（供学术交流使用）

缅甸联邦共和国网络安全法

编译：西北政法大学涉外刑事法治与国别检察司法研究中心

目 录

缅甸联邦共和国网络安全法

第一章 名称、生效与管辖权

1. 名称

本法称为《网络安全法》。

2. 生效

本法自总统通过通告指定的日期起生效。

3. 管辖权

(a) 任何人犯有本法规定的下列犯罪，应根据本法进行审理与判刑：

(1) 在本国境内或根据本国现行法律注册的船舶或航空器上实施的犯罪；

(2) 在国家网络空间内或连接到国家网络空间的其他任何网络空间中实施的犯罪。

(b) 居住在国外的缅甸公民犯有本法规定犯罪的，应根据本法进行审理与判刑。

第二章 定义

4. 释义

下列用语应具有以下含义：

(a) “国家”指缅甸联邦共和国；

(b) “中央委员会”指根据本法由联邦政府组建的网络安全中央委员会；

(c) “指导委员会”指由中央委员会组建的网络安全指导委员会；

(d) “主管部”指负责执行本法事项的部；

(e) “相关部委或机构”指联邦政府指定的与网络安全事项相关的任何联邦部或联邦级机构，包括国防部、内政部和缅甸中央银行；

(f) “主管司”指主管部内被分配负责执行本法事项的司；

(g) “侦查小组”指经中央委员会同意，由指导委员会设立以根据本法规定进行侦查的小组；

(h) “网络安全”指保护信息、网络资源或电子信息免受未经授权的访问、披露、传输、分发、使用、干扰、修改或销毁，或保护关键信息基础设施免受未经授权的使用、中断、修改、销毁及相关企图；

(i) “网络安全服务”指利用网络资源或类似技术及相关设备提供网络安全服务的业态。该术语还包括主管部随时确定的服务；

(j) “网络安全服务提供商”指获准在本国境内提供网络安全服务的个人或组织。包括对可执行活动的指导或描述；

(k) “数字平台服务”指利用网络资源或类似技术及相关设备，使用户能够在线展示、传输、分发或使用信息的业态；

(l) “数字平台服务提供商”指向本国境内提供可使用的数字平台服务的个人或组织；

(m) “信息”指数据、数据库、声音、文本、图像、代码、符号、信号、视频、软件或应用程序；

(n) “电子信息”指通过电子技术（包括传真和电子邮件）、电磁波技术或任何其他技术创建、传输、接收或存储的信息；

(o) “数据”指可以存储在网络或计算机系统中各种格式的数据；

(p) “网络资源”指计算机、计算机系统、计算机程序、网络、网络设备、数据库，或与这些要素及相关设备相关的发展技术；

(q) “计算机”指能够通过电子技术、电磁波技术或任何其他技术进行提示，以获取、存储、传输、处理，并在需要时检索和使用信息，并使用数学和逻辑方法使用信息的设备；

(r) “计算机程序”指在计算机系统运行期间，引用数据并使计算机系统执行特定操作的一组指令或描述；

(s) “计算机系统”指通过各种设备组成的、可使用程序进行自动数据处理的系统，或由互连或相关设备组成的设备系统。该表述还包括与计算机系统连接并使用的任何类型的可移动存储介质系统；

(t) “网络”指通过电信技术创建的、用于互连和使用网络资源或类似技术及相关设备的连接集合；

(u) “VPN（虚拟专用网络）”指使用特定技术在原始网络内设置的安全保障系统，以确保连接网络时的安全性；

(v) “网络设备”指网络运行执行中使用的任何物理基础设施项目，或此类项目的组合；

(w) “数据分析”指利用网络资源或类似技术及相关设备，出于网络安全目的收集、分析和检查任何信息或其部分的过程；

(x) “恶意软件”指破坏或损害网络资源的恶意代码；

(y) “网络空间”指利用网络资源或类似技术及相关设备，在网络内或互连网络之间发送、通信、分发或接收电子信息的环境；

(z) “网络攻击”指在网络空间利用网络资源或类似技术及相关设备，对国家行政、财政、经济、执法、国家安全及公共安全，以及国家内的生命财产造成危害或损害，或以任何方式中断、扭曲、暂停或破坏信息通信的行为；

