所载的《电讯（截取及取览）法令》第 5F 条的推定条文。

3.110　至于储存于通讯系统内的数据，我们于上文提到，这类数据显然不受《截取通讯及监察条例》规管。[69] 因此我们提议，建议的非法截取罪不应适用于这类数据（我们认为这类数据反而应受第 2 章建议的非法取览罪规管）。

香港法例的蓝本

3.111　我们研究的所有司法管辖区中，相关法规各有不同。就作为香港的参考对象而言，《示范法》第 8 条（*"非法截取数据等"*）与我们的构思最为相近：

> "任何人如在无合法辩解或理由的情况下，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非公开传送；或
>
> (b) 来自某电脑系统并载有电脑数据的电磁发射；[70]
>
> 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。"

3.112　上述罪行的拟定方式须加以修改，以反映我们的其他建议。举例来说，香港的条文：

68　第 3.21 至 3.24 段。

69　第 3.25 段。

70　《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"。

(a) 应订定该条文适用于在没有"权限"下进行的截取，而非没有"理由"依据的截取（后者的概念似乎较广）；

(b) 不应只限适用于"非公开"传送；及

(c) 应包含有关截取须"为不诚实或犯罪目的"而进行这个犯罪意念。

建议 4

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）第 8 条为蓝本，包括犯罪意念（即"蓄意"截取）。

社会可能视为正当调查的行为

3.113 在第 2 章，我们提到建议的非法取览罪可能会对网络安全从业员造成影响。我们在建议 2 提出以下问题：在未获授权下为网络安全目的而取览，应否有特定的免责辩护或豁免。[71]

[71] 第 2.110 至 2.114 段。

3.114 我们在考虑建议的非法截取罪时，同样亦讨论到该罪行会否无意间对社会可能视为正当调查的行为造成影响。

3.115 我们欢迎社会各界就这个议题发表意见。

真实业务进行的截取

真实业务进行截取的情况普遍

3.116 尽管大多数人很可能会同意恶意截取他人数据是不当行为，例如藉着设置虚假 Wi-Fi 热点（可能利用具误导性的服务设定识别码），提供 Wi-Fi 热点或电脑供顾客或雇员使用的真实业务（咖啡店、酒店、购物商场、雇主等），在提供网络连接之余，还应否获准截取传送的数据，这个问题值得商榷：

(a) 随着数据分析面世，即使是真实业务，也可能有动机截取属于或关于顾客的数据，并可能从中获益，而顾客却未必察觉这些能够进行（据我们理解是经常进行）的数据分析何其深入。

(b) 在雇佣关系中，雇主可能会怀疑雇员有若干行为（例如犯罪，或违反雇佣合约的限制性契诺，向竞争对手或准雇主披露机密商业资料），因此或会想截取和分析往来雇员电脑的数据传送。

被截取的数据的用途

3.117 在上述例子和类似情况下被截取的数据可能有不少用途，我们在下文概述部分用途：

(a) 网络系统供应商一直向购物商场的东主推销一种新业务。具体而言，购物商场内的网络系统可追踪连接至该系统的器材（购物商场顾客的智能电话、平板电脑等）所在位置，藉此追踪持有这些器材的顾客的活动。这些位置数据可：

(i) 显示这些器材的使用者较常光顾哪些商店（他们便会是这些商店的目标顾客）；[72] 及

(ii) 利便按照位置提供服务（例如“推送”相关广告这项服务现已相当普遍）。

---

72 购物商场的东主或会认为，这类资料有助优化租户组合和决定适当的租金水平等。

(b) 网络器材设有一项标准功能，显示在该等器材所提供网络服务的用户当中，哪些网站最受欢迎。互联网服务供应商便可把所截取的用户数据提供予内容排名公司进行分析。

条款及条件

3.118 上述业务可根据若干条款及条件提供 Wi-Fi 热点或电脑供人使用，而有关条款及条件可保留权利截取和使用顾客或雇员的数据（例如进行流量分析和其他种类的数据分析）。这类截取和使用数据的权限属于合约性质。

3.119 在某些情况下，实在无从确定有多少顾客或雇员会细阅或明白这些条款及条件。其中有关考虑是，尽管不论有关业务规模大小，同一行为（截取数据）原则上理应导致同一法律后果，规模较大的业务一般有能力拟定周全细密的条款及条件，而这些条款及条件往往不容协商，并且向有关业务倾斜。

3.120 可更有效保障顾客和雇员的其中一个方法，是规定业务须具有法定权限，方可合法截取数据，即截取必须符合法例施加的若干规定。不过，假如只有根据法定权限方可进行数据分析，而不能根据合约权限进行该分析，我们预见不少数据分析工作将须终止。有人或会认为这样过分严苛。

征询公众回应

3.121 在上述各段中，[73] 我们已概述多个可能出现的例子和情况，说明各类专业及真实业务可能截取数据和使用截取或传送的数据。我们竭力确保我们的建议公平对待各方持份者，并公正地平衡兼顾他们的利益，因此在应否准许上述各段所识别的各类数据截取和使用的问题上，我们希望收到公众的意见。若公众在这方面的回应是肯定的，我们亦欢迎公众进一步建议应准许哪类专业及业务截取数据和使用截取或传送的数据，以及建议有关准许应否附带任何条件或限制。假如能够全面识别相关的例子及情况，我们便可更周详考虑应如何拟定建议的免责辩护或豁免（例如新订的电脑网络罪行法例是否可藉参照公认的法律概念，比如有合理目的或合法权限及不含恶意，从而对这些例子及情况作一般描述），以及这些免责辩护或豁免应如何施行（例如如何履行举证责任）。

---

73 第 3.113 至 3.120 段。

3.122 我们冀望公众能就以下建议5内的咨询问题发表意见。

建议5

小组委员会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实业务（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）？

第 4 章　非法干扰电脑数据

引言

4.1　我们会在本章探讨第三类依赖电脑网络的罪行，即非法干扰电脑数据，而非法干扰电脑系统则会在下一章集中讨论。概括而言，就此主题而订立的罪行，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。

4.2　第 2 章建议订立的非法取览罪，所针对的是入侵电脑系统的初期。随着入侵更进一步，干扰数据便可能构成本章所讨论的罪行。这两项罪行息息相关，特别是因为以下原因：

> "……其中一项支持把纯粹在未获授权下取用系统定为罪行的论据，是该项取用能够造成非蓄意的损坏。"[1]

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。

香港的现行法律

《刑事罪行条例》（第 200 章）

第 60 条

4.4　现时，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一种形式。根据《刑事罪行条例》（第 200 章）第 60(1)及(2)条（*"摧毁或损坏财产"*）：

---

[1] Ian Walden, *Computer Crimes and Digital Investigations* (Oxford University Press, 2007)，第 3.268 段。

"(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) 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。"

4.5 与第 60(1)条相比，第 60(2)条所订罪行显然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。"

1993 年的立法修订

4.6 《1993 年电脑罪行条例》（1993 年第 23 号）将《刑事罪行条例》（第 200 章）就"财产"一词所采用的涵义，扩至包括*"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。"*[2]

4.7 《1993 年电脑罪行条例》继而在《刑事罪行条例》（第 200 章）加入第 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；

---

[2] 《刑事罪行条例》（第 200 章）第 59(1)(b)条。

(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)部分与本章最为相关。

4.8 此外，《1993年电脑罪行条例》：

(a) 将在银行簿册等作出虚假记项罪适用于在电脑作出的记项；[3]

(b) 将入屋犯法罪的适用范围，扩大至包括作为侵入者进入任何建筑物，意图误用在该建筑物内的电脑／电脑程式或数据的人；[4] 及

(c) 将伪造账目罪适用于用电脑保存的纪录。[5]

展示成功执法的案例

4.9 *HKSAR v Chan Chi Kong*[6] 是首宗根据1993年修订的《刑事罪行条例》（第200章）而检控误用电脑的案件。[7] 被告人承认无合法辩解而销毁其雇主在客户办事处安装的电脑档案。高等法院上诉法庭在审理被告人就判刑提出的上诉时裁定，尽管受影响的电脑系统后来得以还原，令有关档案失而复得，原审法庭仍有充分理由判处扣押刑罚。[8]

4.10 在 *HKSAR v Ko Kam Fai*，[9] 男被告人对两名女受害人的电邮帐户进行黑客入侵，更改受害人电脑的数据，令受害人的电邮帐户无法操作。他又向受害人发送含有淫亵内容及强奸威胁的电邮。他承认多

---

3 藉在《刑事罪行条例》（第200章）加入新的第85(2)条。
4 藉在《盗窃罪条例》（第210章）加入新的第11(3A)条。
5 藉在《盗窃罪条例》（第210章）加入新的第19(3)条。
6 [1997] 3 HKC 702, CACC 245/1997（判决日期：1997年9月25日）。
7 根据被告人代表大律师的陈词（见判词第706页H行）。
8 然而，判刑由区域法院所判的监禁两年八个月，缩短至监禁一年九个月。
9 [2001] 3 HKC 181, CACC 83/2001（判决日期：2001年6月20日）。

项刑事恐吓和刑事损坏的控罪，分别违反《刑事罪行条例》（第 200 章）第 24 及 60(1)条。

4.11 由于案中电脑所受损坏属短期性质，故被告人就八项刑事损坏控罪的每一项被判处监禁四个月。两项刑事恐吓的控罪则较为严重，所判处的刑期亦较长（各为监禁 12 个月，这两项控罪的刑期与各项刑事损坏控罪的刑期同期执行）。被告人只针对刑事恐吓的判刑提出上诉，但被驳回。上诉法庭指出，就刑事损坏控罪的较轻判刑而言，*"虽然所判刑期表面上似乎较短，但在本案的特别情况下，刑事恐吓的控罪才是罪行重点"*。[10]

与第 161 条作比较

4.12 虽然《刑事罪行条例》（第 200 章）第 60 条所订最高刑罚（通常是监禁十年）较第 161 条所订最高刑罚（监禁五年）为重，但这两项条文均适用于电脑网络空间。据我们所理解，被控第 161 条所订罪行的人，偶尔也会被控第 60 条所订罪行，作为交替控罪。控方可视乎案情而将第 60 条视为第 161 条的合适后备条文：

(a) 如某电脑因足够稳健而未受损坏，只要有证据证明某人在未获授权下蓄意取用或操作该电脑，便足以根据第 161 条提出控罪。

(b) 然而，若有关证据只显示对电脑数据的更改是源自某些互联网规约地址（可沿该等地址追查犯罪者的身分），根据第 60 条提出控罪可能更为恰当。

(c) 怀有意图或罔顾后果均足以构成第 60 条的犯罪意念。这可能比第 161(1)(a)至(d)条所详述的意图更易证明。[11]

《电讯条例》（第 106 章）

第 25(a)条

4.13 《电讯条例》（第 106 章）第 25(a)条（*"电讯人员以外的人隐匿讯息等"*）订立了以下简易程序罪行：

---

10 同上，第 185 页。

11 根据第 161(1)条，任何人不得有下述意图或目的而取用电脑：

"(a) 意图犯罪；

(b) 不诚实地意图欺骗；

(c) 目的在于使其本人或他人不诚实地获益；或

(d) 不诚实地意图导致他人蒙受损失"。

"任何不属电讯人员或不属虽非电讯人员但其公务与电讯服务相关者的人，如——

(a) 故意隐匿、扣留或阻延拟传递予另一人的讯息；或

(b) [……]

即属犯罪，一经循简易程序定罪，可处第4级罚款[12]及监禁12个月。"

并非针对电脑网络罪行的特定条文

4.14 第25(a)条的措辞看来足以禁止他人抑制构成"讯息"的电脑数据（藉电讯）传送。然而，第25(a)条在应用于电脑数据时会有限制，这些限制与第3章所论述关于第27(b)条的限制相类似：[13]

(a) 由于第25(a)条以电讯为前提背景，故该条的拟定方式——包括对"电讯人员"、"讯息"[14]等的提述——并未能有效应用于电脑网络空间。

(b) 第25(a)条的犯罪行为只涵盖隐匿、扣留或阻延讯息，并无涵盖其他干扰电脑数据的方式（例如删除数据或将数据加密）。

《布达佩斯公约》订定罪行的标准

4.15 就本章而言，《布达佩斯公约》[15]的相关条文是第一节之下的第一篇第四条：

"1. 各缔约方均应采取必要的立法及其他措施，在其本土法律中将下列行为定为刑事罪行：在无权的情况下蓄意损坏、删除、弄坏、更改或抑制电脑数据。

2. 任何缔约方可保留权利，规定第1段所述的行为须造成严重伤害。"

---

12 根据《刑事诉讼程序条例》（第221章）附表8，现为25,000元。

13 第3.14至3.16段。

14 "讯息"的法定定义载于第3.14段。

15 有关《布达佩斯公约》的背景资料，见导言第11段，以及第1章第1.6至1.10段。

4.16 《说明报告》中有关第四条的内容如下：

"60. 本条旨在对电脑数据及电脑程式提供免遭蓄意损坏的保护，使其所受的保护与有体物所受的保护相若。这里受保护的法定权益，是所储存电脑数据或电脑程式的完整性，以及有关数据或程式的正常运作或使用。

61. 在第1段，'损坏'数据和'弄坏'数据这两种重迭的作为，尤其涉及对数据及程式的完整性或资讯内容作出不利的更改。'删除'数据等同于摧毁有体物，即是把数据销毁至难以辨识。抑制电脑数据指以下行动：阻止或终止可取用电脑或数据载体的人获取储存于电脑或数据载体的数据。'更改'一词指修改现有数据。因此，本段既涵盖输入病毒和特洛伊木马等恶意程式码，也涵盖对数据因此而造成的修改。

62. 上述作为只有在'无权'的情况下作出，方可予以惩处。网络设计中固有的常见活动或普遍的操作或商业惯例，例如在拥有人或操作人的授权下测试或保护电脑系统的安全性，又或在系统操作人获取新软件（例如准许接达互联网但会停用先前安装的相类程式的软件）时重新设定电脑的作业系统，均是在有权的情况下作出的，因此不会被本条定为罪行。为方便进行匿名通讯（例如匿名邮件转发系统的活动）而修改流量数据，或为进行安全通讯（例如将数据加密）而修改数据，原则上应视为对私隐的合法保障，故应视为在有权的情况下进行。然而，缔约方不妨把某些涉及匿名通讯的滥用行为（例如更改数据包的标头资料以隐藏犯罪者身分）定为罪行。

63. 此外，犯罪者须'蓄意'行事。

64. 第2段容许缔约方就有关罪行作出保留，使缔约方可规定有关行为须造成严重伤害。至于何谓严重伤害，则留待本土法律解释……"[16]

[16] 《说明报告》第60至64段。

其他司法管辖区的法定体制

澳大利亚

主要概念的法定定义

4.17 读者可能记得第 3 章提到，《刑事法典》（联邦）（Criminal Code (Cth)）第 10.7 部定为不合法的主要行为种类有：在未获授权下取览电脑数据、在未获授权下修改电脑数据，以及在未获授权下损害电子通讯。[17]

4.18 我们在研究有关罪行前，宜先研究第 476.1(1)条如何界定第二类及第三类非法行为（"损害往来某电脑的电子通讯"的定义已在第 3 章列明，但值得在此重述）：

> "**电子通讯**指藉导向电磁能或无导向电磁能而以任何形式传达资料。"
>
> "就存于某电脑内的数据而言，**修改**指：
>
> (a) 更改或移除该等数据；或
>
> (b) 对该等数据作出增补。"
>
> "**损害往来某电脑的电子通讯**包括：
>
> (a) 阻止进行上述通讯；或
>
> (b) 在该电脑所使用的电子联网或网络上损害上述通讯；
>
> 但不包括纯粹截取上述通讯。"

4.19 根据上述定义，上述以粗体表示的词语与非法干扰电脑数据相对应，尽管该等词语涉及该罪行不同的层面。

---

17 第 3.32 段。

《刑事法典》（联邦）第 477.1 条

4.20 第 477.1 条（*"在未获授权下作出取览、修改或损害，并意图干犯严重罪行"*）已在第 2 章论述，讨论侧重于有关在未获授权下取览电脑数据的第 477.1(1)(a)(i)条。[18]

4.21 第 477.1(1)(a)(ii)及(iii)条与本章相关，规定任何人如导致"在未获授权下修改存于某电脑内的数据"，或导致"在未获授权下损害往来某电脑的电子通讯"，而该人知悉该行为未获授权，并意图藉该行为而干犯（或利便干犯）违反联邦、各州或领地法律的严重罪行，即属犯罪。

4.22 "严重罪行"是可处终身监禁或为期五年或以上监禁的罪行。[19] 任何人违反第 477.1(1)条，可处不超过适用于严重罪行的刑罚。

《刑事法典》（联邦）第 477.2 条

4.23 如证据未能证明有干犯（或利便干犯）严重罪行的意图，则第 477.2 条（*"在未获授权下修改数据，以导致损害"*）仍可能适用：

> "(1) 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。
>
> 刑罚：监禁 10 年。
>
> (3) 即使没有实际上损害或不会实际上损害：
>
> (a) 对存于某电脑内的数据的取览；或

---

18 第 2.21 段。

19 《刑事法典》（联邦）第 477.1(9)条。

(b) 上述数据的可靠性、保安或操作，

任何人仍可被裁定犯违反本条的罪行。

(4) 违反本条罪行的定罪判决，可作为违反第 477.3 条罪行（在未获授权下损害电子通讯）的控罪的交替裁决。”

4.24 第 477.2(3)条似乎旨在明确地表明，任何人如罔顾自己在未获授权下作出的修改会否实际上造成第 477.2(3)条所描述的损害，即属干犯第 477.2(1)条所订罪行。然而，由于第 477.2(1)(c)(ii)条采用了广泛的措辞来表达损害的对象，因此任何人譬如在电脑系统引入类似计时炸弹的软件（即经设计以在未来某时间无需进一步干预而损害数据，或在某事件发生时损害数据的软件），便可能干犯第 477.2(1)条所订罪行。我们亦于下文第 4.73 段对美国的相关法例提出类似观点。

《刑事法典》（联邦）第 477.3 条

4.25 相反，如根据第 477.3 条（*“在未获授权下损害电子通讯”*）提出控罪，实际损害则是重要元素：

“(1) 任何人在以下情况，即属犯罪：

(a) 该人导致在未获授权下损害往来某电脑的电子通讯；及

(b) 该人知悉该项损害未获授权。

刑罚：监禁 10 年。

(3) 违反本条罪行的定罪判决，可作为违反第 477.2 条罪行（在未获授权下修改数据，以导致损害）的控罪的交替裁决。”

4.26 根据第 477.2(4)及 477.3(3)条，第 477.2(1)及 477.3(1)条所订罪行（分别适用于修改数据和损害通讯）互为法定交替罪行。由于这两项罪行均最高可处十年监禁，被告人能够指称因作出交替裁决而可能造成不公的机会不大。然而，我们并不清楚为何有关法例就违反第 477.2(1)条的非法干扰（即使没有导致实际损害）和违反第 477.3(1)条的非法干扰，订定相同的法定最高刑罚。第 477.2(1)条所订的罪责，是归因于罔顾在未获授权下修改数据是否可能导致实际损害，而第

477.3(1)条则规定电子通讯须受损害，但没有明确提到犯罪者"意图导致该项损害"。[20]

《刑事法典》（联邦）第 478.1 条

4.27 第 478.1 条（*"在未获授权下取览或修改受限数据"*）及第 478.2 条（*"在未获授权下损害存于电脑纪录碟等内的数据"*）可视为另一组分别处理修改和损害的条文。虽然这些条文所订立的罪行并非法定交替罪行，但两者的最高刑罚相同，均最高可处两年监禁。

4.28 第 478.1 条规定如下：

> "(1) 任何人在以下情况，即属犯罪：
>
> (a) 该人导致在未获授权下取览或修改受限数据；及
>
> (b) 该人意图导致该项取览或修改；及
>
> (c) 该人知悉该项取览或修改未获授权。
>
> 刑罚：监禁 2 年。
>
> (3) 在本条中：
>
> ***受限数据***指符合以下说明的数据：
>
> (a) 存于某电脑内；及
>
> (b) 其取览受与该电脑任何功能相关的存取控制系统所限。"

4.29 第 477.2 及 478.1 条所订罪行均适用于在未获授权下修改数据。两者的共通点是就犯罪意念而言，犯罪者须知悉有关修改未获授权。然而：

---

[20] 《2001 年电脑网络罪行法案》(Cybercrime Bill 2001)在《刑事法典》加入第 477.2 及 477.3 条，该法案的摘要说明解释了这两项条文把最高刑罚订为监禁十年的背景。第 477.2 条的刑罚相等于《刑事罪行法令》（Crimes Act）当时所订电脑罪行的刑罚，以及《刑事法典》所订欺诈罪及伪造罪的刑罚。至于第 477.3 条的刑罚，则*"确认了利用电脑进行可靠通讯的重要性，以及如该等通讯受到损害，即可造成相当大的损坏"*。然而，并无其他二手资料解释为何第 477.2 及 477.3 条的犯罪行为不同，最高刑罚却相同。

(a) 犯罪者只要罔顾后果，便足以符合第 477.2(1)(c)条的规定，但要符合第 478.1(1)(b)条的规定，犯罪者须意图导致有关修改。

(b) 此外，第 477.2(1)(a)条并没有如第 478.1(1)(a)条那样，规定有关数据须属“受限数据”。

第 477.2 条所订罪行的最高刑罚较重，显示第 477.2 条的罪行理应较第 478.1 条严重，但上述两点看来与此不符。

《刑事法典》（联邦）第 478.2 条

4.30 正如上文所述，第 478.1 及 478.2 条所订罪行的最高刑罚相同，均最高可处两年监禁。后述条文的内容如下：

“任何人在以下情况，即属犯罪：

(a) 该人导致在未获授权下损害存于以下事物内的数据的可靠性、保安或操作：

(i) 电脑纪录碟；或

(ii) 信用卡；或

(iii) 其他用作以电子方式储存数据的器材；及

(b) 该人意图导致该项损害；及

(c) 该人知悉该项损害未获授权。

刑罚：监禁 2 年。”

4.31 第 477.3 及 478.2 条所订罪行分别适用于在未获授权下损害电子通讯，以及在未获授权下损害数据的可靠性、保安或操作。这两项罪行的共通元素，是犯罪者知悉有关损害未获授权。

4.32 尽管如此，第 477.3 条并没有如第 478.2(b)条那样，提述犯罪者意图导致有关损害，这似乎有违常理，因为前者大概是为了订立较严重的罪行，才订明较重的最高刑罚。

加拿大

《1985 年刑事法典》第 430(1.1)条

4.33 与澳大利亚法例相比，加拿大法例较为精简。相关条文是《1985 年刑事法典》（Criminal Code 1985）第 430(1.1)条（*"与电脑数据有关的损害"*）：

> "任何人如故意
>
> (a) 销毁或更改电脑数据；
>
> (b) 使电脑数据变得无意义、无用或无效；
>
> (c) 妨碍、中断或干扰合法使用电脑数据；或
>
> (d) 妨碍、中断或干扰正在合法使用电脑数据的人，或拒绝让有权取览电脑数据的人取览电脑数据，
>
> 即属导致损害。"

与《示范法》的相似之处

4.34 《1985 年刑事法典》第 430(1.1)条就犯罪行为订定的条文，措辞几乎与《示范法》第 6 条（*"干扰数据"*）的下述条文相同：

> "(1) 任何人无合法辩解或理由而蓄意或罔顾后果地作出任何以下作为：
>
> (a) 销毁或更改数据；
>
> (b) 使数据变得无意义、无用或无效；
>
> (c) 妨碍、中断或干扰合法使用数据；或
>
> (d) 妨碍、中断或干扰正在合法使用数据的人；或
>
> (e) 拒绝让有权取览数据的人取览数据，
>
> 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。
>
> (2) 不论上述人士的作为所造成的影响属暂时性或永久性，第(1)款亦适用。"

第 430(1.1)条所指的损害

4.35 《1985 年刑事法典》第 430(1.1)条就"损害"所订的某些特点值得留意：

(a) 就犯罪行为而言，第 430(1.1)条针对的是受禁后果，而没有把任何特定行为定为不合法，该条亦无提述获得授权或未获授权的概念。该条看来适用于故意藉不作为（即不作出某行为）而导致受禁后果的被告人。[21] 另外，该条的法律措辞似乎足以涵盖以物理手段损坏电脑数据的情况（例如把强力磁铁放在旧式软磁碟附近）。

(b) 就犯罪意念而言，被告人须故意导致有关损害。根据第 429(1)条：

> "就本部而言，如任何人藉作出某作为或不作出该人有责任作出的作为而导致某事件发生，而该人知悉该作为或不作为颇有可能会导致该事件发生，并罔顾该事件是否发生，则该人须视为故意导致该事件发生。"

导致损害的刑事后果

4.36 《1985 年刑事法典》第 430 条订明在不同情况下导致"损害"的刑事后果。根据第 430(5)条：

"任何人导致与电脑数据有关的损害，即属

(a) 犯可公诉罪行，可处为期不超过 10 年的监禁；或

(b) 犯可循简易程序定罪而惩处的罪行。"

4.37 此外，某些其他款亦可能适用于与电脑数据有关的损害。举例来说，第 430(2)条有以下规定：

> "任何人如导致损害以致生命受到实际危害，即属犯可公诉罪行，可处终身监禁"。

---

21 《1985 年刑事法典》第 430(5.1)条提供支持这项解释的依据。根据该条：
"任何人故意作出某作为或故意不作出该人有责任作出的作为，而如该作为或不作为相当可能构成损害导致生命受到实际危害，或构成与财产或电脑数据有关的损害……"
即属犯罪。

英格兰及威尔斯

《英格兰误用电脑法令》第 3 条

4.38 《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"*）及第 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"*）显示两层式的做法。我们会先研究第 3 条：

"(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；及

(c) 下文第(2)款或第(3)款适用。

(2) 如上述人士意图藉作出有关作为而——

(a) 损害任何电脑的操作；

(b) 阻止或阻碍取览存于任何电脑内的任何程式或数据；或

(c) 损害上述程式的操作或上述数据的可靠性；或

(d) 致使上述(a)至(c)段提述的任何事宜得以作出，

则本款适用。

(3) 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。

(4) 上文第(2)款所提述的意图，或上文第(3)款所提述的罔顾后果，不一定要涉及——

(a) 任何特定电脑；

(b) 任何特定程式或数据；或

(c) 任何特定种类的程式或数据。

(5) 在本条中——

(a) 凡提述作出某作为，即包括提述导致作出某作为；

(b) '作为'包括一连串作为；

(c) 凡提述损害、阻止或阻碍某些事宜，即包括提述暂时如此行事。

(6) 任何人犯本条所订罪行——

(a) 一经在英格兰及威尔斯循简易程序定罪，可处为期不超过12个月的监禁或不超过法定最高罚款，或两者兼处；

(b) [……]

(c) 一经循公诉程序定罪，可处为期不超过10年的监禁或罚款，或两者兼处。"

展示成功执法的案例

4.39 *R v Victor Lindesay*[22] 是根据《英格兰误用电脑法令》第3条成功执法的例子。该案的案情与 *HKSAR v Chan Chi Kong* 相似。[23] 林德赛（Lindesay）先生承认三项导致在未获授权下修改电脑内容的控罪。虽然所造成的损坏并非永久，但他被判处监禁九个月。

4.40 英格兰上诉法院维持判刑，并指出：

> "……不管上诉人的不满是多么实在，不管上诉人是多么出于一时冲动而作出报复，也不管上诉人须对这些作为负责是多么难免会被揭发，事实毕竟是上诉人利用自己的技术及对前雇主业务的认识，给完全无辜的机构带来大量工作、不便及忧虑。依本院判断，判处即时执行的监禁刑罚以反映上诉人破坏诚信，实属恰当。"[24]

---

22 [2001] EWCA Crim 1720; [2002] 1 Cr App R (S) 86.

23 第4.9段。

24 见上文注脚22，第373页（第15段）。

《英格兰误用电脑法令》第 3ZA 条

4.41　任何人违反第 3 条，可处为期不超过十年的监禁或罚款，或两者兼处。第 3ZA 条所订的最高刑罚严重得多，该条内容如下：

"(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——

(a) 对任何地方的人类福祉的损害；

(b) 对任何地方的环境的损害；

(c) 对任何国家的经济的损害；或

(d) 对任何国家的国家安全的损害，

即属'关键性'损害。

(3) 就第(2)(a)款而言，某作为只有导致以下情况，方属导致对人类福祉的损害——

(a) 人命损失；

(b) 人类患病或受伤；

(c) 货币、食物、水、能源或燃料的供应受到干扰；

(d) 通讯系统受到干扰；

(e) 交通设施受到干扰；或

(f) 关乎卫生的服务受到干扰。

(4) 就第(2)款而言，某导致损害的作为是否——

(a) 直接导致该损害；

(b) 该损害的唯一或主要成因，

均属无关重要。

(5) 在本条中——

(a) 凡提述作出某作为，即包括提述导致作出某作为；

(b) '作为'包括一连串作为；

(c) 凡提述某国家，即包括提述某地区，以及提述某国家或地区的任何地方、部分或区域。

(6) 除非第(7)款适用，否则任何人犯本条所订罪行，一经循公诉程序定罪，可处为期不超过14年的监禁或罚款，或两者兼处。

(7) 如任何人——

(a) 因导致第(3)(a)或(3)(b)款所述种类的人类福祉严重损害的作为而干犯本条所订罪行，或因产生导致该损害的重大风险的作为而干犯该罪行；或

(b) 因导致国家安全严重损害的作为而干犯本条所订罪行，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。"

第3及3ZA条的犯罪行为

4.42 这两项条文的犯罪行为均包括*"就某电脑作出任何未获授权的作为"*。就第3ZA条而言，该作为还须导致*"关键性严重损害"*，或产生导致*"关键性严重损害"*的重大风险。

4.43 "作为"一词示明任何人不会因着不作为而干犯上述任何条文所订罪行。另外，按照这两项条文的草拟方式，似乎无须证明实际损害，方能定罪。

4.44 此外，似乎物理作为亦可构成这两项条文的犯罪行为。在这方面，我们在上文讨论加拿大法律时曾举出把强力磁铁放在旧式软磁碟附近的例子。[25] *R v Nicholas Alan Whiteley*[26] 指出，在《英格兰误用电脑法令》实施前，这样做可能构成《1971 年刑事损坏法令》(Criminal Damage Act 1971) 第 1(1)条 (*"摧毁或损坏财产"*) 所订的罪行。[27] 该法令第 10(5)条现须加以考虑：

> "就本法令而言，修改电脑的内容不得视为损坏任何电脑或电脑储存媒体，但如该项修改对该电脑或电脑储存媒体的影响，是损害其物理状况，则作别论。"

4.45 鉴于第 10(5)条，修改电脑的内容而没有损害电脑的物理状况，应根据《英格兰误用电脑法令》而非《1971 年刑事损坏法令》提出检控。

第 3 及 3ZA 条的犯罪意念

4.46 至于犯罪意念方面，这两项条文均规定被告人须知悉其作为未获授权，并规定被告人须：

(a) 意图导致（如属第 3 条）指明类型的损害[28] 或（如属第 3ZA 条）"关键性严重损害"；[29] 或

(b) 罔顾上述损害会否发生。

中国内地

《中国刑法》第二百八十六条第二款

4.47 根据《中国刑法》第二百八十六条第二款：

> "违反国家规定，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，后果严重的，依照前款的规定处罚。"

（底线后加）

---

25 第 4.35(a)段。

26 (1991) 93 Cr App R 25.

