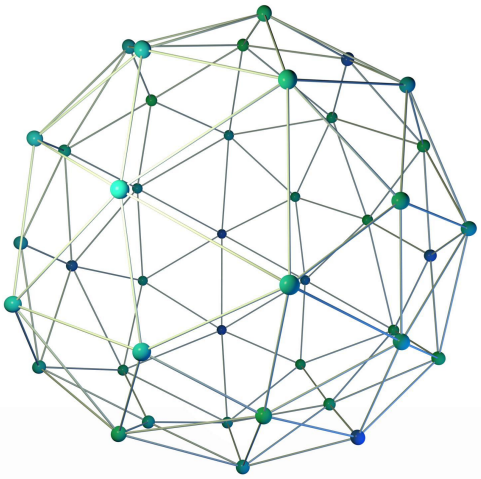
公安部第三研究所
网络安全法律研究中心

全球网络安全政策法律发展年度报告（2022）



公安部第三研究所网络安全法律研究中心

360 集团法务中心

前　言

背景

同悠久的文明史相比，人类进入数字时代的时间并不长，但由信息技术革命引发的社会变革却是空前深刻而彻底的，这也导致网络安全议题成为迄今为止“最具魅力”的法律关注。在全球网络安全政策立法兴起的数十年中，2022 年也许并不特殊——这一年并没有里程碑式的标志性立法出台，也没有足以引发规范系统调整的重大安全事件发生——一切都在按部就班：欧盟在 GDPR 之外着力完善它的“三驾马车”，美国在不断制造竞争以维系数字霸权，而中国仍然在尝试建立作为“第三条道路”的数据要素市场。

但这可能恰恰预示了一个新的网络安全法治时代的到来，一个通过建构过程来塑造“安全阶梯”的时代。2022 年，一个明显可以观察到的事实是，在网络安全领域，尽管自遥远的“机房”时代就形成的安全内涵并没有发生根本变化，但“法律的工具化”和“工具的法律化”都在变得更为激进。在现实主义者看来，“去中心化”的网络结构使人类社会重回霍布斯所描述的“自然状态”，后工业时代形成的世界格局和主体间关系都变得不再稳定，这或许可以解释为何“进攻性”的政策法律会越来越多的出现。

信息技术革命在本质上就是一场资源替代的革命，当数据资源代替传统物质资源成为主导性的可利用资源时，由数据驱动的人类历史提供了难能可贵的“变局”机会，这必然导致“冲突与对抗”在“冷战”之后再次成为世界的主流。尽管共识和合作仍然存在，但自由主义者所推崇的“相互依赖”似乎正在变得更加困难，例如，“零信任”和“弹性”就成为各国 2022 年网络安全政策法律的主题词。作为一项秉要执本的“话语力量”，政策法律对于获得新的“主导权”无疑发挥着越来越重要的作用。正如全球数据保护领域逐渐接受欧盟 GDPR 对于“欧洲主义”的传播产生的积极意义，面对愈发多元的网络安全诉求，各国都在积极寻求自己的“主战场”。

在这种情况下，“安全”和“发展”在各个维度都陷入了不可避免的“零和困境”，休谟问题变得更加突出。鉴于信息技术的快速发展变动，网络安全在相当长的时期内都将是一项“待开发”的法律议题，这使得我们对于全球网络安全

政策法律的观察工作更有意义。

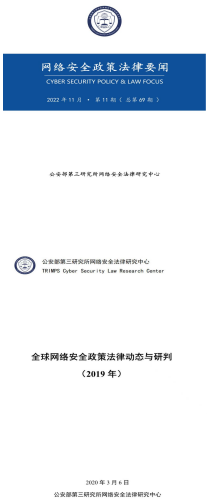
为贯彻落实党的二十大精神，深入研究国内外网络安全政策法律态势，护航高质量发展，公安部第三研究所网络安全法律研究中心与360集团法务中心联合撰写《全球网络安全政策法律发展年度报告（2022）》，密切跟踪、系统掌握全球网络与数据领域立法热点及敏感问题，积极探索推动中国式现代化网络与数据安全法治发展道路。

导读

报告共分为四大部分：第一部分重点研判2022年全球网络安全政策法律态势，宏观把握立法走向；第二部分通过对2022年法律规制“行动域”的划分，梳理美国、欧盟、英国、法国、德国、俄罗斯、澳大利亚、加拿大、新西兰、新加坡、日本、韩国、巴西、中国等国家和地区在同一“行动域”的立法情况，直观展示全球立法特点和核心内容；第三部分特别新增“2022年全球网络安全研究分析报告盘点”，通过跟踪分析境内外政府机构、知名智库、安全公司发布的网络空间安全威胁、趋势与法治分析报告，更直观、更深刻、更全面地理解全球网络安全政策法律演进的内生驱动；第四部分综合历年特别是2022年以来的全球网络与数据安全态势，对2023年及后续短期内的网络安全政策、立法趋势进行研判。

沿革

作为网络安全领域的专业智库，自2017年起公安部第三研究所网络安全法律研究中心每月整理网络安全政策法律要闻，持续跟进全球相关动态，连续五年编制并向社会公开发布《全球网络安全政策法律发展年度报告》，为产学研各界提供研究素材、指明研究方向、勘定研究前沿，以期为促进我国网络与数据安全法治建设提供助力。



出品方

公安部第三研究所网络安全法律研究中心

360 集团法务中心

平台支持

信安未来

参编单位

密码法治实践创新基地

西交苏州信息安全法学所

网络安全等级保护与安全保卫技术国家工程研究中心

信息网络安全公安部重点实验室

数字丝路安全智库

西交科教院网络安全法治研究所

上海市信息网络安全管理协会互联网安全法律服务专家委员会

广东新兴国家网络安全和信息化发展研究院

江苏竹辉律师事务所

北京中企数安咨询有限公司

致　谢

感谢以下人员对本报告的指导和贡献：

专家指导组

马民虎　西交苏州信息安全法学所 所长

严　明　公安部第三研究所/第一研究所 原所长

宋燕妮　全国人大常委会法工委经济室 原副巡视员

金　波　公安部第三研究所 所长助理

焦　娇　360 集团 副总裁/总法律顾问

陈欣新　中国社会科学院法学研究所 研究员

吴松洋　公安部第三研究所 研究员

杨　涛　公安部第三研究所 研究员

黄道丽　公安部第三研究所 研究员

孙艳玲　360 集团法务中心 高级总监

于月霞　宁夏公安厅网安总队 总工程师

鲍　亮　公安部第三研究所 副研究员

易　晨　中国香港港专学院副教授/内地联络处 处长

李　晶　国网湖北省电力有限公司数字化部网络安全处 副处长

侯　亮　国泰君安证券股份有限公司 首席信息安全专家

刘紫千　天翼安全科技有限公司 总经理

张麾军　中国移动通信集团重庆有限公司 高级项目经理

刘春梅　上海市信息网络安全管理协会 秘书长

编制撰写组

梁思雨　何治乐　原　浩　李亚齐　张　淼　王彩玉　俞少华

王明一　陈敬然　马　宁　方　婷　胡文华　胡柯洋　谢永红

声　明

本报告倾注编写团队大量心血，希望每位读者能从中收获知识和见解。在撰稿过程中，编写团队力求尽善尽美，经专家指导组倾力指导、精准把脉，编写团队人员反复琢磨修改最终定稿。由于时间仓促等局限性，难免存在纰漏，请读者朋友们批评、斧正。

目　录

一、概览：2022 年全球网络安全形势与政策法律态势

2022 年，是世界百年未有之大变局加速演进，深刻影响全球网络安全政策法律态势的一年。这一年，百年变局与世纪疫情交织，全球网络安全形势日益复杂，国际局势剑拔弩张，不稳定不确定因素显著增多，由国家支持的、大规模持续性网络安全事件频发，脱钩断链风险不断增加，持续校验各国网络与数据安全动态保障能力。提升关键（信息）基础设施安全保护能力、加强供应链韧性、强化网络信息内容治理、重塑数据跨境流动新秩序等问题成为核心关切。

2022 年，是我国新时代网络强国、数字中国建设深入推进，网络空间法治体系持续优化的一年。这一年，我国以习近平新时代中国特色社会主义思想为指引，积极推动网络空间命运共同体建设，强化法治思维，运用法治方式，综合利用立法、执法、司法等手段开展斗争，协调推进国内治理和国际治理，有效应对挑战、防范风险；贯彻落实总体国家安全观，充分发挥法治固根本、稳预期、利长远作用，在激发数字经济活力、落实关键信息基础设施安全保护、加强数据出境安全管理、营造清朗网络空间、强化网络犯罪防治等方面取得新成效，更好维护国家主权、安全、发展利益。

（一）全球网络空间局势动荡，竞争与合作并存

2022 年全球网络空间竞争与博弈持续加剧。受局部地区冲突影响，网络空间冲突对抗风险上升。个别国家将互联网作为维护霸权的工具，联合发起《互联网未来宣言》，列出旨在维护所谓“自由与开放互联网”的五项主张，在互联网领域以意识形态划线，煽动网络空间分裂和对抗，用集团性“帮规”破坏全球性互联网治理原则。北约发布新的《北约 2022 年战略概念》，首次提及中国，称中国对北约构成“系统性挑战”，表示将强化在网络空间有效运作的能力，利用所有的可用工具，预防、探测、对抗和应对各种威胁。美国国家情报总监办公室发布的《美国情报界年度威胁评估报告》称“中国仍将是美国技术竞争力的最大威胁”，白宫发布的新版《国家安全战略》表示“未来十年是美国与中国竞争的决定性十年”，将动用所有的国家工具来超越战略性对手，并将建立尽可能强大的国家联盟，以增强集体影响力。与此同时，各国持续加强本国网络安全顶层设计，通过战略、总统令等形式明确网络安全保障任务。美国白宫发布《关于确保

美国外国投资委员会认真考虑不断演变的国家安全风险的行政令》，系外国投资委员会（CFIUS）成立以来首份界定外商投资审查中应考量的国家安全因素的行政令，将网络安全和敏感个人数据安全列为重要考量因素。美国总统拜登签署《提升国家安全、国防和情报系统网络安全备忘录》，设定国家安全系统多项网络安全新要求，推进网络安全防御现代化。英国政府发布《政府网络安全战略：2022年至2030年》，系英国首份针对政府的网络安全战略，意在确保公共部门所有政府组织都对已知漏洞和攻击方法具有弹性。

作为全球最大的发展中国家和网民数量最多的国家，我国展现负责任大国担当，加强国际网络空间对话合作，推动互联网全球治理体系变革。正如习近平总书记在党的二十大报告中指出的，中国始终坚持维护世界和平、促进共同发展的外交政策宗旨，致力于推动构建人类命运共同体——一方面，践行共商共建共享的全球治理观，促进大国协调和良性互动，推动构建和平共处、总体稳定、均衡发展的大国关系格局；另一方面，贯彻总体国家安全观，完善国家安全法治体系、战略体系、政策体系，强化网络、数据安全保障体系建设，健全反制裁、反干涉、反“长臂管辖”机制，统筹维护和塑造国家安全，推进国家安全体系和能力现代化。2022年，金砖国家领导人第十四次会晤达成《金砖国家数字经济伙伴关系框架》，系金砖经贸领域第一份数字经济合作专门文件。“中国+中亚五国”外长第三次会晤通过《“中国+中亚五国”数据安全合作倡议》；中国全面推进加入《数字经济伙伴关系协定》谈判。中俄两国发表《中华人民共和国和俄罗斯联邦关于新时代国际关系和全球可持续发展的联合声明》，国家互联网信息办公室与泰王国国家网络安全办公室签署《关于网络安全合作的谅解备忘录》，与印尼国家网络与密码局签署网络安全合作行动计划。同时，面对网络安全保障的现实需求和时代诉求，我国适时修改网络安全领域的基础性立法《网络安全法》，旨在做好《网络安全法》与新实施的法律之间衔接协调，为高质量发展提供有力制度支撑和保障。

（二）关键信息基础设施安全保护加速推进，事件报告成重要关切

2022年勒索攻击等网络安全事件威胁不减，关键信息基础设施的外部攻击仍是重大威胁来源。数字化转型过程中的关键信息基础设施安全保护现代化成为各国亟待解决的现实难题，引发各界对既有政策立法的反思和调整，全球关键信

息基础设施规则体现出威胁攻击与保障防御两端的特点。欧盟2022年5月发布的《欧盟安全联盟战略》第四次进展报告对俄乌冲突国际环境下欧盟面临的安全威胁进行梳理。报告指出，尽管俄乌冲突在很大程度上仍然是通过常规手段推进，溢出效应有限，但也充分说明网络和关键基础设施领域面临的风险是真实存在的，进一步凸显落实现有立法及推动制定中立法的紧迫性。基于此，欧盟加快立法进程，密集推动NIS2指令、《关于关键实体弹性指令的提案》（CER指令）、《数字运营弹性法案》等。其中，CER指令提案将关键实体中为三分之一以上成员国提供基本服务的实体明确为“欧洲具有特定重要性的关键实体”，在安全保护方面获得额外建议，这与澳大利亚4月正式生效的《2022年安全立法修正案（关键基础设施保护）法》相类似。澳大利亚在立法中建立“具有国家意义的系统（SoNS）”制度，在现有关键基础设施保护体系中将一小部分具有国家意义的关键基础设施资产认定为SoNS，并对SoNS赋予更严苛的保护义务。此类立法举措反映出部分国家在当前安全形势下对关键基础设施保护的新探索。同时，被认为是“最严重和最广泛的安全威胁之一”的Log4j漏洞风险持续发酵，美国网络安全审查委员会认为该漏洞将在未来十年甚至更长时间持续引发风险，使得各国对于感知网络安全态势、及时洞察网络安全事件的需求更加迫切。基于此，强制性的事件报告义务成为普遍选择。美国通过《关键基础设施网络安全事件报告法》《投资顾问、注册投资公司和业务发展公司的网络安全风险管理》《银行机构及其银行服务提供者的计算机安全事件报告要求》等，对事件报告提出24小时至72小时不等的时间要求。印度发布《关于<2000年信息技术法>第70B条第（6）款，可信网络的信息安全实践、程序、预防、响应和网络安全事件报告指令》，要求在发现或被告知发生网络安全事件后6小时内向CERT-In报告。

我国持续推动关键基础设施安全保护工作，重要的国家标准之一GB/T 39204-2022《信息安全技术 关键信息基础设施安全保护要求》正式发布。交通、能源、证券期货业等行业和领域主管部门加快推动关保工作在本行业、本领域的落地实施。交通运输部发布《公路水路关键信息基础设施安全保护管理办法（征求意见稿）》，就公路水路的关保工作进行专项规定；国家卫生健康委等部门发布《医疗卫生机构网络安全管理办法》、中国证监会发布《证券期货业网络安全管理办法（征求意见稿）》、国家能源局发布《电力行业网络安全管理办法（修

订征求意见稿）》，将关键信息基础设施运行安全作为重要内容之一。从具体内容来看，细化的制度设计主要围绕深化组织机构设置及人员管理，增设专项评审要求、强调全天候态势感知能力，重视压力测试、攻防演练、应急演练等在风险隐患发现方面的作用，加强供应链风险管理和网络安全事件管理等方面展开，突出行业特性，旨在保障关键信息基础设施的持续稳定运行。

（三）全球供应链不稳定因素增多，“国产化”成为关键词

网络空间竞争与博弈的加剧使得网络的互联互通遭遇逆流，逆全球化思潮抬头，“筑墙设垒”“脱钩断链”成为个别国家维护自身科技垄断和霸权地位的工具。美国商务部和国土安全部 2022 年 2 月发布的《美国 IT 行业关键供应链评估报告》指出“新冠疫情加剧 ICT 供应链结构性风险，ICT 生产诸多领域缺乏国内生态。美国虽然在许多产品的 ICT 发展方面处于领先地位，但印刷电路板和显示器等产品的生产与电子组装越来越集中于中国。”对此，报告建议通过适当激励项目或立法推动，支持国内投资和生产关键信息通信技术产品，包括印刷电路板和半导体。8 月，美国通过《2022 年芯片与科学法》，拨款 527 亿美元提振本国半导体制造与研发，并通过限制补贴资格来阻止半导体企业在中国新建或扩大产能。欧盟提出《芯片法案》，将投入超过 430 亿欧元公共和私有资金，用于支持芯片生产、试点项目和初创企业，旨在短期内预测并避免供应链中断，从中期帮助欧盟成为芯片战略市场的领军者。日本总务省网络安全工作组发布修订后的《2022 年 ICT 网络安全综合措施》，要求提高自主应对网络攻击的能力，加强和培育本土网络安全产业，以降低对他国产品和信息的依赖性。

与此同时，“国产化”“供应链韧性”成为关键词。俄罗斯总统普京相继签发俄罗斯联邦第 166 号总统令《确保俄罗斯联邦关键信息基础设施技术独立和安全的措施》和第 250 号总统令《保障俄罗斯联邦信息安全的补充措施》，设定国产化替代目标期限，禁止未经批准采购外国软件和相关服务用于关键信息基础设施重要客体。我国《“十四五”数字经济发展规划》要求“推动关键产品多元化供给，着力提高产业链供应链韧性，增强产业体系抗冲击能力”。习近平总书记在党的二十大报告中提出进一步指示，要求加强重点领域安全能力建设，着力提升产业链供应链韧性和安全水平，在关系安全发展的领域加快补齐短板，提升战略性资源供应保障能力，严密防范系统性安全风险。

（四）数据跨境流动新秩序加速构建

欧美隐私盾协议无效后，如何构建欧美数据跨境流动新秩序成为双方重点工作之一。3 月，欧盟委员会主席与美国总统拜登发表声明，宣布欧盟和美国已就跨大西洋数据流动的新框架达成“原则性共识”。10 月，拜登签署《关于加强美国信号情报活动保障的行政令》，对情报监视活动赋予进一步的保障措施，旨在落实 3 月双方发布的框架，为重建有效数据传输机制提供制度支撑。行政令发布后，美国国会研究会发布《欧盟-美国数据隐私框架：背景、实施和下一步》报告，提出进一步担忧，表示美国白宫在未来有权撤销行政令，一旦行政令撤销，欧盟公民将失去基于行政令获得的保障措施和救济途径。同时，欧洲法院可能认为行政令规定的措施不足以缓解对美国监视的担忧。报告认为欧洲可能会继续要求修订 FISA 第 702 条。同月，《英美政府间就获取电子数据打击严重犯罪的协定》生效，作为《云法案》框架下的首份协定，将允许两国执法机构在获得适当授权的情况下，在没有法律障碍的前提下，直接从高科技公司获取与严重犯罪相关的电子数据。

我国修订后的《网络安全审查办法》正式施行，将网络平台运营者开展数据处理活动影响或者可能影响国家安全等情形纳入网络安全审查范围。《数据出境安全评估办法》正式发布，以《网络安全法》《数据安全法》《个人信息保护法》为上位法依据，标志着我国探索多年的数据出境安全评估制度落地。办法发布后，北京、江苏、上海等多省市网信部门开通申报和咨询通道，指引数据处理者申报数据出境安全评估。我国司法部发布《国际民商事司法协助常见问题解答》，进一步明确涉诉数据信息的跨境调取规则。《网络安全标准实践指南—个人信息跨境处理活动安全认证规范》《个人信息出境标准合同规定（征求意见稿）》相继发布，进一步细化个人信息跨境提供规则。

（五）立法威慑和平台责任成为信息内容治理的首选路径

一直以来，网络空间都是各国塑造国际形象、提升国际影响力的重要舞台。俄乌冲突期间，两国在“舆论战”中的表现充分说明打击外国信息操纵与干扰，强化在线平台，特别是对舆论走势有着强大主导力的大平台非法和有害内容治理能力的重要性。

一方面，通过将发布特定类型违法有害信息的行为定义为犯罪，强化法律的

威慑力。俄罗斯总统普京签署三项修正案，修订《俄罗斯联邦刑法典》《俄罗斯联邦刑事诉讼法典》《俄罗斯联邦行政违法法典》，将军事相关信息的传播纳入刑事规制范畴，明确公开发布俄罗斯联邦武装部队相关虚假信息、诋毁俄罗斯武装力量公开行动及呼吁对俄罗斯进行制裁三类行为的刑罚规则。另一方面，加强平台识别和防范违法有害信息的能力，以及在信息内容治理方面的主体责任。美国网络安全和基础设施安全局发布《准备和减轻针对关键基础设施的外国影响行动》，为关键基础设施所有者和运营商如何识别和减轻错误信息、虚假信息和不实信息（MDM）风险提供指导。在美国白宫发布的大型科技平台改革六项原则中，再次呼吁对《通信规范法》第230条进行根本性改革，以限缩对大型科技平台的特殊法律保护。欧盟《数字服务法》正式通过，要求在欧盟经营的大型门户网站和社交媒体公司必须加强对非法内容的审查，及时删除非法和有害的在线内容，包括仇恨言论、虚假信息和假货交易信息等。同时，《欧盟处理恐怖主义内容在线传播条例》开始施行,要求网络平台接到成员国当局发出的删除命令后，必须在一小时内删除恐怖主义内容。我国建立健全网络综合治理体系，推动形成良好网络生态。国家互联网信息办公室等部门发布《移动互联网应用程序信息服务管理规定》《互联网用户账号信息管理规定》《互联网弹窗信息推送服务管理规定》，要求互联网信息服务提供者落实主体责任，并提出“在互联网用户账号信息页面展示合理范围内的账号的互联网协议地址归属地信息”的要求。

（六）网络犯罪打击更加精细，犯罪防治成为重点

随着勒索攻击、电信网络诈骗等违法犯罪活动持续威胁国家、社会和个人合理利益，各国开始普遍加强网络犯罪打击力度。美国总统拜登签署《优化网络犯罪度量法》，旨在提升网络犯罪数据可见性、提高网络犯罪打击效率。美国司法部发布《2022年-2026年战略计划》，将提升网络安全和打击勒索攻击作为“保护美国国家安全”的战略目标，并做出将DOJ采取扣押或没收手段的勒索攻击结案数量增加10%的承诺。《欧洲刑警组织条例》修正案生效，规定“只要是为支持特定正在进行中的犯罪调查，能够在不明确数据主体类别的情况下处理个人数据。”但欧盟数据保护专员公署认为修正案削弱了数据保护基本权利，扩大欧洲刑警组织权力的同时并未建立强有力的数据保护措施。