(za) “网络犯罪”指利用网络资源或类似技术及相关设备，在网络空间实施、企图实施、教唆、怂恿或作为共犯参与本法规定的任何犯罪或现行法律规定的任何应受惩罚的犯罪的行为；

(aa) “网络安全威胁”指试图利用网络资源或类似技术及相关设备在网络空间损害网络安全的行为；

(ba) “数字实验室”指能够对存储的电子数据进行识别、检索、处理、分析和报告的技术辅助实验室；

(ca) “在线赌博系统”指利用网络资源或类似技术及相关设备，实现以金钱、具有货币价值的东西或约定作为金钱转让的赌注（无论是否有奖品）的机会游戏和技能游戏的赌博系统；

(da) “网络安全团体”指经指导委员会按规定许可，在本国境内开展网络安全活动而不寻求利润的组织。

第三章 目标

5. 目标

本法的目标如下：

(a) 确保网络资源、关键信息基础设施和电子信息的安全使用；

(b) 利用电子技术保护和维护国家主权与稳定，抵御网络安全威胁、网络攻击或网络滥用；

(c) 系统地发展网络安全服务；

(d) 有效侦查和起诉网络犯罪；

(e) 支持基于网络资源的数字经济。

第四章 中央委员会的设立、职责与权力

6. 设立

联邦政府：

(a) 为实现本法目标，应设立网络安全中央委员会，由副总统担任主席，主管部的联邦部长担任副主席，相关部的联邦部长及相关联邦级机构的主席担任成员。

(b) 在设立中央委员会时，应任命秘书和联合秘书并分配职责。

(c) 如有必要，可根据(a)款的规定重组中央委员会。

7. 职责与权力

中央委员会的职责和权力如下：

(a) 为国家网络空间的健康和安全发展制定网络安全政策、战略或行动计划；

(b) 为指导、监督和协调网络安全政策、战略或行动计划的实施，并与区域及其他国家、国际和地区组织开展合作；

(c) 促进网络安全人力资源的开发；

(d) 促进网络安全及网络犯罪预防所需基础设施的发展；

(e) 在相关政府部门和组织之间提供协调和指导，以支持网络安全、网络犯罪预防、执法和司法；

(f) 提供指导，确保关键信息基础设施的网络安全服务按照网络

安全计划进行协调；

(g) 确定公众连接的国家网络空间内关键信息基础设施的信息存储；

(h) 按规定授权设立国家数字实验室和数字实验室；

(i) 必要时指导相关部委或机构发布在线金融服务的政策、法规、条款、命令和指示；

(j) 执行联邦政府随时分配的网络安全相关职责。

第五章 指导委员会的设立、职责与权

8. 设立

中央委员会：

(a) 为执行和监督本法下的网络安全活动，应设立指导委员会，由主管部的联邦部长担任主席，相关部委的副部长或常任秘书、相关联邦级机构的副主席或常任秘书、网络安全专家和非政府组织代表担任成员，并由主管司的司长担任秘书。