27 *"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。"*

28 损害任何电脑的操作、阻止或阻碍取览任何程式或数据、损害上述程式的操作，或损害上述数据的可靠性（第 3(2)条）。

29 第 3ZA(2)及(3)条。

展示成功执法的案例

4.48 在最高人民检察院第九批指导性案例的第34号案例，[30] 被告人冒用其他互联网使用者的身分登录他们的购物网站帐户，删改这些互联网使用者在某网购平台上给予一些网上卖家的劣评。被告人因为对计算机信息系统内的数据（即该网购平台上的劣评）进行修改，被裁定犯了第二百八十六条第二款所订罪行。法院将该等差评数据视为该购物平台计算机信息系统的"重要组成部分"。

新西兰

《新西兰法令》第250(2)条

4.49 新西兰的法例方案与英格兰及威尔斯的相类似，有关法例既订有基本罪行，亦订有加重形式，后者以被告人的作为所导致的更严重后果为基础。

4.50 《新西兰法令》第250(2)条（*"损坏或干扰电脑系统"*）订立以下基本罪行。就本章而言，第250(2)条规定如下：

> "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。"

4.51 第250(2)(c)条会在第5章探讨。

删除电脑数据或软件

4.52 第250(2)(a)及(b)条提述多种作为，其中包括删除电脑数据或软件。相关的问题是，这是否意味着要令有关数据或软件不可复原（"擦除"），还是即使有关数据或软件可轻易复原，仍会产生刑事法律责任？后述情况的例子如下：

---

30 李骏杰等破坏计算机信息系统案。

(a) 如某人正使用文字处理器编辑文件，而另一人在未获授权下删除当中某些内容，“复原”功能可能有助复原被删除的内容。

(b) 在某人删除电脑内的档案后，或可在“资源回收筒”、“垃圾桶”或同等位置找到有关档案，再把它复原。

(c) 如相关储存媒体存有备份或影像，便能够还原被删除的档案。[31]

4.53 某评论员注意到，*Police v Robb*[32] 一案强调了擦除和可复原的删除之间的分别。正如基督城（Christchurch）地区法院所指，有关电脑档案看来：

> “……只是被删除，而不是被擦除。擦除涉及在删除前先将档案的数据盖写。人们普遍认为被擦除的档案无迹可寻，亦无法复原。”[33]

4.54 上述评论员将该法院的裁定概述如下：

> “根据法官的说法，删除本身并不构成损坏或干扰电脑系统而违反［《1961 年刑事罪行法令》（Crimes Act 1961）］第 250 条。另外，要证明损坏或干扰电脑系统的刑事罪行，便须豁除数据是在无意或意外的情况下删除。法官指出，擦除档案要求在单纯删除之外再另作有意的决定，但档案是否被故意删除，并不能用法证方法断定。”[34]

4.55 对于该法院裁定须证明*“故意采取步骤确保有关数据无法复原，即擦除数据”*，[35] 该评论员有以下批评：

> “国会在［《1961 年刑事罪行法令》第 250(2)条中］使用‘删除’一词的用意，不可能是表示该档案的全部或部分须完全无法复原……国会的用意……不可能是电脑的正常操作可包括在他人蓄意进行旨在妨碍某机器或系统

---

31 一如 *HKSAR v Chan Chi Kong* 的情况（引用于第 4.9 段）。

32 [2006] DCR 388（该书面决定似乎没有网上版）。

33 同上，第 27 段，引述于：
David Harvey, *internet.law.nz selected issues* (LexisNexis NZ Limited, 4th edition, 2015)，第 7.92 段。

34 David Harvey, *internet.law.nz selected issues* (LexisNexis NZ Limited, 4th edition, 2015)，第 7.93 段。

35 *Police v Robb*，第 40 段，引述于 David Harvey, *internet.law.nz selected issues* (LexisNexis NZ Limited, 4th edition, 2015)，第 7.93 段。

妥善操作的活动后采取介入补救步骤，使该机器或系统可以操作。"[36]

4.56 除非根据上述评论员的论点而采取较宽松的解释，否则按照 *Police v Robb*[37] 所裁定对第 250(2)条的解释，假如 *HKSAR v Chan Chi Kong*[38]（该案中被删除的档案最终还原，不过是在即时启动紧急应变程序之后）在新西兰发生，该条相当可能会不适用于该案的案情。

第 250(2)条的犯罪意念

4.57 第 250(2)条以"蓄意或罔顾后果地"行事，形容进行犯罪行为的犯罪意念，而有关未获授权的犯罪意念，则是知悉或罔顾后果。有两点观察可以提出：

(a) 该法例虽然可提述被告人是"故意或罔顾后果地"进行犯罪行为，但却选用了"蓄意或罔顾后果地"。有学者认为，就新西兰的刑事法律而言，*"显然'故意'可用作'意图'的同义词"*。[39] 与此比较，根据美国法学会（American Law Institute）的《模范刑法典》（Model Penal Code）：[40]

> "除第 2.05 条另有规定外，任何人除非就某罪行的每项关键元素特意、[41] 故意、[42] 罔顾后果地[43] 或疏忽[44] 行事（视乎法律规定），否则该人不属犯罪。"[45]

---

36 见上文注脚 34，第 7.94 段。

37 [2006] DCR 388.

38 第 4.9 段。

39 Kris Gledhill, "The Meaning of Knowledge as a Criminal Fault Element: Is to Know to Believe?" (2019) 45(2) University of Western Australia Law Review 216，第 228 页。

40 《模范刑法典》并非法律，但正如美国法学会所指，该法典*"对于美国实体刑事法律的广泛修订和编纂，发挥了重要作用"*。见美国法学会，《模范刑法典》，登载于 https://www.ali.org/publications/show/model-penal-code/（于 2022 年 5 月 3 日浏览）。

41 *"任何人在以下情况，即属就某罪行的关键元素特意地行事：*
(i) 如该元素涉及该人的行为的性质或后果，该人有意识地以进行属该性质的行为或导致该后果为目的；及
(ii) 如该元素涉及伴随情况，该人察觉到该等情况存在，或相信或希望该等情况存在。"（第 2.02(2)(a)条）

42 *"任何人在以下情况，即属就某罪行的关键元素故意地行事：*
(i) 如该元素涉及该人的行为的性质或伴随情况，该人察觉到其行为属该性质，或察觉到该等情况存在；及
(ii) 如该元素涉及该人的行为的后果，该人察觉到其行为实际上肯定会导致该后果。"（第 2.02(2)(b)条）

43 *"凡任何人有意识地不理会某罪行的关键元素存在的重大不合理风险，或有意识地不理会其行为会导致该关键元素的重大不合理风险，即属就该关键元素罔顾后果地行事。该风险须具有以下性质及程度：在顾及行事者行为的性质及目的，以及该人所知的情况后，该人不*

因此根据该法典，“特意”（界定为性质与“蓄意”相类似）与“故意”属不同概念。

(b) 相比之下，罔顾后果的涵义更为清晰。新西兰最高法院在 *Cameron v R*[46] 中裁定：

> “在……的案件中，如并非以规定至少实际知悉或怀有意图的字眼来界定所涉罪行，我们认为［*R v G*[47]］所阐释的罔顾后果，将（至少通常甚或定当）足以符合情况及后果这两方面的犯罪意念规定。就上述目的而言，如有以下情况，即构成罔顾后果：
>
> (a) 被告人意识到：
>
> i. 其行动确实可能会引致受禁后果；及／或
>
> ii. 受禁情况确实可能存在；及
>
> (b) 考虑到该风险后，该等行动属不合理。”[48]

《新西兰法令》第 250(1)条

4.58 至于加重罪行方面，根据《新西兰法令》第 250(1)条：

> “任何人蓄意或罔顾后果地摧毁、损坏或更改任何电脑系统，并知悉或理应知悉相当可能会导致生命受危害，可处为期不超过 10 年的监禁。”

4.59 表面上，该条文只涵盖摧毁、损坏或更改电脑系统，但不涵盖电脑数据。然而，在一些被告人的作为“相当可能会导致生命受危

理会该风险涉及严重偏离守法的人如处于行事者的情况便会遵守的行为标准。”（第 2.02(2)(c)条）

44 *“凡任何人应察觉到有某罪行的关键元素存在的重大不合理风险，或察觉到其行为会导致该关键元素的重大不合理风险，即属就该关键元素疏忽地行事。该风险须具有以下性质及程度：在顾及行事者行为的性质及目的，以及该人所知的情况后，该人没有意识到该风险涉及严重偏离合理的人如处于行事者的情况便会采取的谨慎标准。”*（第 2.02(2)(d)条）

45 第 2.02(1)条。

46 [2017] NZSC 89.

47 [2003] UKHL 50; [2004] 1 AC 1034.

48 *Cameron v R*，第 73 段，引用于 Nick Chisnall, “Case Note: *Cameron v R* [2017] NZSC 89 – Controlled Drug Analogues, Indeterminacy and *Mens Rea* under the Misuse of Drugs Act 1975” [2017] NZCLR 256, 第 262 页。

害”的案件中，可以想象到该人除摧毁、损坏或更改了整体电脑系统之外，应该亦销毁、损坏或更改了电脑数据。事实上，该条文可说是与第 4 章及第 5 章同时相关。

4.60 另一方面，获得授权这概念显然与第 250(1)条无关，这与第 250(2)条有所不同。鉴于前者涉及生命受危害，这点可以理解。

《新西兰法令》第 258(1)条

4.61 第 250(1)条所订罪行的最高刑罚（监禁十年）与第 258(1) 条（*“意图欺骗而更改、隐藏、销毁或复制文件”*）所订的相同。第 258(1)条载列如下：

> “任何人——
>
> (a) 更改、隐藏或销毁任何文件，或导致任何文件被更改、隐藏或销毁；或
>
> (b) 制造文件或导致文件被制造，而该文件的全部或部分属任何其他文件的复制文本，
>
> 并意图以欺骗手段取得任何财产、特权、服务、金钱利益、得益或有值代价，或意图导致任何其他人蒙受损失，可处为期不超过 10 年的监禁。”[49]

4.62 法院在 *R v Johannes Hendrik Middeldorp*[50] 中裁定，在上文引述的第 258(1)(b)条中，“文件”一词包括储存于电脑硬碟的电脑档案（代表扫描影像），以及已发送或接收的电邮的附件（代表影像）。按逻辑推断，第 258(1)(a)条中“文件”一词亦应同样诠释。基于这一点，凡电脑数据被更改、隐藏或销毁，有关条文亦会适用。

4.63 如将第 250(1)条针对电脑的罪行与第 258(1)条适用于一般情况的罪行加以比较，便可见以下潜在的重大差异：罔顾后果足以构成前述条文的犯罪意念，但不足以构成后者的犯罪意念。

---

49 第 258(2)条阐述如下：

“在有第(1)款所提述的意图而作出有关更改或制造有关文件后，违反该款的罪行即告完成，即使犯罪者未必有以下意图亦然——

(a) 某特定的人应使用被更改或制造的文件，或应按照该文件行事；或

(b) 某特定的人应基于被隐藏或销毁的文件并不存在而行事；或

(c) 某特定的人应被诱使作出或不作出任何行为。”

50 [2015] NZHC 951.

新加坡

《新加坡误用电脑法令》第 5 条

4.64 《新加坡误用电脑法令》第 5 条（*"在未获授权下修改电脑资料"*）与本章相关：

> "(1) 除第(2)款另有规定外，任何人知悉任何作为会导致在未获授权下修改任何电脑的内容，并作出该作为，即属犯罪，一经定罪——
>
> (a) 可处不超过$10,000 的罚款或为期不超过 3 年的监禁，或两者兼处；及
>
> (b) 如属第二次或其后每次定罪，则可处不超过$20,000 的罚款或为期不超过 5 年的监禁，或两者兼处。
>
> (2) 如因本条所订罪行而导致任何损坏，被裁定犯该罪行的人可处不超过$50,000 的罚款或为期不超过 7 年的监禁，或两者兼处。
>
> (3) 就本条而言，如有关作为并非针对——
>
> (a) 任何特定程式或数据；
>
> (b) 任何种类的程式或数据；或
>
> (c) 存于任何特定电脑内的程式或数据，
>
> 均属无关重要。
>
> (4) 就本条而言，未获授权的修改是否属永久性或仅属暂时性，或是否拟属永久性或拟仅属暂时性，均属无关重要。"

未获授权的修改

4.65 至于犯罪行为方面，该法令第 2(7)及(8)条阐释未获授权的修改这个主要概念：

> "(7) 就本法令而言，如藉着操作有关电脑或任何其他电脑的任何功能——

(a) 存于有关电脑内的任何程式或数据遭更改或删抹；

(b) 在该电脑所收纳的内容上任何程式或数据有所增加；或

(c) 发生任何会损害任何电脑的正常操作的作为，

即属出现修改任何电脑的内容，而造成导致上述修改的任何作为，须视为导致该项修改的作为。

(8) 凡有人因其作为而导致第(7)款所提述的修改，而该人——

(a) 本身无权决定应否作出该项修改；及

(b) 未获有此权利的人同意该项修改，

该项修改即属未获授权。"

犯罪意念

4.66 该法令订明的犯罪意念，是知悉犯罪者的作为会导致未获授权的修改。因此，单是罔顾后果，并不足以招致刑事法律责任。

如涉及"受保护电脑"可加重惩罚

4.67 上文所详细论述的司法管辖区均订有基本罪行，并订有以更严重后果（例如犯罪者意图或导致生命受危害）为基础的加重罪行。

4.68 《新加坡误用电脑法令》则采用另一做法。除了第5(1)条（该条订明适用于再犯者的最高刑罚较重）及第5(2)条（根据该条可对导致"任何损坏"的犯罪者判处更重的最高刑罚）之外，第11(1)条还把最重的最高刑罚预留给涉及取用"受保护电脑"的案件：

"(1) 如有人在干犯第3、5、6或7条所订罪行的过程中取用任何受保护电脑，被裁定干犯该罪行的人可处不超过$100,000的罚款或为期不超过20年的监禁，或两者兼处，以代替该等条文所订明的刑罚。

(2) 就第(1)款而言，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或程式或数据是在与下述各项有直接关连的情况

下使用的，或对下述各项属必要的——

(a) 新加坡的安全、防务或国际关系；

(b) 与执行刑事法律有关的机密资料来源的存在或身分；

(c) 提供与通讯基础建设、银行及金融服务、公共事业、公共交通或公开密码匙基础建设直接有关的服务；或

(d) 保障公众安全，包括与必要紧急服务（例如警务、民防及医疗服务）有关的系统。

(3) 为根据本条提出的检控的目的，已就有关电脑、程式或数据而言，如被告人获展示电子警告或其他警告，而该警告述明在未获授权下取用该电脑或取览该程式或数据，可根据本条处以较重刑罚，则须推定被告人知悉第(2)款提述的所需事实，直至相反证明成立。”

4.69 《新加坡误用电脑法令》述明在制订加重罪行时，涉及某类数据或电脑系统可作为加重刑罚的因素。

美国

《电脑欺诈及滥用法案》内的《美国法典》第 18 篇第 1030(a)(5)条

4.70 正如第 1 章[51] 及第 2 章[52] 所指，《电脑欺诈及滥用法案》（Computer Fraud and Abuse Act，《美国法典》第 18 篇第 1030 条）是美国应对电脑网络罪行的主要联邦法例。任何人如作出与第 1030(a)条所述各种情境有关的作为，可按第 1030(c)条的规定予以惩处。

4.71 《美国法典》第 18 篇第 1030(a)(5)条订立与本章相关的罪行，该条分为三个部分：

“(A) 故意导致向某受保护电脑传送程式、资料、代码或指令，并因着该行为而在未获授权下蓄意导致该电脑

---

51 第 1.10(b)段。

52 第 2.81 段。

损坏；

(B) 在未获授权下蓄意取用某受保护电脑，并因着该行为而罔顾后果地导致损坏；或

(C) 在未获授权下蓄意取用某受保护电脑，并因着该行为而导致损坏及损失。”

对受保护电脑所导致的损坏

4.72 以上三个部分均关乎对“受保护电脑”所导致的“损坏”。《美国法典》第 18 篇第 1030(e)(8)条把“损坏”界定为*“对数据、程式、系统或资料的完整性或可用性造成任何损害”*。

4.73 在这宽广的定义下，某人如作出某些行为（例如蓄意地散播电脑病毒，或安装类似计时炸弹的软件），尽管这些行为不会即时导致损坏，它们已等同实际干扰电脑数据，带来在较后时间发生损坏的风险，有关罪行似乎也适用于该人。虽然上述干扰可能仍未发生，但该人的作为已损害数据的完整性。“损坏”的定义，亦会涵盖在未获授权下将数据加密而损害数据可用性的情况。

4.74 《美国法典》第 18 篇第 1030(e)(2)条把“受保护电脑”界定为：

“(A) 某财务机构或美国政府专用的电脑，或如属并非如此专用的电脑，则指由某财务机构或美国政府所使用或为其而使用的电脑，而构成有关罪行的行为会影响由该财务机构或美国政府对该电脑的使用或为其而对该电脑的使用；

(B) 用于或影响州际或对外贸易或通讯的电脑，包括位于美国境外而以影响美国州际或对外贸易或通讯的方式使用的电脑；或

(C) 符合以下说明的电脑——

(i) 属投票系统的一部分；及

(ii) (I) 用作联邦选举的管理、支援或行政；或

(II) 曾在州际或对外贸易中运作或在其他方面影响州际或对外贸易”。

未获授权

4.75 《美国法典》第 18 篇第 1030(a)(5)条中三个部分均订有*"未获授权"*的规定，但所联系的元素并不相同，其中(A)部分是导致损坏，而(B)及(C)部分则是取用受保护电脑。因此，就(A)部分而言，*"即使有关传送已获授权，如所导致的损坏未获授权，被告人仍可能须负上法律责任"*。[53]

4.76 《美国法典》第 18 篇第 1030(a)(5)条的三个部分都没有提述被告人在超逾授权范围下行事的情境，而《美国法典》第 18 篇第 1030(a)(1)、(a)(2)及(a)(4)条却明确考虑到该情境。[54]

4.77 由于这个分别，联邦上诉法院第五巡回法庭（Fifth Circuit Court of Appeals）在 *US v Phillips*[55] 中得出以下结论：《美国法典》第 18 篇第 1030(a)(5)条*"只适用于对［相关电脑］完全没有取用授权的使用者"*。该法庭引用述明《美国法典》第 18 篇第 1030(a)(5)条会*"针对'外界人士'"*的国会纪录，并指出：

> "国会藉使入侵行为的性质局部取决于电脑使用者所具备的授权级别，从而区分'获授权取用电脑的内部人员'与'入侵电脑的外界黑客'。"[56]

(A)部分的传送

4.78 (A)部分的"传送"一词已有司法解释。看来：

(a) 该词涵盖*"通过电讯线路或藉着直接输入"*而感染电脑的情况；[57] 及

(b) *"只要导致所需的损坏，即便是打字和盖写数据的作为，该条文也可涵盖"*。[58]

---

53 Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd edition, 2015)，第 117 页，引用 *Lockheed Martin Corp v Speed*, 2006 US Dist LEXIS 53108 (MD Fla 2006)，第 21 页。

54 第 2.83 至 2.88 段探讨在未获授权下行事的人与在超逾授权范围下行事的人有何分别。

55 477 F 3d 215 (5th Cir 2007).

56 同上，第 219 页。

57 Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd edition, 2015)，第 121 页，引用 *Lloyd v US*, 2005 US Dist LEXIS 18158 (D NJ 2005)。

58 同上，第 122 页，引用 *International Airport Centers LLC v Citrin*, 440 F 3d 418 (7th Cir 2006)。

(C)部分的损失

4.79 (C)部分规定，被告人的作为须导致“损坏及损失”。根据《美国法典》第 18 篇第 1030(e)(11)条：

> “‘损失’一词指任何受害人的合理费用，包括对某罪行作出回应的费用、进行损坏评估的费用，以及将有关数据、程式、系统或资料还原至该罪行发生前状态的费用，还包括因服务受阻而损失的收入、招致的费用或引致的其他相应损害赔偿”。

犯罪意念

4.80 《美国法典》第 18 篇第 1030(a)(5)条的三个部分的犯罪意念，可概述并对照如下：

(a) 根据(A)部分，被告人须故意导致传送程式等，并蓄意导致损坏。

(b) (B)部分规定，取用受保护电脑须是蓄意的，并规定被告人须罔顾后果地导致损坏。

(c) (C)部分亦规定，取用受保护电脑须是蓄意的，但并无就导致损坏及损失订明任何意念元素。

小组委员会的看法

禁止在未获授权下蓄意干扰数据

4.81 在讨论开首，我们便意会到更改电脑数据实属常见。每逢有人操作电脑（例如启动或登入电脑）或电脑与互联网有互动，数据便难免会被更改。常见的更改数据例子如下：

(a) 社交媒体平台会在使用者张贴照片或网页连结时，检查该使用者提供的数据。该平台可能会修改或移除部分数据（例如照片的元数据）。

(b) 电邮伺服器会扫描电邮的附件，如发现附件具危险性，便会将之移除。

(c) 网站可能会在访客的电脑内储存“小型文字档案（cookies）”，[59] 藉以更改该电脑的数据或在该电脑上增加数据。

4.82 虽然数据会遭蓄意更改（因为这些更改是社交媒体平台、电邮伺服器或网站管理人有意导致的），但很多电脑使用者大概都会认为上述情境可以接受。

4.83 更改数据可能已获适用的条款及条件授权，但亦有可能未获明确授权。举例而言，据我们了解，互联网服务供应商在营运电邮服务或对其基础设施进行升级时，如使用者数据的内容仍然完整无损，就不一定会把数据在形式上的改变通知使用者。

4.84 与此同时，如 *HKSAR v Chan Chi Kong*[60] 之类的案件显示了干扰电脑数据可带来的伤害。原则上，法律应禁止可能导致或已导致伤害的干扰。按照逻辑，这类干扰会属未获授权，亦可能是蓄意作出的。

4.85 接下来的问题是，法定的干扰数据罪应采用甚么准则，令该罪行只针对涉及（潜在或实际）伤害的案件，而非针对获普遍接受的情况（如上述社交媒体平台、电邮伺服器及网站的例子）。鉴于现行针对刑事损坏的法例，我们认为问题的症结最终在于有关干扰是否有合理辩解支持。

4.86 因此，我们建议应将无合法权限或合理辩解而蓄意干扰（损坏、删除、[61] 弄坏、更改或抑制）电脑数据定为罪行。议定这个大方向后，我们再以现行法律——具体而言为《刑事罪行条例》（第 200 章）与刑事损坏有关的第 59 至 64 条——为蓝本，讨论建议罪行的各个方面。

犯罪行为

4.87 就犯罪行为而言，我们认为，《刑事罪行条例》（第 200 章）第 59(1A)条所详述的“误用电脑”概念[62] 似乎大致上足以涵盖与本章相关的想象情境。

---

59 *“网页伺服器发送给浏览器的数据包，浏览器其后每次接达同一伺服器时会将该数据包发还，用作识别使用者或追踪使用者接达伺服器的情况。”*见：Oxford University Press, “Lexico.com”（2021 年），网址为 https://www.lexico.com/definition/cookie（于 2022 年 5 月 3 日浏览）。

60 第 4.9 段。

61 即使可利用某些数据复原工具将数据复原。

62 第 4.7 段。

4.88 虽然第 59(1A)条并不包括加拿大《1985 年刑事法典》第 430(1.1)(b)条所示的一般条文，[63] 但看来没有情境受该一般条文所涵盖，却未被纳入上述香港条文的涵盖范围。该一般条文大概反映加拿大对损坏电脑本质上属损坏电脑数据的看法。

犯罪意念

4.89 目前，“误用电脑”属刑事损坏的一种形式。这样合乎情理，因为该项误用情形与刑事损坏实体财产类同。为保持一致，这两种刑事损坏的形式应采用相同的犯罪意念（即怀有意图或罔顾后果）。

4.90 香港订立刑事损坏罪的法例，主要是以英格兰及威尔斯《1971 年刑事损坏法令》为蓝本，而该法令则是根据法律委员会（Law Commission）的建议而制定的。[64] 正如法律委员会的报告书所解释，[65] 前身法例《1861 年恶意损坏法令》（Malicious Damage Act 1861）所订的大部分罪行，均规定被告人须“非法及恶意”行事。法律委员会不建议采用该等字眼；[66] 我们认为并无任何理由恢复旧例，规定须怀有恶意干犯建议的罪行。

合法辩解

4.91 法律委员会在同一份报告书中，将（当时建议的）刑事损坏罪背后的理念描述如下：

> “虽然被告人不必提出有合法辩解的争论点，但只有在被告人确实提出该争论点，或证据显示可能有合法辩解时，有关问题方会出现。该罪行的定义所用措辞，旨在订明如有关问题出现，控方有责任证明无合法辩解。”[67]

4.92 在香港，《刑事罪行条例》（第 200 章）第 64(2)条就两项合法辩解订定条文，并同时保留任何获法律承认的其他合法辩解或免责辩护。

---

63 使电脑数据*“变得无意义、无用或无效”*（见第 4.33 段）。

64 法律委员会，*Criminal Law Report on Offences of Damage to Property*（1970 年），法律委员会第 29 号，登载于 https://www.lawcom.gov.uk/project/criminal-law-report-on-offences-or-damage-to-property/（于 2022 年 5 月 3 日浏览）。

65 同上，第 16 页（第 42 段）。

66 同上，第 17 页（第 44 段）及第 18 页（第 48 段）。

67 同上，第 18 页（第 48 段）。

4.93 第一项合法辩解适用于以下情况：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，或会予以同意。后者指的是无须实际上获得同意。被告人只要是诚实地相信有关事情，则即使没有充分理由支持，也可以援引这项合法辩解，[68] 但在现实中，被告人相信的事情亦不应过于牵强。这项合法辩解看来足以涵盖上述社交媒体平台、电邮伺服器及网站的情况。[69] 另一假设情境是，技术人员在未事先取得电脑拥有人的同意下，对电脑套用最新的保安修补程式。

4.94 第二项合法辩解则以需要保护财产、财产权利或财产权益为基础。这似乎适用于以下例子：某人须移除电脑内的病毒，以保护该电脑的数据。

4.95 我们的结论是，维持上述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，实属恰当。

加重罪行

4.96 我们在上文提到，在加拿大，与电脑数据有关的损害可处为期不超过十年的监禁，而任何人导致损害以致生命受到实际危害，则可处终身监禁。[70] 这些最高刑罚与香港适用于刑事损坏罪（包括"误用电脑"）的最高刑罚相同。[71]

4.97 我们认为，加拿大及香港对涉及和不涉及生命受危害的案件加以区分，是有据可依的。一个涉及生命受危害的假设情境是，某人干扰机场控制塔系统、铁路信号系统等所处理的电脑数据。

4.98 我们认为保留《刑事罪行条例》（第 200 章）第 60(2)条所订的加重罪行较为可取。

把有关罪行改列于新法例

4.99 总括而言，我们一致认为现有体制整体上令人满意。鉴于我们建议制定一项针对电脑网络罪行的特定法例，[72] 我们提议有关"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。

---

68 《刑事罪行条例》（第 200 章）第 64(3)条。
69 第 4.81 段。
70 第 4.36 至 4.37 段。
71 第 4.5 段。
72 第 2.90 段。

建议 6

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。

第 5 章　非法干扰电脑系统

引言

5.1　我们会在本章探讨第四类依赖电脑网络的罪行，即非法干扰电脑系统。概括而言，就此主题而订立的罪行，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。

5.2　鉴于非法干扰电脑数据与非法干扰电脑系统息息相关，本章会在第 4 章讨论的基础上再作探讨。以下学术评论，可谓贴切恰当：

> "虽然电脑系统的运作受阻通常是因为数据曾被修改，但即使数据未经修改，若对电脑的取用受阻或电脑的运作受限，上述情况也有可能发生；拒绝服务攻击便是一例。"[1]

5.3　本章所探讨的各种不当行为之中，最佳例子就是拒绝服务攻击，这涉及*"中断获授权使用者取用某电脑网络，通常是出于恶意而导致的"*。[2] 这类攻击还有一种分散进行的加强模式，称为分布式拒绝服务攻击，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"*。[3]

5.4　分布式拒绝服务攻击通常（但并不一定）藉"僵尸网络（botnet）"发动。犯罪者可在网上散布恶意软件（例如透过在网页提供带有病毒的超连结，让不虞有诈的互联网使用者点击），令被入侵的电脑受暗中控制。每台被入侵的电脑称为"僵尸电脑（bot）"（即机械人），因此，"僵尸网络"一词指一组被入侵的电脑，而僵尸电脑越多，则僵尸网络越强大。举例来说，犯罪者可遥距指示僵尸网络内所有电脑同时重复向同一网页发出请求。如寄存该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。有关电脑的拥有人很可能是无辜的，在出现这种情况时还蒙在鼓里。

1　Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd edition, 2015)，第 113 页。

2　Oxford University Press, "Lexico.com"（2021 年），网址为 https://www.lexico.com/definition/denial_of_service（于 2022 年 5 月 3 日浏览）。

3　同上。

5.5 若某电脑系统看来受到分布式拒绝服务攻击，关键的事实争论点，可能在于共同导致该结果的各方是否意图攻击该系统。举例而言，透过电脑系统提供的紧急热线服务可能会被大量来电占线。究竟是很多人碰巧同时致电该热线，还是有人控制成百上千台电脑一起致电该热线，必须加以区分。后者与分布式拒绝服务攻击较为类近。

5.6 除分布式拒绝服务攻击外，还出现了一种干扰电脑系统的新方式，称为慢速攻击（slow attack）。分布式拒绝服务攻击与餐厅有多名顾客同时点餐的情况相类似，而慢速攻击则犹如餐厅某名顾客用多枚小额硬币结账，令餐厅的正常服务受到干扰。分布式拒绝服务攻击会导致目标电脑系统产生大量日志纪录，而慢速攻击则可能只令目标电脑系统长时间忙于处理有关请求。

香港的现行法律

《刑事罪行条例》（第 200 章）

第 60 条

5.7 正如第 4 章所述，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。"

从上文提述*"(a)、(b)或(c)段"*可见，这三段并非相连。第 4 章考虑过当中的(b)及(c)段，而(a)段则与本章最为相关。

涉及分布式拒绝服务攻击的案例

5.8 案例已确立分布式拒绝服务攻击可构成第 59(1A)条所界定的"误用电脑"。在*香港特别行政区 诉 朱婷婷*这宗裁判法院上诉案件，[4] 高等法院原讼法庭法官黄崇厚裁定，原审裁判官的以下裁断*"绝无问题"*：[5] 由于被告人在 49 分钟之内由一个互联网规约地址发出七千多次尝试浏览网站<www.police.gov.hk>的分布式拒绝服务攻击，该网站的伺服器已符合第 59(1A)(a)条中被刑事损坏的涵义。

5.9 被告人获裁定上诉得直，主要理由是案中证据未能证明被告人是引发该次攻击的人。因此，无须考虑犯罪意念的问题。尽管如此，黄崇厚法官在指出*"定罪基础是上诉人罔顾后果"*，[6] 并提述罔顾后果的一般准则后[7]（该等准则由终审法院在*冼锦华 诉 香港特别行政区*［*Sin Kam Wah v HKSAR*］订立），[8] 对于应如何处理犯罪意念的问题，提出以下看法：

> "以本案而言，如果事实裁定是上诉人［即被告人］是在相关情况下按了［被告人进入国际黑客组织网页后版面所示的按钮而］引致警方网站被损坏的人时，即使已确立了她知悉风险，顾及她所做的只是按了一个按钮，那是版面所示的唯一的按钮，不过那是什么按钮在证据上没有细节，上诉人见到的版面有什么也须细察。她的行为是否属不合理，［裁判法院］是必须小心考虑而作出裁定的。"[9]

5.10 分布式拒绝服务攻击能阻碍正常取用电脑或限制电脑的预定运作，但第 59(1A)(a)条所用的措辞则更为广泛。在*香港特别行政区 诉 朱峻玮*（*HKSAR v Chu Tsun Wai*，"***朱峻玮案***"），[10] 被告人参与一次以某银行网站为目标的分布式拒绝服务攻击，但由于该银行的伺服器拥有足够的剩余容量处理有关请求，该伺服器的其他操作并未遭受

---

4 [2017] 4 HKLRD 651, HCMA 33/2016（判决日期：2016 年 10 月 11 日）。

5 同上，第 656 页（第 22 段）（*"这裁定绝无问题"*）。

6 同上，第 664 页（第 79 段）。

7 同上，第 664 页（第 81 及 82 段）。

8 任何人在以下情况，即属罔顾后果地行事：
(1) (a) ……就某情况而言，该人察觉到有该情况存在或将会存在的风险；
(b) ……就某结果而言，该人察觉到有该后果将会产生的风险；而
(2) ……在该人所知的情况下，承担该风险属不合理
（*冼锦华 诉 香港特别行政区* (2005) 8 HKCFAR 192, FACC 14/2004［判决日期：2005 年 5 月 26 日］）。

9 见上文注脚 4，第 665 页（第 91 段）。

10 (2019) 22 HKCFAR 30, [2019] HKCFA 3.

影响，因此该次攻击并不成功。终审法院对第 59(1A)(a)条的解释及应用如下：

> "本席认为，电脑按所设定的运作方式运作，关键并不在于电脑如何运行（或未能运行），而是在于电脑拥有人拟用电脑去**办**什么**事情**。电脑如何运行视乎生产商如何制造电脑而定，但该法规的关键则是在于电脑拥有人设定电脑去办什么事情。有关的网站和伺服器旨在提供银行服务，而非用以处理大量旨在对该银行及其客户带来不便和为攻击者引来公众关注的请求。"[11]（强调之处乃原文所有）

5.11 终审法院又提到，进行分布式拒绝服务攻击在某程度上与向收件人发送大量电邮相类似。[12] 后一情境见于 *Director of Public Prosecutions v Lennon*，[13] 案中英格兰高等法院分庭（Divisional Court）指出，电脑拥有人就收取电邮所给予的一般同意：

> "……显然并不涵盖并非为与该拥有人通讯，而是为干扰该拥有人正常操作及使用其系统而发送的电邮。"[14]

5.12 终审法院的结论是，将*朱峻玮*案所涉的分布式拒绝服务攻击*"形容为误用该银行的电脑相当贴切"*，[15] 并应维持根据第 59(1A)(a)条对被告人所作的定罪。终审法院的判决理据显示，若 *Director of Public Prosecutions v Lennon* 的案情在香港发生，第 59(1A)(a)条很可能同样适用。

5.13 虽然*香港特别行政区 诉 朱婷婷*[16] 没有引用第 59(1A)(c)条，但由于目标电脑系统会因应分布式拒绝服务攻击而产生日志纪录，这类攻击原则上也可能涉及该条。*朱峻玮*案间接显示，第 59(1A)(c)条可能与分布式拒绝服务攻击相关。[17]

---

11 同上，第 36 页（第 13 段）。终审法院的判决由非常任法官贺辅明勋爵（Lord Hoffmann）颁布，而其他所有法官均表示同意。

12 同上，第 37 页（第 14 段）。

13 [2006] EWHC 1201 (Admin).