与此同时，各国将网络犯罪预防列为重点工作之一，强调潜在犯罪行为的发

现与防范。澳大利亚发布《2022 年打击网络犯罪国家计划》，从预防与保护，调查、打击与起诉，以及恢复三方面提出具体措施，将支持行业发挥领导力，预防网络犯罪威胁。澳大利亚《2022 年电信服务提供商（客户身份验证）判定规则》生效，要求识别客户高风险交易，保护风险客户，对高风险交易实施多因素身份验证。习近平总书记在党的二十大报告中强调，推动公共安全治理模式向事前预防转型，加强重点行业、重点领域安全监管，加强个人信息保护，依法严惩群众反映强烈的各类违法犯罪活动，在社会基层坚持和发展新时代“枫桥经验”，建设人人有责、人人尽责、人人享有的社会治理共同体。我国正式通过《反电信网络诈骗法》，着力加强预防性法律制度构建，推动形成全链条反诈、全行业阻诈、全社会防诈的打防管控格局。《全国人大常委会 2022 年度立法工作计划》也将制定网络犯罪防治法列为预备审议项目之一。

（七）后量子密码的“超前性”与人工智能的“适度性”并存

2022 年，各国政策立法同步推进人工智能、后量子密码、元宇宙、数字货币等未来技术的推动创新与安全治理，尤其注重后量子密码的超前部署，以及强调对人工智能安全治理的“适度性”。

一直以来，密码安全问题就是算法构筑的“难解性”与计算能力之间的博弈。但这一传统的攻防关系随着量子计算的成熟而变得不再稳定，量子计算提供的强大计算能力将使现有的绝大部分公钥密码算法被攻破，迄今为止最为有效的“安全屏障”可能不再可靠[1]。基于此，为预防量子计算对网络安全造成的潜在威胁，美国在后量子密码领域超前布局。国家标准与技术研究院确定了四种后量子加密算法。白宫发布《关于加强国家量子倡议咨询委员会的行政命令》《关于促进美国在量子计算领域领导地位的同时降低易受攻击的密码系统风险的国家安全备忘录》，推动美国在量子信息科学方面的举措，同时减轻量子计算对国家和经济安全构成的风险。网络安全和基础设施安全局发布《为关键基础设施做好后量子密码准备》专项文件，为关键基础设施及政府网络的所有者、运营者向后量子密码转型提供指引。国家安全局发布《商业性国家安全算法组件 2.0》，提出针对国家安全系统的后量子算法要求。

[1] 寰球密码简报（第 50 期）| 量子计算：密码安全的“矛与盾”——美国近期关于量子信息科学的持续性政策观察. 链接：https://mp.weixin.qq.com/s/toATSOxLDxKUGNpVex5gTA

与此同时，各国对人工智能的安全治理更加理性，着重强调监管的“适度性”。欧洲议会通过《关于数字时代人工智能的决议》，指出欧盟不应总是将人工智能作为一种技术进行监管，监管干预的程度应与人工智能系统的特定使用风险成正比。英国发布《国家人工智能战略——人工智能行动计划》与《建立一种支持创新的人工智能监管方法》，同样强调监管的合比例性，要求遵循技术的“适应性”和“自主性”。我国六部门联合发布《关于加快场景创新以人工智能高水平应用促进经济高质量发展的指导意见》，将协同治理作为基本原则之一，要求尊重人工智能发展规律，发挥政府和市场的积极性，共同为场景创新提供制度供给，促进人工智能创新发展与监管规范相协调。正如党的二十大报告要求，必须坚持解放思想、实事求是、与时俱进、求真务实，得出符合客观规律的科学认识，形成与时俱进的理论成果，更好指导中国实践，构建新一代信息技术、人工智能等一批新的增长引擎。

二、回顾：2022 年全球网络安全政策法律内容盘点

（一）网络主权保障与国际合作

1. 五眼联盟就俄罗斯对关键基础设施构成的网络威胁发布警报

4 月 20 日，五眼联盟国家网络安全当局联合发布网络安全警告《俄罗斯国家支持的和犯罪团体的网络安全威胁》(Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructures)，旨在提醒关键基础设施组织，俄罗斯可能会支持更多的恶意网络活动反击其受到的前所未有的经济制裁和美国及其盟友对乌克兰提供的物质支持。

警报认为，网络安全威胁主要来源于俄罗斯国家支持的网络行动、俄罗斯阵营的网络威胁团体和俄罗斯阵营的网络犯罪团体。俄罗斯国家支持的网络行动主要源于以下五个政府和军事组织的网络威胁行为者：俄罗斯联邦安全局（FSB）所属的第 16 中心和第 18 中心、俄罗斯外国情报局（SVR）、俄罗斯总参谋部情报总局（GRU）所属第 85 特种服务中心（GTsSS）、俄罗斯总参谋部情报总局特种技术中心（GTsST）、俄罗斯国防部所属中央化学与力学研究所（TsNIIKhM）。警告对上述俄罗斯部门的网络行动类型、特点、攻击目标、技术手段、曾经实施过的网络行动进行列举分析。

为此，警告给出预防网络安全事件、加强身份识别和访问管理、强化保护性控制和架构、完善漏洞和配置管理四方面的具体措施清单。警告敦促关键基础设施组织的网络防御者在识别恶意活动时谨慎处理。当检测到潜在 APT 或勒索软件时应当以官方推荐的方式应对，并向适当的网络和执法机构报告网络安全事件。当局强烈反对向犯罪分子支付赎金。

2. 北约发布新《北约 2022 年战略概念》

6 月 29 日，北约发布新的《北约 2022 年战略概念》（NATO 2022 Strategic Concept）文件，首次提及中国，强调中国对北约的价值观和安全造成挑战，表示要保持对华建设性的接触。北约战略概念大约每十年更新一次，是北约第二重要的文件。之前的版本在 2010 年的北约里斯本峰会上获得通过。

此次更新的版本明确北约在未来十年有三大核心任务，即威慑和防御、危机预防与管理、合作安全，将俄罗斯称为北约成员国安全和欧洲大西洋地区和平稳定的“最大且直接的威胁”，称中国对北约构成“系统性挑战”。网络安全方面，北约表示将加快数字化转型，强化北约网络防御、网络和基础设施安全，增加对新兴和颠覆性技术的投资。文件明确保持安全使用和不受限制地进入网络空间是有效威慑和防御的关键。北约将强化在网络空间有效运作的能力，利用所有的可用工具，预防、探测、对抗和应对各种威胁。北约承认国际法在网络空间的适用性，并将促进网络空间负责任行为。

我国外交部发言人赵立坚回应称，北约所谓的新“战略概念”文件，罔顾事实，颠倒黑白，顽固坚持对华系统性挑战的错误定位，抹黑中国对外政策，对中国正常的军事发展和国防政策说三道四，鼓动对抗对立，充满冷战思维和意识形态偏见。中方对此严重关切，坚决反对。

3. 美国与以色列发表联合声明/签署谅解备忘录，加强网络安全合作

3 月 2 日，美国国土安全部（DHS）和以色列国家网络局（National Cyber Directorate）发布联合意向声明，扩大网络安全和新兴技术领域的合作，增强两国对不断演变的威胁的抵御能力。声明中，双方将合作研发，提高网络安全和恢复能力，打击勒索软件等共享网络威胁，加强关键基础设施网络安全。此外，声明重申将利用两国技术部门创新和创造力的支持进一步加强公私伙伴关系。通过此次合作，双方预期实现以下成果：（1）促进采用高影响力和成熟的网络安全技术；（2）加强网络安全信息共享和能力建设；（3）促进专家交流，加强对网络威胁和技术机遇的合作风险管理。

8 月 25 日，美国财政部和以色列财政部（MOF）宣布敲定关于网络安全合作的双边谅解备忘录（MoU），加强以下领域合作：（1）与金融部门有关的信息共享，包括有关事件和威胁的网络安全信息；（2）员工培训和考察访问，以促进网络安全领域的合作；（3）能力建设活动，例如进行跨境网络安全演习。

4. 美国商务部发布《全球跨境隐私规则声明》

4 月 21 日，美国商务部发布《全球跨境隐私规则声明》(Global Cross-Border

Privacy Rules Declaration）。美国、加拿大、日本、大韩民国、菲律宾、新加坡、中国台湾正式对外宣告成立全球跨境隐私规则（Cross-Border Privacy Rules，简称 CBPR）论坛。这一举动本质上是将亚太经合组织（APEC）框架下的 CBPR 体系转变成一个全球所有国家都可以加入的体系。

根据声明，全球 CBPR 论坛的目标是：（1）在 CBPR 和处理者隐私认可（PRP）系统的基础上建立一个国际认证系统；（2）通过推广 CBPR 和 PRP 系统，支持数据的自由流动和有效的数据保护和隐私；（3）提供一个论坛，就相关事宜进行信息交流和合作；（4）定期审查成员的数据保护和隐私标准，以确保项目要求与最佳实践相一致；（5）促进与其他数据保护和隐私框架的互操作性。

5. 美国发布《互联网未来宣言》

4 月 28 日，美国及其拉拢的 60 个国家及地区联合发布《互联网未来宣言》（A Declaration for the Future of the Internet）。宣言的签署者包括英国、加拿大、以色列、中国台湾、乌克兰等美国军事盟友及经济伙伴，也是拜登政府继其 2021 年底组织民主峰会后，再次打着美西方价值观旗号破坏冷战后国际秩序的又一新动作。

宣言列出了旨在维护“自由与开放互联网”的五项主张二十二个措施，包括：（1）保护人权和基础自由——提升网络安全并继续打击网络暴力、推进互联网安全与平等使用、重申打击非法网络有害内容及活动的承诺、约束互联网及算法工具的滥用；（2）全球性互联网——限制政府下令的互联网封锁、限制对合法内容的屏蔽、推动符合美西方价值观的信息自由流动、加强研发合作及标准制订、鼓励安全威胁信息共享；（3）包容性和可承受的互联网——推动可承受、包容性及可靠的网络访问、支持数字技能获得与提升、培养网络的多样性文化及多语种内容信息资讯；（4）数字生态系统中的信任——合作打击网络犯罪、保护个人隐私及数据、提倡和使用可靠的网络基础设施及服务提供商、支持基于规则的全球性数字经济；（5）互联网多边治理——保护和强化互联网多边治理体系、打击旨在削弱互联网技术基础设施的行为。

对此，我国外交部发言人赵立坚表示，不论是搞所谓的“互联网未来联盟”还是《互联网未来宣言》，都掩盖不了美国及一些国家在互联网问题上的政策本

质，即以意识形态划线，煽动分裂和对抗，破坏国际规则，并试图将自己的标准强加于人。这份所谓的《宣言》就是分裂互联网，挑动网络空间对抗的最新例证。美方这一行径，不管如何包装，其实还是新瓶装旧酒。美方以“民主”为借口对早已不得人心的“清洁网络计划”改头换面，企图搞封闭排他的“小圈子”。网络空间是人类共同的活动空间，网络空间的未来应由世界各国共同掌握。

6. 美国三部门联合发布警报，披露中国国家支持的网络行为者积极利用的顶级漏洞

10 月 6 日，美国国家安全局（NSA）、网络安全和基础设施安全局（CISA）和联邦调查局（FBI）发布联合网络安全咨询文件《中国国家支持的网络行为者积极利用的顶级漏洞》（Top CVEs Actively Exploited By People’s Republic of China State-Sponsored Cyber Actors），披露自 2020 年以来中国国家支持的网络行为者积极利用的常见漏洞，涵盖远程执行代码、任意文件读取、通过欺骗绕过身份验证等漏洞类型。

警报对组织提出一系列网络安全建议，包括：（1）尽快更新并修补系统，优先修补警报中发现的漏洞和其他已知的被利用漏洞；（2）尽可能采用多因素身份验证，要求所有帐户拥有唯一的强密码，若有迹象表明密码已泄露，立即更改密码；（3）拦截过时或未使用的网络协议；（4）升级或更换停产设备；（5）转向零信任安全模型。

7. 美韩发表联合声明，将加强网络安全合作

5 月 21 日，美国白宫发布《美韩领导人联合声明》（United States-Republic of Korea Leaders’ Joint Statement）。声明指出，双方致力于捍卫人权并建立一个开放的互联网，以确保全球信息的自由流动。为实现这一目标，韩国准备与美国一道签署《互联网未来宣言》。双方还将继续深化韩美在地区和国际网络政策方面的合作，包括加强在威慑网络对手、关键基础设施安全、打击网络犯罪和相关洗钱犯罪、保护加密货币和区块链应用、能力建设、网络演习、信息共享等方面的合作。

8. 美日印澳发表联合声明，将采取集体措施加强网络安全

5 月 24 日，美国、日本、印度和澳大利亚举行“四方安全对话”（Quad）会议，发布《Quad 联合领导人声明》（Quad Joint Leaders’Statement）。

声明指出，在日益数字化且网络威胁复杂的世界中，四方认识到迫切需要采取集体方法来加强网络安全。为了实现四方领导人关于自由和开放的印太地区的愿景，四方承诺通过共享威胁信息、识别和评估数字产品和服务供应链中的潜在风险来改善国家关键基础设施防御，以及调整政府采购的基线软件安全标准，利用集体购买力改善更广泛的软件开发生态系统，使所有用户都能受益。

四国将建立有弹性的网络安全体系，其中澳大利亚将牵头推动对关键基础设施的保护，印度将牵头改善供应链弹性和安全，日本将牵头发展网络安全劳动力，美国则将牵头制定软件安全标准。这些工作将以新的联合网络原则为指导，而该原则的目标是防范网络事件，使各国及国际社会为潜在的网络事件做好准备，并在发生网络事件时快速有效地作出回应。四国还将加强 CERT 之间的信息共享，并通过协调四国政府软件采购机制中的网络安全标准来提高软件及托管服务提供商的安全水平。

9. 美国和乌克兰签署合作备忘录，扩大网络安全合作

7 月 27 日，美国网络安全和基础设施安全局（CISA）和乌克兰国家特别通信和信息保护局（SSSCIP）签署合作备忘录，将从由美国及其西方盟友提供支持的对俄军事网络对抗层面，扩展至关键基础设施网络安全保护、网络威胁情报共享、网络攻击响应信息共享、加强与私营网络安全公司合作、网络安全联合研究及演练、联合网络安全项目实施等新领域。

10. 《英美政府间就获取电子数据打击严重犯罪的协定》生效

10 月 3 日，英美两国于 2019 年 10 月 3 日签署的《英美政府间就获取电子数据打击严重犯罪的协定》（Agreement between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime）正式生效。

协定允许美国和英国的执法机构在获得适当授权的情况下，在没有法律障碍的前提下，直接从高科技公司获取与严重犯罪相关的电子数据，包括恐怖主义、儿童性虐待和网络犯罪。具体内容方面，协定基本延续《云法案》的相关规定：（1）指令程序。签发国指定机构直接向服务提供商发出指令，服务提供商提供的信息直接提供给签发国指定机构；（2）指令目标。仅限于获取与严重犯罪预防、侦查、调查和起诉相关的信息，必须针对特定账户，并将特定个人、账户、地址、个人设备或其他特定标识符确定为指令目标。指令有权要求拦截无线或有线通信及相关延伸活动，但要求限定在固定且有限的周期内，不应超出实现指令目的合理必要的时间，且只有当同一信息不能以更为温和的方式合理获取时才能发布该指令；（3）使用限制。未经接收方同意，签发国不能将数据转移给第三方政府或国际组织，除非根据接收方国内法，该数据已经依法公开；（4）执行异议。收到指令的提供者有合理理由认为协定不能妥善适用于该指令时，有权提出具体异议。异议应在收到指令后的合理时间内向签发国指定机构提出。收到异议后，指定机构应作出回应。若异议未得到解决，双方同意的情况下，提供者可将该异议提交至接收方指定机构。双方指定机构可为解决此类异议进行协商，并定期或在必要时举行会晤，以讨论和解决本协定下提出的任何问题；（5）执行审查。在协定生效一年内以及之后定期，双方应对每一方的协定遵守情况进行审查，审查内容包括指令的发出和传输是否满足本协定目的和条款要求，根据指令获取的数据处理情况以确定协定下的程序是否需要调整。

11. 日澳签署新《日澳安全保障联合宣言》

10 月 22 日消息，日本与澳大利亚近日签署新的《日澳安全保障联合宣言》。宣言指出，未来 10 年，两国将继续积极致力于深化和扩大双边全面关系，加强在网络、太空、重要新兴技术、电信等领域的相关合作，构建包容且透明的制度、规范及标准。两国将共同努力，保持开放、自由、安全的技术环境；加强网络防御，提高对网络威胁的共识。

12. 中俄发表联合声明，重申将深化国际信息安全领域协作

2 月 4 日，中俄两国元首举行会谈，发表《中华人民共和国和俄罗斯联邦关

于新时代国际关系和全球可持续发展的联合声明》，集中阐述中俄在民主观、发展观、安全观、秩序观方面的共同立场，其中包括数字经济、国际科技发展环境、国际信息安全领域协作等方面的合作发展规划。

双方重申将深化国际信息安全领域协作，推动构建开放、安全、可持续、可及的信息通信技术环境。双方强调《联合国宪章》确立的“不使用武力、尊重国家主权和基本人权及自由、不干涉内政”等原则适用于信息空间，重申联合国在应对国际信息安全威胁领域的关键作用，支持联合国制定该领域新的国家行为准则。双方认为应联合国际社会制定信息网络空间新的、负责任的国家行为准则，包括具有法律效力的规范各国信息通信技术领域活动的普遍性国际法律文件。双方认为由中方提出、俄方原则支持的《全球数据安全倡议》为工作组讨论制定数据安全等国际信息安全威胁的应对措施提供了基础。双方支持打造国际化的互联网治理体系，认为各国平等享有互联网治理权，主权国家有权管控和保障本国网络安全，任何企图限制国家网络主权的行为不可接受，应促进国际电信联盟在解决有关问题上发挥更加积极的作用。

两国有关部门还签署《信息化和数字化领域合作协议》等一系列重点领域合作文件。

13. 《“中国+中亚五国”数据安全合作倡议》发布

6 月 8 日，“中国+中亚五国”外长第三次会晤举行，会晤通过《“中国+中亚五国”数据安全合作倡议》。

倡议指出，中国+中亚五国欢迎国际社会在支持多边主义、兼顾安全发展、坚守公平正义的基础上，为保障数据安全所作出的努力，愿共同应对数据安全风险挑战并在联合国等国际组织框架内开展相关合作。中亚各国支持中方提出的《全球数据安全倡议》。倡议指出，在遵守国内法和国际法基础上，各方建议各国及各主体：就防范全球信息安全所面临的挑战和威胁，保障数据安全，开展协调行动与合作；增进在保障数据安全和使用信息技术领域的互信；应以事实为依据全面客观看待数据安全问题，积极维护全球信息技术产品和服务的供应链开放、安全、稳定；各国应尊重他国主权、司法管辖权和对数据的安全管理权，未经他国法律允许不得直接向企业或个人调取位于他国的数据。

14. 中国国家互联网信息办公室与泰国国家网络安全办公室签署网络安全合作谅解备忘录

7 月 5 日，我国国家互联网信息办公室与泰王国国家网络安全办公室签署《关于网络安全合作的谅解备忘录》，双方同意进一步加强网络安全领域交流合作，维护网络空间稳定。

15. 中国国家互联网信息办公室与印尼国家网络与密码局签署网络安全合作行动计划

7 月 29 日消息，我国国家互联网信息办公室近日与印尼国家网络与密码局签署网络安全合作行动计划，双方将在 2021 年签署的《关于发展网络安全能力建设和技术合作的谅解备忘录》基础上，进一步深化两国网络安全能力建设合作。

16. 中国全面推进加入《数字经济伙伴关系协定》谈判

8 月 22 日，我国商务部新闻发言人表示，中国加入《数字经济伙伴关系协定》（DEPA）工作组已正式成立，意味着我国全面推进加入 DEPA 的谈判。工作组将由 DEPA 成员政府代表组成，智利担任主席，在工作组框架下与中国开展磋商，推进中国加入进程。中方将在加入工作组框架下，全面做好加入 DEPA 的准备，与 DEPA 成员开展实质性谈判，持续推进加入进程。

DEPA 由新西兰、新加坡、智利于 2019 年 5 月发起、2020 年 6 月签署，是全球首份数字经济区域协定。2021 年 11 月 1 日，商务部部长王文涛代表中国正式提出加入申请。

17. 中国证监会、财政部与美国监管机构签署审计监管合作协议

8 月 26 日，中国证券监督管理委员会、财政部与美国公众公司会计监督委员会（PCAOB）签署审计监管合作协议，将于近期启动相关合作。

中国证监会表示，近年来，我国《数据安全法》《个人信息保护法》等信息安全相关法律法规陆续施行，相关市场主体的信息安全责任更加明确，操作上更加有章可循。企业无论上市与否，都有义务严格遵守本国法律法规。近期中国证监会等部门完善了境外上市相关保密和档案管理规定，对规范审计工作底稿信

息安全管理提出明确要求，进一步落实上市公司信息安全的主体责任，同时为上市企业和会计师事务所依法依规保管和处理涉密敏感信息提供了更加细化和可执行的指引，有助于在满足会计审计要求的前提下做好底稿编制工作，并依法保护相关信息安全。合作协议对于审计监管合作中可能涉及敏感信息的处理和使用作出明确约定，针对个人信息等特定数据设置专门的处理程序，为双方履行法定监管职责的同时保护相关信息安全提供可行路径。

18. 美国白宫发布《提升国家安全、国防和情报系统网络安全备忘录》

1 月 19 日，美国总统拜登签署《提升国家安全、国防和情报系统网络安全备忘录》（Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems，简称 NSM）。

NSM 旨在落实第 14028 号行政令《改善国家网络安全》，设定国家安全系统的多项网络安全新要求，强化国家安全局（NSA）、国防部、情报机构和其他联邦机构的网络安全保护能力，推进新形势下网络安全防御现代化。总体来看，NSM 从明确网络安全技术落地应用时间表与指引、强化 NSA 对国家安全系统的管理与指导地位、确保跨域解决方案安全性、提升网络安全风险感知能力、构建国家安全系统云技术网络安全和事件响应协作机制、引入基于特殊任务需求的例外情况等六大维度，加强网络安全保障，细化国家安全系统网络安全标准。

19. 美国 BIS 发布《信息安全管制：网络安全物项》

5 月 26 日，美国商务部工业和安全局（BIS）公布一项针对网络安全物项出口管制的最终规则《信息安全管制：网络安全物项》（Information Security Controls: Cybersecurity Items），自发布之日起生效。2021 年 10 月，BIS 曾发布这一规则的暂行规定，此次发布的是最终版本。

新规主要包括以下内容：（1）出于国家安全与反恐原因，对“可用于监视、间谍活动或其他破坏、瘫痪或损害网络或设备”的特定网络安全物项引入新的出口管制措施。其中，网络安全物项主要是针对“入侵软件”相关的实物、软件和技术，出口管制措施指出口上述网络安全物项至因国家安全或反恐而受到出口管制的区域的，原则上需要向 BIS 申请许可证；（2）修订经授权的网络安全出口

