香港法律改革委员会

电脑网络罪行小组委员会

《依赖电脑网络的罪行及司法管辖权事宜》咨询文件

摘要

（咨询文件载有法律改革委员会（“法改会”）辖下电脑网络罪行小组委员会（“小组委员会”）所提出的建议及咨询问题，供咨询公众意见之用。本摘要为咨询文件内容的概要，所采用的简称及界定用语与咨询文件相同，有意提出意见者宜参阅咨询文件全文。咨询文件可于法改会的网站下载，网址是：https://www.hkreform.gov.hk，亦可向香港中环下亚厘毕道 18 号律政中心东座 4 楼法改会秘书处索取。

回应者应于 2022 年 10 月 19 日或之前将意见送达小组委员会秘书。）

导言

研究范围

1. 2019 年 1 月，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；
>
> (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。”

项目的三个划定部分

2. 咨询文件关乎项目以下三个部分的第一部分：

(a) 第一部分处理依赖电脑网络的罪行[1]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，[2]并尝试应对数码时代的宏观挑战，包括数据主权，[3]而第二部分的范围须待适当时候再作讨论；及

(c) 第三部分会处理证据及执法（程序）事宜。

第一部分研究的五类依赖电脑网络的罪行

3. 咨询文件研究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，即：

(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。

4. 小组委员会展开研究后，《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，[4]小组委员会研究电脑网络罪行这课题时已将此考虑在内。

---

1 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。例子包括黑客入侵、散播电脑病毒，以及分布式拒绝服务攻击。

2 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。例子包括在网上散布儿童色情物品、设立仿冒诈骗网站，以及网上起底。

3 数据主权亦称为电脑网络、数码或技术主权。数据主权所指的，是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这个概念。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。见 Julia Pohle & Thorsten Thiel, "Digital Sovereignty", Internet Policy Review: Journal on internet regulation (2020), Vol 9, Issue 4，第 8 页。

4 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。

建议背后的指导原则

5. 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。

第 1 章：电脑网络罪行的归类

6. 在联合国的层面，电脑网络罪行既没有确切的清单，也无法巨细无遗地逐一胪列。文献列述了多种电脑网络罪行的归类方法，以及多组用于有关归类的术语。联合国毒品和犯罪问题办公室（United Nations Office on Drugs and Crime）的网络犯罪问题全球方案（Global Programme on Cybercrime），区分"依赖电脑网络的罪行"及"借助电脑网络的罪行"。[5]

7. 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》**）处理四类罪行，[6] 其中"损害电脑数据及系统的机密性、完整性和可用性的罪行"这类别大致上对应咨询文件的重心。

8. 我们的比较研究涵盖七个司法管辖区，当中澳大利亚、加拿大、英格兰及威尔斯和美利坚合众国是《布达佩斯公约》的缔约方，其余三个司法管辖区（即中国内地、新西兰和新加坡）则与香港一样，并非缔约方。

第 2 章：非法取览程式或数据

9. 概括而言，就非法取览程式或数据而订立的罪行，旨在应对损害电脑系统安全的危险威胁及攻击，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。黑客入侵是这罪行最典型的例子。

---

5 联合国毒品和犯罪问题办公室，"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）。

6 这些罪行是损害电脑数据及系统的机密性、完整性和可用性的罪行、电脑相关罪行（包括电脑相关伪造及欺诈）、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），以及关于侵犯版权和相关权利的罪行。

香港的现行法律

10. 根据《刑事罪行条例》(第 200 章)第 161 条("**第 161 条**"),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,

即属犯罪。

11. 根据*律政司司长 诉 郑嘉仪*(*Secretary for Justice v Cheng Ka Yee*),[7] 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 条。因此,举例来说,如任何人使用自己的电脑设立仿冒诈骗网站,第 161 条并不适用。

12. 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。[8]

13. 第 161 条的"获益"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,例如某人先前无法取览的资料。[9]

14. 根据《电讯条例》(第 106 章)(**《电讯条例》**)第 27A 条("**第 27A 条**"),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。

15. 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。

16. 案例显示,控方倾向根据第 161 条检控黑客入侵事件,这可能是因为控方显然难以证明第 27A 条所订的犯罪意念。此犯罪意念涉及两方面,即被告人:

---

7 (2019) 22 HKCFAR 97, [2019] HKCFA 9.