14 同上，第 9 段。

15 见上文注脚 10，第 37 页（第 15 段）。

16 [2017] 4 HKLRD 651, HCMA 33/2016（判决日期：2016 年 10 月 11 日）。

17 见上文注脚 10，第 37 页（第 18 段）。

《布达佩斯公约》订定罪行的标准

5.14 根据《布达佩斯公约》第一节之下的第一篇第五条：[18]

> “各缔约方均应采取必要的立法及其他措施，在其本土法律中将下列行为定为刑事罪行：在无权的情况下蓄意藉输入、传送、损坏、删除、弄坏、更改或抑制电脑数据，从而严重阻碍电脑系统的运作。”

5.15 《说明报告》对第五条的评注如下：

> “65. 上述行为在［欧洲委员会（Council of Europe）关于电脑相关罪行的］第(89) 9号建议内称为破坏电脑。本条旨在把蓄意藉使用或影响电脑数据，阻碍合法使用电脑系统（包括电讯设施）定为罪行。这里受保护的法定权益，是电脑系统或电讯系统的操作人及使用者能够让系统正常运作的权益。有关文本以中立的方式拟定，确保各种功能均受保护。
>
> 66. ‘阻碍’一词指干扰电脑系统正常运作的行动。该项阻碍须藉输入、传送、损坏、删除、更改或抑制电脑数据而造成。
>
> 67. 该项阻碍还须是‘严重’的，方可处以刑事制裁。各缔约方应自行决定该项阻碍应符合甚么准则，才可视为‘严重’。举例来说，任何缔约方可规定该项阻碍须导致某最低限度的损坏，方可视为严重。草拟人员将以下阻碍视为‘严重’：向某系统发送数据，而发送的形式、规模或频密程度会对拥有人或操作人使用该系统或与其他系统通讯的能力，有重大的不利影响，例如藉着会产生‘拒绝服务’攻击的程式、会妨碍或大大减慢该系统的操作的恶意代码（如病毒），或会向收件人发送大量电子邮件以阻断该系统通讯功能的程式。
>
> 68. 该项阻碍须在‘无权’的情况下造成。网络设计中固有的常见活动或普遍的操作或商业惯例，均是在有权的情况下作出的。这些活动或惯例的例子包括：在拥有人或操作人的授权下测试或保护电脑系统的安全性，

---

[18] 有关《布达佩斯公约》的背景资料，见导言第 11 段，以及第 1 章第 1.6 至 1.10 段。

又或在系统操作人安装会停用先前安装的相类程式的新软件时，重新设定电脑的作业系统。因此，这类行为即使造成严重阻碍，也不会被本条定为罪行。

69. 为商业或其他目的而发送非应邀的电邮，尤其是大量发送或频密地发送这类讯息（‘滥发讯息’），可能会对收件人造成滋扰。草拟人员认为，只有在通讯受蓄意及严重阻碍的情况下，才应把这类行为定为罪行。然而，缔约方可在本土法律中以另一方式处理上述阻碍，例如可将特定的干扰作为定为行政罪行，或订明该等作为须受制裁。有关文本留待缔约方在本土法律中决定，有关系统的运作应受到何种程度——局部或全面、暂时或永久——的阻碍，才能达到足以处以行政制裁或刑事制裁的伤害门槛。

70. 该罪行须是蓄意干犯的，即犯罪者须有造成严重阻碍的意图。”[19]

其他司法管辖区的法定体制

澳大利亚

《刑事法典》（联邦）第 477.3 条

5.16 第 1 章[20] 指出，《刑事法典》（联邦）（Criminal Code (Cth)）中的电脑网络罪行条文，乃源于 2001 年发表的《示范法典委员会报告书》。根据该报告书的建议，《示范刑事法典》（Model Criminal Code）第 4.2.6 条所订罪行*“针对的是拒绝服务攻击”*，[21] 以及*“发送大量电邮，令收件邮箱容量不胜负荷以致系统崩溃等手段”*。[22] 该报告书阐述如下：

> “并不是凡通讯受损都会对数据造成损害……攻击可透过各种不同形式进行：可向系统发送大量不需要的讯息，阻断连接目标电脑的通讯链路，亦可诱使目标电脑产生足够的讯息量来阻止进行通讯，还可更改位址，以及将讯息重新导向。以上述及类似方式损害通讯，统称为

19 《说明报告》第 65 至 70 段。
20 第 1.10(g)段。
21 《示范法典委员会报告书》第 91 页。
22 同上，第 137 页。

'拒绝服务攻击'。虽然有些攻击涉及损害数据，有些则不会。"[23]

5.17 《示范法典委员会报告书》所建议的相关罪行，后来制定为《刑事法典》（联邦）第 477.3 条（*"在未获授权下损害电子通讯"*），第 4 章已介绍该条。[24] 根据第 477.3 条，任何人如导致*"在未获授权下损害往来某电脑的电子通讯"*，而该人知悉该项损害未获授权，即属犯罪。

5.18 正如第 4 章提到，[25]《刑事法典》（联邦）第 476.1 条把*"损害往来某电脑的电子通讯"*界定为包括*"阻止进行上述通讯"*或*"在该电脑所使用的电子联网或网络上损害上述通讯"*，但不包括*"纯粹截取上述通讯"*：

(a) 由于上述定义并非详尽无遗，第 477.3 条不只适用于干扰系统的案件，亦适用于其他情况。《示范法典委员会报告书》支持此观点，据该报告书所述，现已制定为第 477.3 条的建议罪行旨在有：

> "……极之广泛的适用范围，由涵盖短暂及轻微的伤害，以至涵盖造成严重经济损失或导致业务活动、政府活动或社会活动受严重干扰的行为。行为只要损害单一无关重要讯息的通讯，即属违反有关禁止规定……一旦接受应就蓄意损害电子资料施加刑事法律责任，那么损害收取或传送该等资料的能力的行为，便须同样纳入受禁范围。"[26]

(b) 不过，第 476.1 条提述*"阻止"*或*"损害"*[27] 通讯，可能意味着假如攻击电脑系统失败（像*朱峻玮*案那样），便不会构成第 477.3 条所订罪行。

5.19 《示范法典委员会报告书》所建议的罪行及制定为第 477.3 条的罪行，均规定被告人须知悉某项损害未获授权。然而，前者还规定，被告人须意图损害往来有关电脑的电子通讯或罔顾会否造成上述损害，第 477.3 条则没有这项规定。

---

23 同上，第 171 页。
24 第 4.25 至 4.26 段。
25 第 4.18 段。
26 《示范法典委员会报告书》第 171 页。
27 第 3.32 段。

《刑事法典》（联邦）第 477.1 条

5.20 第 477.1 条（*"在未获授权下作出取览、修改或损害，并意图干犯严重罪行"*）已在第 2 章[28] 及第 4 章[29] 论述；该条亦与本章相关。

5.21 根据第 477.1(1)(a)(iii)条，任何人如导致*"在未获授权下损害往来某电脑的电子通讯"*，而该人知悉该项损害未获授权，并意图藉该项损害而干犯（或利便干犯）违反联邦、各州或领地法律的*"严重罪行"*，即属犯罪。

5.22 第 477.1(1)(a)(iii)条可视为在第 477.3 条之上，引入意图干犯或意图利便干犯*"严重罪行"*的规定。因此，诸如分布式拒绝服务攻击等不当行为，除可能构成第 477.3 条所订罪行外，也可能构成第 477.1(1)(a)(iii)条所订罪行。

5.23 *"严重罪行"*是可处终身监禁或为期五年或以上监禁的罪行。[30] 任何人根据第 477.1(1)(a)(iii)条被定罪，可处不超过适用于严重罪行的刑罚。[31]

加拿大

分布式拒绝服务攻击的判例

5.24 加拿大《1985 年刑事法典》（Criminal Code 1985）第 430(1.1)条（*"与电脑数据有关的损害"*）与《示范法》第 6 条（*"干扰数据"*）的相似之处，已在第 4 章指出。[32] 然而，该法典看来并没有与《示范法》第 7 条（*"干扰电脑系统"*）相对应的条文。第 7 条载列如下：

> "(1) 任何人无合法辩解或理由而蓄意或罔顾后果地：
>
> (a) 阻碍或干扰某电脑系统的运作；或
>
> (b) 阻碍或干扰正在合法使用或操作某电脑系统的人；

---

28 第 2.21 段。
29 第 4.21 段。
30 《刑事法典》（联邦）第 477.1(9)条。
31 同上，第 477.1(6)条。
32 第 4.34 段。

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。

在第(1)款中，就电脑系统而言，‘阻碍’包括但不限于：

(a) 截断电脑系统的电力供应；

(b) 导致对电脑系统的电磁干扰；

(c) 以任何方式破坏电脑系统；及

(d) 输入、删除或更改电脑数据。”

5.25 加拿大皇家骑警（Royal Canadian Mounted Police）所处理的下述事件，说明了在加拿大可如何向须为分布式拒绝服务攻击负责的人提出检控：

“2012 年，皇家骑警［即加拿大皇家骑警］对某分布式拒绝服务攻击进行调查，该次攻击源自下议院属下办事处，针对魁北克政府的门户网站‘www.gouv.qc.ca’，导致该网站超过两天无法被进入。在刑事调查期间，皇家骑警使用登录名称、建筑物进出纪录、监察影像及数码证据（被检取的电脑设备）来识别疑犯的身分，该疑犯是获得‘www.gouv.qc.ca’的管理权限而上载恶意软件的政府网络管理员。2013 年，该疑犯就两项在未获授权下使用电脑控罪及一项损害控罪，被裁定罪名成立，判处软禁。”[33]

《1985 年刑事法典》第 342.1(1)条

5.26 虽然关于上述分布式拒绝服务攻击的法院文件似乎未能供公众查阅，但“在未获授权下使用电脑”的控罪颇有可能是根据第 2 章所提述的《1985 年刑事法典》第 342.1(1)条（*“在未获授权下使用电脑”*）提出的：[34]

---

33 加拿大皇家骑警，*Cybercrime: an overview of incidents and issues in Canada*（2014 年），第 8 页，登载于 http://www.rcmp-grc.gc.ca/en/cybercrime-an-overview-incidents-and-issues-canada（于 2022 年 5 月 3 日浏览）。

34 第 2.28 段。

"任何人意图欺诈并在无表面权利的情况下作出以下作为，即属犯可公诉罪行，可处为期不超过10年的监禁，或属犯可循简易程序定罪而惩处的罪行：

(a) 直接或间接取得任何电脑服务；

(b) 藉电磁、声音、机械或其他器材直接或间接截取某电脑系统的任何功能，或导致藉电磁、声音、机械或其他器材直接或间接截取某电脑系统的任何功能；

(c) 直接或间接使用某电脑系统，或导致直接或间接使用某电脑系统，意图干犯(a)或(b)段所订罪行，或就电脑数据或某电脑系统干犯第430条所订罪行；或

(d) 使用、管有、非法传送或准许他人取览某电脑密码，而该密码会使某人能够干犯(a)、(b)或(c)段所订罪行。"

《1985年刑事法典》第430(1)条

5.27 在上述分布式拒绝服务攻击中，《1985年刑事法典》第430(1)条（*"损害"*）可作为提出损害控罪的依据，该条的内容如下：

"任何人如故意

(a) 摧毁或损坏财产；

(b) 使财产变得危险、无用、无法操作或无效；

(c) 妨碍、中断或干扰合法使用、享用或操作财产；或

(d) 妨碍、中断或干扰正在合法使用、享用或操作财产的人，

即属导致损害。"

5.28 第430(1)条适用于与一般财产有关的损害，其措辞与第4章所介绍的第430(1.1)条（*"与电脑数据有关的损害"*）相类似。[35] 由于

[35] 第4.34段。

《1985 年刑事法典》已订有第 430(1)条，这或可解释为何该法典并无针对非法干扰电脑系统的特定条文。

英格兰及威尔斯

在《英格兰误用电脑法令》制定时的第 3 条

5.29 《英格兰误用电脑法令》于 1990 年 8 月 29 日生效时，第 3 条（*"在未获授权下修改电脑资料"*）订立以下罪行：

"(1) 任何人在以下情况，即属犯罪——

(a) 该人作出任何作为，导致在未获授权下修改任何电脑的内容；及

(b) 该人在作出该作为时，具所需的意图及所需的知悉。

(2) 就上文第(1)(b)款而言，所需的意图，指意图导致修改任何电脑的内容，并藉如此行事而——

(a) 损害任何电脑的操作；

(b) 阻止或阻碍取览存于任何电脑内的任何程式或数据；或

(c) 损害上述程式的操作或上述数据的可靠性。

(3) 有关意图不一定要针对——

(a) 任何特定电脑；

(b) 任何特定程式或数据，或任何特定种类的程式或数据；或

(c) 任何特定修改或任何特定种类的修改。

(4) 就上文第(1)(b)款而言，所需的知悉，指知悉该人意图导致的任何修改未获授权。

(5) 就本条而言，未获授权的修改或其属上文第(2)款所述类别的任何预定影响是否属永久性或仅属暂时性，或是否拟属永久性或拟仅属暂时性，均属无关重要。

(6) 就［1971 年第 48 章］《1971 年刑事损坏法令》（Criminal Damage Act 1971）而言，修改电脑的内容不得视为损坏任何电脑或电脑储存媒体，但如该项修改对该电脑或电脑储存媒体的影响，是损害其物理状况，则作别论。

(7) 任何人犯本条所订罪行——

(a) 一经循简易程序定罪，可处为期不超过 6 个月的监禁或不超过法定最高罚款，或两者兼处；及

(b) 一经循公诉程序定罪，可处为期不超过 5 年的监禁或罚款，或两者兼处。"

5.30 某评论员指出，对于上述条文是否适用于分布式拒绝服务攻击及类似不当行为这问题，当时有*"相当激烈的争辩"*。[36] 此外，在 *Director of Public Prosecutions v Lennon*[37]（以案件呈述方式提出的上诉），法院裁定当时的第 3 条可适用于电邮轰炸，至于裁定该条并不适用的初审裁决则*"备受传媒广泛批评"*。[38]

《2006 年警察及司法法令》所带来的改革

5.31 在上述背景下，《2006 年警察及司法法令》（Police and Justice Act 2006）第 36 条藉新条文（标题是*"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"*）取代原有的《英格兰误用电脑法令》第 3 条。制定为《2006 年警察及司法法令》的法案的注释述明：

"301. 这项修订旨在确保订定完备的条文，将各种形式的拒绝服务攻击定为罪行。在此等攻击中，攻击者拒绝受害人取用特定资源，方法通常是阻止某项服务的

---

36 Neil MacEwan, "The Computer Misuse Act 1990: lessons from its past and predictions for its future" [2008] Crim LR 955，第 959 页。

37 引用于*朱峻玮*案第 36 页（第 14 段）。见上文第 5.11 段。

38 见上文注脚 36，第 960 页。

合法使用者取用该项服务（例如藉发送电邮等行动，令某网站的互联网服务供应商不胜负荷）……。”

现行的《英格兰误用电脑法令》第 3 条

5.32　2008 年 10 月 1 日，英格兰及威尔斯实施新的第 3 条。其后，《2007 年严重刑事罪行法令》（Serious Crime Act 2007）及《2015 年严重刑事罪行法令》（Serious Crime Act 2015）再进一步修订该条。第 4 章已载述第 3 条的现行版本，[39] 但我们在此再引述该条，以便与原有版本作比较：

“(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；及

(c) 下文第(2)款或第(3)款适用。

(2) 如上述人士意图藉作出有关作为而——

(a) 损害任何电脑的操作；

(b) 阻止或阻碍取览存于任何电脑内的任何程式或数据；或

(c) 损害上述程式的操作或上述数据的可靠性；或

(d) 致使上述(a)至(c)段提述的任何事宜得以作出，

则本款适用。

(3) 如上述人士罔顾有关作为是否会造成上文第(2)款(a)至(c)段所述的任何事宜，则本款适用。

(4) 上文第(2)款所提述的意图，或上文第(3)款所提述的罔顾后果，不一定要涉及——

(a) 任何特定电脑；

---

[39] 第 4.38 段。

(b) 任何特定程式或数据；或

(c) 任何特定种类的程式或数据。

(5) 在本条中——

(a) 凡提述作出某作为，即包括提述导致作出某作为；

(b) '作为'包括一连串作为；

(c) 凡提述损害、阻止或阻碍某些事宜，即包括提述暂时如此行事。

(6) 任何人犯本条所订罪行——

(a) 一经在英格兰及威尔斯循简易程序定罪，可处为期不超过12个月的监禁或不超过法定最高罚款，或两者兼处；

(b) [……]

(c) 一经循公诉程序定罪，可处为期不超过10年的监禁或罚款，或两者兼处。"

5.33 由于目标电脑的操作不必受到实际损害，故现行的第3条可能适用于如*朱峻玮*案中失败的分布式拒绝服务攻击。根据第3(2)及(3)条，如攻击者意图导致有关损害或罔顾会否造成有关损害，便已足够。

《英格兰误用电脑法令》第3ZA条

5.34 如非法干扰电脑系统导致《英格兰误用电脑法令》第3ZA条所指的*"关键性严重损害"*，或产生导致该条所指的*"关键性严重损害"*的重大风险，该项干扰便可能构成第3ZA条所订罪行。由于第4章已探讨该条，[40] 似乎没必要在此再论述该条。

[40] 第4.41至4.46段。

中国内地

《中国刑法》第二百八十五及二百八十六条

5.35 《中国刑法》第二百八十五条第二款订明："*违反国家规定，……对［不属国家事务、国防建设、尖端科学技术领域的］计算机信息系统实施非法控制*"，须给予处罚。

（底线后加）

5.36 第二百八十六条第一款，是另一项关于干扰电脑系统的条文，针对令该系统无法正常运行的行为：

> "违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役；后果特别严重的，处五年以上有期徒刑。"

（底线后加）

犯罪行为

5.37 第二百八十五条第二款与第二百八十六条第一款的分别，在于对计算机信息系统进行的行为，即"*实施非法控制*"与"*对……功能进行删除、修改、增加、干扰，造成……系统不能正常运行*"。实际上，这两条看来可作为检控案件的交替理由。

5.38 在中国最高人民法院发布的第 26 批指导性案例的第 145 号案例，[41] 犯罪者通过向网站服务器植入木马程序，对计算机信息系统内的数据进行增加、修改，以提高赌博网站广告被搜寻引擎命中机率。法院裁定，这种行为只导致犯罪者对该系统实施非法控制，但未造成该系统功能的破坏，或不能正常运行，因此裁定这种行为并未符合第二百八十六条第一款的规定。然而，犯罪者就第二百八十五条第二款所订罪行，被裁定罪名成立。[42]

5.39 另外，最高人民检察院第九批指导性案例的第 35 号案例[43] 作出以下指示：通过修改计算机信息系统（即案中的智能手机）的登

---

41 《最高人民法院关于案例指导工作的规定》第七条规定，中国最高人民法院发布的指导性案例，各级人民法院审判类似案例时应当参照。

42 张竣杰等非法控制计算机信息系统案。

43 曾兴亮、王玉生破坏计算机信息系统案。

录密码而锁定有关设备，导致合法使用者不能取用或正常使用的行为，亦构成第二百八十六条第一款所订罪行。

新西兰

《新西兰法令》第 250(2)(c)条

5.40 我们在第 4 章介绍《新西兰法令》第 250(2)条（*"损坏或干扰电脑系统"*）时，提到本章会探讨第 250(2)(c)条。[44] 根据第 250(2)(c)条：

> "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……
>
> (c) 导致任何电脑系统——
>
> (i) 发生故障；或
>
> (ii) 拒绝向任何获授权使用者提供服务，
>
> 可处为期不超过 7 年的监禁。"

5.41 第 250(2)条以*"蓄意或罔顾后果地"*行事，形容进行犯罪行为的犯罪意念，而有关未获授权的犯罪意念，则是知悉或罔顾后果。关于犯罪意念的问题，我们在第 4 章[45] 提出的各点均适用于第 250(2)条各段，包括(c)段，故不必在此重复。

5.42 就第 250(2)(c)条适用的情境而言，某评论员有以下评析：

> "7.96 第 250(2)(c)条的适用范围广泛。举例而言，如软件被拙劣地或罔顾后果地编入缺损程式，根据该条，软件生产商可能须负上法律责任。此外，任何人罔顾后果地透过电邮发送病毒，亦须负上法律责任，但有意见认为使用者应该安装最新的防毒软件，亦应对他们转发的电邮格外谨慎。
>
> ……
>
> 7.98 该款亦可能适用于滥发电邮者。滥发电邮者如对于发送大量电邮对邮件伺服器可能造成的影响掉以轻

---

44 第 4.50 至 4.51 段。

45 第 4.57 段。

心，罔顾后果这项元素便颇有可能适用。非应邀的邮件必须大量涌入，才能拖垮互联网服务供应商的邮件伺服器，导致服务发生故障或拒绝提供服务。因此，第250(2)(c)条不会普遍适用于所有滥发电邮者。"[46]

《新西兰法令》第250(1)条

5.43 第4章亦有提及第250(1)条，[47] 这是另一项针对非法干扰电脑系统的条文：

"任何人蓄意或罔顾后果地摧毁、损坏或更改任何电脑系统，并知悉或理应知悉相当可能会导致生命受危害，可处为期不超过10年的监禁。"

5.44 上文引述的评论员将第250(1)及(2)条比较如下：

"……第250(1)条可适用于已获授权取用电脑系统的人，但第250(2)条规定，取用电脑系统的人须未获授权，并：

(1) 知悉自己未获授权；或

(2) 罔顾自己是否已获如此授权。

换言之，任何获授权对系统作出某些行为（如移动或删除档案）的人（例如系统管理员），均可干犯第250(1)条所订罪行。第250(2)条则规定，有关行为元素须缺乏权限，或须涉及罔顾是否已获授权这项元素。"[48]

5.45 该评论员重点评论有关授权的问题，凸显了在涉及第250(2)条及其他司法管辖区相类法规的情况下，获得授权的重要性。举例而言，流动数据服务供应商可能会因公平使用政策而获得合约权利，可在数据使用量超过指明限额时，限制客户的数据传输速度，或暂停某些数据服务。虽然这些安排会限制客户透过其器材正常使用数据服务，但客户接纳公平使用政策，实际上对施加这些限制给予授权。若然服务供应商在公平使用政策所预期的情况下启动这些安排，便不必担心会招致潜在的刑事法律责任。

---

46 David Harvey, *internet.law.nz selected issues* (LexisNexis NZ Limited, 4th edition, 2015)，第7.96及7.98段。

47 第4.58段。

48 见上文注脚46，第7.90段。

新加坡

《新加坡误用电脑法令》第 7 条

5.46 《新加坡误用电脑法令》第 7 条（*"在未获授权下妨碍使用电脑"*）订明相关罪行如下：

> "(1) 任何人在没有权限或合法辩解的情况下——
>
> (a) 故意干扰、中断或妨碍合法使用某电脑；或
>
> (b) 故意阻挠或阻止取览储存于某电脑的任何程式或数据，或损害该程式或数据的效用或效能，
>
> 即属犯罪，一经定罪——
>
> (c) 可处不超过$10,000 的罚款或为期不超过 3 年的监禁，或两者兼处；及
>
> (d) 如属第二次或其后每次定罪，则可处不超过$20,000 的罚款或为期不超过 5 年的监禁，或两者兼处。
>
> (2) 如因本条所订罪行而导致任何损坏，被裁定犯该罪行的人可处不超过$50,000 的罚款或为期不超过 7 年的监禁，或两者兼处。"

5.47 虽然《新加坡误用电脑法令》的罪行条文主要是建基于加拿大和英格兰及威尔斯的相应条文，但该法令并没有加入任何注释，指其他司法管辖区的任何法例条文是第 7 条的蓝本（该法令对其他条文则有这样做）。

没有权限或合法辩解的情况

5.48 若按第 7 条的字面理解，如在具有权限或合法辩解的情况下作出(a)及(b)段所载的行为，则不属犯罪。*"没有权限"*一词，亦见于第 3 条（*"在未获授权下取览电脑资料"*）及第 6 条（*"在未获授权下使用或截取电脑服务"*）。就取览电脑程式或数据的情况而言，第 2(5)条对该词解释如下：

"就本法令而言，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，即属未获授权取览或在没有权限的情况下取览——

(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。"

若以类似方式理解第 7 条的*"没有权限"*，似乎属合理之举。

5.49 在《新加坡误用电脑法令》中，*"合法辩解"*一词仅在第 7 条出现一次，亦没有定义。这与香港《刑事罪行条例》（第 200 章）第 64(2)条形成对比，该条就刑事损坏（包括*"误用电脑"*）的控罪，订定两项合法辩解。[49]

第 7 条的适用范围

5.50 《新加坡误用电脑法令》第 7 条措辞宽广。在概念上，该条的应用并不限于分布式拒绝服务攻击及类似的不当行为。某评论员对一宗相关案件有以下描述：

"一名曾受雇于 SMC Marine Services 的系统工程师，被控离职前秘密地在他开发的程式内设定密码，涉嫌令前雇主无法对有关系统进行检查、修改或升级。这可构成《[误用电脑]法令》第 5 条（在未获授权下修改）或第 7 条（在未获授权下妨碍）所订罪行。案中公司亦在高等法院展开民事诉讼，寻求禁制令防止其机密资料外泄。"[50]

5.51 案中前雇主成功申请临时禁制令，防止其指称的版权外泄及遭侵犯，[51] 而有关民事诉讼据报亦告完结。案中系统工程师被控非法修改电脑系统，但最终因法院裁定控方*"未有在排除合理疑点的情况下履行举证责任"*而获判无罪。[52]

---

49 第 4.92 至 4.94 段。

50 Gregor Urbas, "An Overview of Cybercrime Legislation and Cases in Singapore" (ASLI Working Paper No 001, Dec 2008)，第 14 页。

51 *SMC Marine Services (Pte) Ltd v Thangavelu Boopathiraja and Others* [2008] SGHC 29.

52 The Straits Times, "Man cleared of sabotage"（2009 年 6 月 3 日），登载于 https://www.asiaone.com/News/AsiaOne%2BNews/Crime/Story/A1Story20090603-145841.html（于 2022 年 5 月 3 日浏览）。

不同情况的最高刑罚

5.52 《新加坡误用电脑法令》就所订罪行订明一致的最高刑罚。以下概述的最高刑罚量刑基准，同样适用于根据第 5 条（*"在未获授权下修改电脑资料"*）[53] 或第 7 条被定罪的人：

(a) 初犯者可处不超过 10,000 新加坡元的罚款或最多三年监禁，或两者兼处。

(b) 对再犯者订定的最高刑罚较重（不超过 20,000 新加坡元的罚款或最多五年监禁，或两者兼处）。

(c) 导致实际损坏的犯罪者的最高刑罚，包括不超过 50,000 新加坡元的罚款或最多七年监禁，或两者兼处。

(d) 如犯罪者取用任何*"受保护电脑"*，[54] 则《新加坡误用电脑法令》第 11(1)条订明更重的最高刑罚（不超过 100,000 新加坡元的罚款或最多 20 年监禁，或两者兼处）。

美国

《电脑欺诈及滥用法案》内的《美国法典》第 18 篇第 1030(a)(5)条

5.53 虽然有人认为，发动分布式拒绝服务攻击如同静坐示威[55]（即示威者占据某地方后拒绝离开，直至他们的要求得到满足的抗议形式），[56] 应属合法，[57] 但看来美国已清楚确立这样做可能会违反下文所载的《美国法典》第 18 篇第 1030(a)(5)条。正如第 4 章所述，[58] 任何人如作出以下作为，可按第 1030(c)条的规定予以惩处：

---

53 第 4.64 段。

54 有关法定定义载于第 4.68 段。

55 例子见 Chris Peterson, "In Praise of [Some] DDoSs?"（2009 年 7 月 21 日），登载于 http://www.cpeterson.org/2009/07/21/in-praise-of-some-ddoss/（于 2022 年 5 月 3 日浏览）：*"在某程度上，分布式拒绝服务攻击如同静坐。两者的核心概念均包括过度利用稀缺资源（前者利用伺服器周期，后者则利用柜台空间）来将他人排除在外，以达到政治效果。两者均属非暴力，但有损经济。两者均可具有政治性质，有关罪行因而可置于上述背景下考虑。"*

56 Oxford University Press, "Lexico.com"（2021 年），网址为 https://www.lexico.com/definition/sit-in（于 2022 年 5 月 3 日浏览）。

57 例子见 Mike Masnick, "Anonymous Launches White House Petition Saying DDoS Should Be Recognized As A Valid Form Of Protest"（2013 年 1 月 11 日），登载于 https://www.techdirt.com/articles/20130111/08053821642/anonymous-launches-white-house-petition-saying-ddos-should-be-recognized-as-valid-form-protest.shtml（于 2022 年 5 月 3 日浏览）。

58 第 4.70 至 4.71 段。

"(A) 故意导致向某受保护电脑传送程式、资料、代码或指令，并因着该行为而在未获授权下蓄意导致该电脑损坏；

(B) 在未获授权下蓄意取用某受保护电脑，并因着该行为而罔顾后果地导致损坏；或

(C) 在未获授权下蓄意取用某受保护电脑，并因着该行为而导致损坏及损失。"

美国的分布式拒绝服务攻击

5.54 举例而言，某网上期刊载有以下记项，该记项的日期为2001年1月19日：

"美国阿拉斯加地区法院的前电脑系统管理员史葛.丹尼斯（Scott Dennis）因为对美国纽约东区地区法院的伺服器发动三次拒绝服务攻击，被阿拉斯加地区法院判处监禁六个月以及履行240小时的社会服务……丹尼斯承认一项违反《美国法典》第18篇第1030(a)(5)(C)条的非重刑罪。谷柏（Cooper）补充说：'美国地区法院系统并非首次受到攻击'；华盛顿州西区地区法院也曾受攻击。丹尼斯已不再于美国地区法院任职。亦见联邦调查局的新闻公报。"[59]

5.55 涉及分布式拒绝服务攻击的案件持续在美国发生。某宗瞩目案件的犯罪者承认：

"……一项故意导致向某受保护电脑传送程式、资料、代码及指令，并因着该行为而蓄意导致该电脑损坏的控罪。"[60]

这显然是根据《美国法典》第18篇第1030(a)(5)(A)条提出的控罪。犯罪者被判处监禁六年。[61]

---

59 Tech Law Journal, "News Briefs from January 11-20, 2001", 登载于 http://www.techlawjournal.com/home/newsbriefs/2001/01b.asp（于2022年5月3日浏览）。

60 克利夫兰联邦调查局（Federal Bureau of Investigation Cleveland）, "Akron Man Arrested and Charged for DDoS Attacks"（2018年5月10日）, 登载于 https://www.fbi.gov/contact-us/field-offices/cleveland/news/press-releases/akron-man-arrested-and-charged-for-ddos-attacks（于2022年5月3日浏览）。

61 美国司法部, "Akron man sentenced to six years in prison for launching denial of service attacks that shut down web sites for the city of Akron and the Akron Police Department"（2019年10月3日）,

令语音信箱系统及电邮系统不胜负荷

5.56 上述案件的法院文件似乎没有网上版。要了解《美国法典》第 18 篇第 1030(a)(5)条如何把非法干扰电脑系统定为不合法，参考 *Pulte Homes, Inc v Laborers' International Union of North America*[62] 会有所启发，纵使该案属源自劳资纠纷的民事案件。[63]

5.57 普尔特公司（Pulte）是这宗案件的雇主，它指称工会 LIUNA *"以数以千计的电话来电及电邮，轰炸普尔特公司的销售办事处及其中三名营业主任"*，[64] 引致以下后果：

> "这些来电堵塞了普尔特公司的语音信箱系统，令客户无法联络该公司的销售办事处及营业代表，而该公司的一名雇员甚至被迫关掉工作手机。电邮所造成的破坏更加严重：这些电邮令该公司的系统（该系统对收件匣的电邮数目设有限制）不胜负荷，以致该公司的雇员无法查阅与业务有关的电邮，或向客户及供应商发送电邮，正常业务运作因而陷入停顿。"[65]

5.58 联邦上诉法院第六巡回法庭处理《美国法典》第 18 篇第 1030(a)(5)条的全部三个部分，并就普尔特公司根据《美国法典》第 18 篇第 1030(a)(5)(A)条提出的 *"传送申索"*，作出以下裁定：

> (a) 在应用"损坏"的法定定义（即 *"对数据、程式、系统或资料的完整性或可用性造成任何损害"*）时：[66]
>
> > "……凡进行的传送会削弱健全的电脑系统（或同样地，进行的传送会降低原告人使用数据或系统的能力），即属导致损坏。LIUNA 的一连串来电及电邮，正被指称有如此效果。"[67]

登载于 https://www.justice.gov/usao-ndoh/pr/akron-man-sentenced-six-years-prison-launching-denial-service-attacks-shut-down-web（于 2022 年 5 月 3 日浏览）。

62 648 F 3d 295 (6th Cir 2011). 联邦上诉法院第六巡回法庭（Court of Appeals for the Sixth Circuit）的意见书（即判词），日期为 2011 年 8 月 2 日，登载于其网站，网址为 http://www.ca6.uscourts.gov/opinions.pdf/11a0200p-06.pdf（于 2022 年 5 月 3 日浏览）。

63 《美国法典》第 18 篇第 1030 条同时订立若干电脑网络罪行，并订明民事诉讼因由。

64 见上文注脚 62，第 2 页。

65 见上文注脚 62，第 3 页。

66 《美国法典》第 18 篇第 1030(e)(8)条。

67 见上文注脚 62，第 7 页。

(b) 进行初审的地区法院，要求普尔特公司*"指称 LIUNA **知悉** 其来电及电邮会对普尔特公司的电脑系统造成伤害"*[68]，或*"LIUNA 完全清楚其电邮活动的**实际**后果"*[69]（强调之处乃原文所有），实属错误。普尔特公司只要：

> "……指称 LIUNA 是有意识地为了对普尔特公司的电脑系统导致法定意义上的损坏而行事——此标准并不要求完全知悉有关事实"，[70] 便已足够。

因此，上诉法院恢复普尔特公司在初审时被驳回的*"传送申索"*。

5.59 然而，上诉法院确认地区法院以下裁定：普尔特公司未能根据《美国法典》第 18 篇第 1030(a)(5)(B)及(C)条就*"取用申索"*作出陈述。上诉法院裁定：

> "为了就取用申索作出陈述，原告人必须作出多项指称，其中包括被告人'在未获授权下蓄意取用某受保护电脑。'（《美国法典》第 18 篇第 1030(a)(5)(B)、(C)条）。……我们无须决定 LIUNA 的来电及电邮有没有取用普尔特公司的电脑，因为即使有，普尔特公司也没有指称该项取用是'在未获授权下'作出的。"[71]

> "LIUNA 使用非受保护公共通讯系统，这推翻了普尔特公司指称 LIUNA'在未获授权下'取用其电脑的说法。普尔特公司容许所有公众人士联络其办事处及营业主任：该公司并没有指称例如 LIUNA 或任何其他人需要密码或代码，才能致电或发送电邮给该公司。反之，普尔特公司的电话系统及电邮系统，一如非受保护网站，'是向公众开放的，故［LIUNA］获授权使用［这些系统］。'见［*Int'l Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418, ］第 420 页。另外，普尔特公司虽有就通讯的数目、频密程度及内容作出投诉，但对于一个或数个来电，或一封或数封电邮，却连一项未获授权指称也没有。因此，普尔特公司的投诉，充其量只算是指称 LIUNA 超逾获授权的取用范围。"[72]

---

68 见上文注脚 62，第 8 页。
69 见上文注脚 62，第 9 页。
70 见上文注脚 62，第 9 页。
71 见上文注脚 62，第 10 页。
72 见上文注脚 62，第 11 至 12 页。

5.60 正如上诉法院在 *Pulte* 案所指，[73] 最高法院在 *Leocal v Ashcroft*[74] 裁定，任何法规不论应用于刑事或非刑事案件，解释须一致。因此，可以预计法院在非法干扰电脑系统（例如藉着对网站发动分布式拒绝服务攻击）的检控中，亦会以同样方式解释《美国法典》第 18 篇第 1030(a)(5)条。

小组委员会的看法

一致处理干扰数据及干扰系统

5.61 正如第 4 章及上文所论述，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主要方式，是将两者视为*"误用电脑"*，即刑事损坏的一种形式。由于这两类不当行为部分互相重迭，故上述法律立场实属合理。

5.62 从案例可见，现有法例的整体施行情况理想。举例来说，*朱峻玮*案展示了但凡干扰电脑系统，不论成功与否，均可能招致刑事法律责任。这与我们的方针一致：纯粹在无权的情况下取用整台电脑或其任何部分，应定为罪行，如意图进行其他犯罪活动而取用电脑，则应构成加重罪行。

5.63 我们认为，针对干扰数据及干扰系统的现行体制有贯彻一致的优点，应予保存。因此，我们建议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。

新法例应采用现有条文

5.64 我们在建议 6(c)提出，应把《刑事罪行条例》（第 200 章）第 59(1A)及 60 条关于"误用电脑"的部分改列于新法例。

5.65 我们在拟订该项建议时，曾考虑如"误用电脑"的概念不再属刑事损坏罪的涵盖范围，而是一项并非载于《刑事罪行条例》（第 200 章）的新订独立罪行，是否仍可引用以有关"误用电脑"的现行法律为依据的案例（例如*朱峻玮*案）。

---

73 见上文注脚 62，第 8 页。

74 543 US 1 (9 Nov 2004).