许可例外机制，即 ACE 许可例外机制。ACE 许可例外机制允许向大多数目的地和最终用户出口、再出口和转移“网络安全物项”，但在出口目的地限制、政府最终用户限制、非政府最终用户限制和最终用途限制情形下，不能适用 ACE 许可例外，仍然需要向 BIS 申请许可证。此次发布的最终规则明确“密码分析程序、网络渗透工具、自动网络漏洞分析和响应工具等技术”不能适用 ACE 许可例外；（3）为回应公众对 2021 年 10 月暂行规定的意见，最终规则中添加符合“政府最终用户”定义的详细说明清单，进一步澄清和明确 ACE 许可例外中“政府最终用户”的定义。清单中包括“更敏感的政府最终用户”和“不太敏感的政府最终用户”等类别。

20. 美国白宫发布《关于管理 2024 财年预算网络安全优先事项的备忘录》

7 月 22 日，美国白宫发布《关于管理 2024 财年预算网络安全优先事项的备忘录》（Administration Cybersecurity Priorities for the FY 2024 Budget，M-22-16），概述了联邦民事行政部门（Federal Civilian Executive Branch，简称 FCEB）向管理和预算办公室（OMB）提交的 2024 年财政预算中应明确的网络安全优先事项。

备忘录指出，预算重点包括三个优先事项：提高政府网络防御能力和弹性、深化关键基础设施防御的跨部门合作、加强数字化未来的基础。对于第一个优先领域，FCEB 应在其预算中优先考虑信息技术现代化和实施零信任；对于第二个优先领域，预算应确保部门风险管理机构有足够的资源履行《2021 财年国防授权法》规定的职责；对于第三个优先领域，各机构应优先考虑人力资本、有形基础设施和供应链风险管理。OMB 将与国家网络总监办公室（Office of the National Cyber Director，ONCD）联合审查联邦机构在这些优先事项上的进展，确定潜在差距及解决方案。OMB 还将与 ONCD 协调，向机构提供反馈，说明优先事项是否得到充分解决，以及是否与总体网络安全战略相一致。

21. 美国正式通过《2022 年芯片与科学法》

8 月 9 日，美国总统拜登签署《2022 年芯片与科学法》（CHIPS and Science Act of 2022），使其正式成为法律。

该法主要分为三部分：A 部分为聚焦于半导体产业的《2022 年美国芯片法》，其中芯片基金宏观分配管理、联邦财政补助管理配套、联邦财政补助禁令规定、投资税收抵免相关规定与我国半导体产业发展息息相关；B 部分为普适于其他诸多行业关键学科的《研发、竞争和创新法》，其中美国研发创新资金投入、“美国制造”禁令规定、外国人才招募禁令规定、针对中国的研究安全限制性规定与竞争条款亟需警醒；C 部分为《2022 年最高法院安全资金法》，与半导体无直接关联。

同日，白宫发布简报《<芯片与科学法>将降低成本、创造就业、增强供应链并对抗中国》（CHIPS and Science Act Will Lower Costs, Create Jobs, Strengthen Supply Chains, and Counter China），表示新法将致力于实现以下目标：（1）巩固美国在半导体领域的领导地位；（2）促进美国在无线供应链方面的创新；（3）推进美国在未来技术方面的全球领导地位；（4）促进区域经济增长和发展；（5）为更多的美国人提供 STEM 机会，让其参与高薪的技术工作；（6）在 STEM 和创新方面为全美国创造机会和公平。

《2022 年芯片和科学法》中包含了“护栏条款”，即接受资助的公司至少 10 年内不能在中国或其他“令人担忧的国家”进行新的高科技投资，除非它们生产的是技术含量较低的成熟制程芯片，只为当地市场服务。

22. 美国发布《2022 年美国芯片与科学法：芯片资金战略》

9 月 6 日，为落实《2022 年芯片和科学法》，美国商务部发布《2022 年美国芯片与科学法：芯片资金战略》（CHIPS for AMERICA：A Strategy for the CHIPS for AMERICA Fund），落实拨给“美国芯片基金”计划的 500 亿美元。战略显示，上述 500 亿美元资金中，约 280 亿美元将用于资助建立先进制程芯片的制造和封装设施，约 100 亿美元将用于扩大在汽车等领域使用的成熟制程芯片制造，另外约 110 亿美元计划投入到半导体领域研发。通常认为，28 纳米及以下的制程属于先进制程。

美国商务部部长雷蒙多表示，根据该战略，美国将在半导体领域建立“护栏”以确保那些获得资助的企业不会将最新技术送到海外，从而危及美国国家安全。如果获得资助的企业和机构未能履行某些承诺，商务部将“毫不犹豫地收回

资金”。商务部的目标是在明年 2 月前开始向相关企业收集资金申请，并可能在明年春天开始拨款。申请者必须“以资本投资财务披露的形式”提供证据，证明所寻求的资金对于进行投资是“绝对必要的”。

9 月 20 日，白宫宣布成立 CHIPS 美国办公室，负责落实 500 亿美元投资。办公室的具体职位将设在白宫和商务部，并披露了办公室主要成员，包括在大型项目管理、财务和政府问责需求方面有经验的高管。

23. 美国 BIS 宣布对 ECAD 软件实施出口管制

8 月 15 日，美国商务部工业和安全局（BIS）发布的《落实 2021 年瓦森纳协定第 1758 条第四项技术的某些决定》（Implementation of Certain 2021 Wassenaar Arrangement Decisions on Four Section 1758 Technologies）正式生效。

BIS 将通过修订 5 个美国出口管制编码（又称：ECCN）以及增加 1 个新的 ECCN，以实施对四种技术的出口管制。四种管制技术中最受瞩目的是：“专门设计”用于“开发”具有任何“Gate-All-Around Field-Effect Transistor”（GAAFET）结构的集成电路（IC）的计算机辅助电子设计软件（ECAD 软件）。BIS 为该技术增加了新 ECCN 编码，即：3D006。

BIS 认为，ECAD 软件是一类用于设计、分析、优化和测试集成电路或印刷电路板性能的电脑软件，被用于军事和航空航天防御的各种应用中设计复杂的集成电路。而 GAAFET 技术方法是实现 3 纳米及以下技术节点的关键，该技术可以使生产更快、更节能、更耐辐射的集成电路成为可能，可推进许多商业及在国防和通讯卫星的军事应用。因此，新增管制 ECAD 软件意味着美方旨在限制专门设计用于开发 3 纳米及以下技术节点关键的 GAAFET 结构的集成电路的设计软件的出口、再出口、在美国以外的一国国内转让的行为。

24. 美国白宫发布《关于实施 2022 年芯片与科学法的行政令》

8 月 25 日，美国白宫发布《关于实施 2022 年芯片与科学法的行政令》（Executive Order on the Implementation of the CHIPS Act of 2022），落实《2022 年美国芯片与科学法》中 527 亿美元半导体制造与研发补助，设置六

大优先事项，包括保护纳税人资金、满足经济与国家安全需求、确保半导体领域长期领导地位、做强做大区域制造业与创新集群、促进私营部门投资、为广泛利益相关者和社区创造利益等。

25. 美国白宫发布《关于确保外国投资委员会考虑不断演变的国家安全风险的行政令》

9 月 15 日，美国白宫发布《关于确保美国外国投资委员会认真考虑不断演变的国家安全风险的行政令》（Executive Order on Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States）。这是 1975 年外国投资委员会（CFIUS）成立以来，首份针对国家安全因素进行界定和部署的行政令。

行政令指出，由于交易中可能会涉及外国主体（包括外国政府）的法律环境、意图或能力，即使是出于商业目的的经济交易，如果直接或间接涉及外国对手或特别关注的其他国家的投资，仍然可能会给美国国家安全带来不可接受的风险。为此美国政府要继续应对这些不断演变的风险，包括对美国企业的外国投资进行严格审查。

根据行政令，CFIUS 应考虑任何外国交易在四个领域的影响，以使 CFIUS 更好地与拜登政府的国家安全优先事项保持一致：关键供应链弹性、技术领先地位、网络安全和敏感个人数据。网络安全方面，行政令指出，对美国来说，重要的是确保外国对美国企业的投资不会削弱美国网络安全。包括有能力和意图实施网络入侵或其他恶意网络活动的海外投资，例如旨在影响联邦、州、部落、地方或地区办公室选举结果的活动、威胁美国关键基础设施运营或影响美国通信的机密性、完整性或可用性，可能会对国家安全构成风险。国会在《外国直接投资法》第 1702（c）（6）条中，将“加剧或创造新的网络安全漏洞”确定为 CFIUS 在考虑所管辖交易产生的国家安全风险时应考虑的因素。数据安全方面，行政令指出，CFIUS 应考虑在有权访问或存储美国人的敏感数据（包括健康和生物数据）的美国企业中的海外投资，海外投资者可能会采取行动威胁美国国家安全，与其相关的第三方也可能导致该交易构成这种威胁。

26. 美国白宫发布《关于加强美国信号情报活动保障的行政令》

10 月 7 日，美国白宫发布《关于加强美国信号情报活动保障的行政令》（Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities），指示美国将采取的步骤，以落实拜登总统和欧盟委员会主席冯德莱恩于2022年3月宣布的美国在欧盟-美国数据隐私框架(EU-US DPF）下的承诺。

行政令主要规定以下内容：（1）为美国的信号情报活动增加进一步保障措施，要求进行这类活动只能出于明确的国家安全目标；只在为推进有效的情报优先事项所必需时进行，并且只在与该优先事项相称的范围和方式下进行。同时，考虑到所有人的隐私和公民自由，无论其国籍或居住国如何；（2）规定通过信号情报活动收集的个人信息的处理要求，并扩大法律、监督和合规官员的责任，以确保采取适当行动来纠正不合规事件；（3）要求美国情报界人士更新政策和程序，以反映行政令中包含的新的隐私和公民自由保障措施；（4）建立多层机制，使符合条件的国家和区域经济一体化组织的个人获得独立和有约束力的审查，在认为其个人数据被美国信号情报部门以违反美国法律的方式收集时，能够寻求补救；（5）呼吁隐私和公民自由监督委员会审查情报界的政策和程序，以确保其符合行政令，并对补救程序进行年度审查。

这些步骤将为欧盟委员会提供基础，以支撑通过关于欧美数据跨境流动新的充分性决定。它还将为使用标准合同条款和具有约束力公司规则将欧盟个人数据转移到美国的公司提供更大的法律确定性。

27. 美国白宫发布《国家安全战略》

10 月 12 日，美国政府发布新版《国家安全战略》（National Security Strategy），重申加强国家数字防御和打击网络犯罪分子的承诺。战略详细说明为加强国家网络安全所采取的一系列措施，并粗略提到外国对手所构成的网络威胁挑战。

战略提出：（1）美国正在与盟友和合作伙伴密切合作，为关键基础设施制定标准，以快速提高网络弹性，并建立集体能力以快速响应攻击；（2）建立创新的合作伙伴关系，以扩大执法合作，打击网络犯罪分子及其网络洗钱活动，应

对来自犯罪分子的破坏性网络攻击；（3）致力于加强规范以减轻网络威胁并增强网络空间的稳定性，目标是阻止来自国家和非国家行为者的网络攻击，并将使用所有适当的国家力量工具果断地应对网络空间中的敌对行为，包括破坏或削弱重要国家职能或关键基础设施的行为；（4）将继续推动遵守联合国大会批准的负责任国家网络空间行为框架；（5）通过跟踪、归因和防御网络空间中恶意行为者的活动来保护投资并增强弹性；（6）在军事方面投资于一系列先进技术，包括在网络和太空领域、导弹打击能力、可信 AI 和量子系统的应用，同时及时向战场部署新能力；（7）将包括网络空间在内的军事领域和包括信息技术在内的非军事领域进行整合，以实施综合威慑；（8）将制定道路规则，包括迫切需要更新技术、网络空间、贸易和经济的道路规则；（9）将优化国家治理方式，包括强化网络外交、对新兴技术的关注和网络安全服务。

此外，战略强调了一个观点，即美国的领导力是克服所谓“全球威胁”的关键。关于该战略中的中国部分，拜登政府声称“将优先考虑保持对中国的持久竞争优势，同时约束仍然非常危险的俄罗斯”，还宣称“中国是唯一一个既有重塑国际秩序意图的竞争者，也逐渐拥有经济、外交、军事和科技力量来日益推进这一目标”。此外，战略声称“未来十年是美国与中国竞争的决定性十年”。

28. 美国商务部发布临时最终规则

10 月 13 日，美国商务部工业与安全局（BIS）的临时最终规则《实施额外出口管制：特定先进计算和半导体制造物项、超级计算机和半导体最终用途、实体清单修改》（Implementation of Additional Export Controls: Certain Advanced Computing and Semiconductor Manufacturing Items; Supercomputer and Semiconductor End Use; Entity List Modification）在联邦公报上正式公布，并开始为期 60 天的意见征询期，持续到 2022 年 12 月 12 日。该规则修订《出口管理条例》（EAR），聚焦“高性能计算芯片和超级计算机”出口，于 2022 年 10 月 7 日、12 日和 21 日分阶段生效，要点包括：

一是在《商业控制清单》（CCL）中新增多个半导体管制物项。新列入 EAR 管制范围的物项主要有高性能计算芯片（3A090），包含高性能计算芯片的计算机、电子组件或元件（4A090），开发生产前述计算机、电子组件或元件的专用

软件（4D090）及特定先进半导体制造设备（3B090）等。BIS 将“区域稳定”（RS）新列为针对我国的出口管制原因，对上述物项向我国出口许可的申请明确采取“推定拒绝”政策——除非适用“部件和设备的维修更换”等许可例外，新增半导体物项出口、再出口、转移（国内）或视为出口至我国主体前，要向美国商务部申请许可。此处管制逻辑为“特定物项→不特定最终用途、用户”。

二是引入三项外国直接产品（FDP）规则，扩大域外管辖范围。引入“先进计算”与“超级计算机”FDP 规则——若特定外国（如中国或第三国）制造的先进计算物项和超级计算机物项是受美国《出口管理条例》（EAR）管辖的特定 19 项 ECCN 编码所规定规格技术或软件的直接产品，或制造该物项的主要生产设备或其组件是美国原产技术和软件的直接产品，且用于中国集成电路晶圆生产或中国超级计算机研发等用途，那么该外国制造物项适用“推定拒绝”审查政策，出口至我国要向美国商务部申请许可。

三是强化对“超级计算机”和我国半导体制造最终用途的管制。满足特定条件的半导体设备，对于中国大陆晶圆厂的出口受到限制，主要影响 18 纳米或以下的 DRAM 芯片、128 层或以上的 NAND 闪存芯片、14 纳米或以下的逻辑芯片等。设备的出口需要申请许可证与严格审查。

为减少新规对半导体供应链的短期影响，BIS 正在建立一个临时通用许可证（Temporary General License），以允许在中国境内进行特定、有限且与在中国境外使用产品相关的制造活动，且 BIS 正在确认可用于合规性程序、协助开展尽职调查的示范认证（model certificate）。

29. 欧盟委员会提出《芯片法案》

2 月 8 日，欧盟委员会提出《建立加强欧洲半导体生态系统措施框架的法规提案》（Proposal for a Regulation establishing a framework of measures for strengthening Europe's semiconductor ecosystem），简称《芯片法案》（Chips Act）。法案指出欧盟将投入超过 430 亿欧元公共和私有资金，用于支持芯片生产、试点项目和初创企业。其中 110 亿欧元用于加强现有研发和创新，确保部署先进的半导体工具以及用于原型设计、测试的试验生产线等。到 2030 年，欧盟计划将在全球芯片生产的份额从目前的 10%增加到 20%。

法案将确保欧盟拥有必要的工具、技能和技术能力，实现包括先进芯片设计、制造、封装等方面的提升，以保证欧盟地区的半导体供应链稳定并减少外部依赖。法案主要提出三方面内容：1）提出“欧洲芯片倡议”，即通过汇集来自欧盟、成员国和现有联盟相关第三国和私营机构资源力量，组建“芯片联合事业群”，提供110亿欧元用于加强现有研究、开发和创新；2）建设新的合作框架，即通过吸引投资和提高生产力来确保供应安全，以提高先进制程芯片供应能力，通过提供基金为初创企业提供融资便利；3）完善成员国与委员会之间的协调机制，通过收集企业关键情报以监控半导体价值链，建立危机评估机制，以实现半导体供应、需求预估和短缺情况的及时预测，从而能够迅速地做出反应。

10月10日,欧盟委员会与27个成员国联合发起关于半导体价值链的磋商，旨在从半导体供应链中的公司和依赖半导体提供产品或服务的公司处收集意见、证据和数据。本次咨询将持续到11月11日，是朝着建立风险评估、提高价值链透明度和抵御潜在风险的能力以及使决策者能够正确应对半导体短板迈出的第一步。咨询的结果将有助于为《芯片法案》中提出的监管机制指明方向，比如确定适当的早期预警指标，以预测半导体供应链的未来短缺并防止半导体危机。

30. 英国国防部发布《国防网络弹性战略》

5月9日，英国国防部发布《国防网络弹性战略》（Cyber Resilience Strategy for Defence），概述国防部建立更强大国防网络弹性的愿景。战略明确七个战略重点，分别是设计安全；治理、风险和合规性；快速检测和响应；人员与文化；工业；安全基础；实验、研究和创新。战略的实施将采用以下指导原则：适应性方法；安全且有弹性；全力以赴；协作、整合和凝聚力。

战略的实现途径包括：（1）构建安全的数字骨干网；（2）成功交付防御性网络计划；（3）关注网络安全的装备能力计划，以确保防御设计的安全；（4）嵌入现代安全工作方式；（5）转向与行业建立新的安全关系；（6）加速用于采购网络能力的敏捷商业结构；（7）在国防部内部开发和雇用具有适当网络技能的劳动力；（8）在战略贡献者的组织内建立网络防御组织；（9）创建和测试运营弹性计划；（10）为网络弹性的各个方面制定明确和商定的问责制。

31. 英国内政部提出《国家安全法案》

5 月 11 日，英国内政部提出《国家安全法案》（National Security Bill）。内政部表示，外国对英国的敌对活动威胁正在增加。这些威胁持续存在且形式多样，包括间谍活动、外国对政治体系的干预、破坏、虚假信息、网络行动等。英国必须能够阻止、发现和干扰那些试图通过暗中行动损害英国国家利益、敏感信息、商业机密和民主生活方式的国家行为者。

法案拟议措施主要包括：改革现有的间谍法；打击国家支持的破坏活动和外国干涉的新罪行；强化警察在调查国家威胁活动方面的权力；提供权力，允许在早期阶段解决国家威胁；引入新的最后手段，约束那些造成威胁但尚未达到检控门槛的个人。法案新增“蓄意破坏罪”（Sabotage）和“外国干涉罪”（Foreign Interference）。“蓄意破坏罪”旨在解决由国家支持的对英国资产造成的严重威胁，包括对英国安全或利益至关重要的场所、数据和基础设施的攻击。“外国干涉罪”旨在打击外国干涉活动。如果外国势力通过秘密影响、虚假信息和攻击英国选举进程，不恰当地干预英国民主和公民社会，将构成犯罪。同时，法案将预备行为纳入约束范围，对那些准备实施构成国家威胁犯罪和其他有害活动的人进行刑事定罪。

10 月 18 日，公共法案委员会（Public Bill Committee）完成对《国家安全法案》的修订，目前法案仍处于下议院报告阶段。修正案的内容包括：（1）删除“报告来自外国势力的虚假信息”；（2）国务卿必须任命个人或机构负责审查来自外国势力的虚假信息对国家安全构成威胁或潜在威胁的程度；（3）根据前款进行的审查，必须包括外国对选举干预程度的评估。

32. 意大利发布首个国家网络安全战略及战略实施计划

5 月 25 日，意大利政府发布《2022 至 2026 年意大利国家网络安全战略》（STRATEGIA NAZIONALE DI CYBERSICUREZZA 2022-2026）及《2022 至 2026 年意大利国家网络安全战略实施计划》（PIANO DI IMPLEMENTAZIONE STRATEGIA NAZIONALE DI CYBERSICUREZZA 2022-2026）。

战略认为意大利面临三方面的网络安全威胁，分别是：网络犯罪分子、黑客或国家发动的网络攻击；政府控制或影响的公司所开发的技术对供应链造成的

干扰；虚假信息活动、假新闻、“深度造假”和通过网络领域传播错误信息来操纵和分化公众舆论。

对此，战略提出五大应对支柱：确保公共部门和行业数字化转型的网络弹性；实现国家和欧洲数字战略自主权；预测网络威胁的演变；建立有效的网络危机管理机制；处理与混合威胁有关的在线虚假信息。战略确定了三大基本目标以更好地应对挑战，分别是：（1）保护。即通过旨在管理和减轻风险的系统性方法保护国家战略资产，具体涉及技术筛选、法律框架、态势感知、公共行政网络弹性、国家基础设施、密码学、打击网上虚假信息；（2）响应。即通过部署增强的国家监控、检测、分析和响应能力以及启动国家网络安全生态系统流程对国家网络威胁、事件和危机做出响应，具体涉及危机管理、国家网络服务、网络演习、归因、打击网络犯罪和威慑能力；（3）发展。即有意识且安全地发展能够响应市场需求的数字技术、研究和产业竞争力。

33. 加拿大发布声明，以“国家安全”为由禁止华为中兴参与5G网络建设

5月19日，加拿大政府发布政策声明《保护加拿大通信系统》（Securing Canada’s Telecommunications System），以“国家安全”为由，禁止本国电信系统使用华为、中兴两家中国公司的产品和服务。

根据该声明，禁止加拿大电信公司在其网络中使用华为、中兴两家中企的任何产品或服务，已经安装这些设备的加拿大电信公司被要求停止使用并拆除设备。加政府希望电信公司在2022年9月之前停止从华为和中兴采购新的4G或5G设备与服务；在2024年6月之前停止使用新的或现有的5G设备与服务；在2027年12月之前停止新的或现有的4G设备与服务。加拿大政府表示将在“短时间”内提交一项法案，对《电信法》进行修订，支持在电信系统中抵御金融、电信、能源和运输部门的国家安全风险。

美联社提到，加拿大是“五眼联盟”中最后一个禁止在5G网络建设中使用华为设备的国家。早在特朗普时期，美国政府就开始游说并施压“五眼联盟”其他国家在电信网络中禁用华为。加拿大创新、科学与工业部长承认，在宣布禁令前，加方“安全机构进行了全面审议并与最密切的盟友进行了磋商”。

34. 俄罗斯第 263-FZ 号联邦法部分条款生效，日用户超过 50 万的外国互联网公司应在俄罗斯设立分支机构

1 月 4 日，俄罗斯第 263-FZ 号联邦法《关于外国人在俄罗斯联邦境内的信息和电信网络活动》（О деятельности иностранных лиц в информационно-телекоммуникационной сети "Интернет" на территории Российской Федерации）中的部分条款生效。该法第 5 条第 3 款要求日用户总数超过 50 万人的外国互联网公司必须在俄罗斯设立分支机构、代表处或授权法人实体，并提交相关资料。