8 同上,第 38 段。

9 *香港特别行政区 诉 秦瑞麟*(*HKSAR v Tsun Shui Lun*) [1999] 3 HKLRD 215, HCMA 723/1998(判决日期:1999 年 1 月 15 日),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。

(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"*。

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（25,000 元），而根据第 161 条循公诉程序定罪则可处监禁五年。

小组委员会的看法

宜制定针对电脑网络罪行的特定法例

18. 目前，香港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。

19. 相比之下，我们的比较研究所审视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。这些司法管辖区的做法有助确保做到协调统一、周全完备和贯彻一致（例如主要概念的定义）。我们建议制定一项针对电脑网络罪行的特定法例，当中包括我们建议的罪行，藉以全盘改革现行法律。

主要词语的定义

20. 据我们所观察，目前"电脑"（computer）在字典中的涵义反映现今的科技状况。[10]我们亦有考虑"电脑"在《证据条例》（第 8 章）中的定义（该定义就在刑事法律程序中接纳文件证据而拟定），[11]以及俄罗斯联邦于 2017 年向联合国提交的《联合国合作打击网络犯罪公约》草案（Draft United Nations Convention on Cooperation in Combating Cybercrime）（**《俄罗斯公约》**）对"资讯及通讯科技器材"的定义。[12] 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，其他司法管辖区的法例亦广泛使用"电脑"一词。

---

10 见《牛津英文字典》（Oxford English Dictionary）（2022 年 3 月）。该字典指"电脑"是*"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"*。

11 《证据条例》（第 8 章）第 22A(12)条将"电脑"界定为*"任何用作储存、处理或检索资料的装置"*。

12 《俄罗斯公约》第四条第(o)款将"资讯及通讯科技器材"界定为*"任何用于或设计用于自动处理和储存电子资料的硬件组件的集合体（组合体）"*。

21. 尽管如此，我们紧记任何法定定义，包括“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演进。我们固然信任法院可因应科技进步而灵活地解释任何定义，以尽量体现真正的立法原意，但法定定义在实际应用上仍可能会出现困难，这是因为被告人或会极力提出各种技术性论点，辩称某“器材”在法律上并不构成立法机关原意中的“电脑”。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，然而，若政府落实我们的建议，法律草拟专员可在立法阶段进一步考虑这个议题。

把纯粹在未获授权下取用或取览定为不合法

22. 在香港（第 27A 条）及某些其他司法管辖区，纯粹在未获授权下取用或取览已属犯罪。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。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。

23. 我们曾详尽讨论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的情境到底有多类似。就此而言，我们必须指出，鉴于虚拟空间的设计和运作的固有特点，在某些获广泛接受的情况下，网上用户均已默示给予取览程式或数据的授权。举例来说，我们一般并不预期网上用户须事先寻求明示授权，方可在另一用户浏览的网页上展示广告。正如搜寻器在扫描有关互联网规约地址前，通常不会事先取得网站的同意。我们认为，应继续容许这些已获视为给予默示授权的惯常做法。在这基础上，小组委员会大多数成员认为，纯粹在未获授权下取用或取览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。我们认为，这种做法与处理现实世界中对等行为的方式一致，并使法律明确，因为要定夺在未获授权下取用或取览应实际在何时定为不合法，可能并不容易（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）。

取用或取览的未获授权性质

24. 新法例应明文订定，只有在未获授权下取用或取览，方会受禁，从而提供指引以消除不必要的争议。至于应如何阐述取用或取览的未获授权性质，我们认为，英格兰及威尔斯的《1990 年误用电脑法令》（Computer Misuse Act 1990，**《英格兰误用电脑法令》**）第 17(5)

及(8)条（如上议院在 *R v Bow Street Metropolitan Stipendiary Magistrate, Ex parte United States (No 2)*[13] 所解释），就当地的在未获授权下取览电脑资料罪所采用的拟定方式较为可取。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及情况而定。

25. 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。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。正如在现实世界那样，按常理判断这项方针应适用于定夺某项取用或取览在电脑网络空间上是否已获授权。

取览程式或数据

26. "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。[14] 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。

合理辩解可作为免责辩护

27. 我们建议订定以合理辩解为基础的概括性免责辩护，因为这样能更有效兼顾公众利益，应付未能预见的情况，并给予法院弹性。

加重罪行

28. 单靠建议的简易程序罪行，将不足以应对犯罪者或会在取览程式或数据后进一步带来可能严重的伤害（例如安装间谍软件，或勒索受害人）。

29. 我们建议，在未获授权下取览并意图进行其他犯罪活动，应构成加重罪行。至于哪些其他犯罪活动应藉这种加重罪行而受到惩处，《英格兰误用电脑法令》第 2(2)条的拟定方式可作为考虑起点。

---

13 [2000] 2 AC 216.