5.66 我们认为，只要在草拟新法例时小心谨慎，并适当参考现行的法例措辞（尤其是借机会将相关案例的基本法律原则编纂为法例条文），我们便可相信新法例的目的会如实反映，在建议的修改落实后，"误用电脑"背后的政策及立法原意亦因此能保持清晰明确。

可厘清"误用电脑"一词

5.67 假设建议 6(c)得以落实，便可藉着将相关条文从《刑事罪行条例》（第 200 章）迁往新法例的机会，完善*"误用电脑"*的法定概念。举例而言，以下做法似乎会有好处：

(a) 厘清如攻击的破坏力巨大，导致目标电脑完全不能运作，这会否涉及第 59(1A)(a)条——*"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"*——在新法例中的对等条文；及

(b) 将诸如*"损害任何电脑的操作"*[75] 的概念纳入*"误用电脑"*的定义。

建议罪行的适用范围

5.68 最重要的是，新法例应保留现有法律的广度，不宜过于局限。举例来说，除了现有法律已涵盖的情境外，我们认为建议的罪行应适用于上述比较研究所提到的以下各方：

(a) 攻击电脑系统失败的人；[76]

(b) （如软件被蓄意或罔顾后果地编入缺损程式）软件的生产商；[77] 及

(c) 故意并在未获授权下对电脑系统作出任何更改的人，而该项更改可能导致合法使用者不能取用或正常使用系统。[78]

---

75 根据《英格兰误用电脑法令》第 3 条，任何人如*"就某电脑作出任何未获授权的作为"*，而该人知悉该作为未获授权，并意图*"损害任何电脑的操作"*等，或罔顾是否会引致上述后果，即属犯罪。见第 5.32 段。

76 见第 5.33 段，内容关乎《英格兰误用电脑法令》第 3 条。

77 见第 5.42 段，内容关乎《新西兰法令》第 250(2)(c)条。

78 见第 5.50 段，内容关乎《新加坡误用电脑法令》第 7 条。

建议 7

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。

合法辩解

5.69 读者可能会记得，第 2 章曾提及在环球层面，总会有人（包括但不限于网络安全从业员）在电脑网络空间测试他人的电脑，而目标电脑的拥有人往往并不知情，更不用说授权测试。[79]

5.70 用作进行这些测试的工具唾手可得，在互联网搜寻一下便可轻易找到，不只在暗网才有。现时已有各种各样的测试工具可导致不同程度的入侵。有些工具只会扫描电脑系统一次，不会对系统造成损坏，但另一些工具则可持续进行扫描（比方说持续扫描几小时）。另

[79] 第 2.112(a)段。

外还有一些工具可对电脑系统造成重大损坏。关键问题在于如何使用有关工具。

5.71 基于上述背景，我们详细讨论了因任何理由而扫描（或以类似的形式测试）他人的电脑，在新法例下应否足以视为建议的非法干扰电脑系统罪的合法辩解。就使用测试工具的网络安全从业员而言，对于法律应如何平衡他们的利益与社会大众的利益这问题，我们初步认为，实行较严格的规管体制可能对网络安全从业员造成损失，而在未获授权下使用测试工具可能对目标电脑系统的管理人及拥有人造成损坏或损失，两者比较之下，前者的损失看来没有那么广泛。

5.72 公众对建议 8 所载的咨询问题发表意见，会有助我们确定立场。具体而言，(a)段主要针对网络安全专业人员，而(b)段则涉及非保安专业人员（例如搜寻器营运人、电脑终端使用者等）。

建议 8

小组委员会邀请公众就以下问题提交意见书：

(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；[80] 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）：

[80] RFC6335 的资料登载于互联网工程专责组（Internet Engineering Task Force）的网站，网址为 https://datatracker.ietf.org/doc/rfc6335/（于 2022 年 5 月 3 日浏览）。

(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？

第 6 章　提供或管有用作犯罪的器材或数据

引言

6.1　我们会在本章探讨导言所提及的第五类（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。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。

6.2　如任何人实际使用器材或数据，举例来说对电脑进行黑客入侵，即会构成非法取览罪的犯罪行为。本章的重点，是应否将纯粹提供或管有有关器材或数据（例如管有存有勒索软件的记忆棒）定为独立的罪行，以及如应该的话，应如何拟定该罪行。

6.3　这类器材及数据的例子，包括：

(a) 用于测试网络的软件，例如某些软件可通过进行渗透测试，评估电脑系统对分布式拒绝服务攻击的承受能力；

(b) 破解密码工具，该工具可能是软件，亦可能是实物器材；及

(c) 消磁器，它可通过消除磁性储存媒体（例如硬碟）的磁性，销毁该媒体中的数据。

6.4　任何人可能不需要任何特别硬件，仅是使用软件也能干犯电脑网络罪行。

香港的现行法律

《刑事罪行条例》（第 200 章）

第 62 条

6.5　对于第 2 至 5 章所论述的依赖电脑网络的罪行，香港处理该等罪行的法例条文主要载于《刑事罪行条例》（第 200 章）及《电讯

条例》（第 106 章）。按照逻辑，如任何条文与本章相关，并拟适用于前数章所介绍的依赖电脑网络的罪行，该等条文固然应载于该两条条例内。

6.6 我们宜先审视《刑事罪行条例》（第 200 章）。第 59(1A)条订明在该条例的第 VIII 部中，*"摧毁或损坏财产（to destroy or damage any property），就电脑而言，包括误用电脑"*。因此，第 VIII 部第 62 条（*"管有任何物品意图摧毁或损坏财产"*）所订可处监禁十年的以下罪行，[1] 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。"

实际上可能产生的问题

6.7 第 62 条适用于意图摧毁或损坏财产的人，如有人意图导致或意图准许他人摧毁或损坏财产，该条亦适用。对于兼具合法及非法目的之物品，以及只可作非法用途的物品，该条并没有加以区分。

6.8 至于保管或控制有关物品的人，是否须负上法律责任，主要视乎该人的意图。由于人的意念属主观性质，在执法过程中可能出现举证问题。

对受禁物的解释

6.9 第 62 条的英文文本用*"anything"*一词来描述受禁物，而中文文本的对应词则是*"任何物品"*。

6.10 按照一般的说法，*"anything"*一词并不限于有形物，如从以下角度考虑，该词的涵盖范围似乎比*"任何物品"*更广：虽然实物显然属于*"任何物品"*的范围，但该词的惯常涵义会否明确引伸至某些可利便干犯第 62 条所订罪行的无形物，则是截然不同的问题。就干犯*"误用电脑"*罪的情况而言，下述例子可带出该问题：

---

[1] 《刑事罪行条例》（第 200 章）第 63(2)条。

(a) 电脑软件或数据（例如恶意软件及登入凭证）；

(b) 提供黑客入侵服务或类似服务；及

(c) 有关利用漏洞（exploit）的专门知识。

6.11 如*"anything"*与*"任何物品"*的涵盖范围可能不同，《释义及通则条例》（第1章）第10B条（*"两种法定语文本条例的释疑"*）即可发挥作用：

"(1) 条例的中文本和英文本同等真确，解释条例须以此为依据。

(2) 条例的两种真确本所载条文，均推定为具有同等意义。

(3) 凡条例的两种真确本在比较之下，出现意义分歧，而引用通常适用的法例释义规则亦不能解决，则须在考虑条例的目的和作用后，采用最能兼顾及协调两文本的意义。"

6.12 在*T诉警务处处长*（*T v Commissioner of Police*），[2] 终审法院须审理的主要争论点是：在《公众娱乐场所条例》（第172章）下*"公众娱乐"*的定义[3]中，*"admitted"*一词应如何解释。虽然这宗上诉主要是依据该法例的英文文本来争辩，[4] 但终审法院就该争论点作出裁定时，亦考虑了*"admitted"*的中文对应词*"让……入场"*。[5] 举例而言，终审法院常任法官李义接纳以下看法：

"……'公众娱乐'定义的中文文本，尤其是'入场'一词的使用，带有'特定地点'的涵义，而……英文文本并不带有这个涵义……由于两个真确文本之间存在差异，所以便须……解决……"[6]

---

2 (2014) 17 HKCFAR 593.

3 即*"……让公众入场的任何娱乐，而不论是否收取入场费"*（第2条）。

4 见上文注脚2，第679页（第284段）（终审法院非常任法官廖柏嘉勋爵［Lord Neuberger of Abbotsbury］）。

5 见上文注脚2，第607页（第11(5)段）（终审法院首席法官马道立）、第625页（第82段）（终审法院常任法官李义）、第648页（第166段）（终审法院常任法官邓国桢）、第666页（第232段）及第671页（第253段）（终审法院常任法官霍兆刚），以及第679页（第284段）（终审法院非常任法官廖柏嘉勋爵）。

6 见上文注脚2，第625页（第82段）（终审法院常任法官李义）。

6.13 终审法院亦确认了下述重要原则：

> "……法庭不能够对一项法例条文作出该条文所使用的经按照其文意和法定目的理解的语言所不能承载的解释"。[7]

6.14 终审法院大比数裁定，*"admitted"*一词应解释为*"在主动意义上表示出给予某人准许进入或出入或让人入内"*。[8] 该法例的中文文本似乎比英文文本更为具体，如中文文本未有影响法院有关裁决，它至少为该裁决提供支持。

6.15 在解释《刑事罪行条例》（第 200 章）第 62 条时，一种可能的说法是，该条的文意及目的均要求*"anything"*及*"任何物品"*涵盖有形物及无形物，但有人可能会认为这样解释该条，似乎会令*"任何物品"*的惯常涵义过度延伸。另一个可能性，是把*"anything"*及*"任何物品"*一并理解为只传达两者兼具的概念。根据该论点，若采取这种做法，无形物便可能被排除在第 62 条的范围外，这无助于将第 62 条应用于电脑网络空间。

第 62 条与刑事损坏罪相关

6.16 此外，《刑事罪行条例》（第 200 章）第 62 条禁止保管或控制任何意图用作摧毁或损坏财产的物品，亦即用作干犯该条例第 60 条所订罪行的物品。对于其他条文所订罪行（例如该条例第 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。

《电讯条例》（第 106 章）

6.17 《电讯条例》（第 106 章）虽然并无与《刑事罪行条例》（第 200 章）第 62 条相对应的条文，但该条例设立了无线电通讯器具的发牌制度。[9] 就本咨询文件而言，似乎没有必要详细描述该制度。我们只需指出，在该制度适用的情况下，违反有关规定，即属犯罪。[10]

---

7 见上文注脚 2，第 655 页（第 195 段）（终审法院常任法官霍兆刚），类似看法见第 607 页（第 12 段）（终审法院首席法官马道立）。

8 见上文注脚 2，第 670 页（第 250 段）（终审法院常任法官霍兆刚）。

9 《电讯条例》（第 106 章）第 8(1)及 9 条；《电讯（电讯器具）（豁免领牌）令》（第 106Z 章）第 5 及 7 条。

10 见下文第 6.20 段，1-a-i。

6.18 该制度可能适用于可用作干犯《电讯条例》（第106章）第27A、27(b)及25(a)条所订罪行的电脑或智能电话，而我们在第2、3及4章分别论述建议的非法取览罪、非法截取数据罪及非法干扰数据罪时，已提及该等条文。[11]

6.19 我们认为，现有的发牌制度并不足以打击电脑网络罪行。举例来说，该制度的其中一个限制是涵盖范围狭窄，只适用于无线电波等电讯技术。现行法律的不足，正是应订立特定的新罪行的部分原因。

《布达佩斯公约》订定罪行的标准

6.20 根据《布达佩斯公约》第一节之下的第一篇第六条：[12]

> "1 各缔约方均应采取必要的立法及其他措施，在其本土法律中将下列在无权的情况下蓄意作出的行为定为刑事罪行：
>
> a 生产、出售、为使用而获取、输入、分发或以其他方式提供：
>
> i 经设计或改装以主要用作干犯第二至五条所订任何罪行的器材[13]（包括电脑程式）；
>
> ii 可藉以取用整个电脑系统或其任何部分的电脑密码、取用码或类似数据，
>
> 并意图使该器材、电脑密码、取用码或数据用作干犯第二至五条所订任何罪行；及
>
> b 管有上文a i或ii段所提述的物品，并意图使该物品用作干犯第二至五条所订任何罪行。任何缔约方可依法规定须管有一定数量的这类物品，方会招致刑事法律责任。
>
> 2 如本条第1段所提述的生产、出售、为使用而获取、输入、分发或以其他方式提供或管有，并非以干犯

---

11 第2.11、3.12及4.13段。

12 有关《布达佩斯公约》的背景资料，见导言第11段，以及第1章第1.6至1.10段。

13 本章所论述罪行涵盖的器材，亦可能构成无线电通讯器具，故须受《电讯条例》（第106章）的发牌制度所规限。

本《公约》第二至五条所订罪行为目的（例如是为了在获授权下测试或保护电脑系统），则本条不得解释为施加刑事法律责任。

3 各缔约方可保留不应用本条第1段的权利，但该项保留不得涉及出售、分发或以其他方式提供本条第1 a ii段所提述的物品。”

6.21 《说明报告》对第六条的评注如下：

“71. 本条将蓄意作出关乎某些可被误用作干犯……[《布达佩斯公约》第二至五条所订]……罪行的器材或取用数据的特定非法作为，另行规定为独立的刑事罪行。由于犯这些罪行往往需要管有取用方法（‘黑客工具’）或其他工具，因此获取该等工具作犯罪之用的诱因强烈，以致可能形成一种生产及分发该等工具的黑市……

72. 第1(a)1段把生产、出售、为使用而获取、输入、分发或以其他方式提供……器材……定为罪行。‘分发’指将数据转发给他人的主动作为，‘提供’则指将器材放在网上供他人使用……所包括的‘电脑程式’指以下例子：经设计以更改甚至销毁数据或干扰系统操作的程式……或经设计或改装以取用电脑系统的程式。

73. 草拟人员曾详尽讨论，应否将有关器材限于经设计为专门或特别用作犯罪的器材……有意见认为这样是过于狭窄……至于把所有（即使是合法生产及分发的）器材纳入涵盖范围的替代方案，亦遭否决。只有意图干犯电脑罪行这项主观元素，将成为判处刑罚的决定性因素……《公约》将其范围限于涉及经客观设计或改装以主要用作犯罪的器材的案件……

74. 第1(a)2段把生产、出售、为使用而获取、输入、分发或以其他方式提供可藉以取用整个电脑系统或其任何部分的……数据，定为罪行。

75. 第1(b)段把管有列于第1(a)1或1(a)2段的物品定为罪行。缔约方获准……依法规定管有一定数量的这类物品。所管有物品的数量，可直接证明有犯罪意图……

76. 该罪行须是在无权的情况下蓄意干犯的……还须有特定（即直接）意图，将有关器材用作干犯《公约》第二至五条所订任何罪行。

77. 第 2 段清楚列明，为了在获授权下测试或保护电脑系统而制作的工具，并不受该条所涵盖……

78. ……第 3 段容许缔约方根据所作保留……在本土法律中规限该罪行的范围。然而，各缔约方有责任至少把出售、分发或提供第 1 (a) 2 段所述的……数据，定为罪行。"[14]

其他司法管辖区的法定体制

澳大利亚

《刑事法典》（联邦）第 478.3 条

6.22 澳大利亚《刑事法典》（联邦）（Criminal Code (Cth)）第 478.3 条（*"管有或控制数据，并意图干犯电脑罪行"*）订有一项与本章相关的罪行：

"(1) 任何人在以下情况，即属犯罪：

(a) 该人管有或控制数据；及

(b) 该人作出该项管有或控制的意图，是使该等数据被该人或他人：

(i) 用作干犯违反第 477 分部的罪行；或

(ii) 用作利便干犯该罪行。

刑罚：监禁 3 年。

(2) 即使干犯违反第 477 分部的罪行并不可能，任何人仍可被裁定犯违反本条的罪行。

---

[14] 《说明报告》第 71 至 78 段。

企图犯罪不属犯罪

(3) 企图干犯违反本条的罪行，不属犯罪。

管有或控制数据的涵义

(4) 在本条中，凡提述某人管有或控制数据，即包括提述该人：

(a) 管有任何存有或载有该等数据的电脑或数据储存器材；或

(b) 管有任何记录该等数据的文件；或

(c) 控制存于他人管有的电脑内的数据（不论是在澳大利亚境内或境外）。”

6.23 《刑事法典》（联邦）第 478.3(1)(b)(i)条所提述的第 477 分部（*“严重电脑罪行”*），包括：

(a) 第 477.1 条（*“在未获授权下作出取览、修改或损害，并意图干犯严重罪行”*）；

(b) 第 477.2 条（*“在未获授权下修改数据，以导致损害”*）；及

(c) 第 477.3 条（*“在未获授权下损害电子通讯”*）。

这些罪行实质上与第 2 至 5 章所论述的建议罪行相对应。

《刑事法典》（联邦）第 478.4 条

6.24 除《刑事法典》（联邦）第 478.3 条外，第 478.4 条（*“生产、供应或取得数据，并意图干犯电脑罪行”*）亦与本章相关。这两项条文的结构相类似：

“(1) 任何人在以下情况，即属犯罪：

(a) 该人生产、供应或取得数据；及

(b) 该人作出上述作为的意图，是使该等数据被该人或他人：

(i) 用作干犯违反第 477 分部的罪行；或

(ii) 用作利便干犯该罪行。

刑罚：监禁 3 年。

(2) 即使干犯违反第 477 分部的罪行并不可能，任何人仍可被裁定犯违反本条的罪行。

企图犯罪不属犯罪

(3) 企图干犯违反本条的罪行，不属犯罪。

生产、供应或取得数据的涵义

(4) 在本条中，凡提述某人生产、供应或取得数据，即包括提述该人：

(a) 生产、供应或取得存于或载于电脑或数据储存器材内的数据；或

(b) 制作、供应或取得记录该等数据的文件。"

6.25 第 478.3 及 478.4 条源于《示范法典委员会报告书》*"为配合"*《布达佩斯公约》*"第六条的规定"*而建议的《示范刑事法典》（Model Criminal Code）第 4.2.7 及 4.2.8 条。[15] 第 478.3 及 478.4 条所订立的罪行成为一组，具有以下共通点：

(a) 两项罪行均规定须有以下意图：被告人或他人将数据用作干犯违反《刑事法典》（联邦）第 477 分部的罪行，或将数据用作利便干犯该罪行。罔顾后果或仅是知悉数据可用作上述目的，并不足够。

(b) 两项罪行均只针对数据，而非针对任何实物。然而，两者均把管有或控制数据（第 478.3 条）或生产、供应或取得数据（第 478.4 条），界定为包括某些涉及有形物的情境。

15 《示范法典委员会报告书》第 92 页。

加拿大

《1985 年刑事法典》第 342.1(1)条

6.26 第 2 及 3 章曾提及加拿大《1985 年刑事法典》（Criminal Code 1985）第 342.1(1)条（*"在未获授权下使用电脑"*）。[16] 第 342.1(1)(d)条订明，任何人：

> "意图欺诈并在无表面权利的情况下……使用、管有、非法传送或准许他人取览某电脑密码，而该密码会使某人能够干犯(a)、(b)或(c)段所订罪行"，

即属犯罪。

6.27 第 342.1(1)(a)、(b)及(c)条分别处理：

(a) 取得任何电脑服务；

(b) 截取某电脑系统的任何功能；及

(c) 使用某电脑系统，意图干犯(a)或(b)段所订罪行，或就电脑数据或某电脑系统干犯第 430 条所订罪行。

6.28 根据第 342.1(2)条，就电脑密码而言，*"非法传送"*指*"出售、从加拿大输出、向加拿大输入、分发或以任何其他方式处理"*。该条把*"电脑密码"*界定为*"任何可藉以取得电脑服务或使用电脑系统的电脑数据"*。该定义范围虽广，但显然不包括比如有关利用漏洞的专门知识。

《1985 年刑事法典》第 342.2(1)条

6.29 若要更广泛地规管用作干犯电脑网络罪行的*"器材"*，便须改用第 342.2(1)条（*"为在未获授权下使用电脑系统或导致损害而管有器材"*）。根据该条，任何人：

> "无合法辩解而制造、管有、出售、要约出售、输入、为使用而取得、分发或提供经设计或改装以主要用作干犯第 342.1 或 430 条所订罪行的任何器材，并知悉该器材已用作或拟用作干犯该罪行"，

即属犯罪。

---

16 第 2.28 及 3.40 段。

6.30 第 342.2(4)条以非尽列无遗的方式，将*"器材"*界定为包括*"(a)某器材的零件；及(b)第 342.1(2)款所指的电脑程式"*。就*"器材"*一词而言，某评论员引用两宗案例，[17] 并提出以下评析：

> "该条通常不适用于诸如并非**主要**为干犯相关罪行而设计的电脑等物品。然而，法院曾经裁定，该条适用于为了记录与信用卡帐户有关的个人身分号码而安装的数码摄像机。"[18] （强调之处乃原文所有）

6.31 第 342.2(1)条的措辞与第 327(1)条（*"管有器材以取得使用电讯设施或服务"*）相同，但后者适用于：

> "经设计或改装以主要用作在没有支付合法费用下使用电讯设施或取得电讯服务的任何器材"。

《1985 年刑事法典》第 191(1)条

6.32 我们还应提述第 191(1)条（*"管有等"*），该条是关乎截取通讯（而非电脑网络罪行）的条文。根据第 191(1)条，任何人：

> "管有、出售或购买任何电磁、声音、机械或其他器材或其任何零件，并知悉该器材的设计使该器材主要对暗中截取私人通讯有用"，

即属犯罪。

6.33 第 191(1)及 342.2(1)条均引入某器材的*主要*用途这个概念，而关乎电脑密码的第 342.1(1)(d)条则没有此概念。

英格兰及威尔斯

《英格兰误用电脑法令》第 3A 条

6.34 在英格兰及威尔斯，《2006 年警察及司法法令》（Police and Justice Act 2006）第 37 条在《英格兰误用电脑法令》加入新的第 3A 条。制定为《2006 年警察及司法法令》的法案的注释，概述该新订条文，并如下解释条文的背景：

---

17 *R v Singh* 2006 ABPC 156 及 *R v Coman* 2004 ABPC 18。

18 Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd edition, 2015)，第 140 页。

"302. ……新订条文订立三项新罪行，各项罪行一经循公诉程序定罪，可处监禁两年或罚款，或两者兼处。这些罪行是：

- 制造、改装、供应或要约供应某物品，意图使该物品用作干犯(或用作协助干犯)第 1 条[19] 或第 3 条[20] 所订罪行（新订条文的第(1)款）；
- 供应或要约供应某物品，并相信该物品相当可能会被如此使用（第(2)款）；
- 取得某物品，以使该物品被供应作如此使用（第(3)款）。

如任何人就多项物品而被控第(2)款所订罪行，控方便须就该等物品中任何一件或多于一件特定物品，证明其案情属实。若只证明该人相信某部分涉案物品相当可能会在与第 1 或 3 条所订罪行有关连的情况下使用，并不足够。

303. 订立这些新罪行的背景，是由于电子工具（例如可用作对电脑系统进行黑客入侵的'黑客工具'）现成市场不断扩张，而且越来越多人在与有组织罪行有关连的情况下，使用这类工具。此外，《2001 年欧洲委员会电脑网络罪行公约》（2001 Council of Europe Cybercrime Convention）第 6(1)(a)条规定，须把分发或提供可藉以取用电脑系统的电脑密码或类似数据，并意图犯罪这行为定为罪行。这些新罪行是为了实施这项规定而订立的……。"

6.35 《英格兰误用电脑法令》加入第 3A 条后，《2015 年严重刑事罪行法令》（Serious Crime Act 2015）第 41(2)条在《英格兰误用电脑法令》加入第 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"*），第 4 及 5 章已论述该条。[21] 因此，第 3A 条提述*"第 1、3 或 3ZA 条所订罪行"*，作为意图使用某*"物品"*而干犯的罪行。此外，《2015 年严重刑事罪行法令》第 42 条亦扩大了《英格兰误用电脑法令》第 3A(3)条的范围。

---

19 在未获授权下取览电脑资料。

20 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。

21 第 4.41 及 5.34 段。

6.36 经上述修订后，《英格兰误用电脑法令》第 3A 条（*"制造、供应或取得用于第 1、3 或 3ZA 条所订罪行的物品"*）的现行内容如下：

"(1) 任何人制造、改装、供应或要约供应任何物品，并意图使该物品用作干犯（或用作协助干犯）第 1、3 或 3ZA 条所订罪行，即属犯罪。

(2) 任何人供应或要约供应任何物品，并相信该物品相当可能会用作干犯（或用作协助干犯）第 1、3 或 3ZA 条所订罪行，即属犯罪。

(3) 任何人取得任何物品，并——

(a) 意图将该物品用作干犯（或用作协助干犯）第 1、3 或 3ZA 条所订罪行；或

(b) 以使该物品被供应用作干犯（或用作协助干犯）第 1、3 或 3ZA 条所订罪行，

即属犯罪。

(4) 在本条中，'物品'包括以电子形式所存的任何程式或数据。

(5) 任何人犯本条所订罪行——

(a) 一经在英格兰及威尔斯循简易程序定罪，可处为期不超过 12 个月的监禁或不超过法定最高罚款，或两者兼处；

(b) [……]

(c) 一经循公诉程序定罪，可处为期不超过 2 年的监禁或罚款，或两者兼处。"

有关罪行的范围

6.37 《英格兰误用电脑法令》实施 30 年后，部分社会人士开始提倡改革该法令。[22] 举例而言，某跨行业组织在其报告书中认为，第 3A 条有*"过度刑事化的显著风险"*，[23] 并对此阐述如下：

---

[22] 例子见 Cyber Up 运动，网址为 https://www.cyberupcampaign.com/cma-30th-birthday（于 2022 年 5 月 3 日浏览）。

"3.54 ……首先，《误用电脑法令》第 3A 条没有将‘物品’局限于为用作犯罪而设计或制作的物品，更遑论将‘物品’局限于‘主要’为该目的而设计或制作的物品。即是说，只要有关事物用作犯罪，就连虚拟私有网络软件（VPN）及让通讯得以安全进行的洋葱路由器（the onion router，简称 Tor）亦会纳入该罪行的范围内……

3.55 第二，如有关行为是供应或要约供应工具，第 3A 条只规定须证明某人‘相信相当可能’该等工具会被非法使用……这较广泛的意念元素的主要问题，在于所有保安及威胁研究人员均**知悉**（而非仅是相信）不法之徒‘相当可能’会使用黑客工具或像 VPN 这样的匿名工具来利便犯罪，因此，保安及威胁研究人员也会落入该罪行的范围内。

3.56 第三，第 3A 条并无提及……正当理由……

3.57 第四，第 3A 条并没有将管有单独定为罪行。管有只是作为其他行为（即制造、供应、要约供应及取得）的一部分而间接获视为罪行……

3.58 这些规定的综合效果，是令那些同时供应或要约供应具有双重用途的黑客工具、VPN 及 Tor 的人，及／或那些取得该等工具以作自用或供应予他人的人，受第 3A 条约束。以下人士也会因而落入该罪行的范围内：保安及威胁情报研究人员；可能取得 VPN 或 Tor 以确保通讯安全的举报者，以便他们透露在未获授权下取览的数据（《误用电脑法令》第 1 条）；以及供应这类工具（例如 SecureDrop）并相信有关工具会用作收取数据（特别来自举报者的数据）的新闻工作者（第 3A(2)条）。"[24]（强调之处乃原文所有）

展示成功执法的案例

6.38 以上负面评论并不适用于犯罪者明显难逃其责的情况。在 *R v Lewys Martin*[25] 这宗相关案件，被告人承认多项控罪，包括两项根据

---

23 Criminal Law Reform Now Network, *Reforming the Computer Misuse Act 1990*（2020 年），第 2 章，第 4.23 段，登载于 http://www.clrnn.co.uk/publications-reports/（于 2022 年 5 月 3 日浏览）。

24 同上，第 2 章，第 3.54 至 3.58 段。

25 [2014] 1 Cr App R (S) 63.