该分支机构、代表处或授权法人实体负责处理以下事项：（1）处理俄罗斯公民的申诉；（2）遵守法院判决和俄罗斯国家机构的决定；（3）代表其外国母公司的利益；（4）根据有关信息、信息技术和信息保护的法律规定，采取措施限制对信息的访问或删除非法传播的信息。俄罗斯联邦通信、信息技术和大众传媒监督局于 2021 年 11 月发布一份需要遵守这一要求的外国互联网公司名单，其中包括 Google、Twitter 和 Meta Platforms。

该法于 2022 年 1 月 1 日生效，除前述规定外，还规定多项强制措施以确保合规，包括在搜索引擎中标记不合规网站。此外，杜马还强调违反该法规定的处罚措施，例如禁止不法组织进行货币交易，以及部分和完全封锁其在俄罗斯境内的资源。

35. 俄罗斯发布总统令《关于确保俄罗斯联邦关键信息基础设施技术独立与安全的措施》

3 月 30 日，俄罗斯总统普京签署第 166 号总统令《关于确保俄罗斯联邦关键信息基础设施技术独立与安全的措施》（О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации），要求从 31 日起禁止在国家采购中未经相关部门许可为重要国家基础设施部门购买外国软件。从 2025 年开始，国家重要基础设施部门将完全禁

止使用外国软件。

根据总统令，任何客户（地方政府参与的组织除外）如果没有获得“俄罗斯联邦政府授权的执行机构”的批准，不能购买用于“俄罗斯联邦关键信息基础设施”的外国软件，也不能购买“运行此类软件所需的服务”。这类关键基础设施包括医疗、制造业、通信、交通、能源、金融和市政设施运营的至关重要的信息系统和电信网络。

36. 俄罗斯发布总统令《关于保障俄罗斯联邦信息安全的补充措施》

5 月 1 日，俄罗斯总统普京签署第 250 号俄罗斯联邦总统令《关于保障俄罗斯联邦信息安全的补充措施》（О дополнительных мерах по обеспечению информационной безопасности Российской Федерации）。

总统令要求，联邦行政机关、俄罗斯联邦主体最高行政机关、国家基金、国有企业（公司）和其他依法成立的组织、战略企业、战略股份公司和俄罗斯经济的系统构成组织、关键信息基础设施主体法人的负责人应履行下列义务：（1）赋予机关/组织副负责人信息安全保障职权，包括检测、预防、消除计算机攻击后果和应对计算机事件；（2）在机关/组织建立信息安全保障内部机构，承担检测、预防、消除计算机攻击后果和应对计算机事件的职能，或将这些职能赋予一个现有的内部机构；（3）在必要时引入其他组织实施本机关/组织信息安全的保障措施。在此情况下，只能引入具备保密信息技术保护许可证的组织；（4）向联邦安全局公职人员提供通过互联网不受阻碍（包括远程）地访问属于本机关/组织或由其使用的信息资源，并落实联邦安全机关根据监测结果作出的指示；（5）赋予机关/组织负责人该机关/组织信息安全保障的个人责任。

总统令要求，自 2025 年 1 月 1 日起，禁止机关/组织使用来源国为对俄罗斯联邦、俄罗斯法人和自然人采取不友好行为的国家的信息保护手段，或生产者是这些国家管辖的组织，由这些国家直接或间接控制或关联。

37. 俄罗斯杜马通过法案，对未能开设俄罗斯办事处的 IT 运营商处以罚款

7 月 14 日，俄罗斯总统普京签署《关于俄罗斯联邦行政侵权法（通信和信

息领域个别侵权行为的行政责任）的修正案》（О внесении изменений в Кодекс Российской Федерации об административных правонарушениях（в части уточнения административной ответственности за отдельные правонарушения в области связи и информации））。修正案规定，如果日用户超过500，000人的外国互联网运营商未能在俄罗斯开设分支机构、代表处或授权法律实体，则该运营商可能会被处以年收入最高10%的罚款；多次违法的，罚款最高将占年收入的20%。

38. 乌克兰发布总统令，实施《乌克兰网络安全战略实施计划》

2月2日，乌克兰国家特殊通信和信息保护局（DSSZZI）宣布，乌克兰总统发布总统令，决定实施国家安全和国防委员会在2021年12月30日通过的《乌克兰网络安全战略实施计划》（Plan for Implementing the Cyber Security Strategy of Ukraine）。

实施计划要求国家网络安全协调中心在六个月内更新网络安全战略的实施情况。网络安全战略的优先事项和主要目标包括引入有效的网络防御、打击网络空间的颠覆活动以及确保数字服务安全。具体来说，将包括以下内容：（1）建立一个全国性的网络安全系统，包括实时自动检测网络攻击的技术能力；（2）与国际合作伙伴，特别是与欧盟和北约成员国就网络空间破坏性活动进行信息交换；（3）参考最佳实践，为公共和私营部门制定网络安全基本要求和建议；（4）网络安全研发应涉及最新技术，特别是云和量子计算技术、5G网络、物联网和AI。

39. 日本总务省发布修订后的《2022年ICT网络安全综合措施》

8月12日，日本总务省网络安全工作组发布修订后的《2022年ICT网络安全综合措施》（ICT サイバーセキュリティ総合対策 2022）。以该文件为指引，内政和通信部（MIC）将与相关组织和私营部门合作，进一步推进网络安全工作。

文件主要关注以下内容：（1）确保信息和通信网络的安全性和可靠性。电

信运营商应当采取积极的网络安全措施，修订电信业务法，建立重大事故威胁报告制度，同时开展电信运营商的网络安全措施示范项目，防范供应链风险，确保物联网、云服务和智慧城市的网络安全；（2）提高自主应对网络攻击的能力。加强和培育日本本土的网络安全产业，以降低对他国产品和信息的依赖性，同时建立网络安全综合智力和人力资源开发平台（CYNEX），广泛培养网络安全人才；（3）促进国际合作。通过东盟-日本网络安全能力建设中心（ASEAN-Japan Cyber Security Capacity Building Centre，简称 AJCCBC）加强与印度-太平洋地区国家的合作，继续实施信息通信技术支持项目和美日全球数字连接计划，以支持日本企业向东盟地区的扩张，促进信息流动。

40. 乌兹别克斯坦通过《网络安全法》

4 月 15 日，乌兹别克斯坦共和国总统签署通过《网络安全法》（О КИБЕРБЕЗОПАСНОСТИ），于 2022 年 7 月 17 日生效。

该法确立“网络安全基本原则”，包括：（1）合法性；（2）在网络空间中应保护个人、社会和国家利益的可持续性；（3）该法是网络安全监管的唯一依据；（4）本地开发商应持续参与创建网络安全系统；（5）对网络安全国际合作持开放态度。该法明确以下领域的信息系统属于“关键设施”（critical facilities）：公共行政和公共服务、国防、国家安全、执法、燃料和能源工业（包括核能）、化工和石化行业、公共卫生、住房和公用事业服务、银行和金融、运输、信息和通信技术。国家安全局是该国网络安全领域的监管机构。

41. 越南批准《推动网络空间发展到 2025 年、展望 2030 年的网络空间安全战略》

8 月 10 日，越南批准《推动网络空间发展到 2025 年、展望 2030 年的网络空间安全战略》（Chiến lược An toàn, An ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn 2030），旨在积极应对网络空间挑战，实现“2030 年发展愿景”——成为网络安全自主国家，保障网络空间安全、稳定、繁荣。

战略指出，越南公安部将：（1）制定并完善从中央到地方同步、统一的网络安全保护政策和法律，全面规制利用网络侵犯国家安全和社会秩序的违法犯罪

活动，提升维护国家网络空间主权的能力；（2）制定并完善保护国家数据与个人数据安全的政策法律，明确国内外组织和企业在收集、存储、处理越南公民数据以及维护越南网络空间主权等方面的责任义务；（3）研究、审查、修改并补充网络安全规范文件，提升统一性、全面性、同步性，满足预防、打击网络犯罪和及时解决争端的要求；（4）制定并完善《网络安全法》实施指导性文件以及关于网络安全产品和服务经营条件的法律文件，特别关注用于国家安全重要信息系统的产品和服务以及国家机关信息系统。

42. 荷兰内阁公布《2022-2028 年国家网络安全战略》

10 月 10 日，荷兰内阁公布《2022-2028 年荷兰国家网络安全战略》（Nederlandse Cybersecuritystrategie 2022-2028）。

战略提出四项主要目标：（1）提高政府、公司和社会组织的网络应对网络事故的恢复能力；（2）在荷兰境内提供安全和创新的数字产品；（3）应对来自官方和犯罪分子的数字威胁；（4）增加网络安全专家数量，开展数字安全教育，并提高公民面对网络事故的恢复能力。

为实现上述目标，战略将国家网络安全中心、数字信托中心和数字服务提供商网络安全事件响应小组合并为一个国家网络安全机构。内阁还指出，该战略将每年接受审查，并在 2025 年进行针对战略的评估研究，以确保该战略可能的修改，并提出相应的后续建议。

43. 国务院办公厅发布《要素市场化配置综合改革试点总体方案》

1 月 6 日，国务院办公厅发布《要素市场化配置综合改革试点总体方案》，旨在以综合改革试点为牵引，支持具备条件的地区结合实际大胆改革探索，尊重基层首创精神，注重总结经验，及时规范提升，为全国提供可复制可推广的路径模式。

总体方案要求完善公共数据开放共享机制、建立健全数据流通交易规则、拓展规范化数据开发利用场景、加强数据安全保护。聚焦数据采集、开放、流通、使用、开发、保护等全生命周期的制度建设，推动部分领域数据采集标准化，分级分类、分步有序推动部分领域数据流通应用，探索“原始数据不出域、数据可

用不可见”的交易范式，实现数据使用“可控可计量”，推动完善数据分级分类安全保护制度，探索制定大数据分析和交易禁止清单。

44. 国务院发布《“十四五”数字经济发展规划》

1 月 12 日，国务院发布《“十四五”数字经济发展规划》，明确“十四五”时期推动数字经济健康发展的指导思想、基本原则、发展目标、重点任务和保障措施。规划部署了八项重点任务，包括充分发挥数据要素作用、大力推进产业数字化转型、健全完善数字经济治理体系、着力强化数字经济安全体系等。

数据要素方面，规划要求强化高质量数据要素供给、加快数据要素市场化流通、创新数据要素开发利用机制。支持市场主体依法合规开展数据采集，聚焦数据的标注、清洗、脱敏、脱密、聚合、分析等环节，提升数据资源处理能力，培育壮大数据服务产业。

数字经济安全方面，规划要求增强网络安全防护能力、提升数据安全保障水平、切实有效防范各类风险。提升网络安全应急处置能力，加强电信、金融、能源、交通运输、水利等重要行业领域关键信息基础设施网络安全防护能力，支持开展常态化安全风险评估，加强网络安全等级保护和密码应用安全性评估。健全完善数据跨境流动安全管理相关制度规范。

45. 国务院发布《“十四五”市场监管现代化规划》

1 月 27 日，国务院发布《“十四五”市场监管现代化规划》，旨在创新和完善市场监管，推进市场监管现代化。

规划要求引导平台经济有序竞争。推动完善平台企业数据收集使用管理、消费者权益保护等方面的法律规范。强化平台内部生态治理，督促平台企业规范规则设立、数据处理、算法制定等行为。健全事前事中事后监管制度，制定大型平台企业主体责任清单，建立合规报告和风险评估制度。

规划要求建立数据要素市场化流通标准和规则，保护数字经济领域各方主体权益。推动完善重点产业质量认证制度体系，加大网络安全认证制度推行力度，加快战略性新兴产业领域质量认证制度建设，大力推行高端品质认证和新型服务认证，加快研究和完善国家数据安全标准与认证认可体系。

46. 中国《网络安全审查办法》正式施行

2 月 15 日，国家互联网信息办公室等十三部门联合修订发布的《网络安全审查办法》正式施行。

办法将网络平台运营者开展数据处理活动影响或者可能影响国家安全等情形纳入网络安全审查范围，要求掌握超过 100 万用户个人信息的网络平台运营者赴国外上市必须申报网络安全审查。办法规定为了防范风险，当事人应当在审查期间按照网络安全审查要求采取预防和消减风险的措施。此外，办法对审查工作机制成员进行扩充，增加中国证券监督管理委员会作为国家网络安全审查工作机制成员。

47. 全国人大常委会 2022 年度立法工作计划

5 月 6 日，全国人大常委会发布《2022 年度立法工作计划》。工作计划提出，2022 年，继续审议的法律案包括突发事件应对法（修改）等 ；初次审议的法律案包括治安管理处罚法（修改）、金融稳定法、能源法等；预备审议项目包括修改反间谍法，制定电信法、网络犯罪防治法等。

工作计划要求，加强重点领域、新兴领域、涉外领域立法，统筹推进国内法治和涉外法治，着力解决法治领域突出问题，健全国家治理急需、满足人民日益增长的美好生活需要必备的法律制度，助力解决事关全局、事关长远、事关人民福祉的紧要问题。强化对国家重大发展战略的法治保障，积极推进国家安全、科技创新、公共卫生、生物安全、生态文明、防范风险等重要领域立法，加快数字经济、互联网金融、AI、大数据、云计算等领域立法步伐，加强民生领域立法，回应人民群众反映强烈的突出问题，填补法律制度薄弱点和空白区。

48. 党的二十大报告关于网络强国、数字经济与法治元素的内容

10 月 16 日，中国共产党第二十次全国代表大会在人民大会堂开幕。习近平总书记代表第十九届中央委员会向大会作报告，强调网络强国建设与数字经济发展，并部署推进法治中国建设。

（1）强调网络强国建设与数字经济发展

建设现代化产业体系，坚持把发展经济的着力点放在实体经济上，推进新

型工业化，加快建设制造强国、质量强国、航天强国、交通强国、网络强国、数字中国。我们确立和坚持马克思主义在意识形态领域指导地位的根本制度，社会主义核心价值观广泛传播，中华优秀传统文化得到创造性转化、创新性发展，文化事业日益繁荣，网络生态持续向好，意识形态领域形势发生全局性、根本性转变。我们要建设具有强大凝聚力和引领力的社会主义意识形态，牢牢掌握党对意识形态工作领导权，全面落实意识形态工作责任制，巩固壮大奋进新时代的主流思想舆论，加强全媒体传播体系建设，推动形成良好网络生态。提高公共安全治理水平，坚持安全第一、预防为主，完善公共安全体系，提高防灾减灾救灾和急难险重突发公共事件处置保障能力，加强个人信息保护。

推动战略性新兴产业融合集群发展，构建新一代信息技术、人工智能、生物技术、新能源、新材料、高端装备、绿色环保等一批新的增长引擎。加快发展物联网，建设高效顺畅的流通体系，降低物流成本。加快发展数字经济，促进数字经济和实体经济深度融合，打造具有国际竞争力的数字产业集群。

强化国家安全工作协调机制，完善国家安全法治体系、战略体系、政策体系、风险监测预警体系、国家应急管理体系，完善重点领域安全保障体系和重要专项协调指挥体系，强化经济、重大基础设施、金融、网络、数据、生物、资源、核、太空、海洋等安全保障体系建设。

（2）部署推进法治中国建设

报告用“坚持全面依法治国，推进法治中国建设”一个章节部署法治建设。报告指出，全面依法治国是国家治理的一场深刻革命，关系党执政兴国，关系人民幸福安康，关系党和国家长治久安。必须更好发挥法治固根本、稳预期、利长远的保障作用，在法治轨道上全面建设社会主义现代化国家。

报告强调，要坚持走中国特色社会主义法治道路，建设中国特色社会主义法治体系、建设社会主义法治国家，围绕保障和促进社会公平正义，坚持依法治国、依法执政、依法行政共同推进，坚持法治国家、法治政府、法治社会一体建设，全面推进科学立法、严格执法、公正司法、全民守法，全面推进国家各方面工作法治化。

完善以宪法为核心的中国特色社会主义法律体系。坚持依法治国首先要坚持依宪治国，坚持依法执政首先坚持依宪执政，坚持宪法确定的中国共产党领导

地位不动摇，坚持宪法确定的人民民主专政的国体和人民代表大会制度的整体不动摇。加强宪法实施和监督，健全保证宪法全面实施的制度体系，更好发挥宪法在治国理政中的重要作用，维护宪法权威。加强重点领域、新兴领域、涉外领域立法，统筹推进国内法治和涉外法治，以良法促进发展、保障善治。推进科学立法、民主立法、依法立法，统筹立改废释纂，增强立法系统性、整体性、协同性、时效性。完善和加强备案审查制度。坚持科学决策、民主决策、依法决策，全面落实重大决策程序制度。

扎实推进依法行政。法治政府建设是全面依法治国的重要任务和主体工程。转变政府职能，优化政府职责体系和组织结构，推进机构、职能、权限、程序、责任法定化，提高行政效率和公信力。深化事业单位改革。深化行政执法体制改革，全面推进严格规范公正文明执法，加大关系群众切身利益的重点领域执法力度，完善行政执法程序，健全行政裁量基准。强化行政执法监督机制和能力建设，严格落实行政执法责任制和责任追究制度。完善基层综合执法体制机制。

严格公正司法。公正司法是维护社会公平正义的最后一道防线。深化司法体制综合配套改革，全面准确落实司法责任制，加快建设公正高效权威的社会主义司法制度，努力让人民群众在每一个司法案件中感受到公平正义。规范司法权力运行，健全公安机关、检察机关、审判机关、司法行政机关各司其职、相互配合、相互制约的体制机制。强化对司法活动的制约监督，促进司法公正。加强检察机关法律监督工作。完善公益诉讼制度。

加快建设法治社会。法治社会是构筑法治国家的基础。弘扬社会主义法治精神，传承中华优秀传统法律文化，引导全体人民做社会主义法治的忠实崇尚者、自觉遵守者、坚定捍卫者。建设覆盖城乡的现代公共法律服务体系，深入开展法治宣传教育，增强全民法治观念。推进多层次多领域依法治理，提升社会治理法治化水平。发挥领导干部示范带头作用，努力使尊法学法守法用法在全社会蔚然成风。

49. 国务院办公厅发布《国务院 2022 年度立法工作计划》

7 月 14 日，国务院办公厅发布《国务院 2022 年度立法工作计划》。计划指出，2022 年，提请全国人大常委会审议治安管理处罚法修订草案，预备提请全

国人大常委会审议电信法草案、人民警察法修订草案、保守国家秘密法修订草案。拟制定、修订的行政法规包括未成年人网络保护条例（网信办起草）、网络数据安全管理条例（网信办组织起草）、商用密码管理条例（修订）（密码局起草）。

计划要求，着力提升立法的科学性和针对性。起草、审查法律法规草案时，同一或相近领域有关法律法规应相互衔接，避免出现法律规定之间不一致、不协调、不适应问题。统筹推进国内法治和涉外法治，加强涉外领域立法，补齐涉外法律制度短板，加快我国法域外适用的法律体系建设，坚决维护国家主权、安全和发展利益。健全完善立法风险防范机制。立法工作事关国家安全、政治安全和社会稳定，必须贯彻落实总体国家安全观，坚持底线思维、增强忧患意识，加强立法战略研究，对立法时机和各环节工作进行综合考虑和评估论证，把风险评估贯穿立法全过程，着力防范各种重大风险隐患，为党的二十大胜利召开创造安全稳定的政治社会环境。

（二）网络安全管理

1. 美国 SEC 发布拟议网络安全规则《投资顾问、注册投资公司和业务发展公司的网络安全风险管理》

2 月 9 日，美国证券委员会（SEC）发布拟议网络安全规则《投资顾问、注册投资公司和业务发展公司的网络安全风险管理》（Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies），公开征求意见。

规则主要涉及四方面，分别是网络安全政策和程序、网络安全披露、网络安全事件监管报告、网络安全事件记录。规则要求投资顾问、注册投资公司和业务发展公司在其宣传册和注册报表中公开披露过去两个财政年度发生的网络安全风险和重大网络安全事件。规则要求在发现重大网络安全事件后 48 小时内通知 SEC，还要求制定广泛的政策和程序，包括书面信息安全计划和事件响应计划，以应对网络安全威胁。

2. 美国NIST发布《勒索软件风险管理：网络安全框架简介》

2月23日，美国国家标准与技术研究院（NIST）发布NISTIR 8374《勒索软件风险管理：网络安全框架》（Ransomware Risk Management：A Cybersecurity Framework Profile），旨在支持识别、检测、响应勒索攻击，保护网络与信息系统免受勒索攻击影响，并从勒索攻击事件中快速恢复。

该文件可作为管理勒索攻击事件风险的指南，其中包括帮助衡量组织应对勒索软件威胁和应对事件潜在后果的准备程度，并围绕识别、保护、检测、响应和恢复五个阶段细化勒索攻击风险管理的要求。

3. 美国NSA发布《网络基础设施安全指南》

3月1日，美国国家安全局（NSA）发布《网络基础设施安全指南》（Network Infrastructure Security Guidance），向所有组织提供保护IT网络基础设施、应对网络攻击的最新建议。指南侧重防止现有网络常见漏洞和弱点的设计和配置，旨在指导网络架构师和管理员建立网络最佳实践。

指南介绍了总体网络安全和保护单个网络设备的最佳做法，并指导管理员阻止对手利用其网络。指南是通用的，可以应用于多种类型的网络设备。指南提供的建议涵盖网络设计、设备密码和密码管理、远程登录、安全更新、密钥交换算法等。概括起来，主要包括以下建议：（1）网络体系架构与设计采用多层防御；（2）定期进行安全维护；（3）采用认证、授权和审计来实施访问控制；（4）创建具有复杂口令的唯一本地账户；（5）实施远程记录和监控；（6）实施远程管理和网络业务；（7）配置网络应用路由器以对抗恶意滥用；（8）正确配置接口端口。

4. 美国CISA发布《网络事件信息共享指南》

4月7日，美国网络安全和基础设施安全局（CISA）发布《网络事件信息共享指南》（Guidance on Sharing Cyber Incident Information）。

指南为CISA及其利益相关者提供了关于共享什么、谁应该共享以及如何共享有关异常网络事件或活动信息的明确指导。其中，共享的主体包括关键基础设施所有者和运营商以及联邦、州、地方、地区和部落政府合作伙伴。应当共享的

信息包括：（1）针对系统的未经授权访问；（2）持续时间超过 12 小时的 DOS 攻击；（3）系统上的恶意代码，包括已知的变体；（4）针对系统上的服务进行的有针对性的重复扫描；（5）反复尝试未经授权访问的计算机信息系统；（6）与网络钓鱼攻击相关的电子邮件或移动消息；（7）针对关键基础设施的勒索软件，包括变体和勒索详细信息。

CISA 将使用共享的信息来响应攻击者对美国网络和关键基础设施部门的攻击。这些信息使 CISA 能够快速部署资源并向遭受攻击的受害者提供帮助，分析跨部门的信息共享报告以发现网络威胁趋势，并快速与网络防御者共享该信息以向其他潜在受害者发布预警信息。