14 "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"*，"数据"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"*。在非技术层面上，"数据"亦指*"数码形式的资料"*。见《牛津英文字典》（2022 年 3 月）。

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

30. "网络安全"这个概念是以保护电脑系统免受数码攻击的做法作为根基。[15]我们曾广泛讨论在未获授权下为网络安全目的而取览，显示有不同论据支持和反对禁止在未获授权下为网络安全目的而取览，要平衡兼顾这些互相矛盾的论据实有困难。以下举出部分相关考虑因素及背景：

(a) 在电脑网络空间，总会有人在未获授权下测试（例如以"连接埠扫描"的方式测试）他人的电脑。测试工具既容易获取，又得到广泛使用。这些测试可能是出于善意、商业目的或恶意。

(b) 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，这些公司或会从中牟利。

(c) 网络安全是个不断变化的领域，评审情况亦一直演变。没有业界机构获视为唯一权威。在香港，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。

---

15 例如，"网络安全"一直被理解为*"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"*。网络安全又称为*"资讯科技安全"*。见 Marion and Twede, *Cybercrime: An Encyclopedia of Digital Crime* (ABC-CLIO, 2020), 第 92 页。

(d) 禁止各种未获授权的测试将无法阻止他人从其他司法管辖区扫描在香港的电脑系统，而且会对网络安全公司构成影响，却无法制止罪犯识别这些保安漏洞。

31. 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。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。

32. 我们希望指出，若网络安全业界的专业人员获给予免责辩护或豁免，便会出现如何可确定或核实这类专业人员的身分这个基本问题。可行方案似乎是制订某种形式的评审制度，由法定或行政评审团体备存一份可供查阅的网络安全专业人员名单。因此，我们邀请公众就建议 2(a)(i)及(ii)所载的问题，对评审制度的方式、方法及运作细节发表意见。

33. 另一方面，若社会各界认为，不断演变的评审情况会对实施正式的评审架构造成阻碍，另一可行做法，是在新订针对电脑网络罪行的特定法例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，前提是有可靠的方法确定某网络安全从业员是否符合有关法定规定。我们欢迎公众就载于下文建议 2(a)(iii)的问题提出这方面的意见。

34. 最后，由于非保安专业人员亦可能作出非法取览程式或数据的作为，故我们邀请公众对非保安专业人员就非法取览罪应否有任何合法辩解这问题提出意见，正如我们亦同样在第 5 章就非法干扰电脑系统罪征询公众在这方面的意见。[16]

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：

16 见下文第 80 至 81 段。

(i) 该免责辩护或豁免应否只适用于经认可专业团体或评审团体审定的人士？

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

(iii) 反之，如不属意设立评审制度，则新订针对电脑网络罪行的特定法例应否订明指认的网络安全专业人员须符合某些规定，方可援引建议为网络安全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）？[17]

简易程序案件的时效期

35. 《裁判官条例》（第 227 章）订定一般时效期为所涉事项发生后起计的六个月，但如规管某简易程序罪行的有关法例另有规定则除外。受害人可能在电脑网络罪行案件发生后的两至三个月才向警方报案，而更甚者，是事件被揭发时六个月已届满。警方从互联网服务供应商取得日志纪录，可能需时数月。分析这些日志纪录可能另需数月，还须顾及达至检控决定所需的额外时间。

36. 由于预设时效期或不足够，我们建议把时效期如下述般延长。

---

17 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安全和完整而扫描服务供应商的系统。

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。

第 3 章：非法截取电脑数据

37. 概括而言，就截取电脑数据而订立的罪行，旨在把在没有法律权限的情况下进行的截取定为不合法，从而保障人们的数据通讯私隐权。

香港的现行法律

38. 《基本法》规定，香港居民享有言论自由（第二十七条），他们的通讯自由和通讯秘密受法律的保护（第三十条）。

39. 《香港人权法案》规定，任何人之私生活或通信，不得无理或非法侵扰（第十四条），以及人人有发表自由之权利（第十六（二）条）。

40. 《截取通讯及监察条例》（第 589 章）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。然而，该条例只适用于公职人员，并只规管截取在*"传送过程中"*的通讯。