第 3A 条提出的控罪，这两项控罪关乎被告人电脑上两项名为 Jaindos 及 CyberGhost 的程式。Jaindos 可发动拒绝服务攻击，CyberGhost 则可提供具误导性的互联网规约地址位置资料，让使用者匿名。

《2006 年欺诈罪法令》第 6 及 7 条

6.39 《2006 年欺诈罪法令》（Fraud Act 2006）第 8(1)条界定第 6 条（*"管有用作欺诈的物品等"*）及第 7 条（*"制造或供应用作欺诈的物品"*）中*"物品"*一词的方式，与《英格兰误用电脑法令》第 3A(4)条相同，即包括*"以电子形式所存的任何程式或数据"*。因此，在某程度上，《2006 年欺诈罪法令》第 6 及 7 条显然与《英格兰误用电脑法令》第 3A 条互相重迭。

6.40 上述对过度刑事化风险不满的跨行业组织，将这些条文比较如下：

> "从检控人员的角度来看，要根据［《英格兰误用电脑法令》］第 3A 条提出控罪，看来须证明有关物品可用作干犯第 1 或 3［或 3ZA］条所订罪行。若采用《2006 年欺诈罪法令》第 6 或 7 条，便须证明有关工具可用作干犯欺诈罪……"[26]

《2003 年通讯法令》第 126 条

6.41 为求完整，以下条文值得一提：

(a) 《2003 年通讯法令》（Communications Act 2003）第 126(1)条将以下行为定为不合法：管有或控制可用作取得电子通讯服务，或管有或控制可在与取得该服务有关连的情况下使用的任何事物，并意图以第 126(3)条所详述的方式误用该事物；及

(b) 第 126(2)条订立以下罪行：供应或要约供应同类事物，并知悉或相信其收取人意图以第 126(3)条所详述的方式误用该事物。

6.42 《2003 年通讯法令》第 126(3)条提述某人的下述意图：

(a) 使用有关事物，以不诚实地取得电子通讯服务；

---

[26] 见上文注脚 23，第 1 章，第 4.6 段。

(b) 将有关事物用作与不诚实地取得上述服务有关连的目的；

(c) 不诚实地容许将该事物用作取得上述服务；或

(d) 容许将该事物用作与不诚实地取得上述服务有关连的目的。

中国内地

6.43 《中国刑法》第二百八十五条第三款载有以下罪行：

> "提供专门用于侵入、非法控制计算机信息系统的程序、工具，或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具，情节严重的，依照前款的规定处罚。"
>
> （底线后加）

6.44 就提供程序或工具，第二百八十五条第三款订有两部分，即(i)*"专门用于"*侵入、非法控制计算机信息系统，以及(ii)明知他人会将程序或工具用于该等目的。

6.45 关于第一部分，根据法释〔2011〕19号第二条，具有下列情形之一的程序、工具，应当认定为第二百八十五条第三款规定的*"专门用于侵入、非法控制计算机信息系统的程序、工具"*：

> "（一）具有避开或者突破计算机信息系统安全保护措施，未经授权或者超越授权获取计算机信息系统数据的功能的；
>
> （二）具有避开或者突破计算机信息系统安全保护措施，未经授权或者超越授权对计算机信息系统实施控制的功能的；
>
> （三）其他专门设计用于侵入、非法控制计算机信息系统、非法获取计算机信息系统数据的程序、工具。"

6.46 至于第二部分，如被告人明知他人会将本属中性的程序或工具用于侵入、非法控制计算机信息系统，则提供该程序或工具亦可干犯该罪行。因此，该部分除要求须证明有《中国刑法》第十四条所规定的意图外，还要求证明知悉这项额外意念元素。

6.47 《中国刑法》第二百八十六条第三款是另一项相关罪行条文：

> "故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，依照第一款的规定处罚。"
>
> （底线后加）

6.48 根据法释〔2011〕19号第五条，具有下列情形之一的程序，应当认定为*"计算机病毒等破坏性程序"*：

> "（一） 能够通过网络、存储介质、文件等媒介，将自身的部分、全部或者变种进行复制、传播，并破坏计算机系统功能、数据或者应用程序的；
>
> （二） 能够在预先设定条件下自动触发，并破坏计算机系统功能、数据或者应用程序的；
>
> （三） 其他专门设计用于破坏计算机系统功能、数据或者应用程序的程序。"

新西兰

《新西兰法令》第 251 条

6.49 《新西兰法令》第251条（*"制作、出售、分发或管有用作犯罪的软件"*）订立两项罪行，该等罪行关乎令人能够在未获授权下取用电脑系统的软件或其他资料。

6.50 第251(1)条订立首项罪行。该条侧重于上述软件或资料的供应层面，将任何人（"**甲方**"）的以下作为定为不合法：

> (a) 邀请另一人获取上述软件或资料；或
>
> (b) 要约出售或要约供应该软件或资料，或为出售或供应而展示该软件或资料；或
>
> (c) 同意出售或供应该软件或资料；或
>
> (d) 出售或供应该软件或资料；或
>
> (e) 为出售或供应而管有该软件或资料，

前提是甲方：

(i) 知悉该软件或资料的唯一或主要用途，是用作犯罪；或

(ii) 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（不论甲方是否也宣传该软件或资料对任何其他目的有用）。

6.51 第 251(2)条则针对需求层面，将管有上述软件或资料并意图用它犯罪，定为第二项罪行。

6.52 第 251(1)及(2)条均提述可能犯*"罪"*。这似乎可以是任何性质的罪行，而无须是电脑网络罪行。

《新西兰法令》第 216D 条

6.53 第 216D(1)条（*"禁止处理截取器材等"*）亦与本章相关。该条所禁止的作为与第 251(1)条所指明的作为（列于上文）相同，但第 216D(1)条关乎符合以下说明的任何*"截取器材"*：

(a) 任何人知悉该截取器材的唯一或主要目的，是暗中截取私人通讯；或

(b) 该人表示该截取器材对暗中截取私人通讯有用（不论该人是否也表示该截取器材对任何其他目的有用）。

6.54 根据第 216A(1)条，*"截取器材"*指：

> "用于或可用于截取私人通讯的任何电子、机械、电磁、光学或光电工具、器具、设备或其他器材"

但不包括助听器或相类器材，或获总督豁免的器材。

6.55 《新西兰法令》第 216D(1)(ii)及 251(1)(b)条将宣传或表示某软件、资料或截取器材对非法目的有用的行为，定为不合法。有学者就第 251(1)(b)条提出以下看法，而该看法同样也适用于第 216D(1)(ii)条：

"实际上，该条的目标徒劳无益。任何人只需为可能属非法的程式宣传用作某种合法目的，余下的留给别人想象便可。"[27]

6.56 上述批评看来理据充分。假设被告人没有作出上述宣传或表示，控方便需要依赖（第 216D(1)(i)条或第 251(1)(a)条所订的）交替法律责任基础，即被告人知悉该软件或资料的唯一或主要用途，是用作犯罪，或被告人知悉该截取器材的唯一或主要目的，是暗中截取私人通讯（视乎属何情况而定）。

新加坡

《新加坡误用电脑法令》第 8 条

6.57 《1998 年误用电脑（修订）法令》（Computer Misuse (Amendment) Act 1998，1998 年第 21 号）第 7 条在《新加坡误用电脑法令》加入新的第 6B 条，该条现已重编为第 8 条（*"在未获授权下披露取用码"*），内容如下：

"(1) 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。

(2) 任何人犯第(1)款所订罪行，一经定罪——

(a) 可处不超过$10,000 的罚款或为期不超过 3 年的监禁，或两者兼处；及

(b) 如属第二次或其后每次定罪，则可处不超过$20,000 的罚款或为期不超过 5 年的监禁，或两者兼处。"

---

[27] David Harvey, *internet.law.nz selected issues* (LexisNexis NZ Limited, 4th edition, 2015)，第 7.112 段。

《新加坡误用电脑法令》第 10 条

6.58 《2017 年误用电脑及电脑网络安全（修订）法令》（Computer Misuse and Cybersecurity (Amendment) Act 2017）第 3 条进一步在《新加坡误用电脑法令》加入新的第 10 条（*"取得用于某些罪行的物品等"*），其规定如下：

"(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。

(3) 任何人犯第(1)款所订罪行，一经定罪——

(a) 可处不超过$10,000 的罚款或为期不超过 3 年的监禁，或两者兼处；而

(b) 如属第二次或其后每次定罪，则可处不超过$20,000的罚款或为期不超过5年的监禁，或两者兼处。"

6.59 《新加坡误用电脑法令》第8(1)及10(1)(b)条看来有部分互相重迭。控方或须决定案件应根据哪一条处理。在现实中，这大概不会对被告人造成不公，因为该两条所订的最高刑罚相同。由于我们会在下文建议新法例应以《新加坡误用电脑法令》第8及10条为蓝本，[28]因此可能有空间将这些条文重组或合并，以订立一个更井然有序的法律体制。这方面留待法律草拟专员决定。

与《示范法》作比较

6.60 《新加坡误用电脑法令》第10条另一值得注意的特点是，该条指明适用物品时所采用的措辞，近似《示范法》第9条（*"非法器材"*），但比后者范围更广。以下列出《示范法》第9(1)条，以作比较：

"任何人在以下情况，即属犯罪：

(a) 该人无合法辩解或理由而蓄意或罔顾后果地生产、出售、为使用而获取、输入、输出、分发或以其他方式提供：

(i) 经设计或改装以用作干犯违反第5、6、7或8条的罪行的器材（包括电脑程式）；或

(ii) 可藉以取用整个电脑系统或其任何部分的电脑密码、取用码或类似数据；

并意图使该器材、电脑密码、取用码或数据被任何人用作干犯违反第5、6、7或8条的罪行；或

(b) 该人管有(a)(i)或(a)(ii)节所提及的任何物品，并意图使该物品被任何人用作干犯违反第5、6、7或8条的罪行。"

---

[28] 第6.88(b)段。

美国

《电脑欺诈及滥用法案》内的《美国法典》第 18 篇第 1030(a)(6)条

6.61 根据《美国法典》第 18 篇第 1030(a)(6)条，任何人：

> "意图欺诈并故意非法传送（定义见第 1029 条）任何密码或类似资料，而透过该密码或资料可在未获授权下取用电脑，如——
>
> (A) 该非法传送会影响州际或对外贸易；或
>
> (B) 有关电脑是由美国政府所使用或为美国政府而使用的"，

即可按《美国法典》第 18 篇第 1030(c)条的规定予以惩处。

6.62 根据《美国法典》第 18 篇第 1029(e)(5)条的定义，*"非法传送"*指*"转让予另一人或以其他方式处置而转予另一人，或意图作出转让或处置而取得控制"*。

6.63 有关法例并无界定*"可透过密码或类似资料，在未获授权下取用电脑"*。该用语的惯常涵义包括登入凭证等资料，而视乎*"类似"*一词应如何解释，大概亦会包括有关利用漏洞的专门知识。然而，该用语是否涵盖用作在未获授权下取用电脑的软件，则似乎有商榷余地。

《美国法典》第 18 篇第 1029 条

6.64 无论如何，《美国法典》第 18 篇第 1030(a)(6)条不适用于实物这观点，应不受争议。《美国法典》第 18 篇第 1029(a)条反而就多种行为订立十项独立罪行，其中包括管有、生产、使用及贩运*"取用器材"*。

6.65 以下是《美国法典》第 18 篇第 1029(e)(1)条中*"取用器材"*的定义，该定义包括有形物及无形物：

> "可单独使用或与其他取用器材一并使用，以取得金钱、货物、服务或任何其他有价值事物，或可用作提出资金转账（仅藉纸本文书作出的转账除外）的任何卡、字牌、代码、帐户号码、电子编号、流动识别号码、个人身分

号码，或其他电讯服务、设备或工具标识，或其他取用帐户的方法"。

6.66 对于《美国法典》第 18 篇第 1029 条的一些典型适用范围，美国司法部电脑罪行及知识产权组（Computer Crime and Intellectual Property Section）解释如下：

> "检控人员通常会根据第 1029 条，对多种'仿冒诈骗（phishing）'案件及'使用失窃卡资料（carding）'案件提出检控，前者涉及被告人使用诈骗电邮取得银行帐户号码及密码，后者则涉及被告人购买、出售或转让盗取的银行帐户、信用卡或扣帐卡资料。"[29]

《美国法典》第 18 篇第 2512 条

6.67 除《美国法典》第 18 篇第 1029 条外，*"器材"*一词亦出现在《美国法典》第 18 篇第 2512(1)条，该条本质上禁止任何人蓄意制造、分发、管有和宣传：

> "任何电子、机械或其他器材，而该人知悉或有理由知悉该器材的设计使该器材主要对暗中截取有线、口头或电子通讯有用"。

6.68 《美国法典》第 18 篇第 2512(1)条对某器材的主要用途（而非比如是唯一用途或可能用途）的提述，亦见于《布达佩斯公约》第六条、[30] 加拿大《1985 年刑事法典》第 191(1)及 342.2(1)条，[31] 以及《新加坡误用电脑法令》第 10(2)(a)条[32]（这些条文均于上文论述）。

小组委员会的看法

应订立兼具基本及加重形式的新罪行

6.69 现时，《刑事罪行条例》（第 200 章）第 60 及 62 条共同把刑事损坏定为不合法。如按建议 6(c)所提议，将该条例关于*"误用电*

---

29 H Marshall Jarrett, Michael W Bailie, Ed Hagen and Scott Eltringham, *Prosecuting Computer Crimes* (Office of Legal Education, Executive Office for United States Attorneys, 2nd edition, 2010)，第 102 至 103 页，登载于 https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf（于 2022 年 5 月 3 日浏览）。

30 第 6.20 段。

31 第 6.29 及 6.32 段。

32 第 6.58 段。

*脑"*的条文改列于新法例，在新法例加入与第 62 条[33] 相对应的条文，实属正确之举。我们亦认为，该条文亦应适用于第 2 至 5 章所论述的全部四类依赖电脑网络的罪行。

6.70 在讨论过程中，我们设法解决兼具合法及非法用途的器材及数据所带来的挑战。第 6.3(c)段所提及的消磁器便是一例，财务机构会使用消磁器清除旧硬碟的内容，以策安全。我们相信，在该情况下管有消磁器不会引起任何问题，这点无可争议。相反，如管有消磁器并意图将它用作非法目的（例如破坏），施加刑事法律责任则属合理。

6.71 在现实世界中，*"攻击性武器"*这概念亦有同样的考虑。根据《公安条例》（第 245 章），*"攻击性武器"*[34] 的定义区分以下物品：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、*"适合"*[35] 用作造成伤害的物品，或*"拟供"*用作造成伤害的物品。在应用该定义时：

(a) 在涉及例如下述物品的案件中，无须证明犯罪意图。纯粹在公众地方管有下述物品，便足以招致刑事法律责任：

(i) 枪、开山刀或蝴蝶刀（因为以性质而论，这类物品属*"被制造……以用作伤害他人"*）；或

(ii) 装有刺刀的雨伞，或削尖并装有尖钉的手杖（因为该雨伞或手杖已被"改装"以用作造成伤害）。

(b) 然而，鉴于比如水果刀或"瑞士军刀"这类物品本属中性，有关物品只有在*"由管有或控制该物品的人拟将之作攻击性用途"*的情况下，方属攻击性武器。

6.72 借镜上述分类方法，我们认为应把建议的罪行分为基本及加重两种形式。在个别案件中，除了根据某器材或数据是否被制造或改

---

33 *"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。"

34 第 2(1)条将*"攻击性武器"*界定为：
"任何被制造或改装以用作伤害他人，或适合用作伤害他人的物品，或由管有或控制该物品的人拟供其本人或他人作如此用途的任何物品"。

35 在 *R v Chong Ah Choi & Ors* [1994] 3 HKC 68, HCMA 281/1994（判决日期：1994 年 10 月 4 日），上诉法庭基本上裁定（第 7G 段），*"攻击性武器"*定义中*"适合"*用作造成伤害的部分应不再适用。

装以用作非法用途，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（例如已有人开始利用图像卡来挖掘加密货币），故单靠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。

建议罪行所应适用的器材及数据

就建议罪行的基本及加重形式而言

6.73 电脑网络罪行可藉实物器材而干犯，但没有实物器材亦可干犯有关罪行。举例而言，在网上故意散布勒索软件已可造成破坏。将勒索软件、病毒、其源码及类似事物称为电脑网络武器，其实也不为过。为确保能在电脑网络空间有效执行建议的罪行，我们认为该罪行应适用于有形物及无形物。

6.74 另一方面，鉴于已有新西兰法例作为先例，[36] 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。

6.75 我们也考虑过建议的罪行应否适用于主要用作犯罪的器材或数据，不论该器材或数据能否用作任何合法目的。我们认为，建议的罪行若只适用于没可能有任何合法用途的器材或数据，会过于局限。同样道理，不论被告人的主观意图，任何器材或数据的主要用途，应以客观方式界定。总的来说，我们认为建议的罪行应适用于主要用作（以客观方式界定）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。

6.76 我们亦曾讨论，建议的罪行应否适用于获相信或声称能够（但实际上不能）用作犯罪的器材或数据，例如：

(a) 不正确的密码；或

(b) 据称能够在十分钟内破解密码的破解密码工具，但由于该工具设计不良或有缺陷，经过长久得多的时间后，该工具仍未能破解密码。

6.77 鉴于《刑事罪行条例》（第 200 章）第 62 条并无明确规定有关物品须实际上能够摧毁或损坏财产，我们总结认为，如任何人相信或声称某器材或数据能够用作犯罪，不论该人所信或所声称的是否

---

[36] 见第 6.50 及 6.51 段，当中提述《新西兰法令》第 251(1)及(2)条。

属实，亦应足以构成罪行。此立场符合我们基于*朱峻琦*案所达成的共识，即刑事法律责任不应取决于网络攻击成功与否。

就基本罪行而言

6.78 我们亦建议：

(a) 基本罪行应涵盖被制造或改装以用作犯罪的器材或数据；及

(b) 应依据有关器材或数据的主要用途（以客观方式界定，不论被告人的主观意图为何）评估是否符合(a)项的准则。

6.79 同时，我们建议的做法，将本属中性（例如上文所论述的消磁器）[37] 但被意图用作导致伤害的器材或数据排除在外，原因是如没有该意图，似乎没有理由将有关行为定为罪行。相反，如有该意图，加重罪行便会适用。

就加重罪行而言

6.80 基于上文所解释的看法，我们建议加重罪行应适用于能够用作犯罪的器材或数据，或犯罪者相信或声称能够用作犯罪的器材或数据。

犯罪行为

6.81 《布达佩斯公约》的《说明报告》[38]，以及制定为《2006年警察及司法法令》的法案的注释，[39] 均提到存在*"黑客工具"*及相类工具的市场。为确保法例周全起见，我们相信因应该类市场的蓬勃发展而采取的法定措施，必须针对市场各类参与者，不论他们是该市场的供应方还是需求方。

6.82 因此，我们的建议是，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。

---

37 第 6.70 段。

38 第 6.21 段所引述的《说明报告》第 71 段。

39 第 6.34 段所引述的注释第 303 段。

犯罪意念

就建议罪行的基本及加重形式而言

6.83 我们认为，任何人应仅在蓄意提供或管有上文所述的器材或数据的情况下，方属犯罪。由于很多人都管有软件或电脑数据，甚至在自己不察觉的情况下向他人提供软件或电脑数据，若采用较低的门槛——比如只须罔顾后果，或者完全无须有任何特定意念，似乎不宜。举例而言：

(a) 不法之徒可遥距对不知情人士的电脑植入恶意软件或数据。

(b) 某人可能管有已受到恶意软件感染的电脑档案，但对此毫不知情。该人可能把该档案上载至网上储存空间，以为只有自己才能检索该档案。在现实中，该储存空间的管理人相当可能可取览该档案。如该储存空间不受保护或所受保护不足，该档案甚至可供整个互联网社群取览。

如有关罪行没有规定必须知悉，而单是罔顾后果，或不论被告人的意念如何，亦足以干犯该罪行，该罪行便可能适用于上文情境(a)中毫不知情的人士，以及情境(b)所述的人。该罪行的适用范围似乎会过于广阔。

就基本罪行而言

6.84 如任何人因相信[40]有关器材或数据可用作犯罪而被控基本罪行，该信念即构成须由控方证明的犯罪意念之一部分。

就加重罪行而言

6.85 如任何人被控加重罪行，按照定义，除了须证明上文第 6.83 及 6.84 段所论述的犯罪意念的所有其他方面外，还须证明该人意图将有关器材或数据用作犯罪。

建议让合理辩解作为法定免责辩护

6.86 在公众地方管有攻击性武器并不构成犯罪，前提是具有*"合法权限或合理辩解"*[41]（例如管有人在表演艺术时使用长兵器）。

---

[40] 第 6.76 至 6.77 段。

6.87 我们认为，建议的罪行应同样加入合理辩解这项法定免责辩护，因为任何人或机构可以有各种合法理由而需要可用作犯罪的器材或数据。我们认为，建议的免责辩护，有助避免像上述批评《英格兰误用电脑法令》的跨行业组织所谈及的过度刑事化问题。[42]

建议条文的蓝本

6.88 上文所审视的其他司法管辖区，在草拟罪行方面差异甚大，显示多种不同的可能性。在拟定香港的新法例时，我们提议借鉴以下条文，并将它们加以完善：

(a) 《英格兰误用电脑法令》第 3A 条；及

(b) 《新加坡误用电脑法令》第 8 及 10 条。

6.89 我们曾详加考虑，*"管有"*这概念是否切合建议的罪行拟适用于数据等无形物的用意。说明*"管有"*这法律概念性质的案例，现确立已久。*Archbold Hong Kong 2021* 的以下段落，描述了该概念的要素：

> "如有足够证据证明某人实质控制某事物，即该人有能力在可行范围内及法律规限下，随意使用该事物并有能力禁止他人使用该事物，亦有意图行使该控制权，该人便可被裁定为管有该事物。"[43]
>
> （底线后加）

6.90 换言之，*"管有"*表示有权控制某事物，而该事物并非必定是有形的。事实上，就其他法例而言，*"管有"*亦已特别适用于涉及电脑程式或数据的罪行，例如是《版权条例》（第 528 章）所订的管有侵犯版权物品罪，[44] 以及《防止儿童色情物品条例》（第 579 章）所订的管有儿童色情物品罪。[45] 另外，据我们观察，在我们所比较研究的部分司法管辖区，*"管有"*亦适用于同属无形物的数据、资料、电脑程

---

41 《公安条例》（第 245 章）第 33(1)条。

42 第 6.37 段。

43 *Archbold Hong Kong 2021*，第 29–39 段。

44 根据《版权条例》（第 528 章）第 118(2A)条，任何人如*"未获本款适用的版权作品的版权拥有人的特许，而为任何贸易或业务的目的或在任何贸易或业务的过程中，管有该作品的侵犯版权复制品，以期令某人可为该贸易或业务的目的或在该贸易或业务的过程中，使用该侵犯版权复制品"*，即属犯罪。凭借第 118(2B)条，第 118(2A)条亦保障属"电脑程式"的版权作品。

45 根据《防止儿童色情物品条例》（第 579 章）第 3(3)条，任何人管有儿童色情物品，即属犯罪。第 2(1)条将"儿童色情物品"界定为包括*"以任何方式贮存并能转为"*对儿童作色情描划的照片、影片、电脑产生的影像或其他视像描划*"的资料或数据"*。

式及软件。[46] 基于上述理由，我们认为*"管有"*作为建议罪行的元素，实属恰当。

建议 9

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

---

[46] 举例而言，澳大利亚《刑事法典》（联邦）第 478.3 条把意图犯电脑罪行而*"管有"*或控制数据，定为罪行（见第 6.22 段）。加拿大《1985 年刑事法典》第 342.2(1)条将多项行为定为罪行，包括*"管有"*经设计或改装以主要用作干犯第 342.1 或 430 条所订罪行的器材，而*"器材"*则包括电脑程式（见第 6.29 至 6.30 段）。《新西兰法令》第 251(1)条将多项行为定为罪行，包括*"管有"*用作犯罪的软件或资料（见第 6.50 段）。美国《电脑欺诈及滥用法案》第 1029(a)条将多项行为定为罪行，包括*"管有"*、*"取用器材"*，而凭借第 1029(e)(1)条，*"取用器材"*则包括无形物及数据（见第 6.64 至 6.65 段）。

(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。

管有只可作有害用途的数据

6.91 我们已在上文建议合理辩解可作为一般免责辩护。在结束本章前，我们谨提出以下问题：新法例应否同时就蓄意管有只可用作进行网络攻击的电脑数据（软件或源码）这项罪行，再认可一项特定的免责辩护或豁免。这类电脑数据的例子包括：

(a) 勒索软件；

(b) 病毒；

(c) 建立及管理僵尸网络的软件；及

(d) 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）。[47]

6.92 尽管这几类电脑数据可能有害，但亦有论点认为，比如在以下情况下，法律无须（或不应）把管有该等数据定为罪行：

(a) 大学保存恶意软件，作教学或研究之用；

(b) 开发防毒软件；

(c) 使用恶意软件训练互联网服务供应商电邮伺服器的垃圾邮件过滤器；[48] 及

---

47 上述跨行业组织报告书举出第三及第四项例子。见 Criminal Law Reform Now Network, *Reforming the Computer Misuse Act 1990*（2020 年），第 1 章，第 3.24 段。

48 采用人工智能技术的垃圾邮件过滤器可接受训练，久而久之其性能便可改善。

(d) 其他资讯科技从业人员透过逆向工程，对恶意代码进行研究。

6.93 至于分界线应订于何处，一切视乎情况而定。以现实世界的例子作比拟，任何人即使对研究有兴趣，也不大可能以此为理由，在家中保存爆炸品。在阐述这些意见后，我们期望公众就以下问题提交意见书。

建议 10

小组委员会邀请公众就以下问题提交意见书：

(a) 就蓄意提供或管有电脑数据（软件或源码）这项罪行而言，如该数据只可用作进行网络攻击（例如是勒索软件或病毒），应否有免责辩护或豁免？

(b) 如(a)段的答案是“应该”的话，

(i) 上述免责辩护或豁免应在甚么情况下可用，并应有甚么条款？

(ii) 这种获豁免的管有应否受到规管，以及如应该的话，有甚么规管规定？

第 7 章　香港法庭行使司法管辖权的准则

引言

7.1　本章讨论与电脑网络罪行相关的司法管辖权事宜，并集中探讨香港法庭行使司法管辖权的准则。本章宜先从一般原则着手，继而转谈国际间电脑网络罪行法例处理司法管辖权事宜方面的经验。

7.2　有评论员[1]识别出以下三个各自独立却又环环相扣的司法管辖权范畴：

(a) 规范的司法管辖权，该权关乎立法机关规管若干行为的能力；

(b) 审判的司法管辖权，该权关乎若干行为可否由法庭审理；及

(c) 执行的司法管辖权，该权关乎法律体制要求遵守规定或惩处违规行为的权限。

有关司法管辖权的一般原则

普通法的做法

7.3　一如终审法院在*香港特别行政区　诉　黄得强*（*HKSAR v Wong Tak Keung*，"***黄得强案***"）中述明：

> "一般规则是法庭的刑事司法管辖权受地域所限……这规则适用于普通法罪行及法定罪行。没有域外法律效力的有力推定，在解释订立罪行的法例时适用。"[2]

1　Susan W Brenner and Bert-Jaap Koops, "Approaches to Cybercrime Jurisdiction" (2004) Vol 4, No 1, Journal of High Technology Law，第 5 页；Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd edition, 2015), 第 475 页；David Harvey, *internet.law.nz selected issues* (LexisNexis NZ Limited, 4th edition, 2015)，第 6.206 段；以及 Alisdair A Gillespie, *Cybercrime: Key Issues and Debates* (Routledge, 2016)，第 21 页。

2　(2015) 18 HKCFAR 62，第 74 及 75 页（第 27 及 28 段），FACC 8/2014（判决日期：2015 年 1 月 9 日）。

7.4 因此，一般而言，*"刑事司法管辖权的行使范围不会延伸至涵盖在外地所作的作为"*。[3] 加拿大最高法院（Supreme Court of Canada）在 *Libman v The Queen* 中评述如下：

> "……刑事法的属地管辖原则，是法庭为了回应两项实际考虑而建构的。首先，一个国家一般与外地不法分子的行动甚少会有直接关系。其次，假如某国试图规管那些全部或绝大部分在别国境内发生的事宜，别国或会理所当然感到不悦。基于这些原因，法庭采纳法律在领土以外不适用的推定……"[4]

7.5 除了整体上遵守属地管辖原则外，不少国家亦声称对在悬挂有关国家国旗的船舶上和在该国注册的飞机上所犯的罪行具有司法管辖权，因为这些船舶和飞机*"经常视为该国领土的延伸"*。[5] 在香港，法例确认这类延伸的属地概念：

(a) 根据《航空保安条例》（第 494 章）第 3(1)条：

> "在正在航行但并非在香港境内或上空航行的香港控制的飞机上发生的任何作为或不作为，假如在香港境内发生便会构成香港法律下的某罪行的，即构成该罪行。"

(b) 根据《刑事罪行条例》（第 200 章）第 23B(1)条：

> "任何人的任何作为如——
>
> (a) 在处于公海的香港船舶上作出；及
>
> (b) 无本条则不属一项罪行；及
>
> (c) 在香港作出的情况下，根据香港法律会构成一项罪行，
>
> 则在符合第(5)及(7)款的规定下，无论该人具有何种公民身分或属何种国籍，该作为均构成该项罪行。"

---

3 *Treacy v DPP* [1971] AC 537，第 552 页。

4 *Libman v The Queen* [1985] 2 SCR 178，第 208 页 f 行。

5 《说明报告》第 235 段。

7.6 不幸的是，罪案*"的源头及影响已不再局限于以本地为主"*，而且*"正在以国际规模谋划"*。[6] 某项罪行相当可能只有部分元素在某司法管辖区内发生，而其他元素则在其他地方发生。在"后果罪行"的案件中：

> "如被告人作出受禁行为，造成受禁后果……而有关行为及后果在两个不同的司法管辖区内发生……传统观点认为，这一类罪行须当作仅在罪行完成的地点所犯——也就是最终主要元素发生的地方——这通常称为'终点观点'。"[7]

7.7 然而，加拿大最高法院在 *Libman* 案中采纳较具弹性的观点，拉福里斯特法官（La Forest J）代表该法院说明如下：

> "本席对于属地限制的观点或可概括如下：本席认为，若要某罪行受本国法庭的司法管辖权规限，所需的是构成该罪行的活动的重大部分在加拿大发生。正如现代学者指出，罪行与这个国家之间有'真实及密切联系'便已足够，这是国际公法及国际私法中众所周知的验证标准……"[8]

7.8 其他普通法司法管辖区自此相继仿效，采纳某些比墨守属地管辖原则更具弹性的观点。例如：

(a) 在 *Lipohar v R* 中，[9] 具关键性的事实牵涉多个澳大利亚州份，因而涉及多个司法管辖区。高等法院的多数法官裁定维持上诉人（被告人）在南澳大利亚的定罪，并对司法管辖权的问题评论如下：

> "在本案中，争论点是控罪的主要内容与南澳大利亚之间是否有足够联系。那是探究联系的因素是否足够的问题，当中不涉假定或推定……应灵活应用有关联系的规定，只要与有关司法管辖区有真实联系便已足够。"[10]

(b) 在英格兰及威尔斯，上诉法院（刑事法庭）（Court of Appeal

---

6 *Liangsiriprasert v United States* [1991] 1 AC 225，第 251 页 C 行。
7 见上文注脚 2，第 77 页（第 33 段）。
8 [1985] 2 SCR 178，第 212 页 j 行至 213 页 a 行。
9 [1999] HCA 65。
10 [1999] HCA 65，第 122 及 123 段。

(Criminal Division)) 在 *R v Smith (Wallace Duncan)(No 4)* 中裁定，英格兰的法庭可在以下情况下，行使司法管辖权：

> "……假如最后的作为在英格兰发生，或该罪行的绝大部分〔在英格兰〕所犯，而且并无出于相互尊重的理由而令该罪行不应〔在英格兰〕审讯。"[11]

(c) 在香港，终审法院在*黄得强*案认同英格兰及威尔斯采纳的观点：

> "……暂委法官司徒冕在 *HKSAR v Chan Shing Kong* 中认为，这项源自 *R v Smith (No 4)* 的较宽松观点比较可取，上诉法庭在 *HKSAR v Krieger* 的附带意见中亦表示赞同，两者依我们看来皆是正确之举。"[12]

订明司法管辖权规则的香港法例

7.9 终审法院在*黄得强*案中亦指出，法庭的刑事司法管辖权受地域所限这一般规则，*"可经法律修改"*。[13] 例如，根据《刑事司法管辖权条例》（第 461 章）（**《刑事司法管辖权条例》**）：

(a) 第 2(2)条把《盗窃罪条例》（第 210 章）及《刑事罪行条例》（第 200 章）所订若干欺诈和不诚实的实质罪行，界定为甲类罪行；[14] 及

(b) 第 3 条规定，就任何甲类罪行而言，只要任何*"有关事情"*，或即是说：

> "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）"

是在香港发生的，即使该罪行的其他主要元素在香港以外的任何地方发生，任何人亦可因犯该甲类罪行而被判有罪。

---

11 [2004] QB 1418，第 1434 页 H 行。

12 见上文注脚 2，第 81 页（第 45 段）。

13 同上，第 75 页（第 29 段）。

14 与串谋、企图犯罪及煽惑他人的初步罪行（即第 2(3)条的乙类罪行）互相对照。

7.10 概念上，《刑事司法管辖权条例》第 3 条至少涵盖下述两种情况：

(a) 在香港的人，对在香港境外的受害人（个人）或目标（电脑等物件）作出甲类罪行的部分犯罪行为；及

(b) 在香港境外的人，对在香港的受害人或目标作出部分犯罪行为。

7.11 前段第一种情况大致对应上文所讨论的普通法较宽松观点。第二种情况则可视为反映"客观属地管辖原则"，法庭可据此声称对*"在外地作出而在有关司法管辖区内造成影响的作为"*具有司法管辖权。[15]

7.12 2002 年，政府将《2002 年刑事司法管辖权条例（修订第 2(2)条）命令》拟稿提交予立法会批准。该命令拟稿旨在把以下三项电脑罪行列入甲类罪行：

(a) 《电讯条例》（第 106 章）第 27A 条所订的"藉电讯而在未获授权下取用电脑资料"罪；[16]

(b) 《刑事罪行条例》（第 200 章）第 59 及 60 条所订的与误用电脑有关的"摧毁或损坏财产"罪；[17] 及

(c) 《刑事罪行条例》（第 200 章）第 161 条所订的"有犯罪或不诚实意图而取用电脑"罪。[18]

然而，由于立法会相关小组委员会不支持这份命令拟稿，上述建议最终未有落实。[19]

7.13 除了《刑事司法管辖权条例》外，某些其他条例亦载有条文，就特定罪行订明司法管辖权事宜。例如：

(a) 《刑事罪行条例》（第 200 章）附表 2 载有一系列性罪行

---

15 Ian Walden, *Computer Crimes and Digital Investigations* (Oxford University Press, 2007)，第 5.27 段；类似看法见 Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd edition, 2015)，第 477 页。

16 于第 2 章（第 2.11 段）论述。

17 于第 4 章（第 4.7 段）和第 5 章（第 5.7 段）论述。

18 于第 2 章（第 2.6 段）论述。

19 根据立法会小组委员会于 2004 年 6 月 25 日的报告，一名委员不支持该命令拟稿，因为她认为就电脑罪行的扩大司法管辖权订定的条文，应编在新订的综合条例内，而非在《刑事司法管辖权条例》内。其他某些委员亦同意她的看法。另一委员认为，修订《刑事司法管辖权条例》所载罪行的机制（即由行政长官会同行政会议制定命令，但须事先提交立法会以决议通过），不及三读程序可取。

条文，凡若干类别的人干犯该等罪行，或该等罪行是就若干类别的人而干犯的，该等罪行条文便会具有域外法律效力。

(b) 根据《防止贿赂条例》（第 201 章）第 4 条，任何人"*（不论在香港或其他地方）*"无合法权限或合理辩解，提供任何利益；或任何公职人员"*（不论在香港或其他地方）*"无合法权限或合理辩解，索取或接受任何利益，作为（例如）诱因或报酬，即属犯罪。

普遍获接受的域外管辖权基础

7.14 域外管辖权有四个普遍获接受的基础：

(a) 主动属人管辖原则（建基于犯罪者的国籍）；

(b) 被动属人管辖原则（建基于受害人的国籍）；

(c) 普遍管辖原则，即任何国家对最严重的罪行（例如反人道罪）应具有司法管辖权；及

(d) 保护管辖原则，即一个国家对威胁其国家安全或利益的作为（即使该作为在该国以外发生）应具有司法管辖权。[20]

与电脑网络罪行相关的司法管辖权事宜

电脑网络罪行带来的挑战

7.15 在电脑网络空间发动跨司法管辖区的袭击，资金门槛和技术门槛并不高，这也是电脑网络罪行通常涉及多个司法管辖区的部分原因。表面看来是某国家内的电脑网络罪行案件，亦可能涉及（例如）：