(b) 如有必要，可根据(a)款的规定重组指导委员会。

(c) 允许非公务员的指导委员会成员领取联邦政府确定的津贴和酬金。

9. 职责与权力

指导委员会的职责和权力如下：

(a) 根据指导方针执行中央委员会制定的网络安全政策、战略或行动计划；

(b) 开展与网络安全相关的人力资源开发活动；

(c) 采取措施确保在发生网络攻击时及时响应和保护系统的到位；

(d) 与相关部委或机构协调，确保国家网络安全；

(e) 研究并向中央委员会提交关于国家是否应加入网络安全或网络犯罪公约、条约和协定的事宜；

(f) 根据国家加入的网络安全或网络犯罪公约、条约和协定进行实施与合作；

(g) 与国际组织、区域组织和邻国就网络安全威胁、网络攻击、网络滥用或网络犯罪相关的信息交换、侦查和行动开展合作；

(h) 发布和公布网络安全建议信息以提高公众意识，并报告、公布和预防网络攻击及网络威胁；

(i) 与网络安全事件响应小组协调保护关键基础设施的活动；

(j) 检查、监督和指导关键信息基础设施的信息是否按规定存储；

(k) 授权审查网络安全团体，发布这些团体必须遵守的条款，并对未经许可设立的网络安全团体采取行动；

(l) 确定根据本法收取的许可费、注册费、罚款或其他费用；

(m) 制定关于本国制造、安装或从国外进口的网资源的政策和标准；

(n) 在执行本法时，如有必要进行侦查，经中央委员会同意，设立侦查小组并确定其职责和权力；

(o) 每年至少一次向中央委员会提交活动报告和其他必要报告；

(p) 执行中央委员会随时分配的网络安全相关职责。

10. 工作委员会的设立

指导委员会经中央委员会同意，可设立以下工作委员会并分配职责：

(a) 网络安全工作委员会；

(b) 网络犯罪工作委员会；

(c) 网络防御工作委员会；

(d) 其他必要的工作委员会。

第六章 主管司的职责与权力

11. 秘书处职能

主管司应负责履行中央委员会和指导委员会秘书处团队的办公职能

12. 津贴支付

主管司应支付非公务员身份的指导委员会成员的津贴和酬金。

13. 具体职责

主管司：

(a) 在执行国际和区域网络安全合作倡议时，可根据主管部的指导方针与国际网络安全组织和区域网络安全组织沟通、协调与合作；

(b) 可根据国际标准进行网络安全技术和技能的胜任力测试或竞赛，并颁发证书；

(c) 应根据主管部的指导方针，在国内按行业实施网络安全合作活动；

(d) 经主管部批准，确定网络安全服务许可条款和数字平台服务注册条款；

(e) 应按规定收取根据本法应收取的许可费、注册费、罚款或其他费用；

(f) 负责执行中央委员会制定的网络安全政策、战略、行动计划和指导方针。

第七章 关键信息基础设施保护

14. 关键基础设施的范围

以下基础设施被视为关键信息基础设施：

(a) 国防与安全电子信息基础设施；

(b) 电子政务（e-Government）服务系统基础设施；

(c) 金融电子信息基础设施；

(d) 交通电子信息基础设施；

(e) 电信电子信息基础设施；

(f) 卫生电子信息基础设施；

(g) 电力与能源电子信息基础设施；

(h) 联邦政府同意后，中央委员会随时确定的电子信息基础设施。

15. 识别与维护

中央委员会应指导相关政府部门和政府组织识别、修改和维护关键信息基础设施。

16. 相关部门/组织的义务

相关政府部门和组织应对关键信息基础设施采取以下行动：

(a) 按规定制定网络安全计划；

(b) 设立网络安全事件响应小组；

(c) 任命合适人员作为关键信息基础设施管理和维护负责人；

(d) 每个日历年至少向指导委员会提交一次网络安全报告。

17. 负责人的义务

关键信息基础设施管理和维护负责人：

(a) 应根据数据的[分类]级别，按规定存储与关键信息基础设施相关的信息；

(b) 应按规定分发、发布、发送、接收和存储与关键信息基础设施相关的信息；

(c) 每个日历年至少通过相关政府部门或政府组织向主管部提交一次关于关键信息基础设施的网络安全报告。

18. 监督

在指导委员会的监督下，主管部应监督和检查关键信息基础设施的管理和维护负责人是否按规定采取了网络安全准备措施。

第八章 许可与注册颁发

19. 期限

主管司可将网络安全服务许可期限和数字平台注册期限设定为最短 3 年至最长 10 年。

20. 网络安全服务许可

网络安全服务提供商必须是根据《缅甸公司法》注册的公司，并应按规定向主管司申请以获得营业执照。

21. 审查与决定

主管司应审查根据第 20 条提交的申请是否符合规定，并采取以下行动：