5. 美国《银行机构及其银行服务提供者的计算机安全事件报告要求》全面生效

5 月 1 日，美国联邦存款保险公司（FDIC）、联邦储备系统理事会（Board）和货币审计长办公室（OCC）联合发布的《银行机构及其银行服务提供者的计算机安全事件报告要求》（Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers）规则全面生效。

规则要求，当发生的计算机安全事件达到“应报告事件”级别，受 FDIC 监管的银行机构应在不迟于 36 小时内尽快将事件报告至 FDIC。银行机构可以通过电子邮件、电话或其他 FDIC 认定的类似方式向适格的 FDIC 监管办公室或者 FDIC 指定的联络点报告。

规则将“计算机安全事件”定义为对信息系统或系统处理、存储或传输的信息的保密性、完整性或可用性造成实际损害的事件。“应报告事件”包括已经或可能实质性干扰、损害：（1）银行机构在正常业务过程中开展银行业务、活动或流程，或向其重要客户群体提供银行产品和服务能力的计算机安全事件；（2）银行机构业务线，将导致银行收入、利润或特许经营价值重大损失的计算机安全事件；（3）银行机构相关服务、职能的运转，将对美国金融稳定构成威胁的计算机安全事件。

当银行服务提供商确定其遭遇计算机安全事件，并已经或很有可能造成提供的服务实质性中断或被削弱四小时及以上时间时，应尽快通知每个受影响的客

户银行机构的至少一个指定联络点。如果银行机构以前没有提供指定联络点，则必须通知银行机构的首席执行官和首席信息官或两名承担同等责任的个人。

6. 美国正式通过《2021 年州和地方政府网络安全法》

6 月 21 日，美国正式通过 S2520《2021 年州和地方政府网络安全法》（State and Local Government Cybersecurity Act of 2021），旨在修订《国土安全法》，要求国土安全部通过强化国家通信整合中心协调职责，加强州、地方、部落和地区（SLTT）政府实体与公司、协会和公众在网络安全方面的合作。

本法明确，国家通信整合中心的协调职责包括：（1）在可行范围内，酌情与联邦和非联邦实体（例如跨州信息共享和分析中心）进行协调，向 SLTT 实体提供运营和技术网络安全培训，以解决与网络安全风险和事件相关的网络威胁指标、防御措施、网络安全风险、漏洞、事件响应和管理；（2）为了提升网络威胁态势感知能力并帮助预防网络安全事件，协助 SLTT 实体与联邦政府以及 SLTT 实体之间实时共享网络威胁指标、防御措施、网络安全风险信息、事件信息，以及向 SLTT 实体提供包含可能影响实体或其居民的特定事件和恶意软件信息的通知；（3）通过易于访问的平台和其他方式向 SLTT 实体提供并定期更新关于工具的信息、有关产品的信息、资源、政策、指南、控制措施，以及与信息安全相关的其他网络安全标准和最佳实践程序；（4）与 SLTT 实体的高级官员（包括首席信息官和高级选举官员）合作，并通过全国协会协调 SLTT 实体有效实施与信息相关的工具、产品、资源、政策、指南、控制和程序，以及保护 SLTT 实体的信息系统（包括选举系统）的安全性；（5）向 SLTT 实体提供运营和技术协助，以实施有关信息安全的工具、产品、资源、政策、指南、控制和程序；（6）协助 SLTT 实体制定政策和程序，以根据信息技术行业的国际和国家标准来协调漏洞披露；（7）通过与联邦机构和非联邦实体的接触来促进网络安全教育和意识的提升。

7. 美国国家公路交通安全管理局发布《车辆网络安全最佳实践指南》

9 月 9 日，美国国家公路交通安全管理局（NHTSA）公布《车辆网络安全最佳实践指南》（Cybersecurity Best Practices for the Safety of Modern

Vehicles），对其 2016 年版本进行更新。该文件描述了 NHTSA 对改善汽车行业网络安全的指导意见。

该文件利用了 NHTSA 的研究成果、行业自愿标准以及过去几年机动车网络安全研究的经验教训，并根据 2021 年发布在《联邦公报》的对草案的公众意见进行了更新。虽然该文件不具有约束力，但包含了重要的最佳实践，将影响行业发展。NHTSA 会定期评估网络安全风险以及新出现的最佳实践，并将随着机动车、机动车设备及其网络安全发展，考虑对这些最佳实践的未来更新。

8. 美国 CISA 发布《2023 年至 2025 年战略计划》

9 月 12 日，美国网络安全和基础设施安全局（CISA）发布《2023 年至 2025 年战略计划》(CISA STRATEGIC PLAN 2023-2025)。该计划与国土安全部 2020-2024 财年战略规划保持一致，是 CISA 自 2018 年成立以来发布的首个综合性战略规划，为未来 3 年 CISA 工作指明了方向。

该计划共提出四个战略目标：（1）加强关注网络空间的防御和弹性。增加联邦系统抵抗网络攻击能力、增强 CISA 主动监测能力、增加重要网络安全漏洞的公开透明度与修复能力、实现技术生态的“默认安全(security-by-default)”；（2）降低网络空间攻击风险并提高恢复能力。增强网络风险可见性、风险分析能力、安全和风险应对指导、基础设施和网络安全和韧性、响应威胁和应急事件的能力，支持选举基础设施的风险管理活动；（3）加强政府与私营部门之间的“全国业务合作和信息共享”。优化合作活动规划、加强 CISA 总部与分部融合等；（4）打破组织孤岛，在内部统一机构，提高服务价值。优化 CISA 的资金管理、业务流程；培养并加强 CISA 的高级人才队伍。

9. 美国 CISA 发布约束性操作指令《提高联邦网络上的资产可见性和漏洞检测》

10 月 3 日，美国网络安全和基础设施安全局（CISA）发布约束性操作指令《提高联邦网络上的资产可见性和漏洞检测》(IMPROVING ASSET VISIBILITY AND VULNERABILITY DETECTION ON FEDERAL NETWORKS），以指导联邦民事行政部门（FECB）能更好地解释其网络内容。本指令对联邦行政机构、部门而言是强制性指令，但不适用于法律规定的“国家安全系统”以及国防部或情报部门运营的特

别系统。

CISA 认为对于任何组织机构而言有效管理网络安全风险的基本前提是持续且全面的资产可见性，因此本指令关注两个核心行为：资产发现（asset discovery）和漏洞检测（vulnerability enumeration）。资产发现是可见性的基础，组织机构可以利用资产发现识别其网络中的可寻址 IP 资产，并找到与其关联的 IP 地址（主机）。漏洞检测则负责发现并报告这些资产中的可疑漏洞，通过识别主机属性（比如操作系统、开放端口、应用等），将其与已知漏洞信息匹配来验证资产是否符合安全政策的要求。

根据本指令的规定，在 2023 年 4 月 3 日之前， FCEB 应当针对其联邦信息系统采取以下措施：（1）每 7 天执行一次至少覆盖整个机构 IPv4 空间的自动资产发现；（2）每 14 天针对已发现资产进行漏洞检测；（3）完成发现后 72 小时内自动将漏洞检测结果汇总至持续诊断与缓解系统（CDM）；（4）在收到 CISA 要求后的 72 小时内启动资产发现和漏洞检测程序，并在收到要求后的 7 日内向 CISA 提交可用结果。为使 CISA 自动监测机构的扫描性能，指令规定在 CISA 发布性能数据漏洞检测要求后的 6 个月内，FCEB 应当收集并向 CDM 报告有关数据。2023 年 4 月 3 日前，机构和 CISA 将更新 CDM 配置使得 CISA 分析师能访问目标级漏洞检测数据。本指令颁布后的 6 个月、12 个月、18 个月，FCEB 机构应当分别向 CISA 提交进度报告，内容包括实行本指令过程中的问题和障碍以及预计完成时间，或者在 CDM 项目审查过程中与 CISA 合作。

10. 欧盟《数字市场法》生效

11 月 1 日，欧盟《数字市场法》（Digital Markets Act，简称 DMA）生效。DMA 针对的是大型在线平台，即所谓的“守门人”——它们控制着核心平台服务，如市场、应用商店、在线搜索引擎、社交网络等。

认定为“守门人”需要符合以下条件：（1）对市场产生重大影响。即在过去三个财政年度的每个财政年度中，其在欧盟的年营业额达到或超过 75 亿欧元，或其平均市值或同等公允市场价值至少达到上一财年 750 亿欧元，并在至少三个欧盟成员国提供相同的核心平台服务；（2）提供“核心平台服务”，作为业务用户接触客户和其他最终用户的重要门户。即在上一个财政年度至少有 4500 万

月活跃最终用户和至少 1 万名年活跃业务用户。核心平台服务包括：在线平台类服务、搜索引擎、社交网络服务、视频共享平台服务、NI-IC 服务（如即时语音、文本、图像和文件消息）、操作系统等云计算服务以及在线广告服务；（3）目前或将来具有持久的地位。过去三个财政年度都达到上述用户阈值。满足这些要求的“守门人”需要在达到上述门槛后的 2 个月内告知欧盟委员会，欧盟委员会将在收到此信息后的 45 天内指定他们为“守门人”。

DMA 规定“守门人”需要履行的一系列义务，旨在防止“守门人”对企业和消费者施加不公平的条件。DMA 规定，“守门人”不得在搜索结果中对自己的产品和服务进行更有利排名，不得限制用户在不同应用程序和服务之间切换，应为最终用户提供对数据的实时访问和有效的数据可移植性服务等。法律责任方面，（1）如果达到“守门人”门槛而未能按照 DMA 要求告知欧盟委员会，可能会被处以其上一财政年度全球总营业额 1%的罚款；（2）如果不遵守 DMA 的关键义务，可以处以上一财政年度全球总营业额 10%的罚款，或者在屡次不遵守的情况下处以最高 20%的罚款；（3）在“系统性不遵守”义务的情况下，可以采取额外补救措施，包括结构性补救措施，例如责成“守门人”出售全部或部分业务。DMA 的执行由欧盟委员会负责。成员国可随时要求欧盟委员会展开市场调查，以认定新的“守门人”。

平台须在 DMA 生效之日起六个月，即 2023 年 5 月 2 日起，至 2023 年 7 月 3 日之间向委员会申报“守门人”认定。委员会收到完整申报通知后，将在 45 个工作日内进行认定。认定为“守门人”的，平台将有六个月的时间落实 DMA 要求，即 2024 年 3 月 6 日之前。

11. 英国政府发布《政府网络安全战略：2022 年至 2030 年》

1 月 25 日，英国政府正式发布《政府网络安全战略：2022 年至 2030 年》（Government Cyber Security Strategy：2022 to 2030），系英国首份针对政府的网络安全战略。

战略愿景是确保核心政府职能能够抵御网络攻击，加强英国作为一个主权国家，和作为民主和负责任的网络大国的权威。为实现这一愿景，战略追求一个中心目标——到 2025 年，政府关键职能显著加强以抵御网络攻击，2030 年前，

整个公共部门的所有政府组织都能抵御已知漏洞和攻击方法。

战略共分九章，从背景、方法、网络安全风险管理、网络攻击防御、网络安全事件检测、网络安全事件影响控制、网络安全知识技能及文化培养、成果评估、战略执行等方面进行全面描述。例如在内阁办公室建立新的政府协调中心（GCCC），在公共部门间更好地进行网络安全工作协调。在金融部门网络合作中心（FSCCC）等私营模式成功运行的基础上，GCCC 将更快速地识别、调查和协调政府对公共网络系统攻击的反应，以确保信息共享更及时，实现“统一防御”（Defend As One）。此外，GCCC 还将加强漏洞管理，建立跨政府部门漏洞报告服务体系，以方便安全研究人员及公共部门人员更加方便地汇报公共数字服务系统中存在的漏洞。

12. 英国《监控摄像头指导守则》生效

2 月 11 日，英国生物识别和监控摄像专员公布更新后的《监控摄像头指导守则》（Surveillance Camera Code of Practice），为地方当局和警方适当使用监控摄像头系统提供指导。

守则要求系统运营商遵循以下 12 条指导原则：（1）监控摄像头系统必须始终用于特定目的。监控摄像头系统只能在公共场所用于特定目的，例如保障国家安全、公共安全、国家经济福祉、预防动乱或犯罪、保护健康、道德或保护他人的权利和自由；（2）监控摄像头系统的使用必须考虑到对个人隐私的影响，并定期进行审查，以确保使用的合理性；（3）监控摄像头系统的使用（包括公开的获取信息和投诉联络点）应尽可能透明；（4）监控摄像头系统活动（包括收集、持有和使用图像和信息）应有明确的责任和义务；（5）在使用监控摄像头系统前，必须制定明确的规则、政策和程序，并且必须将这些信息传达给需要遵守的人；（6）存储的图像和信息不应超过监控摄像头系统声明目的中严格要求的范围；（7）对访问保留的图像和信息的行为设限，必须明确规定获得访问权限的人群和访问目的；（8）监控摄像头系统操作主体应考虑与系统及其目的操作、技术和能力相关的标准；（9）监控摄像头系统的图像和信息应采取适当的安全措施，以防止未经授权的访问和使用；（10）监控摄像头系统的使用应建立有效的审查和审计机制，以确保在实践中遵守法律要求、政策和标准，并定期

发布报告；（11）在支持公共安全和执法方面，监控摄像头系统应使用最有效的方式来处理具有证据价值的图像和信息；（12）用于支持监控摄像头系统的信息，如果是出于与其他数据库相比较的目的，如车辆信息等，应准确并保持最新状态。

13. 英国发布首份《建筑业网络安全指南》

2 月 23 日，英国国家网络安全中心（NCSC）与英国特许建筑学会（CIOB）联合发布针对英国建筑业的首份网络安全指南《建筑企业网络安全指南》（Cyber security for construction businesses），帮助中小型建筑企业抵御在线威胁。

指南为中小型建筑企业从设计到移交的每个建设阶段提供了实用建议，并列出行业面临的常见网络威胁，包括鱼叉式网络钓鱼、勒索软件和供应链攻击。指南分为两部分：第一部分旨在帮助建筑企业和管理人员了解网络安全为何如此重要；第二部分旨在为建筑企业内负责 IT 设备和服务的员工提供建议。指南概述了提高网络弹性的七个步骤，包括创建强密码、备份设备、准备和响应事件等。

14. 英国政府发布《2022 年民用核能网络安全战略》

5 月 13 日，英国政府发布《2022 年民用核能网络安全战略》（Civil nuclear cyber security strategy 2022），为英国民用核部门制定未来五年的安全路线。该战略由英国民用核组织、核监管办公室和国家网络安全中心共同制定。

战略概述了 2026 年之前要实现的四个关键目标：（1）优先考虑网络安全，将网络安全作为整体风险管理方法的一部分；（2）主动缓解行业及供应链风险；（3）通过更好地准备和更快、更协作地响应事件来增强弹性，最大限度地减少影响和恢复时间；（4）加强合作以提高网络成熟度、培养技能并促进安全至上的文化。为了实现这些目标，战略提出各种承诺，包括在 IT 和 OT 系统中广泛开展网络对抗模拟评估和其他威胁测试，与国家网络安全中心开展全行业网络事件现场响应演习、为民用核供应链制定网络安全基线标准、广泛的跨行业合作、与先进核技术开发者就网络安全展开合作。

15. 英国国家网络安全中心发布《建筑业合资企业：信息安全最佳实践指南》

8 月 23 日，英国国家网络安全中心（NCSC）和商业、能源和工业战略部（BEIS）

以及国家基础设施保护中心（CPNI）联合发布《建筑业合资企业：信息安全最佳实践指南》（Joint Ventures in the Construction Sector: Information Security Best Practice Guidance），旨在帮助建筑合资企业安全处理与项目创建、存储和共享有关的敏感数据，帮助建筑企业保护敏感数据免受攻击。

指南提供了5个风险管理方法，分别是：（1）企业内建立信息安全治理和问责制；（2）确定负责评估特定信息安全风险和制定共享信息安全战略的员工；（3）了解合资企业特定的信息安全风险和监管要求；（4）制定并商定共享信息安全战略；（5）设计和实施信息安全管理计划。

16. 英国《电子通信（安全措施）条例》草案提交议会：将电信提供商分为三级

10月1日,英国《2022年电信(安全措施)条例》(Electronic Communications (Security Measures) Regulations 2022）正式生效。

条例明确公共电信网络提供者与公共电信服务提供者应当履行的具体安全义务，要点包括：（1）数据保护。应采用适当、相称的技术手段，保护与网络和服务操作相关的数据存储免受恶意侵害,并保护用于管理这些网络和服务的软件和设备；（2）监测分析。应采用适当、相称的措施，强化对网络和服务的接入监测，降低安全损害风险，同时必须确保监控和分析工具不位于中国、伊朗、朝鲜和俄罗斯；（3）供应链安全。应制定应急计划，防止第三方供应中断；采用适当、相称的合同措施，要求第三方供应商识别、披露并减少由供应关系引发的安全风险。

此外，条例还引入防止未经授权访问、强化安全漏洞补救恢复、保障网络架构设计与开发安全、数据安全事件披露报告等义务。英国通信管理局（ofcom）负责监督检查公共电信网络与服务提供者的义务落实情况,不遵守上述义务规定将带来高达10%营业额的罚款，或在继续违规情况下每日10万英镑的罚款。

17. 印度发布《关于<2000年信息技术法>第70B条第（6）款，可信网络的信息安全实践、程序、预防、响应和网络安全事件报告指令》

4月28日，印度计算机应急响应小组（CERT-In）发布《关于<2000年信息技术法>第70B条第（6）款，可信网络的信息安全实践、程序、预防、响应和网

络安全事件报告指令》（Directions under sub-section （6） of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet）。

指令要求，互联网服务提供商、中介机构、数据中心、法人团体和政府机构应当在发现或被告知发生网络安全事件后 6 小时内向 CERT-In 报告。指令明确 20 类应当报告的网络安全事件类型，包括关键网络/系统的定向扫描/探测、对关键系统/信息造成威胁、未经授权访问 IT 系统/数据、拒绝服务（DoS）和分布式拒绝服务（DDoS）攻击、数据泄露（Data Leak）等。

为了进行适当的协调，上述所有实体都需要连接到国家信息中心（NIC）或国家物理实验室（NPL）的 NTP 服务器，并同步系统时钟。实体的所有 ICT 系统日志必须在印度管辖范围内安全保留 180 天，并应与安全事件报告一起或在机构要求时提供给 CERT-In。

指令还对部分特殊主体的数据留存义务提出要求。包括（1）数据中心、虚拟专用服务器（VPS）提供商、云服务提供商、虚拟专用网络（VPN）提供商，应登记下列准确信息，这些信息必须在用户注销或撤销登记(视情况而定)后继续保存 5 年或更长时间(法律规定的期限)：订阅户/客户的有效名称、租用服务的期限、分配给用户的 IPs、注册或登录的邮箱地址/IP 地址/使用服务的时间戳、租用服务的目的、经验证的地址和联系电话、订阅户/客户租用服务的所有权模式；（2）虚拟资产服务提供商、虚拟资产交易提供商和托管钱包提供商应维护“了解你的客户”中获取的所有信息和金融交易记录。其中，交易记录应以准确的方式保存，包括但不限于相关方识别信息、IP 地址、时间戳、时区、交易 ID、公钥（或等效标识符）、涉及的地址或账户（或等效标识符）、交易性质、交易日期、交易金额。

5 月 18 日，CERT-In 发布常见问题解答，重申指令要求。常见问题解答由 44 个问题组成，主要包括三个部分，即基本术语和说明范围、2000 年 IT 法案第 70B 条第(6)款下的指示、向 CERT-In 报告的网络安全事件类型说明。文件指出，那些不遵守规则、未按规定提供信息的人将被处以最高一年的监禁、最高 100,000 卢比的罚款，或两者兼施。

6 月 27 日，CERT-In 发布通知，确认延迟执行指令。CERT-In 指出，指令本应在发布之日起 60 天后生效，但指令定义的微型、小型和中型企业（MSMEs）将延期至 2022 年 9 月 25 日适用该指令。CERT-In 进一步表示，针对数据中心、云服务提供商、VPS 提供商和 VPN 服务提供商的留存注册客户和订户信息的强制要求，也延长至 2022 年 9 月 25 日生效。

18. 加拿大安大略省发布勒索软件应对指南

10 月 13 日，加拿大安大略省信息和隐私专员发布《如何应对勒索软件》指南（How to Protect Against Ransomware），将勒索软件称为“安大略省组织面临的最大威胁”。指南讨论勒索攻击的影响、防范勒索软件的义务、勒索攻击阶段、缓解威胁和保护组织的方法以及应如何应对网络安全事件。

加拿大网络安全中心报告称，2021 年共发生 235 起影响加拿大组织的勒索攻击，由于并非所有事件都进行了报告，因此实际发生的事件数量可能比这一数字高得多。

19. 澳大利亚 ACSC 发布《澳大利亚政府网络事件管理安排》

10 月 14 日，澳大利亚网络安全中心（ACSC）发布《澳大利亚政府网络事件管理安排》（CIMA）。CIMA 不是实操层面的事件管理规定，具体的实施计划需要由政府共同制定。CIMA 颁布后也并不影响现有的国家危机管理安排，如果国家网络事件达到危机水平，CIMA 将服从各机构的危机管理安排，比如《澳大利亚政府危机管理框架》。

国家网络事件是指对多个澳大利亚辖区产生重要影响或可能产生重大影响，或者要求辖区间作出协同回应的网络事件。一旦出现符合上述要求的情况，ACSC 将宣布出现国家网络事件，启动 CIMA 程序。一般而言国家网络事件的认定要求低于启动国家危机安排所需门槛，但是在某些情形下国家网络事件可能上升为一场危机，比如其造成对基础设施的持续性扰乱、严重的经济损害、威胁国家安全或者人民生命健康。

CIMA 规定分为国家网络事件期间的协调行动以及国家网络事件的降级安排。在宣布出现国家网络事件后，国家网络安全委员会（NCSC）作为澳大利亚政

府最高级别的网络安全协调机构，负责为政府网络安全政策和运行能力提供战略监督和协作机制。当网络事件影响力降低后，ACSC 经与 NCSC 协商可宣布确认国家网络事件降级。CIMA 具体规定了各方主体在应对国家网络事件时的角色和职责：州和地方政府就保护其辖区范围内的环境和生命财产安全负首要责任，当国家网络事件出现后，应当通过 NCSC 支持辖区内的事件协调安排，并向 ACSC 提供有关网络风险、漏洞、解决措施的信息；联邦政府的内政部、ACSC 以及 ACSC 的联合网络安全中心（JCSCs）负责协调制定和实施国家网络安全政策；企业和社会等私主体在国家网络事件期间仍应履行保护资产（包括储存在其系统中的信息）的义务。