(a) 在另一司法管辖区的互联网伺服器；或

(b) 总部设于另一司法管辖区的服务供应商（例如社交媒体或通讯软件的营运者）。

7.16 就电脑网络罪行而言，要决定某项事实在何处发生可能不易。例如，云端计算的运作方式，是"*所要求的数据未必处于单一位*

---

[20] Alisdair A Gillespie, *Cybercrime: Key Issues and Debates* (Routledge, 2016)，第 23 页；类似看法见 Ian Walden, *Computer Crimes and Digital Investigations* (Oxford University Press, 2007)，第 5.27 段。

置，而是分散于多个位置"。[21] 在受害人储存于云端的数据被非法取览的案件中，联合国毒罪办《网络犯罪综合研究》（Comprehensive Study on Cybercrime）的以下评述恰当贴切：

> "云数据的处理涉及多个分布在不同国家法域的数据场所或数据中心，而且涉及到不同的私有数据控制者和处理者。在当前条件下，尽管数据地点从技术上讲是可知的，但云计算用户并非总会被告知自己的数据到底存于'何处'。而且，各国对待有关云服务提供商所持数据的数据保护机制和对待关于国家执法侦查活动的管辖方式非常复杂。"[22]

法庭确认电脑网络罪行的挑战

7.17 法庭早已意会经常在电脑网络罪行出现的司法管辖权事宜。例如，英格兰上诉法院在 *R v Governor of Brixton Prison and Another, Ex parte Levin* 中有以下论述：

> "如某项指令几乎是即时性的，并旨在于有关电脑所处的地方生效，若然把指令输入磁碟这事视为只是在键盘所处的遥远地方进行，我们认为未免流于牵强。"[23]

---

21 Alisdair A Gillespie, *Cybercrime: Key Issues and Debates* (Routledge, 2016)，第 25 页。

22 联合国毒罪办，《网络犯罪综合研究》（2013 年 2 月），第 167 页。

23 *R v Governor of Brixton Prison and Another, Ex parte Levin* [1997] QB 65，第 82 页 E 行。上议院后来维持上诉法院的判决，见[1997] AC 741。

7.18　澳大利亚维多利亚最高法院（Supreme Court of Victoria）的基尔勒法官（Gillard J）在 *DPP v Sutcliffe* 中亦表达类似意见：

> "科技已发展至通讯可于一秒内遍达全球的阶段。互联网提供了迅速快捷且相对便宜的通讯方式，让可以取用电脑及电话线的人互相通讯。取用不只限于拥有电脑，企业纷纷以低廉收费提供接达互联网的服务。法律须随着这些转变而发展。"[24]

7.19　*R v Sheppard and Whittle* 的上诉人（被告人）被裁定发布煽动种族仇恨材料罪名成立，违反英格兰及威尔斯《1986 年公安法令》（Public Order Act 1986）第 19 条。涉案材料在互联网上发布。以下在判词中提到的大律师陈词，阐明要断定发布内容应视为在何处发布，有多种可能性：

> "戴维斯先生（Mr Davies）在陈词指出，关于互联网上的发布，主要有三套法学理论。第一，发布只可在其寄存的网页伺服器所在的司法管辖区内审理——来源国理论。第二，互联网上的发布，可在能够下载该项发布的任何司法管辖区内审理——目的国理论。第三，发布除了必然可在其寄存的网页伺服器所在的司法管辖区内审理之外，亦可在该项发布所针对的司法管辖区内审理——指向和针对理论。"[25]

7.20　*Dow Jones and Co Inc v Gutnick*[26] 虽是民事案件，但引述此案亦有助说明。案情关于指称的诽谤性材料在位于美国新泽西的道琼斯（Dow Jones）网页伺服器上发布，但在澳大利亚下载。澳大利亚高等法院裁定，这宗诽谤申索可由澳大利亚的法庭审理，理由是：

24　[2001] VSC 43，第 62 及 63 段。

25　[2010] 1 Cr App R 26，第 402 页。英格兰上诉法院因应案情而信纳它具有司法管辖权，因此拒绝进一步探讨该大律师提出的理论。

26　(2002) 210 CLR 575。

"如属万维网上的材料，直至某人使用网页浏览器把该材料从网页伺服器下载至电脑，该材料才会以可理解的形式提供。也就是在该人下载该材料的地方，声誉才可能会受到损害。因此，该处通常是诽谤侵权行为发生的地方。"[27]

7.21 网上材料在世上任何地方均可能下载得到。假若指称诽谤性的网上发布关乎某在多个司法管辖区均享有声誉的人，如该等司法管辖区各自的法庭采用澳大利亚高等法院的上述理据，便可主张对该项发布具有司法管辖权。*Gutnick* 案的判决*"引起不少争议"*，[28] 例如有评论员警告，该项判决可能会*"对互联网上的言论造成寒蝉效应"*，[29] 另一评论员亦指，该项判决*"凸显澳大利亚与美国法律在互联网司法管辖权上的分歧"*。[30]

7.22 不论采用哪一套司法管辖权原则，行使域外管辖权均须合乎情理，以免涉及*"在没有充分理由下干预别国主权"*。[31] 国际间打击跨境罪案时，应务求避免和解决司法管辖权的消极冲突（即没有国家声称对某宗罪案具有司法管辖权）及司法管辖权的积极冲突（即多个国家声称对某宗罪案具有司法管辖权）。[32] 实际上，解决后一类冲突亦可防止有关司法管辖区出现一罪两审的问题。[33]

---

27 同上，第 607 页（第 44 段）。

28 Richard Garnett, "*Dow Jones & Company Inc v Gutnick*: An Adequate Response to Transnational Internet Defamation?" (2003) 4(1) Melbourne Journal of International Law 196。*Gutnick* 案判决后，学术界多年来对该案一直争论不休。例如见 David Rolph, "Publication, Innocent Dissemination and the Internet after *Dow Jones & Co Inc v Gutnick*" (2010) 33(2) UNSW Law Journal 562 这文章。

29 Nathan W Garnett, "*Dow Jones & Co v Gutnick*: Will Australia's Long Jurisdictional Reach Chill Internet Speech World-Wide?" (2004) 13 Pac Rim L & Pol'y J 61，第 62 页。

30 Brian Fitzgerald, "*Dow Jones & Co Inc v Gutnick*: Negotiating 'American Legal Hegemony' in the Transnational World of Cyberspace" (2003) 27(2) Melbourne University Law Review 590。

31 Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd edition, 2015)，第 483 及 485 页。

32 Susan W Brenner and Bert-Jaap Koops, "Approaches to Cybercrime Jurisdiction" (2004) Vol 4, No 1, Journal of High Technology Law，第 40 及 41 页。

33 如某人就某项罪行曾获判无罪或被定罪，而后來又被控以同一罪行，禁止一罪兩审的规则即告适用，控方因而不得检控该人。这项规则亦适用于在另一司法管辖区曾被定罪或获判无罪的情况。正如终审法院在*杨振邦及其他人 诉 律政司司长*（*Yeung Chun Pong & Others v Secretary for Justice*）(2009) 12 HKCFAR 867 中确认，如*"某人面临第二次审讯，而该次审讯源于与较早前审讯相同或大致相同的事实，不论该较早前审讯是在同一司法管辖区内进行，还是在另一司法管辖区具管辖权的法院内进行"*，法庭亦有酌情决定权，以司法程序遭滥用为理由而搁置检控（第 21 段）。

《布达佩斯公约》的司法管辖权规则

7.23 《布达佩斯公约》[34] 第二十二条订明成员国应如何处理有关第二至十一条所订罪行的司法管辖权事宜。

> "1 在下列情况下，各缔约方均应采取必要的立法及其他措施，对按照本公约第二至十一条订立的任何罪行确立司法管辖权：
>
> a 该罪行发生在其领土内；或
>
> b 该罪行发生在悬挂该缔约方旗帜的船舶上；或
>
> c 该罪行发生在根据该缔约方法律注册的飞机上；或
>
> d 该罪行由其国民所犯，而该罪行根据犯罪地点的刑事法律可予惩处，或该罪行在任何国家的领域管辖权以外发生。
>
> 2 各缔约方可保留权利，完全不应用或只在特定案件或条件下才应用本条第 1.b 至 1.d 段或其任何部分所订的司法管辖权规则。
>
> 3 各缔约方均应采取必要的措施，在指称罪犯在其领土内，而其在接获引渡请求后仅因该人的国籍而不予引渡至另一缔约方时，确立其对本公约第二十四条第 1 段所指罪行的司法管辖权。
>
> 4 本公约不排除缔约方根据其本土法律行使的任何刑事司法管辖权。
>
> 5 如多于一个缔约方声称对按照本公约订立的某项指称罪行具有司法管辖权，有关缔约方须在适当的情况下进行磋商，以期决定最适合提出检控的司法管辖区。"

7.24 第二十二条第 1a 至 1c 段体现属地管辖原则，并显示这项原则延伸至船舶和飞机，上文在考虑司法管辖权的一般原则时，已讨论此点。第 1d 段则以主动属人管辖原则为前提。

---

[34] 有关《布达佩斯公约》的背景资料，见导言第 11 段，以及第 1 章第 1.6 至 1.10 段。

7.25　第 1d 段的第一项限制条款（*"而该罪行根据犯罪地点的刑事法律可予惩处"*），揭示不少国家的引渡法律均有双重犯罪的规定。如在香港应用有关规定，即是指根据某作为作出的地方的法律，以及根据香港法律，该作为均须属罪行，香港的法庭方可行使司法管辖权。[35] 就引渡而言，上议院在 *Norris v Government of the United States of America* [36] 中述明，双重犯罪规定的背后理念是：*"人身自由不得因被请求国根本不承认属刑事的罪行而受到限制"*。[37]

7.26　《说明报告》对第二十二条其他部分的评注如下：

> "237. 第 2 段容许缔约方就第 1 段 b、c 及 d 项定下的司法管辖权基础作出保留。然而，对于根据 a 项确立领域管辖权，或对于根据第 3 段在属于'引渡或检控'（'*aut dedere aut judicare*'）原则下的情况（即该缔约方因指称罪犯的国籍而拒绝引渡，而该罪犯身处其领土内）确立司法管辖权的责任，则不得作出保留。根据第 3 段确立司法管辖权有其必要，以确保如请求引渡的缔约方提出要求，拒绝引渡国民的缔约方在法律上有能力依据本公约第二十四条（'引渡'）第 6 段的规定在其本土进行调查和法律程序作为替代。
>
> ……
>
> 239. 在使用电脑系统犯罪的情况下，有时候会有多于一个缔约方对有关罪行的部分或全部参与者具有司法管辖权。例如，不少利用互联网进行的病毒攻击、欺诈及侵犯版权行为均以多国的受害人为目标。为免工作重迭、对证人造成不必要的不便，或令有关各国的执法官员互相竞争，又或是为了利便法律程序高效公平地进行，受影响的缔约方应进行磋商，以决定适合提出检控的地方。在某些情况下，有关国家选择单一检控地是最有效的做法；在另一些情况下，最佳做法则可能是由某国家检控部分参与者，另一（些）国家则检控其他参与者。两个结果皆为这一段所准许。最后，进行磋商并非一项绝对责任，而是应'在适当的情况下'进行。因此，假如其中一个缔约方知道进行磋商并无必要（例如，它

35　《刑事司法管辖权条例》并没有就甲类罪行（一般传统欺诈及不诚实罪行）施加双重犯罪的规定。

36　[2008] 1 AC 920。

37　同上，第 954 页 H 行。

获另一缔约方确认，该方并无计划采取行动），或假若有缔约方认为进行磋商会有损它进行的调查或法律程序，则可延迟或拒绝进行磋商。"[38]

7.27 上述《说明报告》内的评注反映国际间的普遍做法。根据联合国毒罪办《网络犯罪综合研究》，各国表示，*"它们通常会通过与其他国家的正式和非正式磋商来解决管辖权纠纷这一问题，从而防止双重调查和管辖权冲突"*。[39] 尽管各国普遍并无为解决电脑网络罪行案件的司法管辖权冲突而制定特定法例，[40] 部分地区的文书就国与国之间的法律合作可考虑的因素提供指引。[41]

7.28 根据《基本法》，[42] 中央人民政府负责管理与香港有关的外交事务，而香港获授权依照《基本法》自行处理有关的对外事务。[43] 因此，如香港在有关的对外事务范围以外与外国政府磋商和签订任何双边协议，须获得中央人民政府授权，并由中华人民共和国外交部驻香港特派员公署（"**外交部驻港公署**"）协助。[44] 在任何有关协议签订之前，我们预计，如我们的建议获政府落实推行，相关执法机构及检控机关便会援引新订电脑网络罪行法例分别就五类依赖电脑网络的罪行订明的司法管辖权规则，[45] 而禁止一罪两审的规则适用于在另一司法管辖区曾被定罪或获判无罪的情况，如同适用于在香港曾被定罪或获判无罪的情况。[46]

---

38 《说明报告》第 237 及 239 段。

39 联合国毒罪办，《网络犯罪综合研究》（2013 年 2 月），第 240 页。

40 见上文注脚 39。

41 例如，《欧洲联盟理事会关于攻击信息系统行为的第 2005/222/JHA 号框架决定》（Council Framework Decision 2005/222/JHA on attacks against information systems in the European Union）第 10(4)条及《阿拉伯国家打击信息技术犯罪问题公约》（Arab Convention on Combating Information Technology Offences）（2010 年 12 月 21 日）第 30(3)条列出以下因素：

(i) 有关罪行扰乱其安全或利益的国家；
(ii) 有关罪行在其境内发生的国家；
(iii) 犯罪者是其国民的国家；
(iv) 在其境内发现犯罪者的国家；及
(v) （如情况类似）首个请求引渡的国家。

42 见第十三条及第七章。

43 按照第一百五十一条的规定，有关的对外事务包括在经济、贸易、金融、航运、通讯、旅游、文化、体育等领域同世界各国、各地区及有关国际组织签订有关协议。

44 外交部驻港公署的主要职责载于其网站，网址为 http://www.fmcoprc.gov.hk/chn/zjgs/gszn/202109/t20210903_8903490.htm（于 2022 年 5 月 3 日浏览）。

45 就该五类依赖电脑网络的罪行所建议的司法管辖权规则，分别概述于建议 11、12、13、14 及 15。有关这些规则的考虑，详情见第 7.71 至 7.100 段。

46 见上文注脚 33。

其他司法管辖区的法定体制

澳大利亚

《刑事法典》（联邦）第 15.1 条

7.29 在澳大利亚，《刑事法典》（联邦）（Criminal Code (Cth)）第 476.3 条订明，详列于第 15.1 条的*"扩大地域司法管辖权——甲类"*适用于第 10.7 部所订罪行（即各项电脑罪行）。第 15.1 条篇幅甚长，无需在此列出全文。先从第 15.1(1)条看起：

> "如联邦法律规定本条适用于某罪行，除非有以下情况，否则任何人不属干犯该罪行：
>
> (a) 构成有关指称罪行的行为：
>
> (i) 全部或部分在澳大利亚发生；或
>
> (ii) 全部或部分在澳大利亚的飞机或澳大利亚的船舶上发生；或
>
> (b) 构成有关指称罪行的行为，全部在澳大利亚境外发生，而该行为的后果：
>
> (i) 全部或部分在澳大利亚发生；或
>
> (ii) 全部或部分在澳大利亚的飞机或澳大利亚的船舶上发生；或
>
> (c) 构成有关指称罪行的行为，全部在澳大利亚境外发生，而：
>
> (i) 在有关指称罪行发生时，该人是澳大利亚公民；或
>
> (ii) 在有关指称罪行发生时，该人是藉或根据联邦法律或某州份或某领地的法律成立为法团的法人团体；或
>
> (d) 符合以下所有条件：
>
> (i) 有关指称罪行属附带罪行；

(ii) 构成有关指称罪行的行为，全部在澳大利亚境外发生；

(iii) 构成该附带罪行所关乎的主要罪行的行为，或该行为的后果，全部或部分在澳大利亚发生，或全部或部分在澳大利亚的飞机或澳大利亚的船舶上发生，或该人意图该行为或该行为的后果全部或部分在澳大利亚发生，或全部或部分在澳大利亚的飞机或澳大利亚的船舶上发生。”

7.30 概括第 15.1(1)条而言，澳大利亚的法庭可按以下原则，声称对主要罪行具有司法管辖权：

(a) 属地管辖原则（包括延伸至澳大利亚的船舶及飞机）；

(b) 客观属地管辖原则（构成罪行的行为在澳大利亚境外发生，但其后果在澳大利亚发生）；及

(c) 主动属人管辖原则(适用于澳大利亚的公民及法人团体)。

7.31 第 15.1(2)条接着订定适用于主要罪行的免责辩护：

“如联邦法律规定本条适用于某罪行，则在以下情况下，任何人不属干犯该罪行：

(aa) 有关指称罪行属主要罪行；及

(a) 构成有关指称罪行的行为，全部在外国发生，但并非在澳大利亚的飞机或澳大利亚的船舶上发生；及

(b) 该人：

(i) 并非澳大利亚公民；亦

(ii) 并非藉或根据联邦法律或某州份或某领地的法律成立为法团法人团体；及

(c) 在：

(i) 发生构成有关指称罪行的行为的外国；或

(ii) 发生构成有关指称罪行的行为的外国的部分；

并无该外国的有效法律或该外国部分的有效法律，订立任何相当于首述罪行的罪行。”

7.32 第 15.1(4)条的条文与第 15.1(2)条相若，但适用于附带罪行。[47] 简言之，凡是在澳大利亚境外发生的行为，如发生该行为的司法管辖区并无任何法律把该行为定为罪行，第 15.1(2)及(4)条共同为这类行为订立免责辩护。这两款大致上对应《布达佩斯公约》之下的双重犯罪规定。[48]

《刑事法典》（联邦）第 16.2 条

7.33 《刑事法典》（联邦）第 16.2 条（*“当行为视为部分在澳大利亚发生”*）进一步规定如下：

> “ 发送物件
>
> (1) 〔……〕
>
> 发送电子通讯
>
> (2) 就本部而言，任何人如将电子通讯或导致将电子通讯：
>
> (a) 从澳大利亚境外某点发送至澳大利亚某点；或
>
> (b) 从澳大利亚某点发送至澳大利亚境外某点；
>
> 则该行为视为部分在澳大利亚发生。
>
> 某点
>
> (3) 就本条而言，**某点**包括流动或可能流动的某点，不论是在陆上、地底、大气中、水底、海上或任何其他地方。”

7.34 如某人身处澳大利亚，并发送或导致发送电子通讯，则该行为即属在澳大利亚发生，类似于第 16.2 条的推定条文，并非必要。

---

47 《刑事法典》（联邦）末端的字典将附带罪行界定为*“(a)违反第 11.1、11.4 或 11.5 条的罪行；或(b)违反联邦法律的罪行，但以因第 11.2、11.2A 或 11.3 条实施而产生的罪行为限”*。维多利亚司法学院（Judicial College of Victoria）在其《维多利亚刑事法律程序指南》（Victorian Criminal Proceedings Manual）中述明，附带罪行一词主要*“关乎企图犯罪、煽惑他人、串谋，或依据合谋或共同目的或利用不知情的人而犯的罪行”*（第 1.3 节第 56 段）。

48 关于《布达佩斯公约》第二十二条第 1d 段的第一项限制条款，见第 7.25 段。

这显示第 16.2 条旨在适用于某人在作出有关行为时身处澳大利亚境外的情况。

7.35 如以广义解释第 16.2(2)条，该条实际效果似乎如下：

(a) 只要某人发送或导致发送的电子通讯以*"澳大利亚某点"*为来源地或目的地，即视为符合该人的行为*"部分在澳大利亚发生"*的司法管辖权准则。

(b) 就传入的电子通讯而言（即第 16.2(2)(a)条的情况），无需证明该通讯已进入澳大利亚。

(c) 就输出的电子通讯而言（即第 16.2(2)(b)条的情况），该通讯是否已离开澳大利亚无关宏旨。

7.36 另一解读可能是，须先证明有关电子通讯在部分关键时间，于澳大利亚出现，某人发送或导致发送该电子通讯的行为方可视为完成。这解读可能对传入电子通讯的情况有较大影响。

加拿大

《1985 年刑事法典》第 477.1 条

7.37 在加拿大，根据《1985 年刑事法典》（Criminal Code 1985）第 477.1 条（*"加拿大境外的罪行"*）：

> "如任何人作出某作为或不作为，而假使该作为或不作为在加拿大发生，便会属……联邦法律所订罪行，则在以下情况下，该人即当作在加拿大作出该作为或不作为：
>
> (a) 在加拿大专属经济区内，
>
> (i) 为了勘探或开采、保存或管理该加拿大专属经济区的天然资源……而身处该加拿大专属经济区的人作出该作为或不作为，及
>
> (ii) 该作为或不作为由身为加拿大公民或……永久性居民的人作出，或就身为加拿大公民或……永久性居民的人作出；
>
> (b) 该作为或不作为在加拿大的大陆架内的某地方或大陆架上方的某地方作出，而凭借《海洋法令》

（Oceans Act）第 20 条，该作为或不作为在该地方属犯罪；

(c) 该作为或不作为在加拿大境外，在根据任何国会法令注册或领牌或获发识别号码的船舶上作出，或藉根据任何国会法令注册或领牌或获发识别号码的船舶作出；

(d) 该作为或不作为在加拿大境外于紧追期间作出；或

(e) 加拿大公民在任何国家的领土外，作出该作为或不作为。”

7.38 上文第(a)至(e)段订明的情况当中，体现出主动属人管辖原则的(e)段似乎与电脑网络罪行案件最为相关。

《1985 年刑事法典》第 476(d)条

7.39 凡某罪行是在飞行中的飞机上所犯的，《1985 年刑事法典》第 476(d)条（*“特别司法管辖区”*）将该罪行视为在以下领域分区所犯：

“(i) 该次飞行开始的领域分区，[49]

(ii) 该飞机在该次飞行中经过其上空的任何领域分区，或

(iii) 该次飞行结束的领域分区”。

加拿大法庭作出审判的司法管辖权

7.40 《1985 年刑事法典》第 481.2 条（*“加拿大境外的罪行”*）订明，对于受加拿大法律的域外管辖权所规管的罪行，加拿大法庭审判该罪行的司法管辖权如下：

“除本国会法令或任何其他国会法令另有规定外，如某作为或不作为在加拿大境外作出，而根据本国会法令或任何其他国会法令，该作为或不作为如在加拿大境外作出即属犯罪的话，则不论被告人是否在加拿大，亦可在加拿大任何领域分区内就该罪行展开法律程序，并控告、

---

[49] 《1985 年刑事法典》第 2 条将“领域分区”界定为包括*“文意所适用的任何省、郡、联合郡、镇区、市、镇、教区或其他司法分区或地方”*。

审讯和惩处被告人，其方式犹如该罪行是在该领域分区内所犯一样。”

7.41 *Libman* 案中定下的普通法原则（于上文引述[50]）补充上述条文。根据该原则，加拿大的法庭会对与加拿大有*“真实及密切联系”*的罪行行使司法管辖权。

英格兰及威尔斯

概览

7.42 《英格兰误用电脑法令》：

(a) 在第 1、2、3、3ZA 及 3A 条订立五项罪行；并

(b) 在第 4 至 9 条处理司法管辖权事宜。

7.43 由于《英格兰误用电脑法令》所订的五项罪行各有不同司法管辖权规则，要概述该等规则并不直接简单。概括而言，根据第 4 条（*“本法令所订罪行的领域范围”*）：

(a) 须*“与本地司法管辖权有重大联系”*，方属犯以下条文所订罪行：

(i) 第 1 条（*“在未获授权下取览电脑资料”*）；

(ii) 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”*）；

(iii) 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”*）；

就上述罪行而言，就定罪而须予以证明的任何作为或其他事情是否在*“有关原属国”*[51] 发生，或被告人当时是否身在该处，均无关重要。[52]

(b) 至于第 2 条所订罪行（*“在未获授权下取览，并意图干犯或意图利便干犯其他罪行”*），当中的在未获授权下取览

---

50 第 7.7 段。

51 《英格兰误用电脑法令》适用于英格兰及威尔斯时（该法令同样适用于苏格兰及北爱尔兰），第 4(6)条将这词语界定为英格兰及威尔斯。

52 《英格兰误用电脑法令》第 4(1)条。

无需*"与本地司法管辖权有重大联系"*。[53] 然而，第 2(2)条[54] 显示，意图干犯的其他罪行，须属可根据英格兰法律审讯的罪行。

(c) 如第 3A 条所订罪行（*"制造、供应或取得用于第 1、3 或 3ZA 条所订罪行的物品"*）*"与本地司法管辖权有重大联系"*，则被告人在就该罪行定罪而须予以证明的任何作为或其他事情发生时，是否身处*"有关原属国"*，亦无关重要。[55]

"与本地司法管辖权有重大联系"的涵义

7.44 《英格兰误用电脑法令》第 5 条解释何谓*"与本地司法管辖权有重大联系"*。表面看来，这词组是一项统一概念，适用于第 1、3、3ZA 及 3A 条所订各项罪行。然而，*"与本地司法管辖权有重大联系"*的确切涵义及其含意，却视乎有关罪行而有所不同。这种联系可按第 5 条指明的以下其中一种形式体现：

(a) 被告人是英国国民，当时身处英国以外的国家，而根据该作为发生的国家的法律，被告人的作为构成罪行[56] ——这种形式是基于主动属人管辖原则，适用于第 1、3、3ZA 或 3A 条所订罪行；

(b) 被告人于作出有关作为时，身处*"有关原属国"*[57] ——这种形式反映属地管辖原则，适用于第 1、3 或 3ZA 条所订罪行；

(c) 目标电脑在*"有关原属国"*[58] ——这种形式包含客观属地管辖原则，适用于第 1、3 或 3ZA 条所订罪行；或

---

53 《英格兰误用电脑法令》第 4(3)条。

54 *"本条适用于以下罪行——*
(a) 刑罚为法律所固定的罪行；或
(b) 任何年满 21 岁（就英格兰及威尔斯而言，则为年满 18 岁）且无定罪纪录的人，可处为期 5 年监禁的罪行（或在英格兰及威尔斯，假若没有《1980 年裁判法院法令》〔Magistrates' Courts Act 1980〕第 33 条所施加的限制，则可被如此判刑的罪行）。"

55 《英格兰误用电脑法令》第 4(4A)条。

56 《英格兰误用电脑法令》第 5(1A)条。

57 《英格兰误用电脑法令》第 5(2)(a)、(3)(a)及(3A)(a)条。

58 《英格兰误用电脑法令》第 5(2)(b)、(3)(b)及(3A)(b)条。

(d) 未获授权的作为在*"有关原属国"*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[59] —— 这种形式体现了保护管辖原则，只适用于第 3ZA 条所订罪行。

7.45 鉴于上述机制错综复杂，第 4 及 5 条难免较为复杂。

双重犯罪

7.46 《英格兰误用电脑法令》所订的五项罪行有一个共通点，就是在英格兰及威尔斯的法庭可行使司法管辖权的多个可能事实情况当中，只有一个事实情况有双重犯罪的规定。至于双重犯罪的规定如何适用，该五项罪行可分为以下两组：

(a) 就第 1、3、3ZA 或 3A 条所订罪行而言，上文介绍的*"与本地司法管辖权有重大联系"*的第一种可能形式[60] —— 基于主动属人管辖原则 —— 含有双重犯罪元素，当中规定根据该作为发生的国家的法律，被告人的作为须构成罪行。

(b) 就第 2 条所订罪行而言，如上文所述，[61] 当中的在未获授权下取览无需*"与本地司法管辖权有重大联系"*。然而，第 8 条在以下情况下适用：

(i) 有人被指称犯了第 1 条所订罪行；而

(ii) 该罪行*"与本地司法管辖权有重大联系"*。[62]

第 8(1)条包含双重犯罪的规定：

> "如任何人意图作出或意图利便的事会涉及犯一项该事或其任何部分拟发生的地方的有效法律所订罪行，则该人只有在此情况下方被判犯了可凭借上文第 4(4)条审讯的罪行。"[63]

---

59 《英格兰误用电脑法令》第 5(3A)(c)条。

60 第 7.44(a)段。

61 第 7.43(b)段。

62 《英格兰误用电脑法令》第 4(4)条。

63 第 8(3)条的条文相若，但适用于该条详列的企图犯罪罪行：*"如任何人所构想的事会涉及犯该事或其任何部分拟发生的地方的有效法律所订的罪行，则该人只有在此情况下方被判犯了可凭借《1981 年企图犯罪法令》(Criminal Attempts Act 1981)第 1(1A)条审讯的罪行。"*

中国内地

《中国刑法》

7.47 适用于电脑网络罪行的司法管辖权规则，载于《中国刑法》第六至八条：

> "第六条 凡在中华人民共和国领域内犯罪的，除法律有特别规定的以外，都适用本法。
>
> 凡在中华人民共和国船舶或者航空器内犯罪的，也适用本法。
>
> 犯罪的行为或者结果有一项发生在中华人民共和国领域内的，就认为是在中华人民共和国领域内犯罪。
>
> 第七条 中华人民共和国公民在中华人民共和国领域外犯本法规定之罪的，适用本法，但是按本法规定的最高刑为三年以下有期徒刑的，可以不予追究。
>
> 中华人民共和国国家工作人员和军人在中华人民共和国领域外犯本法规定之罪的，适用本法。
>
> 第八条 外国人在中华人民共和国领域外对中华人民共和国国家或者公民犯罪，而按本法规定的最低刑为三年以上有期徒刑的，可以适用本法，但是按照犯罪地的法律不受处罚的除外。"

7.48 简言之，《中国刑法》容许法庭根据以下原则，对刑事罪行行使司法管辖权：

(a) 属地管辖原则（依据第六条包括犯罪的行为或结果在中国发生的情况，亦延伸至中国的船舶及飞机）；

(b) 主动属人管辖原则（依据第七条适用于任何中国公民）；及

(c) 被动属人管辖原则及保护管辖原则（依据第八条适用于针对中国公民及中国的犯罪，前提是有关罪行可处不少于三年有期徒期，并且符合双重犯罪的规定）。

新西兰

《新西兰法令》第 7 条

7.49 下列的《新西兰法令》第 7 条（*"犯罪地点"*），可与香港的《刑事司法管辖权条例》第 3 条对照：

> "就司法管辖权而言，如任何作为或不作为构成任何罪行的部分，并在新西兰发生，或完成任何罪行所必要的任何事情在新西兰发生，则不论被控该罪行的人在该作为、不作为或事情发生时是否身处新西兰，该罪行亦须当作在新西兰干犯。"

7.50 新西兰法律委员会（New Zealand Law Commission）在其有关误用电脑的报告书内，对第 7 条评述如下：

> "……我们认为，《1961 年刑事罪行法令》（Crimes Act 1961）现有的司法管辖权条文，并不足以处理误用电脑活动。首先，虽然有些情况是涉案黑客或电脑均并非位于新西兰，但误用电脑的影响却可出现在这个国家。在这些情况下，或不可能每次按照《1961 年刑事罪行法令》第 7 条的条文，均成功争辩'构成〔有关〕罪行的部分的任何作为或不作为，或完成〔有关〕罪行所必要的任何事情'是在新西兰内发生的。其次，在不少案件中，根本不可能判断涉案黑客在误用电脑活动发生时身在何处……我们建议应订立条文，赋予新西兰的法庭司法管辖权，审理在任何地方所犯的误用电脑罪行。"[64]

7.51 有评论员并不同意法律委员会这项建议，[65] 该项建议亦显然未有落实。虽然《新西兰法令》于 2002 年加入新订的第 7A 条（*"有*

---

64 新西兰法律委员会，*Computer Misuse: Report 54* (May 1999)，第 26 及 27 页。

65 David Harvey, *internet.law.nz selected issues* (LexisNexis NZ Limited, 4th edition, 2015)，第 6.221 段，注脚 239（*"……笔者认为这项〔建议〕适得其反……订立普遍的司法管辖权会在法律的灰色地带立下危险先例"*）。

关若干跨国罪行的域外管辖权"），[66] 但该项条文只适用于该法令订明的某些罪行，而当中并不包括第 249 至 252 条所订涉及电脑的罪行。

双重犯罪

7.52 《新西兰法令》第 7 条并无包含双重犯罪的原则，但该法令第 8 条（*"有关对新西兰境外船舶或飞机上的罪行的司法管辖权"*）却基于该项原则订定免责辩护，在此引述第 8(1)及(2A)条便足够：

> "(1) 本条适用于在新西兰境外——
>
> (a) 任何人在任何英联邦的船舶上作出的任何作为或不作为；或
>
> (b) 任何人在任何新西兰的飞机上作出的任何作为或不作为；或
>
> (c) 任何人在任何船舶或飞机上作出的任何作为或不作为，而该人在作出该作为或不作为的旅程途中或终结时，在该船舶或飞机上到达新西兰；或
>
> (d) 任何英籍人士在处于公海的任何外国船舶（并非该人所属的船舶）上作出的任何作为或不作为，或在处于任何英联邦国家领海内的任何该等船舶上作出的任何作为或不作为；或
>
> (e) 任何新西兰公民或通常居于新西兰的人在任何飞机上作出的任何作为或不作为：
>
> 但如某非英籍人士在任何船舶或飞机上作出该作为或不作为，而该船舶或飞机当时正用作非英联邦国家的任何武装部队的船舶或飞机，则(c)段并不适用。
>
> (2A) 凡凭借本条赋予的司法管辖权进行任何法律程序，如证明根据在有关作为或不作为发生时被告人属其国民或公民的国家的法律，该作为或不作为假若在该国发生便不属犯罪，即可以此作为免责辩护。"