(a) 如果申请符合规定，应要求申请人支付许可费并颁发许可证；

(b) 如果申请不符合规定，应要求申请人修改申请或拒绝颁发许可证。

22. 续期申请

如果网络安全服务提供商希望继续运营，必须在许可证到期前 6 个月按规定向主管司申请许可证续期。

23. 续期审查

主管司：

(a) 可审查许可证续期申请是否符合规定，并批准或拒绝；

(b) 如果主管司拒绝续期许可证，该拒绝不应影响许可证的剩余期限。

24. 数字平台注册

在本国拥有 10 万或以上用户的数字平台服务提供商，必须是根据《缅甸公司法》注册的公司，并应按规定向主管司申请注册。

25. 注册审查

主管司应审查根据第 24 条提交的申请是否符合规定，并采取以下行动：

(a) 如果申请符合规定，应要求申请人支付注册费并颁发注册证书；

(b) 如果申请不符合规定，应要求申请人修改申请或拒绝颁发注册证书。

26. 注册续期

如果数字平台服务提供商希望继续运营，必须在注册期届满前 6 个月按规定向主管司申请续期。

27. 续期决定

主管司：

(a) 可审查注册续期申请是否符合规定，并批准或拒绝；

(b) 如果主管司拒绝注册续期，该拒绝不应影响注册期的剩余期限。

28. 网络安全团体许可

网络安全团体应按规定获得中央委员会的许可，方可在本国境内开展非营利的网络安全活动。

第九章 服务提供商的义务

29. 网络安全服务提供商的义务

网络安全服务提供商应遵守以下规定：

(a) 根据相关法律法规，获取网络安全服务提供商希望活跃的业

务或行业所需的许可证或文件；

(b) 建立并实施网络安全预防计划，以协助主管司和网络安全事件响应小组；

(c) 就潜在的网络安全威胁和预防措施提供建议；

(d) 制定针对恶意软件或网络攻击的应急响应计划和解决方案；

(e) 在发生恶意软件或网络攻击时，及时实施适当的应急响应计划，解决并[处理]问题，并通知相关利益相关者；

(f) 应用网络安全技术和必要的国际标准；

(g) 防止访问服务的用户信息泄露、损坏或丢失；

(h) 发生异常网络安全事件时立即通知主管司；

(i) 遵守许可证条款；

(j) 按规定编制并提交网络安全工作报告。

30. 数字平台服务提供商的义务

数字平台服务提供商应遵守以下规定：

(a) 根据相关法律法规，获取数字平台服务提供商希望活跃的业务或行业所需的许可证或文件；

(b) 根据访问服务的用户数据的[分类]级别，按规定维护数据存储设备；

(c) 如果数字平台服务提供商希望通过数字平台服务开展任何相关业务或营利性业务，应依照相关法律进行；

(d) 遵守注册证书中的条款。

31. 内容管理义务

数字平台服务提供商应采取充分措施，在服务平台上发生以下任何情况时识别相关信息和网络资源：

(a) 出现煽动仇恨、破坏团结或扰乱和平与秩序的信息；

(b) 出现虚假新闻或谣言；

(c) 披露不适合公众观看的信息；

(d) 任何露骨色情图片、色情视频、儿童色情文本或符号的展示；

(e) 收到关于意图对个人造成社会或经济损害的投诉；

(f) 收到关于侵犯知识产权的投诉；

(g) 煽动、实施、企图实施、协助或教唆恐怖主义行为。

32. 处置义务

如果数字平台服务提供商以任何方式知悉第 31 条规定的任何行为发生，或被主管司就此通知，必须按规定及时阻止、删除、销毁或暂停该行为。

33. 数据留存

数字平台服务提供商应将有关服务用户的以下数据保留 3 年：

(a) 访问服务的用户的个人信息；

(b) 访问服务的用户的使用记录；

(c) 主管司随时指定的数据。

34. 数据提供

如果任何根据现行法律授权的个人或组织书面要求提供第 33 条

中的任何或全部数据，数字平台服务提供商应按规定提供。

35. 配合义务

网络安全服务提供商或数字平台服务提供商应在处理任何网络安全威胁、网络攻击或网络滥用事件时与相关工作委员会合作。

第十章 网络滥用

36. 网络滥用的定义

除非现行法律另有规定，未经授权人许可，为损害网络资源或计算机系统性能而实施的下列任何行为均视为网络滥用：

(a) 恶意更改、修改或删除任何计算机程序或信息，或其状态或质量；

(b) 恶意出售计算机程序或信息，或将其从其原始位置移动、转移或复制到另一个位置、另一个网络资源或任何存储设备；

(c) 以不诚实的意图获取、操作或使用计算机程序或电子信息；

(d) 修改、添加、销毁、改变、损害计算机程序或电子信息的性能，或以任何方式改变其原始状态；

(e) 控制或远程控制计算机系统、计算机程序或电子信息；