41. 根据《电讯条例》第 27(b)条（"**第 27(b)条**"），任何人损坏、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，即属犯罪。

42. 虽然电脑按理应可构成"电讯装置"，如任何人具备所订意图而损坏、移走或干扰电脑，第 27(b)条便会适用，但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。

43. 此外，根据第 27(b)条，拟截取的目标只限于"任何讯息的内容"。这句显然并不涵盖元数据（即关于通讯本身的资料，而非通讯的内容或实质内容）。考虑到元数据对通讯各方的重要性，以及它对

通讯各方以外的人的潜在价值，元数据可与“任何讯息的内容”同样值得受到保障。

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

44. 据我们理解，任何未经编码处理的电脑数据，如在公开网络上传送，便可被外界截取。电脑数据即使被截取，仍可能继续传送。

45. 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。

为不诚实或犯罪目的而截取

46. 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，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。

47. 我们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。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

48. 《布达佩斯公约》第三条处理非法截取电脑数据，该条并无规定有关电脑数据须为私人数据。另外，据我们理解，新西兰的法律委员会（Law Commission）及司法部（Ministry of Justice）已提议以“通讯”取代新西兰《2012 年搜查及监察法令》（Search and Surveillance Act 2012）中对“私人通讯”的提述。我们同样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

49. 互联网采用分层方式，某层的元数据可能是另一层的数据。元数据并非定义明确的概念。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）。

罪行适用于整个传送过程中的数据

50. 某些种类的互联网通讯采用名为"存储转发"传递的机制，即通讯可于前往目的地途中多次暂存在网络上。由此引起的问题是：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。

51. 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，在没有法律权限的情况下截取有关数据便应属犯罪。订立这项罪行的方法之一，是加入类似于澳大利亚《1979 年电讯（截取及取览）法令》（联邦）（Telecommunications (Interception and Access) Act 1979 (Cth)）第 5F 条的条文，以推定通讯何时视为开始经过通讯系统，以及通讯何时视为继续经过该系统。

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）[18] 第 8 条为蓝本，包括犯罪意念（即"蓄意"截取）。

[18] 由英联邦（Commonwealth of Nations）经参照《布达佩斯公约》制定。

社会可能视为正当调查的行为

52. 正如我们就建议的非法取览程式或数据罪（第 2 章），邀请公众对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这个议题提交意见书，我们亦欢迎社会各界就建议的非法截取电脑数据罪会否无意间对社会可能视为正当调查的行为造成影响这个议题发表意见。

真实业务进行的截取

53. 另一议题是：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），应否获准截取传送的数据。该等数据可能有不少用途，例如分析雇员电脑内的数据，以确定他有否违反限制性契诺；以及追踪顾客连接至购物商场内网络系统的智能电话或平板电脑，以查探顾客的喜好。

54. 据我们所观察，规模较大的业务一般有能力就提供 Wi-Fi 热点或电脑供人使用而拟定周全细密的条款及条件。有关条款及条件可保留合约权利截取和使用顾客或雇员的数据。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。

55. 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。由于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，因此在应否准许第 52 及 53 段所述的各类数据截取和使用的问题上，我们邀请公众发表意见。如意见是应准许的话，我们欢迎公众进一步建议应准许哪类专业及业务截取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。我们冀望公众能就以下咨询问题发表意见，这将有助我们考虑应如何拟定建议的免责辩护或豁免。

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

56. 概括而言，就非法干扰（而非截取）电脑数据而订立的罪行，旨在打击蓄意损坏、删除、更改电脑数据等行为，从而保护有关数据的完整性，确保有关数据能正常运作或使用。

57. 非法取览罪与非法干扰数据罪息息相关，因为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。

香港的现行法律

58. 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《刑事罪行条例》第 60(1)条所订刑事损坏的一种形式。第 60(2)条订明的有关加重罪行，适用于意图危害他人生命或罔顾他人生命是否会因而受到危害的被告人。《刑事罪行条例》于 1993 年修订，藉以：

(a) 将该条例就"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……"*；[19] 及

(b) 订明摧毁或损坏财产，就电脑而言，包括"误用电脑"。[20]