---

[66] 第 7A 条反映延伸至船舶和飞机的属地管辖原则、主动属人管辖原则和被动属人管辖原则。

新加坡

《新加坡误用电脑法令》第 13 条

7.53 在新加坡，适用于《新加坡误用电脑法令》的司法管辖权规则载于第 13 条（*"本法令所订罪行的领域范围"*）：

> "(1) 除第(3)款另有规定外，本法令的条文对新加坡内外的任何人均具有效力，不论该人属何种国籍或具有何种公民身分。
>
> (2) 如任何人在新加坡境外任何地方犯本法令所订罪行，则可对该人作出处置，犹如该罪行是在新加坡所犯一样。
>
> (3) 为施行本条，本法令在以下情况下适用——
>
> (a) 就有关罪行而言，被告人在关键时间处于新加坡；
>
> (b) 就有关罪行（即第 3、4、5、6、7 或 8 条所订罪行）而言，有关电脑、程式或数据在关键时间处于新加坡；或
>
> (c) 该罪行导致在新加坡的严重损害，或产生导致在新加坡的严重损害的重大风险。
>
> (4) 在第(3)(c)款中，*"在新加坡的严重损害"*指——
>
> (a) 在新加坡的个人患病、受伤或死亡；
>
> (b) 干扰新加坡任何主要服务供应，或严重削弱公众对新加坡任何主要服务供应的信心；
>
> (c) 干扰政府、国家机关、法定委员会（或政府、国家机关或法定委员会的任何部分）执行任何职务或职能或行使任何权力，或严重削弱公众对政府、国家机关、法定委员会（或政府、国家机关或法定委员会的任何部分）执行任何职务或职能或行使任何权力的信心；或
>
> (d) 损害新加坡的国家安全、防务或对外关系。

……

(5) 就第(3)(c)款而言，导致在新加坡的严重损害的罪行是否——

(a) 直接导致该损害；或

(b) 该损害的唯一或主要成因，

均属无关重要。

(6) 在第(4)(b)款中，'主要服务'指以下任何服务：

(a) 与通讯基础建设、银行及金融服务、公共事业、公共交通、陆上运输基础建设、航空、船运或公开密码匙基础建设直接有关的服务；

(b) 警务、民防或卫生服务等紧急服务。

(7) 在第(4)(c)款中，'法定委员会'指由任何公共法令成立以执行或履行公共职能的法团或并非法团的团体，或根据任何公共法令成立以执行或履行公共职能的法团或并非法团的团体。"

7.54 学术界对第 13 条发表以下意见：

"第 1 及 2〔款〕赋予该法令无限的域外法律效力，但第 3〔款〕则可理解为限制第 1 及 2〔款〕的适用范围。只有与罪行有关的犯罪者、电脑、程式或数据在罪行发生时处于新加坡，该法令方会适用。不过，法令的适用范围依然甚广。数据在关键时间须处于新加坡这项规定，可与西弗吉尼亚订明数据须在传送中经过该州的规定比照。"[67]

在新加坡的严重损害

7.55 如上文所示，《新加坡误用电脑法令》第 13(4)条订明存在*"在新加坡的严重损害"*的四种情况。该法令就该等情况，在第 13(4)(b)及(c)条提供以下例子：[68]

---

67 Susan W Brenner and Bert-Jaap Koops, "Approaches to Cybercrime Jurisdiction" (2004) Vol 4, No 1, Journal of High Technology Law, 第 21 页。

68 根据《诠释法令》（Interpretation Act）第 7A 条（*"例子及说明"*）：

"例 1.——以下例子中的作为，严重削弱公众对主要服务供应的信心，或产生严重削弱公众对这方面的信心的重大风险：

(a) 向公众发布新加坡某医院的病人医疗纪录；

(b) 向公众提供查阅新加坡某银行的客户帐户号码的途径。

例 2.——以下例子中的作为，严重削弱公众对政府、国家机关、法定委员会（或政府、国家机关或法定委员会的任何部分）执行任何职务或职能或行使任何权力的信心，或产生严重削弱公众对这方面的信心的重大风险：

(a) 向公众提供查阅属政府某部门的机密文件的途径；

(b) 向公众发布属于某法定委员会的电脑的取用码。"

7.56 有关司法管辖权乃基于*"罪行导致在新加坡的严重损害，或产生导致在新加坡的严重损害的重大风险"*[69]提出，这体现了保护管辖原则。

美国

《电脑欺诈及滥用法案》（《美国法典》第 18 篇第 1030 条）

7.57 正如之前各章所述，在美国，规管电脑网络罪行的主要联邦法例是《电脑欺诈及滥用法案》（Computer Fraud and Abuse Act），编纂于《美国法典》第 18 篇第 1030 条。

7.58 《电脑欺诈及滥用法案》所订的罪行，不少是指（或包括）作出侵害*"受保护电脑"*的特定刑事作为。第 1030(e)(2)条将*"受保护电脑"*界定为：

"(A) 某财务机构或美国政府专用的电脑，或如属并非如此专用的电脑，则指由某财务机构或美国政府所使用或为其而使用的电脑，而构成有关罪行的行为会

"如某法令包括某条文施行的例子或说明——
(a) 该例子或说明不得视为并无遗漏；及
(b) 如该例子或说明与该条文不相符，则以该条文为准。"

69 《新加坡误用电脑法令》第 13(3)(c)条。

影响由该财务机构或美国政府对该电脑的使用或为其而对该电脑的使用；

(B) 用于或影响州际或对外贸易或通讯的电脑，包括位于美国境外而以影响美国州际或对外贸易或通讯的方式使用的电脑；或

(C) 符合以下说明的电脑——

(i) 属投票系统的一部分；及

(ii) (I) 用作联邦选举的管理、支援或行政；或

(II) 曾在州际或对外贸易中运作或在其他方面影响州际或对外贸易"。

7.59 上文引述的第 1030(e)(2)(B)条中，*"对外"*一词在 *United States v Ivanov*[70] 中解释为国际的意思。有评论员提出以下论点：

"这可能会大幅扩大联邦域外法律的适用范围，因为任何连接上互联网的电脑均可说是用于或影响州际或对外通讯，而有关电脑甚至无需位于美国。只要该电脑连接上互联网，便可形容为以影响美国州际通讯或内外通讯的方式使用。"[71]

7.60 尽管案例已厘清《电脑欺诈及滥用法案》的域外范围，但如要加入有关域外法律效力的提述，*"受保护电脑"*的法定定义似乎并非最适当的位置。本章检视的其他司法管辖区，均已订立特定法例条文，以处理司法管辖权事宜。

案例中的客观属地管辖原则

7.61 另外，法庭在 *Ivanov* 案中亦确认了客观属地管辖原则：

"本案中，伊云洛夫（Ivanov）在公诉书内被控的实质罪行，其拟造成或实际造成的不利影响全部在美国境内发生……纵使〔目标〕电脑是被人藉着从〔美国境外的〕远处发起和控制的繁复程序所取用，亦不改取用电脑的

---

70 175 F Supp 2d 367 (D Conn 2001)。

71 Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd edition, 2015)，第 479 页；类似看法见 Ian Walden, *Computer Crimes and Digital Investigations* (Oxford University Press, 2007)，第 5.18 段（*"这实际上是把领域范围延伸至全球，因为任何连接上互联网的电脑均可能包括在内"*）。

行为（即法规禁止的部分不利影响）是在该等电脑实际所在的地方（即位于康涅狄格弗农〔Vernon〕……）发生这一事实。”

小组委员会的看法

初步考虑

新法例应订明司法管辖权规则

7.62 在电脑网络罪行案件中，犯罪者在一个实际地点进行的作为，可透过互联网在短时间内影响多个实际地点的无数受害人，当中可能涉及电脑网络空间的大量通讯。我们认为，电脑网络罪行的性质，充分支持香港法律适用于域外范围。

7.63 为防止日后的法律程序出现争议，新法例应明确订明适用于所订罪行的司法管辖权规则。这做法兼具教育和阻吓作用，因为任何存心在多个司法管辖区干犯该等罪行的人，便会知道香港的法律立场。

7.64 例如，假若新法例应规定在香港境外的人如入侵在香港的电脑，便属干犯香港法律所订罪行，那么该人若前往香港，便可被拘捕。如该人一直留在香港的司法管辖区范围以外，香港的执法机关可适时向其他司法管辖区的执法机关寻求协助。

7.65 在上述例子中，我们明白该人的作为在该作为作出的地方，可能并不构成罪行。撇开可能与双重犯罪原则相关的问题不谈，我们认为，如该作为对香港造成影响，便有理由支持根据香港法律将该作为定为罪行。[72] 按照我们指导原则的精神，[73] 任何人作出任何作为的权利，须与保障公众免因该作为而可能受害的需要互相平衡，当中须衡量该作为所造成的伤害，与法律对该人作出该作为的权利所拟施加的限制比较，是否更为重大和带来更严重损害。

有理由制定限制较少的司法管辖权规则

7.66 当执法机关决定是否向其他司法管辖区寻求协助时，实际上会考虑该等司法管辖区的执法机关会如何回应。我们知悉，由于大规

---

72 例如因为目标电脑处于香港。

73 导言第 12 段。

模的电脑网络罪行案件在香港并不常见，因此这类协助请求通常并不可行。即使案中损失总额庞大，每名受害人所涉的金钱价值可能不高。

7.67 在上述背景下，据我们理解，如新法例包含多种司法管辖权规则，执法机关及检控部门均认为会有用处。背后的想法是，假如司法管辖权规则设有太多限制，以致香港的罪行不适用于若干应受谴责的行为，便会完全无法提出检控。相比之下，假若罪行适用于这些行为，而检控部门保留酌情权，决定应否提出检控，这做法较为可取，亦可为公众提供保障，切合我们的指导原则。

应专门制定切合各项罪行的司法管辖权规则

7.68 与此同时，我们的比较研究显示，国际惯例是司法管辖区在合理范围内，为其法律的任何域外应用订定条文，这与普通法一般奉行属地管辖原则的做法一致。例如：

(a) 新西兰法律委员会曾建议新西兰的法庭对于在任何地方所犯的误用电脑罪行一律具有司法管辖权，但这项建议显然未有落实。[74]

(b) 虽然《新加坡误用电脑法令》第 13(1)及(2)条似乎赋予该法令无限的域外法律效力，但该等条文的适用范围受第 13(3)条所限。[75]

如有关电脑网络攻击与香港并无任何事实联系及因果联系，香港法律似乎并无理据规管在其他司法管辖区发动，并针对第三方司法管辖区内目标的电脑网络攻击。

7.69 我们认为，香港依循上述国际惯例，亦属恰当。在相互尊重的原则下，香港应能够向其他司法管辖区据理解释其法律立场。我们亦紧记需要顾及不同持份者的利益，而该利益可能会视乎有关罪行而有所不同。因此，我们参照以下事实情况，依次讨论本咨询文件所建议的罪行：[76]

---

74 第 7.50 至 7.51 段。

75 第 7.53 至 7.54 段。

76 为方便讨论，每种事实情况所述的事实，均假定为该事实情况与香港的仅有联系，实际案件可能在多于一种事实情况下发生。

(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；[78]

(b) 犯罪者是"香港人"；[79]

(c) 受害人是"香港人"；

(d) 目标电脑、程式或数据处于香港；及

(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）。

7.70 我们在讨论期间紧记一点，就是决定是否提议采用某种事实情况很大程度上涉及主观判断，并无绝对答案。就各项建议的罪行，我们所建议采用的司法管辖权规则载于下文。

非法取览程式或数据

事实情况(a)、(d)及(e)

7.71 我们认为将事实情况(a)、(d)及(e)应用于这项建议的罪行，应无争议。我们会于下文讨论事实情况(b)及(c)。

事实情况(b)

7.72 支持将事实情况(b)[80]应用于建议的非法取览程式或数据罪的论点是：香港法律应阻吓香港人非法取览储存于例如云端伺服器的数据（不论该伺服器实际位于何处），因为在电脑网络空间上，实际位置通常无关重要。例如，网上电邮系统普遍盛行，一般采用云端技术。云端伺服器已成为罪犯的主要目标，云端储存的重要性可能于未来数年超越普通储存。

7.73 然而，我们留意到，事实情况(b)亦涵盖犯罪者（尽管是"香港人"）、其作为、所用器材、有关数据和受害人全部处于香港境外

---

77 如以术语表达，即如《刑事司法管辖权条例》第 3(1)条所述明：*"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）"*。

78 这种情况会包括犯罪者、其作为及受害人全部均处于香港的案件。

79 其他司法管辖区的法例可能提述有关司法管辖区的国民或公民。就香港的情况而言，我们参考其他法律范畴的现有罪行，建议"香港人"这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。

80 犯罪者是"香港人"。

的案件，而没有任何“香港人”受害。香港的执法机关或难以取证和证明犯罪者的作为。正面来看，如案情严重，受影响司法管辖区的执法机关可能会采取行动，香港的执法机关会适时提供协助。

7.74 权衡所有因素之下，我们不建议将事实情况(b)应用于建议的非法取览程式或数据罪。

事实情况(c)

7.75 就这项建议的罪行而言，事实情况(c)[81] 引起谁是受害人的问题。举例来说，如某人在非洲对欧洲的云端伺服器进行黑客入侵，而该伺服器持有的数据由不同人（包括“香港人”）拥有，那么受害人应是该云端伺服器的拥有人，还是该等数据的拥有人？特别考虑到案中的黑客入侵不一定是针对该云端伺服器的任何特定使用者。

7.76 我们认为，受害人这概念应采用宽广的定义。在上述情况中，该云端伺服器的拥有人及该等数据的拥有人均应视为潜在受害人。此外，为与这项建议的罪行的焦点（非法取览*程式或数据*）一致，重点应是须予保护的数据，而不管最终应视谁人为受害人。

7.77 我们继而得出结论，将事实情况(c)应用于建议的非法取览程式或数据罪，是会有用处的。如采纳前段的考虑因素，只要云端伺服器的拥有人或有关数据的拥有人是“香港人”，这项建议的罪行便会基于事实情况(c)而适用。这个法律立场能尽量扩大这项建议的罪行所提供的保障范围。

双重犯罪

7.78 就这项建议的罪行而言，有人或会认为施加双重犯罪的规定是合理的做法，因为技术上来说，取览程式或数据可轻易发生。如某人在香港境外某地方所作的作为，在该地方并不构成罪行，若要求该人因着该作为而在香港就这项建议的罪行负上法律责任，未必恰当。

7.79 然而，相反的论点是，施加双重犯罪的规定可能有违加强保障公众这目的。除了检控部门需要证明被告人的作为，根据该作为作出的地方的法律属罪行之外，另一相关因素是，某些司法管辖区的法律标准未必能与香港的法律标准比拟。如设有双重犯罪的规定，有人或会故意在电脑网络攻击并不构成罪行的地方发动攻击，藉此逃避法律责任。香港可能最终会更易遭受这类电脑网络攻击。

---

81 受害人是“香港人”。

7.80 我们的比较研究显示，其他司法管辖区对于在电脑网络罪行法例中是否施加双重犯罪的规定，并没有任何主流或统一的做法。我们认为，要解决上述难题，关键在于意会*就严重罪行而言*，支持*不*施加双重犯罪的规定之理据较为有力。我们决定采取折衷方法，即双重犯罪的规定应适用于非法取览程式或数据的*简易程序*罪行，但不适用于*加重*罪行。由于后者涉及被告人在取览有关程式或数据后，意图进行其他犯罪活动，被告人难以辩称不施加双重犯罪的规定，会造成不公。

7.81 我们得出建议的非法取览程式或数据的简易程序罪行应设有双重犯罪的规定这看法时，整体上采纳了《刑事司法管辖权条例》第7条的精神，[82] 该条体现了香港法律下双重犯罪的概念。此外，我们认为，如犯罪者因在香港境外所作的作为而被控这项建议的简易程序罪行，该作为本身或连同就该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。

建议11

小组委员会建议，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皆是）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；

---

82 《刑事司法管辖权条例》第7条对乙类罪行的定罪施加双重犯罪规定，乙类罪行即第6(1)条所指的串谋犯甲类罪行或串谋诈骗，以及第6(2)条所指的企图犯甲类罪行或煽惑他人犯甲类罪行。第7条的内容是：

"(1) 如为实施所协定的行为过程而会在某个阶段涉及——

(a) 一方或超过一方的作为或不作为；或

(b) 其他事情的发生，

而根据在该作为、不作为或事情拟发生的地方的有效法律，该作为、不作为或事情是构成一项罪行的，则任何人只有在此情况下方被判犯了可凭借第6(1)条审讯的罪行。

(2) 如任何人所构想的事会涉及犯一项该事或其任何部分拟发生的地方的有效法律所订的罪行，则该人只有在此情况下方被判犯了可凭借第6(2)条审讯的罪行。"

(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。

非法截取电脑数据

事实情况(a)、(c)、(d)及(e)

7.82 基于上文就首项建议的罪行（非法取览程式或数据罪）所提出的类似理由，我们建议将事实情况(a)、(c)、(d)及(e)应用于建议的非法截取电脑数据罪。

事实情况(b)

7.83 事实情况(b)是犯罪者是"香港人"。就建议的非法截取电脑数据罪而言，其特色倾向支持将新法例的阻吓作用视为重点，这支持采纳事实情况(b)这观点：

(a) 这项建议的罪行不受地域限制。

(b) 假设建议4(a)获采纳，[83] 便须就这项建议的罪行证明被告人怀有不诚实或犯罪目的。

7.84 然而，上文就反对首项建议的罪行采纳事实情况(b)所提出的论点，[84] 在此处同样适用，这些论点扼要覆述如下：

(a) 在只符合事实情况(b)的案件中，很可能并非伤害"香港人"，而是伤害其他司法管辖区的人。由该等司法管辖区的执法机关检控犯罪者，是较为理想的做法。

---

83 第3章。

84 第7.73段。

(b) 由于需要向其他司法管辖区取证，故此在香港提出检控可能并不可行（尤其是当案情错综复杂）。

7.85 此外，虽然有人或会认为香港的法庭应对事实情况(b)的案件具有司法管辖权，因为任何被截取的数据其后均可能在香港被不当使用，但相反的论点则指出，香港的法庭应只在该等数据实际被不当使用时才行使司法管辖权。

7.86 衡量上述考虑因素后，我们不建议将事实情况(b)应用于建议的非法截取电脑数据罪。

双重犯罪

7.87 尽管在电脑网络空间，数据截取难免因着该空间所涉技术而发生，建议的非法截取电脑数据罪只针对怀有不诚实或犯罪目的而行事的人。因此，这项建议的罪行类似非法取览程式或数据的加重罪行，[85] 多于类似非法取览程式或数据的简易程序罪行。[86]

7.88 为贯彻一致，我们认为不应就这项建议的罪行施加双重犯罪的规定。我们提出这项建议，旨在避免罪犯利用该规定，因着他们的作为在香港境外某些地方并不构成罪行（例如因为当地的法律体制未尽完善），而故意在该等地方作出该作为。

建议12

小组委员会建议，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

---

85 我们就此建议不施加双重犯罪的规定（第7.80段）。

86 我们就此建议应施加双重犯罪的规定（第7.80段）。

(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）。

非法干扰电脑数据

事实情况(a)、(c)、(d)及(e)

7.89 同样地，我们相信将事实情况(a)、(c)、(d)及(e)应用于建议的非法干扰电脑数据罪这点并无争议。我们因此提出相应建议，并提议将事实情况(d)[87]应用于这项建议的罪行时，重点应放在目标程式或数据的位置，而非储存目标程式或数据的电脑的位置。

事实情况(b)

7.90 只有事实情况(b)[88]有待讨论。读者会记得我们不建议将事实情况(b)应用于首两项建议的罪行。经考虑后，我们同样不建议将事实情况(b)应用于建议的非法干扰电脑数据罪。

双重犯罪

7.91 我们留意到，如双重犯罪的规定不适用于这项建议的罪行，便会与我们就首两项建议的罪行所提出的建议一致。如是者，任何人如在另一司法管辖区干扰数据，不论该项干扰在当地是否构成罪行，亦可能须根据香港法律负上法律责任。

建议13

小组委员会建议，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；

---

87 目标电脑、程式或数据处于香港。

88 犯罪者是“香港人”。

(b) 受害人是香港永久性居民、通常居于香港的人或在香港经营业务的公司；

(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）。

非法干扰电脑系统

事实情况

7.92 我们建议用相同方式处理前项罪行及这项建议的罪行，[89] 故此我们此处可以相对简略。这两项建议的罪行关系密切，显示两者的司法管辖权范围应该一致，但将事实情况(d)[90] 应用于建议的非法干扰*电脑系统*罪时，重点应放在目标电脑的位置，而非任何程式或数据的位置。

双重犯罪

7.93 我们亦不建议对这项建议的罪行施加双重犯罪的规定。

建议14

小组委员会建议，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在香港经营业务的公司；

---

89 第5章建议7(a)及(b)。

90 目标电脑、程式或数据处于香港。

(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）。

提供或管有用作犯罪的器材或数据

建议的罪行的基本及加重形式，应采用相同的司法管辖权规则

7.94 我们建议，这项建议的罪行应包括基本形式及加重形式，视乎被告人是否意图任何人将有关器材或数据用作犯罪。[91]

7.95 然而，我们认为，由于这项基本罪行适用于被制造或改装以用作犯罪的器材或数据，因此即使是基本罪行，亦应视为严重。虽然这项建议的罪行的两种形式轻重有别，但当中差距不至于足以支持两者有不同的司法管辖权规则。我们提议将同一套司法管辖权规则套用于这两种形式。

事实情况(c)及(d)

7.96 这项建议的罪行的案件未必涉及任何受害人或任何目标电脑、程式或数据，但事实情况(c)[92] 及(d)[93] 分别以这些元素为前提，因此，我们认为这些事实情况并不适合这项建议的罪行。

事实情况(a)、(b)及(e)

7.97 在考虑其他事实情况时，我们紧记这项建议的罪行有两部分：

(a) 就*管有*器材或数据的部分而言，有人或会认为管有这个概念会伴随个人，而个人处于实际位置。然而，假如器材或数据储存于例如云端伺服器，若说是在实际位置管有该器材或数据，未必能反映现实。

(b) 就*提供*器材或数据的部分而言，如实际位置在香港境外的人上载恶意软件到互联网，理论上这套恶意软件可提供予

---

91 第 6 章建议 9(a)及(d)。

92 受害人是“香港人”。

93 目标电脑、程式或数据处于香港。

世界上每个角落任何能接达互联网的人。这项建议的罪行所规管的器材和数据，不少都非常有可能在暗网上找到，而买卖双方的实际位置均无从追踪。

7.98 在上述前提下，加上我们认为这项建议的罪行性质较其余四项建议的罪行独特，[94] 我们建议将事实情况(a)[95]、(b)[96]及(e)[97]应用于这项建议的罪行。

双重犯罪

7.99 我们建议首四项建议的罪行均不应施加双重犯罪的规定，非法取览程式或数据的简易程序罪行则除外。

7.100 我们认为，尽管建议的提供或管有用作犯罪的器材或数据罪性质独特，相同的理据亦适用于该罪行，因此有关建议亦同样适用。我们留意到，我们的建议有助各项建议的罪行贯彻一致。

建议15

小组委员会建议，在以下情况下，就建议的提供或管有用作犯罪的器材或数据罪，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，例如实际身处香港的人在暗网上提供用作犯罪的器材或数据；

(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

---

94 虽然《英格兰误用电脑法令》所订罪行大多规定须*"与本地司法管辖权有重大联系"*，但就第3A条所订罪行而言（*"制造、供应或取得用于第1、3或3ZA条所订罪行的物品"*），这似乎并非必要。见第7.43段。

95 罪行的任何"主要元素"在香港发生，即使其他"主要元素"在其他地方发生。

96 犯罪者是"香港人"。

97 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）。

(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

引言

8.1　在前面各章，我们建议订立五类依赖电脑网络的罪行，并建议应适用于每类罪行的司法管辖权规则。本章：

(a) 载述源自香港案例的相关原则、观点及其他附带意见，表达法庭对电脑网络罪行的看法；

(b) 让读者了解本咨询文件的附录，当中概述香港及其他司法管辖区的现行法律就有关罪行所订的最高刑罚；并

(c) 列出我们就建议的罪行所建议的适当最高刑罚。

香港法庭对电脑网络罪行的看法

8.2　*HKSAR v Chan Chi Kong*[1] 涉及首宗根据《刑事罪行条例》（第200章）第59(1A)及60(1)条就*"误用电脑"*提出的检控。[2] 高等法院上诉法庭有以下论述：

> "香港特别行政区是举世闻名的国际商业及金融中心，商业和银行业的各个范畴均倚赖现代电脑科技。对于那些相当可能损害或有可能损害他人对本港的信任和信心的案件，法院有责任确保施以具阻吓性的刑罚，以防止有类似倾向的其他人犯这类罪行……我们强调，这些罪行均相当严重，必须施以合乎案件情况的刑罚。"[3]

8.3　在*香港特别行政区　诉　秦瑞麟*（*HKSAR v Tsun Shui Lun*），[4] 被告人根据第161条被定罪。高等法院首席法官陈兆恺虽然判他刑期上诉得直，但却驳回他就定罪提出的上诉，并指出：

> "在现代社会，我们的生活均离不开电脑。现今的日常活动均高度倚赖电脑，实难想象没有电脑会是怎样的情况。人们不仅透过电脑进行商业交易，亦以电脑储存机

1　[1997] 3 HKC 702, CACC 245/1997（判决日期：1997年9月25日）。
2　根據被告人代表大律師的陳詞（见判詞第706頁H行）。
3　见上文注脚1，第709页C–E行。
4　[1999] 3 HKLRD 215, HCMA 723/1998（判决日期：1999年1月15日）。

密甚至秘密的资料，医院的电脑化运作更是拯救无数生命。若电脑被误用或滥用，或姑息有犯罪或不诚实意图或目的而取用电脑的行为，便可能会引致严重后果。这些情况均必须避免……

第 161 条涵盖种类极为广泛的犯罪和不诚实活动。时至今日，透过取用他人的电脑并摘取当中所载资料，便可犯非常严重的罪行或欺诈罪，一些例子包括：窜改银行纪录、把大额款项从某一帐户转往另一帐户，以及偷窃顾客名单和业务纪录等秘密程式及数据。有关活动可能非常严重，有这类意图或为这类目的而取用电脑的严重性亦不逊于此。

第 161 条所订最高刑罚为五年监禁……本席认为，若为犯罪或进行欺诈而取用电脑，或该项取用的意图是产生巨大获益或导致他人蒙受严重损失（不论是在经济上或所有权上的损失，还是其他方面的损失），便应判处即时监禁刑罚。若取用并非为个人利益，而是为了破坏他人的系统或者令他人深感尴尬和困扰，也不可排除判监的可能性。但在这宗特别案件中，本席不适宜就第 161 条所订罪行制定判刑指引。”[5]

8.4 在*香港特别行政区 诉 谭曦伦及其他人*（*HKSAR v Tam Hei Lun & Ors*），[6] 上诉法庭同样拒绝就第 161 条颁布判刑指引，因为当时(a)曾根据第 161 条提出的检控少于十宗，而且(b)受该条规管的各类罪行均很大机会未为人认识或了解。[7] 然而，该法庭有以下评析：

“法院就《刑事罪行条例》第 60 及 161 条所订罪行决定适当的刑罚时，无疑须考虑许多因素：首要考虑的，是对受害人造成的损失及损坏，另外是有关罪行对受害人的严重性。有关取用的目的，以及取用者在经济上或其他方面的任何获益，亦会是相关因素。

就目前情况而言，我们认为只需指出，若有人为了获益或某种其他理由而取用他人的电脑，该作为在多方面均与入屋犯法类似。实际发生的情况是，有人曾取用他人的电脑，犹如某人进入某住房或办公室后翻弄抽屉或档

5 同上，第 228 页 H 行–第 229 页 F 行。
6 [2000] 3 HKC 745, HCMA 385/2000（判决日期：2000 年 10 月 9 日）。
7 同上，第 749 页 C 行。

案柜一样。入屋犯法罪的某些层面，无疑并不见于在未获授权下取用电脑，故上述的类比绝非完美。尽管我们表示认为不适宜在目前制定指引，但亦希望指出，除非有极不寻常的情况，否则不适宜就违反第 161 条的罪行判处非扣押刑罚。"[8]

8.5 在 *HKSAR v Ko Kam Fai*，[9] 被告人承认多项（涉及两名受害人的）刑事恐吓控罪和（涉及该等受害人的电脑及电邮帐户的）刑事损坏控罪，分别违反《刑事罪行条例》（第 200 章）第 24 及 60(1)条。鉴于前段所引述*谭曦伦*案中的附带意见，主审法官把这些罪行如同根据第 161 条提出检控的罪行看待，并判处具阻吓性的即时监禁刑罚。上诉法庭赞扬这种做法。[10]

8.6 鉴于*谭曦伦*案中的附带意见，包钟倩薇法官亦在 *HKSAR v Choy Yau Pun*[11] 作出以下裁定：

"……即使就犯罪者的情况而言，社会服务令是可行的判刑选择，亦必需有极不寻常的情况，才可以把社会服务令或任何其他形式的非扣押刑罚视为适当选择，以替代违反第 161 条的罪行的扣押刑罚……

……但实情是他犯了违反第 161 条的罪行，而他更是背叛了顾客的信任而犯罪（这位顾客把自己的电脑交给他维修）。若如同本案的情况，恰当判刑的作用既是阻吓以一般方式违反第 161 条的行为，亦是阻吓背叛信任的话，要把社会服务令视为适当的刑罚便会比平常更难。"[12]

8.7 同样地，在*李闻伟 诉 律政司司长*（*Li Man Wai v Secretary for Justice*），[13] 终审法院表示，第 161 条所订罪行可属严重性质：

"根据《刑事罪行条例》第 161 条可判罚的该类罪行无疑非常严重——该类罪行可视为一种盗窃，每每造成严重后果，而受害人却一直无从得知事情的始末缘由。随着电脑被广泛使用及科技进步，这种非常有用的设备已成

---

8 同上，第 749 页 F 行–第 750 页 A 行。
9 [2001] 3 HKC 181, CACC 83/2001（判决日期：2001 年 6 月 20 日）。
10 同上，第 183 页 H 行及第 185 页 B 行。
11 [2002] 3 HKLRD 156, HCMA 450/2002（判决日期：2002 年 6 月 24 日）。
12 同上，第 159 页 H–I 行及第 160 页 D–E 行。
13 (2003) 6 HKCFAR 466, FACC 6/2003（判决日期：2003 年 11 月 6 日）。

为我们日常生活的一环。因此，保护电脑的完整性，尤其是税务局电脑系统的完整性，就愈发重要。然而，现行法例并非一律惩处在未获授权下取用电脑的各种情况，而是只禁止在未获授权下不诚实地提取和使用资料。案中是否涉及不诚实的情况，正是陪审团须就每宗案件裁断的事实问题。"[14]

8.8 在*廖伟信 诉 香港特别行政区*（*Liu Wai Shun v HKSAR*），[15] 任职软件发展人员的被告人被雇主开除，为了报复雇主，被告人删除一些电脑档案，令拥有相关软件的雇主无法使用该软件。被告人根据《刑事罪行条例》（第 200 章）第 60(1)及 161(1)(a)条被判罪名成立，判处罚款。高等法院原讼法庭驳回他的上诉。终审法院上诉委员会拒绝其上诉许可申请，并论述如下：

"我们希望就刑罚指出以下一点：故意损坏电脑软件及数据的行为，当然可对使用有关软件及数据的机构在经济及其他方面造成极大伤害。本案所造成的损坏可以补救，主要是因为申请人的前雇主采取了防范措施，申请人在这点上算是走运了。这类案件所判处的刑罚，应恰当地反映所造成损坏的严重性。若所引致的损坏更加严重，罚款便不会是足够的刑罚。据我们得悉，上诉法庭已表明这类案件通常应判处扣押刑罚，我们认为上诉法庭的这一表述甚是恰当。"[16]

8.9 在 *HKSAR v Luk Wa*，[17] 法官在判刑时的以下论述，与上述案例相符一致：

"电脑及互联网的使用，是现代日常生活的重要一环。几乎各行各业均须依靠电脑及互联网，才能操作和畅顺运作。电脑和互联网使用的完整性不容破坏，实属至关重要。故此，法院一向极为严肃看待关于不诚实使用电脑的罪行。"[18]

---

14 同上，第 474 页 H–J 行。
15 FAMC 30/2004（判决日期：2004 年 9 月 27 日）。
16 同上，第 7 段（終審法院常任法官李義）。
17 DCCC 17/2011（判决日期：2011 年 2 月 18 日）。
18 同上，第 29 段（邱智立法官）。

8.10 同时，正如另一位法官在*香港特别行政区 诉 梁礼仲*（*HKSAR v Leung Lai Chung*）[19] 判刑时指出，不同案件的判刑会有差异。尤其是，*"循公诉程序起诉的罪行，有别于循简易程序审讯的罪行"*。[20]

香港及其他司法管辖区的现行法律

8.11 本咨询文件的附录，旨在综述香港及其他司法管辖区各项电脑网络罪行的最高刑罚，并附有相关条文的编号（以粗体表示）及标题（以斜体表示）。前面各章已详细探讨这些罪行。附录并无提述《示范法》，这是因为《示范法》没有就当中建议的罪行提出最高刑罚建议。

小组委员会的看法

各项建议的较严重罪行

宜订定划一的最高刑罚

8.12 我们在第 7 章建议，除了建议的非法取览程式或数据的简易程序罪行外，本咨询文件所建议的各项罪行，均不应施加双重犯罪的规定。这项建议反映了我们认为建议的各项非简易程序罪行，均可造成重大伤害这个观点。经讨论后，我们赞成以下罪行应订定划一的最高刑罚：

(a) 建议的非法取览程式或数据的加重罪行（第 2 章）；

(b) 建议的非法截取电脑数据罪（第 3 章）；

(c) 建议的非法干扰电脑数据的基本罪行，以及非法干扰电脑系统的基本罪行（第 4 及 5 章）；及

(d) 建议的提供或管有用作犯罪的器材或数据的加重罪行（第 6 章）。

循简易程序定罪及循公诉程序定罪

8.13 我们亦明白电脑网络罪行所致伤害的严重程度差别甚大，既可轻微至不造成关键性伤害，亦可严重至令某重要系统（例如供电系

---

19 DCCC 416/2009（判决日期：2010 年 2 月 1 日）。

20 同上，第 17 段（源丽华法官）。

统或铁路系统）完全瘫痪。由于导致的后果可以如此迥异，故我们建议，前段(a)、(b)、(c)及(d)项中每项建议的罪行，应订有两项最高刑罚：一项适用于循简易程序定罪，另一项则适用于循公诉程序定罪。