20. 最高人民法院发布《人民法院在线运行规则》

1 月 26 日，最高人民法院发布《人民法院在线运行规则》。规则共五章四十五条，涉及系统建设、应用方式、运行管理等内容。

规则要求各级人民法院应当建设安全保障系统，为人民法院在线运行提供网络和信息安全保障。安全保障系统应当为各类信息基础设施、应用系统和数据资源提供主机安全、身份认证、访问控制、分类分级、密码加密、防火墙、安全审计和安全管理等安全服务。各级人民法院应当开展与等级保护标准相符合的信息系统安全保障建设和测评以及密码应用安全评估；应当确保智慧法院信息系统相关数据全生命周期安全，制定数据分类分级保护、数据安全应急处理和数据安全审查等制度；应当制定应急计划，及时有效处理人民法院在线运行过程中出现的停电、断线、技术故障、遭受网络攻击、数据安全漏洞等突发事件。

21. 国家发展和改革委员会发布《电力可靠性管理办法（暂行）》

4 月 16 日，国家发展和改革委员会发布《电力可靠性管理办法（暂行）》。办法共十一章六十四条，其中第七章为网络安全。

办法规定，电力企业应当落实网络安全保护责任，健全网络安全组织体系，设立专门的网络安全管理及监督机构，加快各级网络安全专业人员配备；落实网络安全等级保护、关键信息基础设施安全保护和数据安全制度，加强网络安全审查、容灾备份、监测审计、态势感知、纵深防御、信任体系建设、供应链管理等

工作；开展网络安全监测、风险评估和隐患排查治理，提高网络安全监测分析与应急处置能力。

22. 国家药监局发布《药品监管网络安全与信息化建设“十四五”规划》

4 月 24 日，国家药监局发布《药品监管网络安全与信息化建设“十四五”规划》。规划提出五项重点任务，包括推进监管数据融合与驱动、筑牢药品智慧监管数字底座、夯实网络安全综合保障能力等。

网络安全方面，规划要求健全网络安全管理制度，建立网络安全责任体系，落实网络安全管理主体责任，升级信息系统安全建设、安全测评、容灾备份等保障措施，完善电子政务内网和外网管理，形成各方协同配合的网络安全防范、监测、通报、响应和处置机制，构建涵盖物理、网络、数据、系统等全方位、多层次的安全防护体系。加强对网络视频会议、电视电话会议等服务保障能力。

23. 中国证监会发布《证券期货业网络安全管理办法（征求意见稿）》

4 月 29 日，中国证监会发布《证券期货业网络安全管理办法(征求意见稿)》。征求意见稿共八章六十六条，对证券期货业网络安全监督管理体系、网络安全运行、数据安全统筹管理、网络安全应急处置、关键信息基础设施网络安全、网络安全促进与发展、监督管理与法律责任等方面提出要求。

征求意见稿规定，核心机构和经营机构应当依法履行网络安全保护义务，对本机构网络安全负责，相关责任不因其他机构提供产品或者服务进行转移或者减轻。信息技术服务机构应当勤勉尽责，对提供产品或者服务的合规性、安全性承担责任。

24. 国务院发布《关于加强数字政府建设的指导意见》

6 月 6 日，国务院发布《关于加强数字政府建设的指导意见》。

指导意见明确数字政府建设的七方面重点任务，具体包括构建协同高效的政府数字化履职能力体系、构建数字政府全方位安全保障体系、构建科学规范的数字政府建设制度规则体系、构建开放共享的数据资源体系、以数字政府建设全面引领驱动数字化发展等方面。安全方面，指导意见要求强化安全管理责任，落

实安全制度要求，提升安全保障能力，提高自主可控水平，筑牢数字政府建设安全防线。

25. 国家能源局发布《电力行业网络安全管理办法（修订征求意见稿）》《电力行业网络安全等级保护管理办法（修订征求意见稿）》

6 月 14 日，国家能源局发布《电力行业网络安全管理办法（修订征求意见稿）》《电力行业网络安全等级保护管理办法（修订征求意见稿）》。

《电力行业网络安全管理办法（修订征求意见稿）》共五章三十五条，规定监管职责、电力企业职责等内容。关键信息基础设施安全保护方面，修订征求意见稿规定，电力行业关键信息基础设施运营者的主要负责人对关键信息基础设施安全保护负总责，要明确一名领导班子成员（非公有制经济组织运营者明确一名核心经营管理团队成员）作为首席网络安全官，专职管理或分管关键信息基础设施安全保护工作。电力行业关键信息基础设施运营单位应当于每年 11 月 1 日前，将当年关键信息基础设施安全保护的专项总结报送国家能源局及其派出机构、地方能源主管部门。

《电力行业网络安全等级保护管理办法（修订征求意见稿）》共六章二十八条，涉及等级划分与保护、等级保护的实施与管理等内容。修订征求意见稿规定，第二级网络每两年应进行一次等级保护测评，第三级及以上网络每年应进行一次等级保护测评。国家能源局及其派出机构结合关键信息基础设施网络安全检查，定期组织对运营有第三级及以上网络的电力企业开展抽查。

26. 国家卫健委等三部门发布《医疗卫生机构网络安全管理办法》

8 月 29 日，国家卫生健康委、国家中医药局、国家疾控局联合发布《医疗卫生机构网络安全管理办法》。办法共六章三十四条，涉及网络安全管理、数据安全管理、监督管理、管理保障等内容。

网络安全管理方面，办法规定，第二级的网络应委托等级保护测评机构定期开展网络安全等级测评，其中涉及 10 万人以上个人信息的网络应至少三年开展一次网络安全等级测评，其他的网络至少五年开展一次网络安全等级测评。

数据安全管理方面，办法规定，各医疗卫生机构应按照有关法规标准，选

择合适的数据存储架构和介质在境内存储，并采取备份、加密等措施加强数据的存储安全。涉及到云上存储数据时，应当评估可能带来的安全风险。数据存储周期不应超出数据使用规则确定的保存期限。

27. 国家互联网信息办公室发布《关于修改〈中华人民共和国网络安全法〉的决定（征求意见稿）》

9 月 14 日，国家互联网信息办公室就《关于修改〈中华人民共和国网络安全法〉的决定（征求意见稿）》公开征求意见，旨在做好《网络安全法》与新实施的法律之间衔接协调，完善法律责任制度，进一步保障网络安全。

征求意见稿具体作出四方面修改：一是完善违反网络运行安全一般规定的法律责任制度。结合当前网络运行安全法律制度实施情况，拟调整违反网络运行安全保护义务或者导致危害网络运行安全等后果的行为的行政处罚种类和幅度；二是修改关键信息基础设施安全保护的法律责任制度。关键信息基础设施是经济社会运行的神经中枢，为强化关键信息基础设施安全保护责任，进一步完善关键信息基础设施运营者有关违法行为行政处罚规定；三是调整网络信息安全法律责任制度。适应网络信息安全工作实际，对违反网络信息安全义务行为的法律责任进行整合，调整了行政处罚幅度和从业禁止措施，新增对法律、行政法规没有规定的有关违法行为的法律责任规定；四是修改个人信息保护法律责任制度。鉴于《个人信息保护法》规定了全面的个人信息保护法律责任制度，拟将原有关个人信息保护的法律责任修改为转致性规定。

28. 工信部印发《网络产品安全漏洞收集平台备案管理办法》

10 月 28 日，工信部印发《网络产品安全漏洞收集平台备案管理办法》。办法共十条，适用于网络产品安全漏洞收集平台，即相关组织或者个人设立的收集非自身网络产品安全漏洞的公共互联网平台，仅用于修补自身网络产品、网络和系统安全漏洞用途的除外。漏洞收集平台备案通过工信部网络安全威胁和漏洞信息共享平台开展，采用网上备案方式进行。

办法规定，拟设立漏洞收集平台的组织或个人，应当通过如实填报网络产品安全漏洞收集平台备案登记信息，主要包括：（一）漏洞收集平台的名称、首页

网址和互联网信息服务（ICP）许可或备案号，用于发布漏洞信息的相关网址、社交软件公众号等互联网发布渠道；（二）主办单位或主办个人的名称或姓名、证件号码，以及漏洞收集平台主要负责人和联系人的姓名、联系方式；（三）漏洞收集的范围和方式、漏洞验证评估规则、通知相关责任主体修补漏洞规则、漏洞发布规则、注册用户的身份核实规则及分类分级管理规则等；（四）通过工业和信息化部通信网络安全防护管理系统，取得的网络安全等级保护备案相关材料；（五）依据有关国家标准和行业标准，实施平台管理等情况；（六）有关主管部门要求提交的其他需要说明的信息。

（三）关键信息基础设施保护

1. 美、日、印、澳就勒索攻击发布联合声明，将互相协助抵御针对关键基础设施的恶意网络活动

9月23日，美、日、印、澳四国发布《关于勒索软件的四国外长声明》（Quad Foreign Ministers’ Statement on Ransomware），旨在加强区域网络安全，提高印太地区国家抵御勒索软件的能力。

声明指出将从以下四方面采取行动：（1）呼吁国家采取行动。声明呼吁各国采取合理措施解决来自其领土内的勒索攻击。面对针对关键基础设施的恶意网络活动，各国有责任相互协助；（2）印度-太平洋地区的复原力和能力建设。声明的愿景是打击勒索攻击对支持印太地区经济发展和安全的网络基础设施的威胁。声明承诺将在能力建设计划和举措方面进一步合作，加强区域网络安全，提高抵御印太地区勒索攻击的抵御能力，将拒绝为该地区的勒索软件参与者提供安全避难所，协助印太地区的合作伙伴加强网络弹性、信任和信心，以及有效的事件响应能力；（3）多利益相关方。声明强调了多利益相关方在建立反勒索软件能力建设方面的重要性，包括促进全球网络专家论坛（GFCE）等现有机制的作用；（4）机制。声明欢迎就可能的新联合国网络犯罪公约进行谈判，作为更广泛地处理网络犯罪的长期手段。同时，声明表示必须以技术中立和灵活的方式起草一项新条约，其中不描述具体的技术或犯罪方法。

2. 美国CISA发布《准备和减轻针对关键基础设施的外国影响行动》

2月18日，美国网络安全和基础设施安全局（CISA）发布《准备和减轻针对关键基础设施的外国影响行动》（Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure），为关键基础设施所有者和运营商如何识别和减轻错误信息、虚假信息和不实信息（MDM）风险提供指导。CISA表示，最近观察到的海外行动表明，外国政府和行为者可以迅速采取行动瞄准美国受众，破坏美国关键基础设施并损害美国利益。此次发布的内容旨在提高关键基础设施所有者和运营商对此类影响的认识。CISA鼓励每个组织的领导者采取积极措施，评估他们因信息操纵而面临的风险。

CISA鼓励所有关键基础设施所有者识别漏洞，对员工进行适当的网络教育，并实施MDM事件响应计划：（1）指定专人负责监督MDM事件响应流程和相关的危机沟通；（2）明确MDM响应的角色和职责，包括但不限于响应媒体询问、发布公开声明、与员工以及利益相关者沟通；（3）确保沟通系统已经设置好，并可以处理收到的问题。手机、社交媒体账户和集中式收件箱应由多人轮流监控，避免出现信息遗漏；（4）确定并培训员工向社交媒体、政府和/或执法部门进行事件报告的程序；（5）考虑用于识别事件、描述信息共享和响应的内部协调渠道和流程。

3. 美国正式通过《关键基础设施网络事件报告法》

3月15日，美国总统拜登签署的《2022年综合拨款法》（Consolidated Appropriations Act, 2022）中，正式通过《2022年关键基础设施网络事件报告法》（Cyber Incident Reporting for Critical Infrastructure Act of 2022），要求关键基础设施领域实体在有理由相信网络事件发生后72小时内，以及因勒索攻击支付赎金后24小时内，向国土安全部报告。

该法所管辖的实体涵盖关键基础设施部门（即PDD-21）中符合CISA确定的定义的实体，包括关键制造业、能源、金融服务、食品和农业、医疗保健、信息技术和运输。在进一步定义覆盖实体时，CISA将考虑一些因素，如损害一个实体可能导致的国家和经济安全后果、该实体是否是恶意网络行为者的目标，以及侵入这样一个实体是否能够破坏关键基础设施。

该法要求，报告网络事件需提交以下信息：（1）网络事件的描述；（2）被利用的漏洞和已实施的安全防御措施,以及用于实施该法所规定的网络事件的战术、技术和程序（如有）；（3）有理由相信应对该事件负责的行为者的身份或联系信息（如有）；（4）被认为或有理由认为被未经授权的人访问或获取的信息类别（如有）；（5）受影响实体的名称和其他信息，包括实体的注册信息等；（6）联系信息以及实体的授权服务供应商（如有）。

国土安全部国家网络安全和通信集成中心（NCCIC）负责根据该法接收和分析报告，并开展以下活动：（1）评估网络事件对公众健康和安全的潜在影响；（2）与适当的联邦部门和机构协调和分享信息，以确定和跟踪赎金支付，包括使用虚拟货币的赎金；（3）在自愿的基础上，促进关键基础设施所有者和经营者之间及时分享与该法所规定的网络事件和赎金支付有关的信息,特别是与正在发生的网络威胁或安全漏洞有关的信息；（4）如果事件构成重大网络事件，对有关事件的细节进行审查，并传播预防或减轻未来类似事件的方法。

4. 美国正式通过《2021 年国家网络安全防范联盟法》

5 月 12 日,美国总统拜登签署《2021 年国家网络安全防范联盟法》(National Cybersecurity Preparedness Consortium Act of 2021），旨在提升关键基础设施安全防护能力。

该法将使国土安全部能够与非营利实体合作，开发、更新和主办网络安全培训，以支持防御和应对网络安全风险。授权国土安全部与由多所大学和培训机构组成的国家网络安全防范联盟（NCPC）合作，对州及地方政府的响应责任人（first responders）和官员进行网络安全培训，支持创建信息共享计划，帮助扩大州和地方应急计划的网络安全风险和事件预防及响应。除州和地方政府外，还将为私营企业和关键基础设施所有者和经营者提供技术援助并举办模拟演习。

5. 美国能源部发布《国家网络信息工程战略》

6 月 15 日，美国能源部发布《国家网络信息工程战略》（National Cyber-Informed Engineering Strategy，简称 CIE 战略），旨在提供一个框架，加强工程培训、工具和实践，构建能够抵御网络攻击的清洁能源弹性系统。战略

鼓励在工程系统设计的早期引入网络安全技术，以减少网络安全风险和漏洞。

战略包括五个支柱，即意识、教育、开发、现有基础设施和未来基础设施，分别提出具体的战略性建议：（1）意识——领导 CIE 宣传活动，制定政策举措并建立合作伙伴关系，开发和推广案例研究，展示将 CIE 应用于现有和新兴基础设施系统的好处，促进 CIE 在能源行业的广泛采用；（2）教育——创建短期 CIE 培训和认证计划，快速培养精通 CIE 的劳动；与学术界合作，将 CIE 原则嵌入本科和研究生阶段课程；与行业雇主合作，确保 CIE 课程和认证保持一致；（3）开发——利用能源部国家实验室、学术界、政府合作伙伴和产业界不断改进和扩展 CIE 的适用性；创建和维护 CIE 工具、案例研究和课程的开源库；（4）现有基础设施——优先考虑通过当前基础设施应用 CIE 并确定所需的升级；识别、记录和推广应用 CIE 的方法；评估和验证通过 CIE 确定的基础设施升级和缓解措施的有效性；将 CIE 嵌入采购决策，并为投资应用 CIE 以保护高优先级现有基础设施的资产所有者提供激励；（5）未来基础设施——推动创建或修订国际标准，以体现 CIE 原则；提供推动研发的市场激励措施，鼓励国内供应商将 CIE 原则应用于其产品；优先支持使用 CIE 标准和方法设计、建造和维护的国家、州和地方基础设施系统项目。

6. 美国运输安全管理局更新《管道网络安全缓解行动、应急计划和测试指令》

7 月 21 日，美国运输安全管理局（TSA）修订并重新发布《管道网络安全缓解行动、应急计划和测试指令》（Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing）。

指令要求管道所有者和运营商应：（1）制定网络分段政策和控制措施，确保在信息系统受到威胁时，运营技术系统仍能继续安全运行；（2）建立访问控制措施，防止针对关键网络系统的未授权访问；（3）建立持续监控和检测政策及程序，用以检测网络安全威胁并纠正影响关键网络系统运行的异常状况；（4）使用基于风险的方法，及时为关键网络系统上的操作系统、应用程序、驱动程序和固件等安装安全补丁和更新，降低未修复系统被利用的风险；（5）制定并执行经 TSA 批准的网络安全实施计划；（6）制定并维护网络安全事件响应计划，包括在遭遇因网络安全事件引发的运营中断或业务严重退化时，管道所有者和运

营商应当采取的措施；（7）制定网络安全评估计划，主动测试并定期审计网络安全措施的有效性，识别并解决设备、网络和系统中的安全漏洞。

指令提出的上述要求是对此前提出的重大网络安全事件报告、建立网络安全联络点、开展年度网络安全漏洞评估等条款的额外补充。

7. 美国CISA发布《关键基础设施向后量子密码迁移的新见解》

8月24日，美国网络安全和基础设施安全局（CISA）发布文件《关键基础设施向后量子密码迁移的新见解》（Preparing Critical Infrastructure for Post-Quantum Cryptography），指出支撑当前加密标准的算法依赖于经典计算机无法解决的数学问题,而量子计算可暴力破解目前广泛使用的公钥密码算法——这使得商业交易、安全通信、数字签名和客户信息的安全难以保证，关键基础设施将面临巨大安全风险。CISA认为，虽然目前还不存在能够破解现行标准中公钥加密算法的量子计算技术，但政府和关键基础设施实体必须共同努力，为新的后量子密码标准做好准备。

为此，CISA对55个类别的国家关键功能（NCF）系统进行清点，根据各NCF面对量子计算对国家关键基础设施预期影响的脆弱性进行分析。基于各NCF对当前加密标准依赖性的紧迫性、需更新的系统规模以及组织升级到新标准的相对成本，CISA将各NCF分为高、中、低优先级，还将影响各NCF向后量子密码转型的因素列为加剧、中性或缓释。

目前CISA总结出三大结论：（1）特定类别NCF有助于其他系统向后量子密码转型。以下四类NCF在支持其他系统的成功转型方面是最重要的：提供互联网内容、信息和通信服务，提供身份管理和信任支持服务，提供信息技术产品和服务，保护敏感信息。CISA建议负责这些NCF的利益相关者与NIST、DHS和其他政府机构紧密合作，确保他们不仅为自己的转型做好准备，而且为支持其他NCF的数字通信转型做好准备；（2）工业控制系统（ICS）向后量子密码转型面临极大挑战。这是由于ICS硬件更换周期长，设备地理分布广。CISA敦促ICS组织将应对量子计算风险的行动纳入硬件更换周期与网络安全风险管理战略考量；（3）数据保密期较长的NCF需大量支持，以确保敏感数据安全。负责国家安全数据、个人身份信息、工业商业机密、个人健康信息和敏感司法系统信息等

的 NCF 易受量子攻击影响。CISA 建议先考虑这些 NCF 的安全，严防数据抓取与利用。

CISA 指出，虽然 NIST 到 2024 年才发布后量子密码标准，但各 NCF 组织领导者应现在就开始为向后量子密码转型做准备，遵循 DHS 在 2021 年 10 月发布的《“后量子密码过渡”路线图》，采取识别系统替换优先级、公钥加密识别、制定加密技术目录、制定关键数据目录等措施。

8. 美国 TSA 发布《铁路网络安全缓解措施与测试指令》

10 月 24 日，美国运输安全管理局（TSA）发布《铁路网络安全缓解措施与测试指令》（Rail Cybersecurity Mitigation Actions and Testing），要求铁路所有者或运营商应向 TSA 提交网络安全实施计划以供审批。在获得 TSA 批准之后，须进一步制定可供 TSA 实施合规性审查的安全措施和要求。此外，铁路所有者或运营商还须提供额外文件，并根据需要为 TSA 提供合规性审查访问权限。在制定网络安全实施计划的过程中，所有者或运营商可以使用以往风险或漏洞评估成果识别关键网络系统，优先考虑与安全指令紧密相关的网络安全措施。

9. 美国 CISA 发布文件，为关键基础设施设立网络安全绩效目标

10 月 27 日，美国网络安全与基础设施安全局（CISA）发布《跨部门网络安全性能目标》（Cross-Sector Cybersecurity Performance Goals，简称 CPGs）文件，旨在帮助私营部门的关键基础设施运营者在其运营中满足基本网络安全准则。CPGs 是一系列文件的集合，包括：设备和网络安全的目标、运营技术系统、事件响应、网络培训、治理和安全获取的指导方针等。CPGs 系自愿遵守，联邦政府不会设立新的机构，迫使运营者采用，或向任何政府机构提供有关 CPGs 相关的报告。

10. 欧盟理事会和欧洲议会就《数字运营弹性法案》达成临时协议

5 月 11 日，欧盟理事会宣布，已与欧洲议会就《数字运营弹性法案》(Digital Operational Resilience Act，简称 DORA）达成临时协议。DORA 旨在预防和减轻网络威胁，确保银行、保险公司和投资公司等欧盟金融实体的弹性运作。为实

现这一目标，DORA 为在金融领域运营的公司和组织的网络和信息系统，以及为其提供 ICT 服务(如云平台或数据分析服务)的关键第三方制定统一的安全要求。根据临时协议，向欧盟金融实体提供关键的第三国信息和通信技术服务的供应商将被要求在欧盟境内建立一个子公司，以便适当地实施监督。

一旦 DORA 被欧盟成员国通过并成为法律，欧盟监管当局将制定所有金融服务机构必须遵守的技术标准，而各自的国家主管当局将发挥合规监督的作用，并在必要时强制执行该法规。该临时协议现在需要得到理事会和欧洲议会的批准，然后进入正式通过程序。

11. 欧盟委员会发布《能源系统数字化——欧盟行动计划》

10 月 18 日，欧盟委员会发布《能源系统数字化——欧盟行动计划》（Digitalising the Energy System - EU Action Plan），推动数据共享，提升能源网络安全。计划提出建立欧盟数据共享框架，支持创新能源服务。建立健全数字化能源系统的关键是基于可信方之间无缝、安全的数据传输，提供、访问、共享能源数据。提升数据共享协同性、建立欧盟协作机制，可增强不同系统和技术方案之间的互操作性，有助于更多创新服务进入市场。此外，要严格遵守欧盟数据主权、网络安全、数据隐私、消费者接受度和互操作性等普遍适用的原则。

12. 欧洲议会通过 NIS 2 指令提案

11 月 10 日，欧洲议会通过 NIS 2 指令提案，即《关于在欧盟范围内实施高水平网络安全措施的指令》（Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148）。

2016 年生效的 NIS 指令是欧盟范围内第一部网络安全相关立法，为欧盟成员国构建网络安全思维方式、制度和监管方法奠定了基础。随着全球网络安全形势的变化，以及 COVID-19 大流行期间日益增加的安全威胁，使得 NIS 指令在保障网络安全方面的缺陷进一步凸显。