(f) 以不诚实的意图分析来自计算机程序或信息的数据。

第十一章 网络犯罪侦查与网络攻击预防

37. 工作委员会的职能

指导委员会根据本法设立的工作委员会，应在指导委员会的监督下履行以下职责：

(a) 防止网络安全威胁、网络攻击或网络滥用发生；

(b) 协助相关执法小组调查网络犯罪并评估网络犯罪风险；

(c) 采取预防措施，避免网络安全威胁、网络攻击或网络滥用可能造成的次生风险；

(d) 评估网络安全威胁、网络攻击或网络滥用事件发生的可能性及其发生后的潜在影响；

(e) 监测和评估相关部门网络安全水平的强弱，并向相关政府部门和组织提出改进网络安全的建议；

(f) 识别、调查网络安全威胁、网络攻击或网络滥用并采取行动；

(g) 评估网络安全服务提供商或数字平台服务提供商的服务；

(h) 为国家数字实验室和数字实验室提供技术支持。

38. 设备扣押

相关工作委员会可按规定扣押以下被认为涉及任何网络安全威胁、网络攻击或网络滥用事件的个人的网络资源进行分析：

(a) 使用或被怀疑使用了被认为涉及网络安全威胁、网络攻击或网络滥用事件的网络资源的人；

(b) 与(a)款中任何人有关联的人。

39. 归还

相关工作委员会在分析完网络资源中的数据并将其送交数字实验室检验后，应按规定将网络资源归还原提供者。

40. 数据分析授权

主管部经联邦政府同意，可指派相关人员或组织进行数据分析并送交数字实验室检验，以便提前识别和预防国家网络空间中的网络安

全威胁或网络攻击。

41. 电信支持

主管部应根据《电信法》，为提供电信服务的公司和组织提供必要支持，以便根据第 40 条进行数据分析和送交数字实验室检验。

42. 检查与控制

为了国防与安全事务、公共利益，或根据任何法律与相关政府部门或政府组织协商，主管部可在必要时进入网络安全服务企业或数字平台服务企业进行视察和控制。

43. 临时措施

主管部经联邦政府同意，出于公共利益需要，可采取以下措施：

(a) 暂时中止数字平台服务或电子信息；

(b) 暂时控制与数字平台服务相关的材料；

(c) 关闭数字平台服务或宣布其不适合公众使用。

44. VPN 许可

任何希望在国家网络空间内建立 VPN 或提供 VPN 服务的人，应按规定获得主管部的许可。

第十二章 证据扣押与专家证言提交

45. 证据扣押

侦查小组可根据本法和任何现行法律的规定，按规定扣押电子证据，以调查网络安全或网络犯罪事项。

46. 设备扣押与分析

在调查网络犯罪时，侦查小组可按规定扣押被认为与调查事项相

关的网络资源或类似技术及相关设备，并进行数据分析和送交数字实验室检验。

47. 实验室设立

相关政府部门或政府机构经中央委员会批准，可设立国家数字实验室或数字实验室，以根据本法和任何现行法律的规定，对存储的电子证据进行识别、获取、处理、分析和报告。

48. 实验室支持

指导委员会应为经中央委员会批准设立的国家数字实验室和数字实验室提供必要的技术支持和人力资源协助。

49. 专家证言

侦查小组可将存储的电子证据送至国家数字实验室或数字实验室进行数据发现、获取、管理和分析，并将产生的调查结果、报告和意见按规定作为专家证言提交给指导委员会或相关法院。

50. 证据争议解决

(a) 如果就电子文件的证据提交产生任何争议，应将此事送交国家数字实验室进行检验。

(b) 国家数字实验室关于检验结果的报告和意见为最终结果。

第十三章 行政措施

51. 对网络安全服务提供商的处理

主管司可对未遵守第29条或第35条规定的网络安全服务提供商

实施以下任何行政命令：

(a) 警告；

(b) 处以罚款；

(c) 在有限期限内暂时吊销许可证；

(d) 吊销许可证。

52. 对数字平台服务提供商的处理

主管司可对未遵守第 30 条、第 31 条、第 32 条、第 33 条、第 34 条或第 35 条规定的数字平台服务提供商实施以下任何行政命令：

(a) 警告；

(b) 处以罚款；

(c) 在有限期限内暂时吊销注册证书；

(d) 吊销注册证书并列入黑名单。

53. 对网络安全团体的处理

指导委员会可解散未经许可设立或不遵守条款的网络安全团体，并可没收该团体的资金，包括该团体拥有的金钱和动产或不动产，作为国家财产。

第十四章 申诉

54. 对拒发许可证的申诉

任何人对主管司根据第 21 条拒绝颁发许可证、根据第 23 条拒绝续期许可证、根据第 25 条拒绝注册或根据第 27 条拒绝续期注册的决定不服的，可在作出该决定或命令之日起 30 天内按规定向主管部申