循公诉程序定罪的最高刑罚

8.14 在仔细讨论时，我们考虑了以下因素：

(a) 裁判法院及区域法院可判处的最高刑罚分别为三年及七年监禁，[21] 高等法院则可判处较重的刑罚。

(b) 建议的非法取览程式或数据的加重罪行，与第 161 条所订现有罪行[22] 性质类似，该现有罪行的最高刑罚为五年监禁。若这项建议的加重罪行的犯罪者意图作出的其他作为，与使（比如说）香港的公共交通系统瘫痪同样令人发指，上述的最高刑罚便似乎与刑责程度并不相称。[23]

(c)《电讯条例》（第 106 章）第 27(b)条[24] 只就损坏、移走或干扰电讯装置，而意图是截取或找出任何讯息的内容，订立*简易程序*罪行。另外，该条并非针对截取*电脑数据*的特定条文。[25] 因此，该条所订最高刑罚（第 4 级罚款[26] 及两年监禁）的参考价值有限。

(d) 建议的非法干扰电脑数据罪及非法干扰电脑系统罪，均关乎目前由《刑事罪行条例》（第 200 章）第 60 条所处理的行为。[27] 根据该条，犯罪者通常可处十年监禁，如案件涉及危害生命，则可处终身监禁。[28]

---

21 见司法机构，《法庭服务简介——裁判法院》：
"裁判法院的最高刑罰一般為監禁 2 年和罰款 10 萬元。但是，當法庭同時處理兩項或以上的可公訴罪行時，裁判官可判處最高 3 年的刑期。就某些條例而言，單一罪行可判處監禁 3 年和罰款 500 萬元。"
亦见司法机构，《法庭服务简介——区域法院》：
"區域法院可審理除謀殺、誤殺和強姦外的所有嚴重刑事案件，可判處的最長監禁刑期是七年。"

22 *"有犯罪或不诚实意图而取用电脑"*（见第 2.6 段）。

23 我们同意，大多数案件的案情都可能较为轻微，故法院无须判处最高刑罚。2015 年至 2020 年 9 月期间，被裁定犯第 161 条所订罪行的犯罪者被判感化令、社会服务令、罚款或监禁 10 日至 1 年零 8 个月不等。

24 *"蓄意损坏电讯装置"*（见第 3.12 段）。

25 第 3.14 至 3.16 段。

26 根据《刑事诉讼程序条例》（第 221 章）附表 8，现为 25,000 元。

27 *"摧毁或损坏财产"*（见第 4.4 及 5.7 段）。

28 《刑事罪行条例》（第 200 章）第 63 条。

(e) 建议的提供或管有用作犯罪的器材或数据的加重罪行，与《刑事罪行条例》（第 200 章）第 62 条所订罪行[29] 类同，后者可处十年监禁。[30]

(f) 至于第 8.12 (a)、(b)、(c)及(d)段所述的各项建议罪行，在刑责程度上与相若罪行如何比较，可参考《盗窃罪条例》（第 210 章）就以下各类具代表性罪行所订的最高监禁刑期：

(i) 盗窃罪可处 10 年监禁；[31]

(ii) 欺诈罪可处 14 年监禁；[32]

(iii) 勒索罪可处 14 年监禁；[33]

(iv) 入屋犯法罪可处 14 年监禁；[34]

(v) 严重入屋犯法罪（即任何人在犯入屋犯法罪时携带任何火器或仿制火器，任何攻击性武器，或任何炸药）可处终身监禁；[35] 及

(vi) 抢劫罪可处终身监禁。[36]

(g) 我们的比较研究显示，其他司法管辖区的最高刑罚各有差异，原因是该等刑罚反映有关罪行的不同定义。其他司法管辖区的判刑原则，亦可能与香港有别。

---

29 *"管有任何物品意图摧毁或损坏财产"*（见第 6.6 段）。
30 《刑事罪行条例》（第 200 章）第 63(2)条。
31 《盗窃罪条例》（第 210 章）第 9 条。
32 同上，第 16A(1)条。
33 同上，第 23(3)条。
34 同上，第 11(4)条。
35 同上，第 12(3)条。
36 同上，第 10(2)条。

8.15 不论我们所建议的监禁年期长度如何，某程度上总有武断成分。我们建议，第 8.12 (a)、(b)、(c)及(d)段所述各项建议罪行的最高监禁刑期应订为 14 年。[37] 我们认为这项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）所订的上述罪行，[38] 以及(b)其他司法管辖区的有关罪行。[39]

循简易程序定罪的最高刑罚

8.16 我们认为，循简易程序定罪的最高监禁刑期若订为两年，便会与关于循公诉程序定罪的案件的上述建议相称。故此我们建议，循简易程序定罪的最高监禁刑期，应订为两年。

建议的非法取览程式或数据的简易程序罪行

8.17 在某程度上，这项建议的罪行与第 27A 条所订的罪行[40] 性质相若。然而，第 27A 条甚少获援引，而且我们认为该条的最高刑罚（第 4 级罚款）[41] 颇轻，故建议的罪行不宜采纳该刑罚。虽然这项建议的罪行适用于在未获授权下取览本身，犯罪者只是"看看"目标电脑的程式或数据，并没有造成干扰，但我们的看法是，即使是简易程序案件，亦应有判监的可能性。

8.18 我们建议，建议的非法取览程式或数据的简易程序罪行的最高监禁刑期，应订为两年，因此该罪行将可在裁判法院审讯。

---

37 除了订立有关罪行的法例外，可能亦须参阅其他法例条文，才能了解所有可供采用的判刑选择。举例来说，即使订立有关罪行的法例没有提述罚款或补偿，裁判官或法庭亦具有司法管辖权：
(a) 根据《裁判官条例》（第 227 章）第 92 条或《刑事诉讼程序条例》（第 221 章）第 113A 条，判处罚款；及
(b) 根据《裁判官条例》（第 227 章）第 98 条或《刑事诉讼程序条例》（第 221 章）第 73 条，命令支付补偿。

38 第 8.14 (f)段。

39 本咨询文件的附录。

40 *"藉电讯而在未获授权下取用电脑资料"*（见第 2.11 段）。

41 根据《刑事诉讼程序条例》（第 221 章）附表 8，现为 25,000 元。

建议的非法干扰电脑数据及非法干扰电脑系统的加重罪行

8.19 正如第 4 及 5 章[42] 所论述，我们：

(a) 认为保留《刑事罪行条例》（第 200 章）第 60(2)条所订的加重罪行较为可取；并

(b) 建议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。

8.20 为求与刑事损坏罪保持贯彻一致，我们提议就建议的非法干扰电脑数据及非法干扰电脑系统的加重罪行，采纳《刑事罪行条例》（第 200 章）第 63(1)条现时订明的最高刑罚，亦即终身监禁。

建议的提供或管有用作犯罪的器材或数据的基本罪行

8.21 正如第 6 章所建议，这项建议的罪行与相关加重罪行的重要区别，在于被告人是否意图使有关器材或数据用作犯罪。[43] 这两种形式可让人们知道不同的刑罚会适用于以下两项罪行：一项是蓄意提供或管有用作犯罪的器材或数据，并意图使该器材或数据如此使用，另一项是蓄意提供或管有用作犯罪的器材或数据，但没有意图使该器材或数据如此使用。

8.22 我们在考虑这项建议的基本罪行的最高刑罚时，曾提出两个方案：

(a) 方案一是五年监禁，这参考了第 161 条所订现有罪行。

(b) 方案二是七年监禁，即相关加重罪行的建议最高刑罚[44] 的一半。

8.23 我们认为，由于这项基本罪行适用于被制造或改装以用作犯罪的器材或数据，因此即使是基本罪行，亦应视为严重罪行。[45] 基于以上原因，我们最终选择了方案二。

---

42 第 4.96 至 4.98 及 5.61 至 5.63 段。
43 建议 9(d)(ii)。
44 第 8.15 段。
45 第 7.95 段。

建议 16

小组委员会建议：

(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：

(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) 就建议的提供或管有用作犯罪的器材或数据罪而言，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。

第 9 章　综合建议及咨询问题

引言

9.1　本章综述按本咨询文件所建议的五类罪行而划分的各项建议及咨询问题。这些建议及咨询问题并非依照它们在前面各章出现的次序逐一罗列，我们希望这种编排方式有助读者对这些建议及咨询问题作出全面整体的考虑。

9.2　为方便读者参阅本咨询文件中的相关讨论，我们会在每类建议的罪行之下，分别标示有关建议。

非法取览程式或数据

——建议 1、2、11 及 16(a)

建议

9.3　在未获授权下取览程式或数据，应在新订针对电脑网络罪行的特定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。*〔建议 1(a)〕*[1]

9.4　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。*〔建议 1(b)〕*[2]

9.5　在以下情况下，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皆是）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；

(c) 目标电脑、程式或数据处于香港；或

1　第 2.89 至 2.106 段。

2　第 2.107 至 2.108 段。

(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。*〔建议 11〕*[3]

9.6 犯罪者应可处下述最高刑罚：

(a) 如属简易程序罪行，可处两年监禁；或

(b) 如属加重罪行，一经循公诉程序定罪，可处 14 年监禁。*〔建议 16(a)〕*[4]

9.7 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）第 1、2 及 17 条为蓝本。*〔建议 1(c)〕*[5]

咨询问题

9.8 在未获授权下取览，应否有任何特定的免责辩护或豁免？

9.9 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：

(a) 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？

(b) 如(a)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？

---

3 第 7.71 至 7.81 段。
4 第 8.12 至 8.18 段。
5 第 2.109 段。

(c) 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？

9.10 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)[6]所述的例子）？*〔建议2〕*[7]

非法截取电脑数据

——建议4、5、12及16(b)

建议

9.11 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。*〔建议4(a)〕*[8]

9.12 建议的罪行应：

(a) 保障一般通讯，而并非只保障私人通讯；

(b) 一般适用于数据（不论有关数据是否元数据）；及

(c) 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。*〔建议4(b)〕*[9]

9.13 在以下情况下，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在香港经营业务的公司；

---

6 第9.30段。
7 第2.110至2.120段。
8 第3.92至3.99段。
9 第3.100至3.110段。

(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）。*〔建议 12〕*[10]

9.14 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。*〔建议 16(b)〕*[11]

9.15 除上文第 9.11 及 9.12 段另有规定外，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）。*〔建议 4(c)〕*[12]

咨询问题

9.16 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）？

9.17 提供 Wi-Fi 热点或电脑供顾客或雇员使用的真实业务（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）？*〔建议 5〕*[13]

非法干扰电脑数据

——建议 6、13 及 16(c)

建议

9.18 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。

9.19 新法例应采用《刑事罪行条例》（第 200 章）所订的以下特点：

---

10 第 7.82 至 7.88 段。
11 第 8.12 至 8.16 段。
12 第 3.111 至 3.112 段。
13 第 3.113 至 3.122 段。

(a) 第 59(1A)(a)、(b)及(c)条所订犯罪行为；[14]

(b) 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）；

(c) 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

(d) 第 60(2)条所订加重罪行。

9.20 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。*〔建议 6〕*[15]

9.21 在以下情况下，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）。*〔建议 13〕*[16]

9.22 犯罪者应可处下述最高刑罚：

(a) 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

---

14 第 59(1A)条把"误用电脑"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。"

15 第 4.81 至 4.99 段。

16 第 7.89 至 7.91 段。

(b) 如属加重罪行，可处终身监禁。〔*建议 16(c)*〕[17]

非法干扰电脑系统

——建议 7、8、14 及 16(c)

建议

9.23 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。

9.24 《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。

9.25 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。

9.26 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：

(a) 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）；

(b) 在软件生产时，在软件编入缺损程式；及

(c) 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。〔*建议 7*〕[18]

9.27 在以下情况下，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在香港经营业务的公司；

(c) 目标电脑处于香港；或

---

17 第 8.12 至 8.16、8.19 至 8.20 段。

18 第 5.61 至 5.68 段。

(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）。*〔建议 14〕*[19]

9.28 犯罪者应可处下述最高刑罚：

(a) 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

(b) 如属加重罪行，可处终身监禁。*〔建议 16(c)〕*[20]

咨询问题

9.29 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？

9.30 就这项建议的罪行而言，非保安专业人员应否有合法辩解，例如：

(a) 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

(b) 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）：

(i) 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

(ii) 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〕*[21]

---

19 第 7.92 至 7.93 段。

20 第 8.12 至 8.16、8.19 至 8.20 段。

提供或管有用作犯罪的器材或数据

——建议 9、10、15 及 16(d)

建议

9.31 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。*〔建议 9(a)〕*[22]

9.32 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。*〔建议 9(b)〕*[23]

9.33 建议的罪行应适用于：

(a) 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

(b) 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。*〔建议 9(c)〕*[24]

9.34 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）：

(a) 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

(b) 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。*〔建议 9(d)〕*[25]

9.35 在以下情况下，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

---

21 第 5.69 至 5.72 段。
22 第 6.73 至 6.79、6.83 至 6.84、6.86 至 6.87 段。
23 第 6.81 至 6.82 段。
24 第 6.76 至 6.77、6.84 段。
25 第 6.73 至 6.80、6.83、6.85 至 6.87 段。

方发生，例如实际身处香港的人在暗网上提供用作犯罪的器材或数据；

(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）。*〔建议 15〕*[26]

9.36 犯罪者应可处下述最高刑罚：

(a) 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

(b) 如属加重罪行，一经循公诉程序定罪，可处 14 年监禁。*〔建议 16(d)〕*[27]

9.37 建议的条文应以英格兰及威尔斯《1990 年误用电脑法令》（Computer Misuse Act 1990）第 3A 条，以及新加坡《1993 年误用电脑法令》（Computer Misuse Act 1993）第 8 及 10 条为蓝本。*〔建议 9(e)〕*[28]

咨询问题

9.38 就蓄意提供或管有电脑数据（软件或源码）这项罪行而言，如该数据只可用作进行网络攻击（例如是勒索软件或病毒），应否有免责辩护或豁免？

9.39 如以上问题的答案是"应该"的话，

(a) 上述免责辩护或豁免应在甚么情况下可用，并应有甚么条款？

(b) 这种获豁免的管有应否受到规管，以及如应该的话，有甚么规管规定？*〔建议 10〕*[29]

---

26 第 7.94 至 7.100 段。
27 第 8.12 至 8.16、8.21 至 8.23 段。
28 第 6.88 段。
29 第 6.91 至 6.93 段。

简易程序的时效期

建议

9.40　　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。*〔建议 3〕*[30]

[30] 第 2.121 至 2.123 段。

附录

建议的罪行	香港	澳大利亚	加拿大	英格兰及威尔斯	中国内地	新西兰	新加坡	美国

建议的罪行	香港	澳大利亚	加拿大	英格兰及威尔斯	中国内地	新西兰	新加坡	美国
(a) 非法取览程式或数据	**《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 4 级罚款，即港币 25,000 元（《刑事诉讼程序条例》（第 221 章）附表 8）	**《刑事法典》（联邦）（Criminal Code (Cth)）第 477.1(1)(a)(i)条——** *"在未获授权下作出取览、修改或损害，并意图干犯严重罪行"*[1] • 不超过适用于有关严重罪行的刑罚	**《1985 年刑事法典》（Criminal Code 1985）第 326(1)(b)条——** *"盗取电讯服务"* • （循简易程序定罪）5,000 加元罚款或 2 年减 1 日的监禁，或两者兼处[2] • （如损失不足 5,000 加元，并循公诉程序定罪）2 年监禁 • （如损失超过 5,000 加元，并循公诉程序定罪）10 年监禁	**《1990 年误用电脑法令》（Computer Misuse Act 1990）第 1 条——** *"在未获授权下取览电脑资料"* • （循简易程序定罪）不超过法定最高罚款[3] 或 12 个月监禁，或两者兼处 • （循公诉程序定罪）罚款[4] 或 2 年监禁，或两者兼处	**《中国刑法》第二百八十五条第一款** • 3 年徒刑或者拘役	**《1961 年刑事罪行法令》（Crimes Act 1961）第 249 条——** *"为不诚实目的而取用电脑系统"* • （作出取用，意图取得财产等或导致损失）5 年监禁 • （作出取用，并藉此取得财产等或导致损失）7 年监禁	**《1993 年误用电脑法令》（Computer Misuse Act 1993）第 3 条——** *"在未获授权下取览电脑资料"* • 5,000 新加坡元罚款或 2 年监禁，或两者兼处 • （第二次或其后每次定罪）10,000 新加坡元罚款或 3 年监禁，或两者兼处	**《美国法典》第 18 篇第 1030 (a)(1)至(4)条（18 USC 1030 (a)(1) to (4)）——** *"与电脑有关的欺诈及相关活动"* • 第(a)(1)款所订罪行 - （通常）罚款[5] 或 10 年监禁，或两者兼处 - （如以往曾被裁定干犯《美国法典》第 18 篇第 1030 条所订其他罪行）罚款或 20 年监禁，或两者兼处

1 《刑事法典》（联邦）第 477.1(9)条将"严重罪行"界定为"可处终身监禁或为期 5 年或以上监禁的罪行"。

2 《1985 年刑事法典》第 787(1)条。

3 《2012 年法律援助、罪犯判刑及惩罚法令》（Legal Aid, Sentencing and Punishment of Offenders Act 2012）第 85 条显示，*"不超过法定最高罚款"*现时指任何款额（即款额无限）的罚款。

4 《2012 年法律援助、罪犯判刑及惩罚法令》第 85 条显示，没有列明最高款额的罚款，指任何款额（即款额无限）的罚款。

5 《美国法典》第 18 篇第 3571 条（18 USC 3571）订明罚款的最高款额（就个人而言，最高为 250,000 美元，就机构而言，最高为 500,000 美元，或以下数额中的较大者：从有关罪行所得总金钱收益的两倍，或对被告人以外的人所造成总损失的两倍）。

建议的罪行	香港	澳大利亚	加拿大	英格兰及威尔斯	中国内地	新西兰	新加坡	美国
	《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"* • （循公诉程序定罪）5 年监禁	**《刑事法典》（联邦）第 478.1 条**—— *"在未获授权下取览或修改受限数据"* • 2 年监禁	**《1985 年刑事法典》第 342.1(1)条**—— *"在未获授权下使用电脑"* • （循简易程序定罪）5,000 加元罚款或不超过 2 年减 1 日的监禁，或两者兼处 • （循公诉程序定罪）10 年监禁	**《1990 年误用电脑法令》第 2 条**—— *"在未获授权下取览，并意图干犯或意图利便干犯其他罪行"* • （循简易程序定罪）不超过法定最高罚款或 12 个月监禁，或两者兼处 • （循公诉程序定罪）罚款或 5 年监禁，或两者兼处	**《中国刑法》第二百八十五条第二款** • （情节严重的）3 年徒刑或者拘役，并处或者单处罚金 • （情节特别严重的）3 年以上 7 年以下徒刑，并处罚金	**《1961 年刑事罪行法令》第 252 条**—— *"在未获授权下取用电脑系统"* • 2 年监禁	• （如导致损坏）50,000 新加坡元罚款或 7 年监禁，或两者兼处 • （如取用受保护电脑）[6] 100,000 新加坡元罚款或 20 年监禁，或两者兼处 **《1993 年误用电脑法令》第 4 条**—— *"意图犯罪或意图利便犯罪而取览"* • 50,000 新加坡元罚款或 10 年监禁，或两者兼处	• 第(a)(2)款所订罪行 - （通常）罚款或 1 年监禁，或两者兼处 - （如为商业利益或私人财务利益等而犯罪）罚款或 5 年监禁，或两者兼处 - （如以往曾被裁定干犯《美国法典》第 18 篇第 1030 条所订其他罪行）罚款或 10 年监禁，或两者兼处

[6] 根据《新加坡误用电脑法令》第 11(2)条：

"……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或程式或数据是在与下述各项有直接关连的情况下使用的，或对下述各项属必要的——

(a) 新加坡的安全、防务或国际关系；

(b) 与执行刑事法律有关的机密资料来源的存在或身分；

(c) 提供与通讯基础建设、银行及金融服务、公共事业、公共交通或公开密码匙基础建设直接有关的服务；或

(d) 保障公众安全，包括与必要紧急服务（例如警务、民防及医疗服务）有关的系统。"

建议的罪行	香港	澳大利亚	加拿大	英格兰及威尔斯	中国内地	新西兰	新加坡	美国
				《2003 年通讯法令》（Communications Act 2003）第 125 条—— *"不诚实地取得电子通讯服务"* • （循简易程序定罪）不超过法定最高罚款或 6 个月监禁，或两者兼处 • （循公诉程序定罪）罚款或 5 年监禁，或两者兼处				• 第(a)(3)款所订罪行 - （通常）罚款或 1 年监禁，或两者兼处 - （如以往曾被裁定干犯《美国法典》第 18 篇第 1030 条所订其他罪行）罚款或 10 年监禁，或两者兼处 • 第(a)(4)款所订罪行 - （通常）罚款或 5 年监禁，或两者兼处 - （如以往曾被裁定干犯《美国法典》第 18 篇第 1030 条所订其他罪行）罚款或 10 年监禁，或两者兼处

建议的罪行	香港	澳大利亚	加拿大	英格兰及威尔斯	中国内地	新西兰	新加坡	美国
								《美国法典》第 18 篇第 2701 条（18 USC 2701）——*"非法取览储存通讯"* • 如犯罪目的在于获得商业利益、作出恶意摧毁或损坏等： - （首次犯罪）罚款或 5 年监禁，或两者兼处 - （其后每次犯罪）罚款或 10 年监禁，或两者兼处 • 如属任何其他情况： - （首次犯罪）罚款或 1 年监禁，或两者兼处 - （如以往曾被裁定干犯《美国法典》第 18 篇第 2701 条所订其他罪行）罚款或 5 年监禁，或两者兼处

建议的罪行	香港	澳大利亚	加拿大	英格兰及威尔斯	中国内地	新西兰	新加坡	美国
(b) 非法截取电脑数据	**《电讯条例》（第 106 章）第 27 条**——*"蓄意损坏电讯装置"* • （循简易程序定罪）第 4 级罚款（即港币 25,000 元）及 2 年监禁	**《1979 年电讯（截取及取览）法令》（联邦）（Telecommunications (Interception and Access) Act 1979 (Cth)）第 7(1)条**——*"不得截取电讯"*[7] • （循简易程序定罪）6 个月监禁 • （循公诉程序定罪）2 年监禁	**《1985 年刑事法典》第 184(1)条**——*"截取"〔私人通讯〕* • （循简易程序定罪）5,000 加元罚款或不超过 2 年减 1 日的监禁，或两者兼处 • （循公诉程序定罪）5 年监禁	**《2016 年调查权力法令》（Investigatory Powers Act 2016）第 3 条**——*"非法截取罪"* • （循简易程序定罪）罚款 • （循公诉程序定罪）罚款或 2 年监禁，或两者兼处	**《中国刑法》第二百八十五条第二款** 见上文。	**《1961 年刑事罪行法令》第 216B 条**——*"禁止使用截取器材"* • 2 年监禁	**《1993 年误用电脑法令》第 6 条**——*"在未获授权下使用或截取电脑服务"* • 10,000 新加坡元罚款或 3 年监禁，或两者兼处 • （第二次或其后每次定罪）20,000 新加坡元罚款或 5 年监禁，或两者兼处 • （如导致损坏）50,000 新加坡元罚款或 7 年监禁，或两者兼处 • （如取用受保护电脑）100,000 新加坡元罚款或 20 年监禁，或两者兼处	**《美国法典》第 18 篇第 2511(1)条（18 USC 2511(1)）**——*"禁止截取和披露有线、口头或电子通讯"* • 罚款或 5 年监禁，或两者兼处

[7] 《1979 年电讯（截取及取览）法令》（联邦）第 105 条订明违反第 7(1)条的最高刑罚。

建议的罪行	香港	澳大利亚	加拿大	英格兰及威尔斯	中国内地	新西兰	新加坡	美国
(c) 非法干扰电脑数据	**《刑事罪行条例》（第 200 章）第 60 条**——*"摧毁或损坏财产"* • （第 60(1)条所订罪行，循公诉程序定罪）10 年监禁 • （第 60(2)条所订加重罪行，循公诉程序定罪）终身监禁 **《电讯条例》（第 106 章）第 25 条**——*"电讯人员以外的人隐匿讯息等"* • （循简易程序定罪）第 4 级罚款（即港币 25,000 元）及 12 个月监禁	**《刑事法典》（联邦）第 477.2 条**——*"在未获授权下修改数据，以导致损害"* • 10 年监禁 **《刑事法典》（联邦）第 477.3 条**——*"在未获授权下损害电子通讯"* • 10 年监禁 **《刑事法典》（联邦）第 478.2 条**——*"在未获授权下损害存于电脑纪录碟等内的数据"* • 2 年监禁	**《1985 年刑事法典》第 430(1.1)条**——*"与电脑数据有关的损害"* • （循简易程序定罪）5,000 加元罚款或 2 年减 1 日的监禁，或两者兼处 • （循公诉程序定罪）以下年期的监禁： - （通常）2 年 - （如损失超过 5,000 加元）10 年 - （如导致生命受到实际危害）终身监禁	**《1990 年误用电脑法令》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"* • （循简易程序定罪）不超过法定最高罚款或 12 个月监禁，或两者兼处 • （循公诉程序定罪）罚款或 10 年监禁，或两者兼处 **《1990 年误用电脑法令》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"* • （通常）罚款或 14 年监禁，或两者兼处	**《中国刑法》第二百八十六条第二款** • （后果严重的）5 年徒刑或者拘役	**《1961 年刑事罪行法令》第 250 条**——*"损坏或干扰电脑系统"* • （通常）7 年监禁 • （如犯罪者知悉或理应知悉相当可能会导致生命受危害）10 年监禁 **《1961 年刑事罪行法令》第 258(1)条**——*"意图欺骗而更改、隐藏、销毁或复制文件"* • 10 年监禁	**《1993 年误用电脑法令》第 5 条**——*"在未获授权下修改电脑资料"* • 10,000 新加坡元罚款或 3 年监禁，或两者兼处 • （第二次或其后每次定罪）20,000 新加坡元罚款或 5 年监禁，或两者兼处 • （如导致损坏）50,000 新加坡元罚款或 7 年监禁，或两者兼处 • （如取用受保护电脑）100,000 新加坡元罚款或 20 年监禁，或两者兼处	**《美国法典》第 18 篇第 1030(a)(5)条（18 USC 1030 (a)(5)）**——*"与电脑有关的欺诈及相关活动"* • 第 (a)(5)(A) 款所订罪行 - （通常）罚款或 1 年监禁，或两者兼处 - （如导致《美国法典》第 18 篇第 1030 (c)(4)(A)(i)条所指明的伤害）罚款或 10 年监禁，或两者兼处 - （如以往曾被裁定干犯《美国法典》第 18 篇第 1030 条所订其他罪行）罚款或 20 年监禁，或两者兼处 - （如犯罪者企图导致或故意或罔顾后果地导致身体受严重损伤）罚款或 20 年监禁，或两者兼处

建议的罪行	香港	澳大利亚	加拿大	英格兰及威尔斯	中国内地	新西兰	新加坡	美国
		《刑事法典》（联邦）第 477.1(1)(a)(ii)及(iii)条、第 478.1 条 见上文。		• （如： - 因导致第(3)(a)款所述种类的人类福祉严重损害（人命损失）或第(3)(b)款所述种类的人类福祉严重损害（人类患病或受伤）的作为而干犯该罪行，或因产生导致该损害的重大风险的作为而干犯该罪行；或 - 因导致国家安全严重损害的作为而干犯该罪行，或因产生导致该损害的重大风险的作为而干犯该罪行） 罚款或终身监禁，或两者兼处				- （如犯罪者企图导致或故意或罔顾后果地导致死亡）罚款或任何刑期的监禁或终身监禁，或两者兼处 • 第 (a)(5)(B) 款所订罪行 - （通常）罚款或 1 年监禁，或两者兼处 - （如导致《美国法典》第 18 篇第 1030 (c)(4)(A)(i)条所指明的伤害）罚款或 5 年监禁，或两者兼处 - （如以往曾被裁定干犯《美国法典》第 18 篇第 1030 条所订其他罪行）罚款或 20 年监禁，或两者兼处

建议的罪行	香港	澳大利亚	加拿大	英格兰及威尔斯	中国内地	新西兰	新加坡	美国
								• 第 (a)(5)(C) 款所订罪行 - （通常）罚款或 1 年监禁，或两者兼处 - （如以往曾被裁定干犯《美国法典》第 18 篇第 1030 条所订其他罪行）罚款或 10 年监禁，或两者兼处

建议的罪行	香港	澳大利亚	加拿大	英格兰及威尔斯	中国内地	新西兰	新加坡	美国
(d) 非法干扰电脑系统	**《刑事罪行条例》（第 200 章）第 60 条** 见上文。	**《刑事法典》（联邦）第 477.2、477.3、477.1(1)(a)(ii)及(iii)、478.1 及 478.2 条** 见上文。	**《1985 年刑事法典》第 430(1.1)条及第 430(4)条** 见上文。	**《1990 年误用电脑法令》第 3 及 3ZA 条** 见上文。	**《中国刑法》第二百八十五条第二款** 见上文。 **《中国刑法》第二百八十六条第一款** • （后果严重的）5 年徒刑或者拘役 • （后果特别严重的）5 年以上徒刑	**《1961 年刑事罪行法令》第 250 及 258(1)条** 见上文。	**《1993 年误用电脑法令》第 7 条——** *"在未获授权下妨碍使用电脑"* • 10,000 新加坡元罚款或 3 年监禁，或两者兼处 • （第二次或其后每次定罪）20,000 新加坡元罚款或 5 年监禁，或两者兼处 • （如导致损坏）50,000 新加坡元罚款或 7 年监禁，或两者兼处 • （如取用受保护电脑）100,000 新加坡元罚款或 20 年监禁，或两者兼处	**《美国法典》第 18 篇第 1030(a)(5)条** 见上文。

建议的罪行	香港	澳大利亚	加拿大	英格兰及威尔斯	中国内地	新西兰	新加坡	美国
(e) 提供或管有用作犯罪的器材或数据	**《刑事罪行条例》（第 200 章）第 62 条**——*"管有任何物品意图摧毁或损坏财产"* • （循公诉程序定罪）10 年监禁	**《刑事法典》（联邦）第 478.3 条**——*"管有或控制数据，并意图干犯电脑罪行"* • 3 年监禁 **《刑事法典》（联邦）第 478.4 条**——*"生产、供应或取得数据，并意图干犯电脑罪行"* • 3 年监禁	**《1985 年刑事法典》第 191(1)条**——*"管有〔用作截取私人通讯的器材〕等"* • （循简易程序定罪）5,000 加元罚款或不超过 2 年减 1 日的监禁，或两者兼处 • （循公诉程序定罪）2 年监禁 **《1985 年刑事法典》第 327(1)条**——*"管有器材以取得使用电讯设施或服务"* • （循简易程序定罪）5,000 加元罚款或不超过 2 年减 1 日的监禁，或两者兼处 • （循公诉程序定罪）2 年监禁	**《1990 年误用电脑法令》第 3A 条**——*"制造、供应或取得用于第 1、3 或 3ZA 条所订罪行的物品"* • （循简易程序定罪）不超过法定最高罚款或 12 个月监禁，或两者兼处 • （循公诉程序定罪）罚款或 2 年监禁，或两者兼处 **《2003 年通讯法令》第 126 条**——*"管有或供应用作违反第 125 条〔即不诚实地取得电子通讯服务〕的器具等"* • （循简易程序定罪）不超过法定最高罚款或 6 个月监禁，或两者兼处 • （循公诉程序定罪）罚款或 5 年监禁，或两者兼处	**《中国刑法》第二百八十五条第三款** • （情节严重的）3 年徒刑或者拘役，并处或者单处罚金 **《中国刑法》第二百八十六条第三款** • （后果严重的）5 年徒刑或者拘役	**《1961 年刑事罪行法令》第 216D 条**——*"禁止处理截取器材等"* • 2 年监禁 **《1961 年刑事罪行法令》第 251 条**——*"制作、出售、分发或管有用作犯罪的软件"* • 2 年监禁	**《1993 年误用电脑法令》第 8 条**——*"在未获授权下披露取用码"* • 10,000 新加坡元罚款或 3 年监禁，或两者兼处 • （第二次或其后每次定罪）20,000 新加坡元罚款或 5 年监禁，或两者兼处 **《1993 年误用电脑法令》第 10 条**——*"取得用于某些罪行的物品等"* • 10,000 新加坡元罚款或 3 年监禁，或两者兼处 • （第二次或其后每次定罪）20,000 新加坡元罚款或 5 年监禁，或两者兼处	**《美国法典》第 18 篇第 1030(a)(6)条（18 USC1030 (a)(6)）**——*"与电脑有关的欺诈及相关活动"* • （通常）罚款或 1 年监禁，或两者兼处 • （如以往曾被裁定干犯《美国法典》第 18 篇第 1030 条所订其他罪行）罚款或 10 年监禁，或两者兼处 **《美国法典》第 18 篇第 2512(1)条（18 USC 2512(1)）**——*"禁止制造、分发、管有和宣传有线、口头或电子通讯的截取器材"* • 罚款或 5 年监禁，或两者兼处

建议的罪行	香港	澳大利亚	加拿大	英格兰及威尔斯	中国内地	新西兰	新加坡	美国
			《1985 年刑事法典》第 342.2(1)条——*"为在未获授权下使用电脑系统或导致损害而管有器材"* • （循简易程序定罪）5,000 加元罚款或不超过 2 年减 1 日的监禁，或两者兼处 • （循公诉程序定罪）2 年监禁					