NIS 2 指令提案主要内容包括：（1）扩大适用范围。根据对经济社会重要性，提案增加新的适用领域，并引入明确的实体规模上限——这意味着特定领域

的所有中型和大型实体将纳入范围。提案为成员国提供一定灵活性，可以确定具有高安全风险的小型实体；（2）不再依据基本服务运营商和数字服务提供商对实体进行分类。提案将根据实体重要性，将实体分为基本类别和重要类别，采取不同监管制度；（3）通过实施风险管理方法来加强并精简实体的安全要求和报告义务。该方法提供了必须应用的基本安全要素的最低清单。提案对事件报告的流程、内容和时间表进行了更精确的规定；（4）强化关键信息和通信技术的供应链网络安全。成员国可以与欧盟委员会和 ENISA 合作，对关键供应链进行协调的风险评估；（5）为国家当局引入更严格的监督措施和执法要求，协调成员国之间的惩罚措施；（6）加强合作小组在制定战略政策决策方面的作用，加强成员国当局之间的信息共享与合作，包括网络危机管理在内的业务合作；（7）建立基本框架，由负责的关键行为者针对整个欧盟新发现的漏洞进行协调漏洞披露，并建立由 ENISA 运营的欧盟登记处。

13. 欧洲议会通过《关于关键实体弹性指令的提案》

11 月 22 日，欧洲议会通过《关于关键实体弹性指令的提案》（Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the resilience of critical entities Directive，简称 CER 指令提案）。

（1）适用范围。提案适用于 11 个行业，分别是能源、交通、银行、金融市场基础设施、医疗、饮用水、废水、数字基础设施、公共管理、太空、食品。

（2）识别关键实体的流程。首先，成员国应梳理出本国基本服务清单，并对基本服务面临的风险开展风险评估。风险评估应考虑所有相关的自然和人为风险，包括事故、自然灾害、突发公共卫生事件、敌对威胁、恐怖主义犯罪等。其次，成员国在识别关键实体时，除了应考虑其提供的基本服务的风险评估结果，还应考虑：1）实体是否提供一种或多项基本服务；2）提供服务所依赖的基础设施是否位于成员国境内；3）一旦实体发生安全事件，是否将对所提供的基本服务或该领域其他基本服务产生重大破坏性影响。

在判断重大破坏性影响时，主要考虑：1）该实体提供的基本服务的用户数量；2）其他部门对该服务的依赖程度；3）安全事件可能对经济、社会运转、环境和公共安全造成的影响程度和持续时间；4）实体在基本服务领域所占的市场

份额；5）可能受事件影响的地理区域；6）实体在维持基本服务水平方面的重要性，以及其他替代方案的可行性。最后，成员国应制定已识别的关键实体清单，并在被确定为关键实体后一个月内通知关键实体运营者。

（3）各主体职责。关键实体应开展风险评估，采取技术和组织措施增强安全弹性，并向当局报告安全事件。关键实体还应对担任敏感职务的人员进行背景调查；成员国当局需要向关键实体提供支持，包括提供具体指引。成员国还需要确保国家当局拥有对关键实体进行现场检查的权力和手段，能够对不遵守指令的行为进行处罚；欧盟委员会将向成员国和关键实体提供补充支持，在欧盟层面对跨国和跨部门风险、最佳实践、方法、跨国培训和演习活动等方面给予支持。

（4）对欧洲具有特定重要性的关键实体：提案将为三分之一以上欧盟成员国提供基本服务的关键实体确定为“对欧洲具有特定重要性的关键实体”。此类关键实体将在如何更好落实风险评估和强化安全弹性方面获得额外建议。

14. 澳大利亚《2022 年安全立法修正案（关键基础设施保护法）》生效

4 月 2 日，澳大利亚《2022 年安全立法修正案（关键基础设施保护法）》（Security Legislation Amendment （Critical Infrastructure Protection） Act 2022，简称 SLACIP 法）正式生效，旨在提高国家关键基础设施框架的安全性和弹性，保护澳大利亚公民所依赖的基本服务免受物理、供应链、网络和人员威胁。

修正案对《2018 年关键基础设施安全法》（SOCI 法）进行修订，主要引入以下关键措施：（1）为责任实体创建和维护关键基础设施风险管理计划；（2）具有国家意义的系统（Systems of National Significance，简称 SoNS）运营商所需的增强网络安全义务的新框架。

修正案建立 SoNs 制度，这些系统是对澳大利亚社会或经济稳定、国防或国家安全最相互关联、最相互依存和最至关重要的资产。只有在该资产具有国家意义时，才有可能被认定为 SoNs。修正案为 SoNs 规定更严苛的网络安全义务，包括：（1）制定网络安全事件应对计划，为网络事件做好准备；（2）进行网络安全演习，以建立网络准备工作；（3）进行漏洞评估，以识别漏洞进行补救；（4）提供系统信息，建立态势感知能力。增强的网络安全义务将支持近实时的威胁信

息共享，为行业提供对新兴网络安全威胁更成熟的理解，并减少对 SoNs 的重大网络攻击风险。

15. 新加坡 CSA 发布《CII 所有者增强 5G 应用网络安全指南》

4 月 29 日，新加坡网络安全局（CSA）发布第一版《CII 所有者增强 5G 应用网络安全指南》（Guidelines for CII Owners to Enhance Cyber Security for 5G Use Cases），旨在帮助关键信息基础设施所有者（CIIO）识别连接到 5G 服务系统后带来的威胁，并提供了降低此类威胁风险的建议。指南内容不具有约束力，旨在提供信息。

指南的受众包括但不限于：（1）CIIO（如高级管理人员、通信网络规划人员及其网络安全团队）；（2）CIIO 的服务和设备提供商（如外包 ICT 团队、安全服务提供商、ICT 设备供应商）。指南在用户设备安全、流量隔离、数据保护、物理安全、5G 威胁意识、5G 服务提供商的支撑要求、访问控制等方面提出具体建议。指南认为 CIIO 在设计其安全政策时应采取零信任原则，还应不断加强其网络安全能力，并在保护其系统免受威胁方面保持警惕。

16. 新加坡金融管理局发布《业务连续性管理指南》

6 月 6 日，新加坡金融管理局发布修订版《业务连续性管理指南》（Guidelines on Business Continuity Management），旨在提升新加坡金融机构业务管理能力，指引其采取措施管理日益复杂的运营环境与安全威胁，向客户提供连续性高质量关键业务服务。

根据指南，金融机构应当：(1)采用以服务为中心的方法(Service-Centric Approach），及时恢复面向客户的关键业务服务；（2）明确支持关键业务的端到端依赖关系（End-To-End Dependencies），解决可能阻碍此类服务有效恢复的问题；（3）加强安全威胁监控和环境扫描（Environmental Scanning），进行定期审计、测试和行业演习。

17. 新加坡 CSA 发布《关键信息基础设施网络安全实践守则》

7 月 4 日，新加坡网络安全局（CSA）发布《关键信息基础设施网络安全实

践守则》（Cybersecurity Code of Practice for Critical Information Infrastructure），旨在明确关键信息基础设施运营者（CIIO）为确保CII网络安全应落实的最低要求。守则包含审计要求、管理要求、识别要求、保护要求、检测要求、响应与恢复要求、网络弹性要求、培训和意识、操作技术与安全要求、特定领域问题等11个章节的内容。

具体来说，（1）审计方面。要求对审计过程中发现的风险进行补救；（2）管理方面。建立和维护框架，以确保网络安全战略与其业务目标相一致，并且为CIIO评估、定义和开展网络安全风险管理工作提供指导；（3）识别方面。协助CIIO识别支持CIIO提供基本服务的关键业务职能的资源和资产，以及相关的网络安全风险，使得CIIO能够集中精力优先保护这些资产；（4）保护方面。CIIO应落实所需的人员、流程和技术控制，以保护CII，限制和控制网络安全事件的影响；（5）检测方面。协助CIIO识别恶意活动或潜在漏洞；（6）响应与恢复方面。建立、管理和实施网络安全事件响应计划和危机沟通计划，为CII应对网络安全事件做好准备；（7）网络弹性方面。保持网络安全防御能力，以维持基本服务稳定运行，并从网络安全事件中快速恢复；（8）培训和意识方面。帮助员工了解网络安全风险，并识别他们在工作中可能遇到的网络安全事件等。

18. 新加坡CSA发布《关键信息基础设施供应链计划》

7月27日，新加坡网络安全局（CSA）发布《关键信息基础设施供应链计划》（Critical Information Infrastructure Supply Chain Programme），在分析当前关键信息基础设施运营者（CIIO）面临的供应链安全风险的基础上，提出五项具体措施，分别是：

（1）风险管理工具包。为CIIO提供可用工具包，通过标准化的供应商管理方法，帮助CIIO识别和管理供应商，评估供应链风险。目标是汇总全国所有1级CII供应商情况，并逐步提高供应链可见性深度；（2）供应商合同条款资源库。为CIIO提供一个可以纳入供应商合同的网络安全要求条款资源库。资源库将包括与常见网络安全风险、运营风险等内容相关的合同条款，CIIO可以使用这些信息指导与新供应商的谈判或更新现有供应商合同。CSA将负责建立并维护资源库，整理并公开分享合同条款；行业主管部门负责在本行业领域推广资源

库；（3）CII 供应商认证计划。建立供应商认证计划，要求供应商满足基本的网络安全要求，通过标准化和认证激励供应商提高其安全能力，同时提高 CIIO 谈判能力，优先选择通过认证的供应商。CSA 将负责协调各部门与 CIIO 之间的合作，以落实供应商认证计划；监督行业主管部门，要求其制定本行业领域的具体认证要求；激励供应商通过认证，提升网络安全能力。行业主管部门负责确定本行业领域认证需求，指导 CIIO 工作实践；（4）建立学习中心。与 CII 利益相关者共享风险管理的知识、良好实践和培训资源，提高 CII 高级领导和采购人员的风险管理意识和理解能力，将关注点从技术层面转向组织管理层面；（5）加强国际合作。加强与各国政府、行业团体的密切合作，共同应对供应链弹性问题。

19. 俄通过《保护关键信息基础设施国家政策基本原则》草案

5 月 20 日，在俄罗斯总统普京主持下，俄罗斯联邦安全委员会会议通过视频会议举行，讨论了提高国家信息基础设施运行稳定性和安全性的问题。会议讨论通过《保护关键信息基础设施国家政策基本原则》草案。目前草案还未发布。

面对信息安全形势，普京在会议上提出三大任务：（1）持续完善关乎国防、经济社会稳定的重要部门关键设施的信息安全保障机制，建设信息安全内部机构，落实负责人个人责任；（2）提高国家机关信息系统和通信网络的安全性，加强数字空间防御，消除薄弱环节，防止保密信息和公民个人信息泄露，严格管控办公设备、通信设备的使用规则；（3）从根本上降低使用外国程序、计算机技术和通信设备的风险，发展国产信息技术和产品，巩固技术主权。

20. 俄罗斯政府批准第 1478 号决议，明确重要 CII 的软件使用要求

8 月 22 日，俄罗斯政府批准第 1478 号决议，明确政府和国有企业在重要的关键信息基础设施（CII）中使用的软件要求，以及协调购买外国软件和向国产软件过渡的规则。

决议关键点主要有：（1）CII 的重要对象只能使用俄罗斯或欧亚软件登记册中包含的软件。某些类型的产品必须具有证明符合联邦安全局和俄罗斯 FSTEC 要求的证书；（2）购买国外软件须经批准。对于超过 1 亿卢布的购买，需要获得委员会的额外批准，该委员会将在俄罗斯数字发展部下成立；（3）俄罗斯数

字发展部将监督国有企业遵守《外国软件采购协调规则》的情况；（4）各部委需要批准重要的CII向俄罗斯软件过渡的部门计划。在此基础上，国有企业必须制定和批准个别的过渡计划。

21. 巴西国家电力能源局《电力部门代理人网络安全政策》生效

7月1日，巴西国家电力能源局（ANEEL）于2021年12月通过的第964号决议《电力部门代理人网络安全政策》（RESOLUÇÃO NORMATIVA ANEEL Nº 964, DE 14 DE DEZEMBRO DE 2021 Dispõe sobre a política de segurança cibernética a ser adotada pelos agentes do setor de energia elétrica）生效。

决议规定了电力部门代理商应采用的网络安全政策的指导方针和最低要求，包括但不限于：（1）落实规范、标准和网络安全最佳实践；（2）以责任感、热情和透明的态度行事；（3）传播网络安全文化；（4）安全使用电能网络和服务；（5）识别、诊断、响应网络安全事件并从中恢复；（6）识别、评估和处理网络风险；（7）寻求代理间的合作，以减轻网络风险。

决议要求电力部门代理商的网络安全政策至少包括：（1）网络安全目标，提供预防、检测、响应和减少网络事件脆弱性的能力；（2）每年应用至少一种网络安全成熟度模型；（3）数据和信息的相关性分类；（4）减少事件脆弱性和满足其他网络安全目标的程序和控制措施；（5）保证关键信息安全的技术措施，包括信息可追溯性措施；（6）进行弹性测试；（7）建立预防、缓解网络事件并从中恢复的机制；（8）建立预防和应对网络事件的程序。

22. 日本发布《关键基础设施网络安全行动计划》

6月17日，日本国家网络安全事件准备和战略中心（NISC）发布《关键基础设施网络安全行动计划》（重要インフラのサイバーセキュリティに係る行動計画），着眼于关键基础设施最近的环境变化，并为提高安全标准和加强信息共享系统提供指导。行动计划建议制定风险管理程序，以加强系统应对能力和安全标准。行动计划详细列出了对关键基础设施运营商、管理层、首席信息安全官、战略管理人员和系统人员的具体要求。

23. 新疆维吾尔自治区通过《新疆维吾尔自治区关键信息基础设施安全保护条例》

3 月 25 日，新疆维吾尔自治区第十三届人民代表大会常务委员会第三十二次会议通过《新疆维吾尔自治区关键信息基础设施安全保护条例》，自 2022 年 6 月 15 日起施行。条例规定，关键信息基础设施保护工作实行部门责任制和运营者主体责任制，并纳入年度网络安全工作责任制考核。

条例规定，网信部门会同通信、公安、工业和信息化、保密、密码管理等有关部门建立网络安全信息共享机制，及时汇总、研判、共享、发布网络安全威胁、漏洞、事件等信息，定期召开联席会议，促进有关部门、保护工作部门、运营者以及网络安全服务机构等之间的网络安全信息共享。网信部门应当统筹协调公安机关和保护工作部门按照法律、法规和相关行业标准，每年统一对本行政区域内的关键信息基础设施开展网络安全检查。在安全检查中发现网络安全风险隐患的，应当责令运营者立即改正或者限期整改。

24. 交通运输部发布《公路水路关键信息基础设施安全保护管理办法（征求意见稿）》

8 月 23 日，交通运输部发布《公路水路关键信息基础设施安全保护管理办法（征求意见稿）》。征求意见稿共六章四十八条，涉及公路水路关键信息基础设施认定、运营者责任和义务、保障和监督管理等内容。

征求意见稿规定，运营者应当设立首席网络安全官，为每个公路水路关键信息基础设施明确一名安全管理责任人。当专门安全管理机构的负责人和关键岗位人员的身份、安全背景等发生变化或必要时，运营者应当根据情况重新进行安全背景审查。运营者应制定网络安全教育培训制度，定期开展网络安全教育培训和技能考核，首席网络安全官、专门安全管理机构负责人和关键岗位人员等公路水路关键信息基础设施从业人员每人每年教育培训时长不得少于 30 个学时。

25. 我国《信息安全技术 关键信息基础设施安全保护要求》获批

10 月 12 日，国家市场监督管理总局（国家标准化管理委员会）发布公告，批准 GB/T 39204-2022《信息安全技术 关键信息基础设施安全保护要求》，自

2023 年 5 月 1 日起施行。

GB/T 39204-2022 在国家网络安全等级保护制度基础上，借鉴我国相关部门在重要行业和领域开展网络安全保护工作的成熟经验，吸纳国内外在关键信息基础设施安全保护方面的举措，结合我国现有网络安全保障体系等成果，从分析识别、安全防护、检测评估、监测预警、主动防御、事件处置等方面，提出关键信息基础设施安全保护要求，要求采取必要措施保护关键信息基础设施业务连续运行，及其重要数据不受破坏，切实加强关键信息基础设施安全保护。

（四）供应链安全

1. 五眼联盟联合发布警报《保护托管服务提供商及其客户免受网络威胁》

5 月 11 日，五眼联盟联合发布警报《保护托管服务提供商及其客户免受网络威胁》（Protecting Against Cyber Threats to Managed Service Providers and their Customers），为托管服务提供商（MSP）及其客户应采取哪些行动降低网络安全风险提供指导。

警报描述了 IT 服务和功能的网络安全最佳实践，重点关注能够在 MSP 与其客户之间就保护敏感数据进行透明度讨论的指导。组织应根据其特定的安全需求并遵守适用的法规，根据其独特的环境实施上述指导。MSP 客户应核实与其供应商的合同安排，包括符合其特定安全要求的网络安全措施。其中对 MSP 及其客户提出的建议包括：基线安全措施和操作控制、启用/改进监控和记录过程、实施多因素身份验证、管理内部架构风险并隔离内部网络、应用最小权限原则、弃用过时的账户和基础架构、更新应用、备份系统和数据、制定和实施事件响应和恢复计划、了解并主动管理供应链风险、提升透明度、管理账户身份验证和授权。

2. 美国-欧盟贸易和技术委员会发布声明，加强 ICT 等供应链弹性

5 月 16 日，美国-欧盟贸易和技术委员会（U.S.-EU Trade and Technology Council，简称 TTC）发布声明，旨在加强 ICT 等供应链弹性。

声明中与数字相关的内容主要包括：（1）打击政府强行关闭互联网。美欧对全面或针对性关闭互联网、停电或者故意降低网络速度的做法保持关注，并准

备建立有效机制，应对政府强行关闭互联网或者降低国内互联网接入的情况；（2）加强 ICT 等供应链弹性。美欧将采取行动，促进半导体等价值链和需求的透明度，提供短缺的早期预警；对 ICT 设备、软件和服务供应商进行评估，共同排查高风险供应商，促进安全、有弹性、多样化、有竞争力的 ICTS 供应链；（3）开发和实施可信赖 AI。美欧将合作开发和实施可信赖的 AI，并将基于现有 AI 立法框架，探讨如何实施政策监管，未来还将提出新的 AI 倡议。工作组还计划推进关于隐私增强技术的共同项目；（4）合作推动网络治理。美欧计划加强行动，反对滥用技术作为镇压工具以及网络威胁工具；将制定一个共同的分析框架，识别外国的信息操纵和干扰，框架最初将重点关注与俄罗斯相关的问题。增强对在线平台上非法和有害行为和内容传播的管制，关注内容审核的透明度、算法放大和研究人员的数据访问。

3. 美国 NIST 发布《软件供应链安全指南》

2 月 4 日，美国国家标准与技术研究院（NIST）发布《软件供应链安全指南》（Software Supply Chain Security Guidance）。指南强调，安全软件开发实践应在整个软件生命周期中进行整合，以减少已发布软件中的漏洞数量，缓解未发现或未解决漏洞的潜在影响，并解决造成脆弱性的根本原因。

软件采购过程中，联邦机构是购买者，而不是生产者，因此需要额外的指导。该指南向联邦机构提供了建议，以确保其采购软件的生产者在整个软件生命周期内遵循基于风险的安全软件开发方法。当联邦机构购买软件或包含软件的产品时，机构应获得软件生产者的证明，证明软件的开发符合政府规定的安全软件开发实践，还可以要求软件生产者提供资料以证明符合性。

指南的适用范围仅限于联邦机构的软件采购，包括固件、操作系统、应用程序和应用程序服务（例如基于云的软件）以及包含软件的产品，不包括已实施的软件（如内部部署或云托管），以及联邦机构购买的软件捆绑、集成或以其他方式使用的开源软件。联邦机构开发的软件不在范围之内。

4. 美国 NIST 更新《系统和组织网络安全供应链风险管理实践指南》

5 月 5 日，美国国家标准与技术研究院（NIST）发布修订版《系统和组织网

络安全供应链风险管理实践指南》（Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations），为组织从各个层面识别、评估并应对供应链中的网络安全风险提供指引。

指南指出，现代产品和服务依赖于供应链，供应链连接制造商、软件开发商和其他服务提供商，构成了全球网络。一方面，供应链促进全球经济发展，但同时也将众多公司和消费者置于风险之中：由于产品的组件和软件来源众多，设备可能在一个国家设计而在另一个国家制造，这意味着产品可能包含恶意软件、易受到网络攻击，而供应链中本身存在的安全漏洞也会影响公司安全基线。

指南主要受众为网络产品、软件和服务收购方以及终端用户。指南帮助组织将网络安全供应链风险考量因素和要求纳入采购流程，并强调风险监控与处置的重要性。由于网络安全风险可能出现在产品生命周期中的任何阶段或供应链中的任何环节，因此指南将潜在安全漏洞纳入考量。

5. 美国正式通过《2021 年供应链安全培训法》

6 月 16 日，美国正式通过 S2201《2021 年供应链安全培训法》（Supply Chain Security Training Act of 2021），意在通过反情报培训管理供应链风险。

本法要求，在本法颁布后 180 天内，总务管理局应通过联邦采购研究所为联邦机构负责供应链风险管理的官员制定培训计划。培训计划的设计应使此类人员做好执行供应链风险管理活动的准备，并识别和缓解在整个采购生命周期中出现的供应链安全风险。培训计划应满足以下条件：（1）考虑到机密信息和其他敏感信息的保护，包括关于当前特定供应链安全威胁和漏洞的信息；（2）培训计划根据需要进行更新。

本法要求，制定培训计划后的 180 天内，管理和预算办公室主任应向要求执行机构采用培训计划的联邦机构发布指南，内容包括允许执行机构将培训计划纳入现有机构培训计划；就如何确定履行供应链风险管理职责对执行机构官员提供指导。此后三年，总务管理局应每年向相关国会委员会和领导层提交一份关于培训计划实施情况的报告。

6. 美国三部门发布《软件供应链安全：开发者实践推荐指南》《软件供应链安全：供应商实践推荐指南》

9 月 1 日，美国网络安全和基础设施安全局 （CISA）、国家安全局 （NSA）和国家情报总监办公室（ODNI）发布《软件供应链安全：开发者实践推荐指南》（Securing the Software Supply Chain: Recommended Practices Guide for Developers)。指南认为软件供应商应负责在客户和软件开发人员之间建立联系。因此，供应商的责任包括通过合同协议、软件发布和更新、通知和漏洞缓解来确保软件的完整性和安全性。指南包含建议的最佳实践和标准，以帮助供应商完成这些任务；同时给出鼓励开发人员参考的行业最佳实践和原则。这些原则包括安全需求规划、从安全角度设计软件架构、添加安全功能以及维护软件和底层基础设施（如环境、源代码审查和测试）的安全性。