55. 对行政处罚的申诉

任何人对根据第 51 条或第 52 条采取的行政处罚不服的，可在作出该决定或命令之日起 30 天内按规定向主管部申诉。

56. 部的裁决

对于根据第 54 条或第 55 条提出的申诉，主管部可确认、修改或取消相关决定或命令。

57. 向中央委员会申诉

任何人对主管部根据第 56 条作出的决定或命令不服的，可在作出该决定或命令之日起 60 天内按规定向中央委员会申诉。

58. 中央委员会裁决

对于根据第 57 条提出的申诉，中央委员会可确认、修改或取消相关决定或命令。

59. 终局性

中央委员会的决定为最终决定，具有确定性。

第十五章 犯罪与刑罚

60. 关键信息基础设施负责人失职

负责管理及维护关键信息基础设施的个人（非公务员），若被判定违反第 17(a)或(b)条的规定，应处以不少于 1 个月但不超过 6 个月的监禁，或不少于 1,000,000 缅元但不超过 10,000,000 缅元的罚款，或两者并罚。

61. 危害关键信息基础设施

任何人被判定实施或企图实施未经授权干扰、破坏、盗窃、损坏、

非法传输、使用、分发、披露、修改或更改关键信息基础设施相关电子信息的，应处以不少于 6 个月但不超过 3 年的监禁，或不少于 5,000,000 缅元但不超过 20,000,000 缅元的罚款，或两者并罚。

62. 无照经营网络安全服务

任何人被判定无照提供网络安全服务的：

(a) 应处以不少于 1 个月但不超过 6 个月的监禁，或不少于 1,000,000 缅元但不超过 10,000,000 缅元的罚款，或两者并罚，且案件相关证据应作为国家财产没收。

(b) 如果违法者是公司或组织，该公司或组织应处以不少于 10,000,000 缅元的罚款，且案件相关证据应作为国家财产没收。

63. 无续期经营

任何人被判定在未续期许可证的情况下继续提供网络安全服务的，应处以不少于 1,000,000 缅元但不超过 5,000,000 缅元的罚款。

64. 无照运营大型数字平台

在本国运营拥有 10 万或以上用户的数字平台服务的个人，被判定无注册运营的，应处以至少 100,000,000 缅元的罚款，且案件相关证据应作为国家财产没收。

65. 无续期运营平台

任何人被判定在未续期注册的情况下继续运营数字平台服务的，应处以不少于 50,000,000 缅元的罚款。

66. 网络滥用（一般）

任何人被判定犯有第 36(a)、(b)、(c)或(d)条规定的任何网络

滥用罪的，应处以不少于 6 个月但不超过 2 年的监禁，或不少于 1,000,000 缅元但不超过 10,000,000 缅元的罚款，或两者并罚。

67. 网络滥用（严重）

任何人被判定犯有第 36(e)或(f)条规定的任何网络滥用罪的，应处以不少于 1 年但不超过 3 年的监禁，或不少于 5,000,000 缅元但不超过 20,000,000 缅元的罚款，或两者并罚。

68. 恶意行为

任何人被判定以不诚实的意图实施或致使他人实施下列任何行为的，应处以不少于 1 年但不超过 2 年的监禁，或不少于 5,000,000 缅元但不超过 20,000,000 缅元的罚款，或两者并罚：

(a) 实施可能损害网络资源或安装恶意软件或导致恶意软件入侵的行为；

(b) 阻止被授权访问网络资源的人访问系统；

(c) 销毁、移除、更改或以其他方式损害网络资源中包含的信息的有用性或有效性；

(d) 以损害为目的，窃取、禁用、销毁或更改计算机上的源代码；

(e) 利用网络资源进行欺骗；

(f) 电子创建、修改或更改信息以伤害他人或贬低其声誉，或电子分发此类数据；

(g) 使用网络发送不需要或未经请求的文本消息、电子邮件或信息。

69. 窃取在线资产

任何人被判定利用网络资源窃取或销毁他人的任何在线金融资产，或以不诚实的意图致使他人这样做的，应处以不少于 2 年但不超过 7 年的监禁，并可处以罚款。

70. 非法 VPN

任何人被判定未经批准设立 VPN 或提供 VPN 服务的：

(a) 应处以不少于 1 个月但不超过 6 个月的监禁，或不少于 1,000,000 缅元但不超过 10,000,000 缅元的罚款，或两者并罚，且案件相关证据应作为国家财产没收。