---

19 《刑事罪行条例》第 59(1)(b)条。

20 《刑事罪行条例》第 59(1A)条将"误用电脑"界定为以下作为，当中(b)及(c)段与非法干扰电脑数据（而非干扰电脑系统）最为相关：

"(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。"

59. 针对电脑网络罪行而言，已有案例展示《刑事罪行条例》第60条（"**第60条**"）成功执行。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。这两项条文的分别之一，在于第60条的犯罪意念（怀有意图或罔顾后果）可能比第161(1)(a)至(d)条所详述的意图更易证明。[21]

60. 根据《电讯条例》第25(a)条（"**第25(a)条**"），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，如故意隐匿、扣留或阻延拟传递予另一人的讯息，即属犯罪。

61. 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：

(a) 由于第25(a)条以电讯为前提背景，故该条的拟定方式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）。

小组委员会的看法

禁止在未获授权下蓄意干扰数据

62. 每逢有人操作电脑或电脑与互联网有互动，数据便难免会被更改。举例来说，电邮伺服器会移除具危险性的电邮附件。网站可能会在访客的电脑内储存"小型文字档案（cookies）"，藉以在该电脑上增加数据。即使上述对电脑数据的更改是蓄意作出的（是电邮伺服器或网站管理人有意导致的），很多电脑使用者大概都会接受这类更改。

63. 与此同时，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。

64. 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。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、[22]弄坏、更改或抑制）电脑数据定为罪行。

---

21 见上文第10段。

22 即使可利用某些数据复原工具将数据复原。

犯罪行为、犯罪意念、合法辩解及加重罪行

65. 我们以现行法律——具体而言为《刑事罪行条例》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。

66. 我们一致认为现有体制（包括所订的犯罪行为、犯罪意念、两项合法辩解及加重罪行）整体上令人满意。

把有关罪行改列于新法例

67. 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，以打击电脑网络罪行，同时删除《刑事罪行条例》第 59(1)(b)及(1A)条（当初在《刑事罪行条例》加入该条，是为了就电脑而言，扩大刑事损坏财产这项一般罪行的涵盖范围）。

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

68. 概括而言，就非法干扰电脑系统（而非电脑数据）而订立的罪行，旨在禁止藉使用或干扰电脑数据，阻碍合法使用电脑系统，从而确保电脑系统能正常运作。

69. 即使数据未经修改，电脑系统的运作也有可能受阻。举例来说，如藉进行分布式拒绝服务攻击[23]或慢速攻击（slow attack），阻碍取用电脑网络或限制电脑网络的运作，便可能导致上述情况。

70. 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，可能在于导致该结果的各方是否意图攻击该系统。

香港的现行法律

71. 如上文所论述，《刑事罪行条例》第 60 条所订刑事损坏的其中一种形式，是第 59(1A)条所界定的"误用电脑"。第 59(1A)(a)条[24]与非法干扰电脑系统最为相关。案例已确立分布式拒绝服务攻击可构成"误用电脑"。[25]

72. 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*），[26]终审法院裁定电脑按所设定的"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。案中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。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影响，因此该次攻击并不成功。尽管如此，终审法院仍裁定维持对被告人的定罪。

73. 另一方面，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第 59(1A)(c)条。[27]

---

23 分布式拒绝服务攻击可藉"僵尸网络（botnet）"（即一组被入侵的电脑）发动。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。有关电脑的拥有人可能是无辜并蒙在鼓里的。

24 见注脚 20。

25 *香港特别行政区 诉 朱婷婷* [2017] 4 HKLRD 651, HCMA 33/2016（判决日期：2016 年 10 月 11 日）。

26 (2019) 22 HKCFAR 30, [2019] HKCFA 3.

27 见注脚 20, 以及*香港特别行政区 诉 朱峻玮* (2019) 22 HKCFAR 30, 第 37 页, [2019] HKCFA 3（第 18 段）。

小组委员会的看法

一致处理干扰数据及干扰系统

74. 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。现有法例的整体施行情况理想。

75. 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

76. 我们曾考虑如"误用电脑"的概念不再属刑事损坏罪的涵盖范围，而是（如建议 6(c)所提议）一项并非载于《刑事罪行条例》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。

77. 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

78. 如将相关条文从《刑事罪行条例》迁往新法例，便可藉此机会完善"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[28] 在新法例中的对等条文；及

(b) 将诸如"损害任何电脑的操作"的概念纳入"误用电脑"的定义。

---

[28] 见上文注脚 20。

建议罪行的适用范围

79. 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下述建议 7(d)所提到的各方。

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

80. 前述部分曾提及,[29] 总会有人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。用作进行这些测试的工具唾手可得，现时已有各种各样的测试工具可导致不同程度的入侵。关键问题在于如何使用有关工具。

81. 我们邀请公众就以下问题提交意见书：扫描（或以类似的形式测试）他人的电脑，应否足以视为建议的非法干扰电脑系统罪的合法辩解。对于法律应如何平衡网络安全从业员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。

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；[30] 及／或

---

29 见上文第 30(a)段。

30 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）。

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

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

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

第 6 章：提供或管有用作犯罪的器材或数据

82. 如任何人将某器材或数据（例如消磁器、破解密码工具或进行渗透测试的软件）实际用作干犯电脑网络罪行，便可因干犯建议的特定依赖电脑网络的罪行而受惩处。概括而言，就提供或管有这类器材或数据而订立的独立罪行，旨在遏制生产、供应和管有可在电脑网络空间作非法用途的器材或数据，藉以防止这类器材或数据被用作干犯电脑网络罪行。

香港的现行法律

83. 根据《刑事罪行条例》第 62 条（"**第 62 条**"），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，以摧毁或损坏财产，即属犯罪。

84. 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，第 62 条并没有加以区分。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。

85. 另外，第 62 条的英文文本用"anything"一词来描述受禁物。按照一般的说法，该词并不限于有形物，涵盖范围亦似乎比中文文本的对应词"任何物品"更广。然而，该中文用词的惯常涵义会否明确引伸至某些无形物，例如恶意软件及有关利用漏洞（exploit）的专门知识，则是截然不同的问题。

86. 此外，第 62 条与第 60 条所订的刑事损坏罪相关。对于其他条文所订罪行（例如第 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。

87. 《电讯条例》虽然并无与第 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。在该制度适用的情况下，违反有关规定，即属犯罪。

88. 该制度可能适用于可用作干犯电脑网络罪行的电脑或智能电话，但我们认为，该制度有所不足。举例来说，该制度的涵盖范围狭窄，只适用于无线电波等电讯技术。

小组委员会的看法

应订立兼具基本及加重形式的新罪行

89. 我们认为，新法例应加入与第 62 条相对应的条文，而该条文亦应适用于咨询文件第 2 至 5 章所论述的全部四类依赖电脑网络的罪行。

90. 兼具合法及非法用途的器材及数据所带来的挑战，与现实世界中攻击性武器所带来的挑战相类似。在应用《公安条例》（第 245 章）对"攻击性武器"的定义时：

(a) 在涉及被"制造"或"改装"以用作伤害他人的物品的案件中，无须证明犯罪意图。纯粹在公众地方管有该物品，便足以招致刑事法律责任；而

(b) 本属中性的物品，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。

91. 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。

建议罪行所应适用的器材及数据

92. 我们认为，为确保能在电脑网络空间有效执行建议的（基本形式及加重形式）罪行，该罪行应适用于有形物及无形物。鉴于已有新西兰法例作为先例，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。根据第 62 条及*朱峻玮*

案，建议的罪行亦应适用于任何人相信或声称能够用作犯罪的器材或数据，不论该人所信或所声称的是否属实。

93. 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。因此，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。

94. 我们建议，基本罪行应涵盖被制造或改装以用作犯罪的器材或数据。我们亦建议，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

95. "黑客工具"及相类工具存有市场。因应该类市场的蓬勃发展而采取的周全法定措施，必须针对市场各类参与者。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。

犯罪意念

96. 我们认为，任何人应仅在行事时知悉有关事实的情况下，方属干犯建议的基本或加重罪行。由于人们管有软件或电脑数据十分普遍，甚至在自己不知悉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。该罪行的适用范围似乎会过于广阔。

97. 如任何人因相信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。

98. 如任何人被控加重罪行，按照定义，除了须证明上文第 96 及 97 段所提及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

99. 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"*。[31] 为免出现过度刑事化的问题，我们认为，建

[31] 《公安条例》（第 245 章）第 33(1)条，例如管有人在表演艺术时使用长兵器。

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。

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

(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》（Computer Misuse Act）（第 50A 章）第 8 及 10 条为蓝本。