(b) 如果违法者是公司或组织，该公司或组织应处以不少于 10,000,000 缅元的罚款，且案件相关证据应作为国家财产没收。

71. 非法在线赌博

任何人被判定未经批准设立在线赌博系统的：

(a) 应处以不少于 6 个月但不超过 1 年的监禁，或不少于 5,000,000 缅元但不超过 20,000,000 缅元的罚款，或两者并罚，且案件相关财产应作为国家财产没收。

(b) 如果违法者是公司或组织，该公司或组织应处以不少于 20,000,000 缅元的罚款，且案件相关证据应作为国家财产没收。

72. 传播不良信息

任何人被判定电子分发、传输、发送、复制或销售不适合公众观看的信息的，应处以不少于 1 个月但不超过 6 个月的监禁，或不少于 1,000,000 缅元但不超过 10,000,000 缅元的罚款，或两者并罚。

73. 违反附属法规

任何人被判定违反根据本法发布的任何规则、条例、条款、通告、命令、指示和程序的：

(a) 应处以不少于 1 个月但不超过 3 个月的监禁，或不少于 1,000,000 缅元但不超过 10,000,000 缅元的罚款，或两者并罚，且案件相关证据应作为国家财产没收。

(b) 如果违法者是公司或组织，该公司或组织应处以不少于 10,000,000 缅元的罚款，且案件相关证据应作为国家财产没收。

74. 未遂与共犯

任何人被判定企图或共谋实施本法规定的任何犯罪，或协助、教唆实施本法规定的犯罪的，应受到本法为该犯罪规定的惩罚。

第十六章 杂项

75. 电子证据的提交

如果根据本法起诉的犯罪的证据难以在法庭上出示，侦查小组可向相关法院提交关于证据如何保存的报告和书面证据。该提交应被视为证据已在法庭上出示，相关法院可依法处理。

76. 现有团体过渡

在本法生效前设立的网络安全团体，应自本法生效之日起 6 个月内获得许可。

77. 费用征收

主管司应按规定收取本法规定的费用和罚款，视同欠税征收。

78. 国际合作与引渡

(a) 如果本法事项需要国际合作，应根据《刑事司法互助法》进行。

(b) 如果本法规定的犯罪是由外国人在国外实施的，应遵守《引渡法》。

79. 公务员责任

如果负责管理及维护关键信息基础设施的人是公务员，且被发现违反第 17(a)或(b)条的规定，应根据《公务员法》对其采取行动。

80. 视同公务员

指导委员会、工作委员会或侦查小组的任何成员（非公务员），在履行本法规定的职责时，应被视为《刑法典》第 21 条规定的公务员。

81. 善意免责

任何被指派依照本法行事的个人或组织，因善意行事而不得被起诉。

82. 起诉许可

依照本法进行的起诉，须事先获得主管部的批准。

83. 排他性管辖

违反本法规定的犯罪，仅依照本法起诉。

84. 可认定罪行

第 60、62、64、66、68、71 和 72 条下的犯罪，是可认定罪行。

85. 民事责任保留

依照本法采取的行政措施或刑事起诉，不免除受行政措施者或违法者因其行为引起的公共损失而应承担的赔偿责任。

86. 豁免权

中央委员会或指导委员会：

(a) 经联邦政府同意，可为公共利益豁免任何政府部门、政府组织或个人的许可、执照或注册要求，并豁免本法原本要求的费用支付。

(b) 在与国家紧急状态、国防与安全或自然灾害相关的情况下，可自行采取行动，无需事先征得联邦政府同意，豁免本法原本要求的许可或执照及费用支付。

(c) 应将根据(b)款处理的事项向联邦政府报告。

87. 技术解释

如果主管部需要澄清本法中任何技术表述或专业表述的含义，可经中央委员会批准发布公告予以澄清。

88. 实施细则

在实施本法规定时：

(a) 主管部经联邦政府批准，可发布规则、条例和条款。

(b) 中央委员会、指导委员会、工作委员会和主管司可发布通告、命令、指示和程序。