管有只可作有害用途的数据

100. 尽管勒索软件、病毒、建立及管理僵尸网络的软件，以及收集软件（harvesting software）等电脑数据只可用作进行网络攻击，实属有害，但亦有论点认为，如管有该等数据的目的是用作例如教学、研究或开发防毒软件，法律无须（或不应）把管有该等数据定为罪行。因此，我们提出以下咨询问题。

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

101. 我们在研究与电脑网络罪行相关的司法管辖权事宜时，集中探讨香港法庭行使司法管辖权的准则。

有关司法管辖权的一般原则

普通法的做法

102. 一般而言，对于普通法罪行及法定罪行，法庭的刑事司法管辖权受地域所限，行使范围不会延伸至涵盖在外地所作的作为。[32]

103. 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，这些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。

104. 然而，多个普通法司法管辖区现已采纳某些更具弹性的观点。香港法庭认同英格兰及威尔斯采纳的观点，根据该观点，法庭可在以下情况下，行使司法管辖权：

(a) 假如最后的作为在有关司法管辖区发生，或该罪行的绝大部分在有关司法管辖区所犯；及

(b) 并无出于相互尊重的理由而令该罪行不应在有关司法管辖区审讯。

订明司法管辖权规则的香港法例

105. 《刑事司法管辖权条例》（第461章）（**《刑事司法管辖权条例》**）第2(2)条把若干欺诈和不诚实的实质罪行，界定为甲类罪行。《刑事司法管辖权条例》第3条规定，就任何甲类罪行而言，只要任何"有关事情"——即是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。

106. 2002年，政府建议把三项电脑罪行[33]列入甲类罪行。该项建议因得不到立法会相关小组委员会支持而未有落实。

---

32 然而，不少国家亦声称对在悬挂有关国家国旗的船舶上和根据该国法律注册的飞机上所犯的罪行具有司法管辖权。见《电脑网络罪行公约说明报告》（Explanatory Report to the Convention on Cybercrime）第235段。

33 这些罪行分别是《电讯条例》第27A条所订的"藉电讯而在未获授权下取用电脑资料"罪、《刑事罪行条例》第59及60条所订的与误用电脑有关的"摧毁或损坏财产"罪，以及《刑事罪行条例》第161条所订的"有犯罪或不诚实意图而取用电脑"罪。

107. 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。[34]

普遍获接受的域外管辖权基础

108. 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。

与电脑网络罪行相关的司法管辖权事宜

法庭已意会电脑网络罪行带来的挑战

109. 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。要决定某项事实在何处发生可能不易。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。[35]

110. 解决司法管辖权的冲突是国际间打击跨境罪案重要的一环。实际上，受影响地方一向通过磋商解决问题，而部分地区的文书亦有就国与国之间的法律合作可考虑的因素提供指引。[36] 在香港签订任何

---

34 例子见《刑事罪行条例》第 153P 及 153Q 条（与附表 2 一并理解），以及《防止贿赂条例》（第 201 章）第 4 条。

35 举例而言，在 *DPP v Sutcliffe* [2001] VSC 43, 第 62–63 段，澳大利亚维多利亚最高法院（Supreme Court of Victoria）承认*"互联网提供了迅速快捷且相对便宜的通讯方式，让……人互相通讯"*，以及取用*"不只限于拥有电脑……法律须随着这些转变而发展。"*

36 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。

有关双边协议之前，须获得中央人民政府授权，[37] 我们预计，如我们的建议获落实推行，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，[38] 而禁止一罪兩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。[39]

小组委员会的看法

初步考虑

111. 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。新法例应明确订明多种适用于所订罪行的司法管辖权规则。检控部门保留酌情权，决定应否提出检控，这做法亦可为公众提供保障，切合我们的指导原则。

112. 香港依循司法管辖区应在合理范围内，为其法律的任何域外应用订定条文这国际惯例，亦属恰当。我们参照以下事实情况，讨论咨询文件所建议的罪行：

(a) 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（比照《刑事司法管辖权条例》第 3 条）；

(b) 犯罪者是"香港人"；

(c) 受害人是"香港人"；

(d) 目标电脑、程式或数据处于香港；及

(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）。

---

37 根据《基本法》，中央人民政府负责管理与香港有关的外交事务，而香港获授权自行处理有关的对外事务（按照第一百五十一条的规定，即经济、贸易、金融、航运、通讯、旅游、文化、体育等领域）。

38 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。见第 113 至 127 段。

39 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）。

非法取览程式或数据

113. 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)。

114. 我们不建议应用事实情况(b)，因为该情况亦涵盖没有任何"香港人"受害的案件。[40] 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。

115. 我们认为应用事实情况(c)，有助加强这项建议的罪行所提供的保障。由于电脑网络罪行所涉的各方可能身处多个司法管辖区，受害人这概念应采用宽广的定义。举例来说，如某云端伺服器持有的数据由另一司法管辖区的人拥有，该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。为与这项建议的罪行的焦点一致，我们的结论是赞成以此方式尽量扩大所提供的保障范围，因为重点应是须予保护的数据。

116. 我们认为，施加双重犯罪的规定可能有违加强保障公众这目的。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。我们提议，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。总括来说，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；

[40] 例如犯罪者（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的案件。

(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

(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

117. 基于类似理由，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。

118. 我们不建议应用事实情况(b)，因为上文就首项建议的罪行所提出的论点——即是很可能并非"香港人"受害，以及在香港提出检控可能并不可行——在此处同样适用。

119. 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。这项建议的罪行类似非法取览程式或数据的加重罪行，多于类似非法取览程式或数据的简易程序罪行。

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

(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

120. 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。

121. 由于我们不建议将事实情况(b)应用于首两项建议的罪行，我们同样不建议将事实情况(b)应用于这项建议的罪行。

122. 我们亦留意到，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。

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；

(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

123. 我们建议用相同方式处理前项罪行及这项建议的罪行。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。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；

(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

124. 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。虽然这两种形式轻重有别，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。

125. 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)及(d)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。

126. 就*管有*器材或数据的部分而言，假如器材或数据储存于例如云端伺服器，若说是在管有人所处的位置管有该器材或数据，未必能反映现实。就*提供*器材或数据的部分而言，如恶意软件被上载到互联

网，理论上这套恶意软件可提供予世界上每个角落任何能接达互联网的人。因此，我们建议将事实情况(a)、(b)及(e)应用于这项建议的罪行。

127. 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。我们认为，相同的理据亦适用于建议的提供或管有用作犯罪的器材或数据罪，因此有关建议亦同样适用。

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

(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

128. 我们在研究香港法庭对电脑网络罪行的看法后，就各项建议的罪行提出适当的最高刑罚。香港及其他司法管辖区就相应的电脑网络罪行所订的最高刑罚，见咨询文件的附录摘要。

129. 概括而言，法庭一致将入侵、损坏或误用电脑的案件，视为严重案件。例如，终审法院上诉委员会指出，故意损坏电脑软件及数据的行为，通常应判处扣押刑罚。[41]

小组委员会的看法

各项建议的较严重罪行

130. 鉴于咨询文件所建议的各项非简易程序罪行，均可造成重大伤害，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）。

131. 我们明白电脑网络罪行所致伤害的严重程度差别甚大，并建议前段(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。

132. 在仔细讨论时，我们考虑了以下因素：各级法庭的判刑权限、现有电脑网络罪行的最高刑罚、《盗窃罪条例》（第 210 章）就某几类具代表性罪行所订的最高刑罚，以及其他司法管辖区相若罪行的最高刑罚。我们认为，我们就上文第 130 段所列的各项建议罪行而建议的最高刑罚（可处 14 年监禁），不但会发挥必要的阻吓作用，亦不会过分偏离我们所参考的最高刑罚。

133. 我们亦认为，循简易程序定罪的最高监禁刑期若订为两年，便会与我们关于循公诉程序定罪的案件的建议相称。

建议的非法取览程式或数据的简易程序罪行

134. 在某程度上，这项建议的罪行与第 27A 条所订的罪行性质相若。然而，第 27A 条甚少获援引，而且该条的最高刑罚（第 4 级罚

---

41 *廖伟信 诉 香港特别行政区*（*Liu Wai Shun v HKSAR*），FAMC 30/2004（判决日期：2004 年 9 月 27 日），第 7 段。

款，现为 25,000 元）看来颇轻。我们认为，即使是简易程序案件，亦应有判监的可能性。我们建议，这项建议的罪行的最高监禁刑期，应订为两年。

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

135. 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 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

136. 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，因此应视为严重罪行，并应可处七年监禁，即相关加重罪行的建议最高刑罚的一半。

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。