10 月 31 日，三部门再次发布《软件供应链安全：供应商实践推荐指南》（Securing the Software Supply Chain: Recommended Practices Guide for Suppliers）。指南认为，软件供应商可以在本次指南中获得指导，通过软件安全检查、保护软件、生产安全良好的软件等措施保护组织免遭损失。NSA 指出，该指南是对 SolarWinds 攻击事件调查结果的反馈。

7. 美国 OMB 发布《通过安全的软件开发增强软件供应链安全备忘录》

9 月 14 日，美国白宫管理和预算办公室（OMB）发布《通过安全的软件开发增强软件供应链安全备忘录》（Enhancing the Security of the Software Supply Chain through Secure Software Development Practices），旨在敦促美国联邦机构遵循美国国家标准与技术研究院（NIST）制定的一系列增强软件供应链安全的标准指南。备忘录针对 2021 年 5 月 12 发布的第 14028 号行政令—《增强软件供应链安全》的要求进行以下三个方面的细化完善：

第一，明确其适用范围主要包括三类软件：（1）适用于各联邦机构使用的，自备忘录生效之日后开发的软件；（2）适用于自备忘录生效之日后因主要版本变更而修改的现有软件；（3）适用于联邦机构通过合同方式合作的其他机构使用的软件。第二，备忘录规定增强软件供应链安全的具体措施：联邦机构在使用软件之前必须获得软件生产商的自我证明；联邦机构可以根据需要从软件生产制

造商处获得符合安全软件开发实践的证明文件；第三，备忘录规定了美国联邦机构、OMB 以及 CISA 应当履行的职责及期限。

8. 欧盟委员会提出《网络弹性法案》

9 月 15 日，欧盟委员会提出《网络弹性法案》（Cyber Resilience Act，简称 CRA），是欧盟范围内针对包括软硬件在内的网络产品安全领域的首部立法。

提案适用于所有在欧盟市场销售的、可直接或间接连接到另一设备或网络的数字产品（Products with Digital Elements）。数字产品是指“任何软件或硬件产品及其远程数据处理解决方案，包括单独投放市场的软件或硬件组件”。也就是说，所有可联网的数字设备和软件均落入提案调整范围。

提案的义务主体包括制造商、进口商和分销商三类，但主要针对的是制造商。提案要求制造商对数字产品的设计、开发和生产进行强制性安全评估；确保漏洞处理到位；并向用户提供必要的信息。具体而言，制造商义务包括以下几项：（1）对数字产品进行网络安全风险评估，并根据评估结果进行设计、开发和生产，以确保设备具备适当的网络安全水平，并且在交付时没有任何已知的可利用漏洞；（2）系统记录与数字产品网络安全相关的所有信息，包括制造商或第三方发现的漏洞，并在适当的情况下更新产品的风险评估报告；（3）起草技术文件，进行产品质量评估，确保其满足“欧盟符合性声明”（EU Declaration of Conformity）要求，并张贴“CE 标志”；（4）通过适当的程序和措施，处理、补救制造商内部或外部反馈的产品潜在漏洞；（5）向数字产品用户提供完整的信息和说明，以便用户在选择和使用此类产品时考虑网络安全；（6）在发现可被积极利用的漏洞的 24 小时内，向欧盟网络安全局报告。

就进口商和分销商而言，提案要求其只能销售符合法律规定基本要求的数字产品，并确保制造商已完成提案要求的合规义务，包括完成网络安全风险评估、起草技术文件、为数字产品张贴 CE 标志、为用户提供所需的信息等。如果进口商或分销商发现数字产品中存在漏洞，必须立即通知制造商，并向市场监管机构通报该数字产品存在“重大网络安全风险”。

成员国将任命市场监督机构，负责执行提案规定的义务。在不合规的情况下，当局可以要求产品制造商终止违规行为并消除风险、禁止或限制产品销售、

下令撤回或召回产品。提案还规定了行政罚款的上限，以供成员国在制定国内立法时参考。

下一步，提案将由欧洲议会和理事会进行审查，一旦获得通过并生效，适用主体将有两年时间适应新要求，但产品制造商报告网络漏洞和事件的义务将在一年后生效。

9. 欧盟理事会通过《关于 ICT 供应链安全的结论》

10 月 17 日，欧盟理事会通过《关于 ICT 供应链安全的结论》（Council conclusions on ICT supply chain security），旨在加强 ICT 供应链安全，迈出解决 ICT 供应链中不必要的战略性依赖关系的第一步。

文件的主要内容包括列举保障 ICT 供应链安全的具体措施（比如公共采购或者国外直接投资审查），详细说明现有及即将出台的网络立法如何保障 ICT 供应链安全，并进一步就关于数字基础设施建设的资金支持机制提出建议。文件强调欧盟及其成员国应当以一种全面、战略性的方式处理网络安全问题，不仅是在面对恶意网络攻击时，日常发展 ICT 过程中也应当适当地考量地缘政治环境。理事会认为应当推出《关键设施韧性指令》（Critical Entities Resilience Directive），在加强供应链应对网络攻击能力的同时，强化应对各种风险的整体能力。成员国应当尽量避免形成与 ICT 产品及服务关联的不必要战略依赖关系。在保证经济开放的同时实现战略自主是欧盟的关键目标。

10. 英国 NCSC 发布《供应链网络安全指南》

10 月 12 日，英国国家网络安全中心（NCSC）发布《供应链网络安全指南》（Supply chain cyber security），供组织有效评估其供应商网络安全。

指南由 NCSC 与跨市场运营弹性小组（CMORG）合作颁布，其主要内容是帮助网络安全专家、风险管理者以及采购专家更好地落实 NCSC 提出的 12 项供应链安全原则。指南指出，根据最新政府数据显示，仅有 13%的企业审查了其直接供应商的风险，审查更广泛的间接供应商的企业比例则更小，仅有 7%。

指南描述了典型的供应商关系和可能让其供应链遭受攻击的潜在漏洞，明确了预期结果并列出组织评估供应链安全的 5 个关键步骤：（1）在开始评估前

明确组织关注供应链网络安全的原因，确定组织中的核心成员，由合适的人支持供应链网络安全，了解组织是如何评估风险的；（2）研发评估供应链网络安全的方法；（3）把形成的方法适用于新的供应关系中，对机构中负责评估供应商的团队进行培训，确保整个合同周期内都能控制网络安全；（4）将现有的评估方案写进供应商合同，确定现有合同并就合同进行风险评估和审查；（5）持续改善，定期评估上述方式及其内容，不断发现新出现的风险并更新相应的供应链网络安全措施，在这一过程中需要注意与供应商之间的协作。

11. 捷克国家安全委员会授权国家网络和信息安全局制定立法，对具有战略重要性的基础设施的供应商进行筛选

9 月，捷克国家安全委员会（BRS）授权国家网络和信息安全局（NÚKIB）制定立法，允许对具有战略重要性的基础设施的供应商进行筛选，从而确保更大的弹性和安全性。

BRS 表示，目前的事态发展表明，供应链安全以及供应商在信息和通信技术领域的可靠性对国家和社会关键实体的安全具有根本性影响，从而对国家安全产生根本性影响。技术供应链引发的网络安全威胁早已为人所知，但在捷克的法律体系中，仍然没有全面的法律解决方案能够针对战略基础设施的这些威胁所带来的风险，并对其进行有效评估和降低。

该项立法将授权相关州当局评估并限制可能有风险的供应商，并将评估外国主体对供应商的影响。筛查仅涉及对捷克运作至关重要的战略基础设施领域，与此基础设施安全性无关的供应商将不会被筛选。

12. 新加坡网络安全局启动《网络安全服务提供商许可框架》

4 月 11 日，新加坡网络安全局（CSA）宣布根据《网络安全法》第 5 部分启动《网络安全服务提供商的许可框架》(Licensing Framework for Cybersecurity Service Providers）。

《网络安全法》规定，在新加坡提供渗透测试和托管安全运营中心（SOC）监控服务两类网络安全服务的供应商必须申请许可证才能继续提供此类服务。CSA 称，其中包括直接从事此类服务的公司和个人、支持这些公司的第三方供应

商以及有权对网络安全服务进行许可的经销商。目前从事其中一种或两种服务类别的现有供应商必须在2022年10月11日之前申请许可证。未能按时取得许可证者将不得不停止提供服务，直到获得许可证为止。

13. 市场监管总局发布《关于开展网络安全服务认证工作的实施意见（征求意见稿）》

7月21日，市场监管总局发布《关于开展网络安全服务认证工作的实施意见（征求意见稿）》。征求意见稿指出，市场监管总局、中央网信办、公安部根据《网络安全法》《认证认可条例》，就开展国家统一推行的网络安全服务认证工作提出意见。

征求意见稿规定，市场监管总局、中央网信办、公安部根据职责，加强认证工作的组织实施和监督管理，鼓励网络运营者等广泛采信网络安全服务认证结果。网络安全服务认证目录由市场监管总局会同中央网信办、公安部根据市场需求和产业发展状况确定并适时调整，现阶段包括检测评估、安全运维、安全咨询和等级保护测评等服务类别。

征求意见稿规定，网络安全服务认证机构应当根据认证委托人提出的认证委托，按照网络安全服务认证基本规范、认证规则开展认证工作，建立可追溯工作机制对认证全过程完整记录。通过认证的网络安全服务机构应当按照有关法律法规、标准规范的要求开展网络安全服务工作，并自觉接受市场监管部门、网信部门、公安部门的监督管理。

（五）数据利用与安全保障

1. 七国集团签署声明，通过《促进可信数据自由流动的行动计划》

5月11日，七国集团发表部长级宣言，承诺在数字化环境、数据、数字市场竞争和电子安全等多个主题上实现共同的政策目标。在数据政策方面，宣言提出“可信数据自由流动”（简称DFFT）这一术语，并指出七国集团已通过《促进可信数据自由流动的行动计划》（G7 Action Plan Promoting Data Free Flow with Trust）。

通过行动计划，七国集团承诺采取以下行动：（1）加强 DFFT 的佐证基础，其中包括更好地了解数据本地化及其影响和替代方案；（2）基于共同点，各国促进未来的互操作性，包括分析标准合同条款 SCC 和增强信任的技术等常见做法；（3）继续开展监管合作，包括围绕隐私增强技术、数据中介、网络跟踪、紧急风险、跨境沙箱以及促进数据保护框架互操作性的监管方法进行讨论；（4）在数字贸易背景下促进 DFFT；（5）分享有关国际数据空间前景的知识，并视为在组织和部门内部进行可信和自愿共享数据的新方法。

2. 美国 FTC 发布两项文件，帮助企业遵守《健康违规通知规则》

1 月 21 日，美国联邦贸易委员会（FTC）发布两项文件，分别是《遵守 FTC 健康违规通知规则》(Complying with FTC's Health Breach Notification Rule)、《健康违规通知规则:业务基础》(Health Breach Notification Rule:The Basics for Business），帮助企业遵守《健康违规通知规则》（HBNR）。

《遵守 FTC 健康违规通知规则》明确了 HBNR 适用主体、什么情况下将触发通知义务、通知对象、如何通知、通知应包含的信息等。在判断是否属于适用主体方面，《健康违规通知规则：业务基础》明确可从以下方面考虑：企业或组织是否有移动应用程序、网站、互联网连接设备或类似技术来保存消费者的健康信息？是否提供产品或服务，或向此类产品发送或接收数据？在为使用这些产品的公司提供服务时，是否处理健康信息？

2009 年 8 月，FTC 发布 HBNR，旨在填补《健康保险流通与责任法》(HIPAA)，明确个人健康记录的供应商（可帮助用户跟踪其健康信息的在线存储库）和为个人健康记录提供第三方应用程序的实体（如计步器等设备，消费者可以将其读数上传到个人健康记录中）在数据违规时的通知义务。HBNR 下的违规行为包括网络安全入侵和未经授权的访问等。

3. 美国白宫发布科技平台监管改革六大原则

9 月 8 日，美国白宫公布大型科技平台监管改革的六项原则，以促进科技行业竞争。

六项原则分别是：（1）促进技术领域竞争。通过建立明确的规则，确保

中小型企业能够在公平的市场环境中竞争；（2）采取强有力的联邦隐私保护措施。对收集、使用、传输和维护个人数据应有明确的限制，包括对定向广告的限制。这些限制应给平台造成压力，以尽量减少他们收集的信息量，而不是让美国公民阅读平台规则。尤其需要对地理位置和健康信息等特别敏感的数据，包括与生殖健康有关的信息，提供强有力的保护；（3）为儿童提供更严格的隐私和在线保护。应要求平台和其他交互式数字服务提供商在产品设计中优先考虑年轻人的安全和福祉，而不是利润和收入，包括限制过度数据收集和针对年轻群体的定向广告；（4）取消对大型科技平台的特殊法律保护。根据《通信规范法》第230条，技术平台目前具有特殊的法律保护，即使平台托管或传播非法、暴力行为或材料，也可以广泛地保护平台免于承担责任。应呼吁对第230条进行根本性改革；（5）提高平台算法和内容审核决策的透明度。平台未能提供足够的透明度，让公众和研究人员了解平台决策和内容推送是如何做出的，以及对用户的潜在影响；（6）禁止歧视性算法决策，确保算法不会歧视受保护的群体。

4. 欧盟EDPB发布《关于数据主体权利——访问权的第01/2022号指南》

1月19日，欧盟数据保护委员会（EDPB）发布《关于数据主体权利——访问权的第01/2022号指南》(Guidelines 01/2022 on data subject rights - Right of access），征询公众意见。指南覆盖访问权的各个方面，并就如何在不同情况下履行访问权提供更精确的指导。此外，指南对访问权的范围、数据控制者应向数据主体提供的信息、访问请求的格式、提供访问的主要方式等内容加以明确。

指南指出，访问权的总体目标是向数据主体提供关于其个人数据处理的充分、透明和易于获取的信息，以便数据主体能够了解并核实处理行为的合法性和所处理数据的准确性。数据主体不需要为访问请求提供理由，数据控制者也不需要分析该请求是否真的有助于数据主体核实合法性或行使其他权利。数据控制者必须处理该请求，除非该请求显然是根据数据保护规则以外的其他规则提出的。访问权包括三个不同的组成部分：确认数据主体的个人数据是否被处理；访问这些个人数据；以及访问有关处理的信息，如目的、数据类别和对象、处理的期限、数据主体的权利以及在向第三国转移时的适当保障措施。

5. 欧盟委员会通过《数据法》草案

2 月 23 日，欧盟委员会通过《数据法》草案（Data Act：Proposal for a Regulation on harmonised rules on fair access to and use of data）。草案涉及数据共享、公共机构访问、国际数据传输、云转换和互操作性等方面规定，旨在确保数字环境的公平性，刺激数据市场，为数据创新驱动提供机会。

草案表示监管对象主要为互联网产品制造商、数字服务提供商和用户等。草案主要内容包括：（1）允许联网设备的用户访问由其产生的数据（通常仅由制造商采集）并可向第三方分享这些数据，以便提供售后或其他数据驱动的创新服务；（2）防止企业滥用数据共享合同，以帮助平衡中小企业的谈判权力。草案将保护中小企业免受强势一方强加的不公平合同条款的影响。委员会还将制定标准化的合同条款，确保数据共享合同的公平；（3）私营部门在紧急情况下向公共部门提供所持有的数据。特别是在发生公共紧急事件或在法律授权获得数据的情况下；（4）允许用户在不同的云数据处理服务提供商之间有效切换，并制定了防止非法数据转移的保障措施。

6. 欧盟委员会主席与美国总统拜登发表声明，宣布已就跨大西洋数据流动的新框架达成“原则性共识”

3 月 25 日，欧盟委员会主席冯德莱恩与美国总统拜登宣布，欧盟与美国就跨大西洋数据传输的新框架达成原则性协议。该框架将促进跨大西洋数据流动，并解决欧盟法院在 2020 年 7 月的 Schrems II 裁决中提出的关切。

根据《跨大西洋数据隐私框架》，美国将制定新的保障措施，以确保情报监视活动在追求确定的国家安全目标方面是必要和相称的，建立一个具有指导补救措施的、有约束力的两级独立补救机制，并加强对情报活动的严格和分层监督，以确保对监视活动的限制。同时，框架将为欧盟公民建立新的机制，如果他们认为自己是情报活动的非法目标，可以寻求补救。

7. 欧盟 EDPB 发布《关于新的跨大西洋数据隐私框架的声明》

4 月 7 日，欧盟数据保护委员会（EDPB）发布《关于新的跨大西洋数据隐私框架的声明》（Statement 01/2022 on the announcement of an agreement in

principle on a new Trans-Atlantic Data Privacy Framework）。声明表示，EDPB 欢迎美国做出的承诺，即在欧洲经济区（EEA）的个人数据被转移到美国时采取“前所未有的”措施保护他们的隐私和个人数据。EDPB 指出，该公告并不构成 EEA 数据出口商可以将数据传输到美国的法律框架。数据出口商必须继续采取必要行动以遵守欧盟法院的判例法(CJEU),尤其是 2020 年 7 月 16 日的 Schrems II 决定。EDPB 将特别关注如何将这一政治协议转化为具体的法律提案。

EDPB 将在收到欧盟委员会的相关文件后，根据欧盟法律、CJEU 判例法和委员会先前的建议，仔细评估新框架可能带来的改进。其中，EDPB 将特别分析出于国家安全目的收集个人数据是否仅限于严格必要和相称的范围。此外，EDPB 将审查宣布的独立补救机制如何尊重 EEA 个人获得有效补救和公平审判的权利。更具体地说，EDPB 将调查该机制下部分新的主管部门在执行其公务时是否可以访问相关信息，包括个人数据，以及它是否可以通过对情报服务具有约束力的决定。EDPB 还将考虑是否引入对机构的决定或不作为的司法补救措施。

8. 欧盟委员会发布《关于欧洲健康数据空间法规的提案》

5 月 3 日,欧盟委员会发布《关于欧洲健康数据空间法规的提案》(Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space Act，简称 EHDS），征求公众意见。

《欧洲数据战略》提议建立特定领域的通用欧洲数据空间。EHDS 是此类的第一个提议，将解决电子健康数据访问和共享方面的特定挑战，是欧盟委员会在健康领域的优先事项之一。EHDS 将创建一个自然人可以轻松控制其电子健康数据的公共空间，还将使研究人员、创新者和政策制定者能够以一种保护隐私的受信任和安全的方式使用这些电子健康数据。此次公开征求意见主要包括两个方面的内容：（1）为医疗保健、科研创新、政策和监管决策而访问和使用健康数据；（2）为健康数据服务和产品建立单一市场。

7 月 12 日，欧盟数据保护委员会（EDPB）和数据保护专员公署（EDPS）就此提案发布联合意见。联合意见指出，尽管加强数据主体对其个人健康数据控制的做法受到普遍欢迎，但应强调的是，提案主要对 GDPR 中已经规定的数据主体权利进行了补充。事实上,提案甚至可能还会削弱对隐私权和数据保护权的保护，

尤其是考虑到与数据二次使用相关的个人数据类别和目的。例如，提案中的一些条款将给已经较为复杂的医疗数据处理规定增加了更多附加内容，因此需要对不同立法中的规定进行进一步说明，尤其要澄清提案与GDPR、成员国法律之间的关系。由于要处理的电子健康数据数量巨大、高度敏感以及存在非法访问的风险，并且要充分确保独立数据保护机构对其的有效监督，两部门呼吁在提案中增加一项要求，将电子健康数据存储在欧洲经济区（EEA），但不影响根据GDPR第五章进行进一步传输。

9. 欧盟EDPB发布《关于GDPR行政罚款计算的第04/2022号指南》

5月16日，欧盟数据保护委员会（EDPB）发布《关于GDPR行政罚款计算的第04/2022号指南》（Guidelines 04/2022 on the calculation of administrative fines under the GDPR），以统一各成员国数据保护机构（DPA）行政罚款的计算方法。

指南明确罚款计算的统一“起算点”，主要考虑三个要素：侵权行为的性质分类、侵权的严重性和企业的营业额。各DPA将遵循相同的方法来计算罚款，进一步提高各成员国罚款实践的协调度和透明度。各DPA仍在确保每笔罚款有效、相称且具有预防作用方面发挥重要作用，个案的特殊情况始终应作为案件的决定性考虑因素。

10. 欧盟EDPB发布《执法领域人脸识别技术应用指南》

5月16日，欧盟数据保护委员会（EDPB）发布《执法领域人脸识别技术应用指南》（Guidelines on the Use of Facial Recognition Technology in the Area of Law Enforcement），征求公众意见。

指南为欧盟和成员国立法者以及执法当局使用面部识别技术系统提供指导。EDPB强调，面部识别工具只能在严格遵守执法指令（LED）的情况下使用。只有在必要和适当的情况下，才应按照《基本权利宪章》的规定使用此类工具。

指南再次呼吁在某些情况下禁止使用面部识别技术，具体包括：（1）在可公开访问的空间中对个人进行远程生物识别；（2）面部识别系统根据个人生物特征、种族、性别以及政治或性取向或其他歧视理由，将个人分类；（3）利用

面部识别或类似技术来推断自然人的情绪；（4）在执法环境中处理个人数据时依赖于一个大规模和不加选择收集个人数据的数据库，例如通过“抓取”在线访问的照片和面部图片。

11. 欧盟委员会发布问答文件，为标准合同条款 SCC 提供应用指导

5 月 25 日，欧盟委员会发布关于 GDPR 下数据传输标准合同条款的问答文件。问答文件仅供参考，不构成法律建议。

2021 年 6 月 4 日，欧盟委员会通过两套标准合同条款，一套供欧洲经济区（EEA）内的控制者和处理者之间使用，另一套用于将个人数据传输到 EEA 以外的国家/地区。此次发布问答文件的目的是提供有关使用 SCC 的实用指南，以协助利益相关者开展合规工作。问答文件涵盖一般性问题、条文修改和签字、SCC 与其他合同条款的关系、控制者和处理者之间的标准合同条款、适用范围和传输场景、根据 SCC 传输个人数据时个人的权利、数据输出方和输入方的义务、当地法律和政府准入等方面的问题。

12. 欧盟正式通过《数据治理法》

5 月 30 日，欧盟议会和欧盟理事会签署通过《数据治理法》（Data Governance Act，简称 DGA）。6 月 3 日，GDA 在《官方公报》上公布。

DGA 作为《欧洲数据战略》的重要组成部分，旨在通过数据共享刺激社会数字经济发展，促进数据的可用性，增加对数据共享的信任并为研究和创新服务及产品建立可信的数据使用环境。DGA 将建立公共部门数据再利用机制、创建可供数据中介机构发展的法律框架、促进数据主体基于公共利益自愿提供数据、成立欧洲数据创新委员会，并为非个人数据的国际访问和传输提供法律保障。

13. 欧盟 EDPB 发布《关于数据跨境传输认证机制的第 07/2022 号指南》

6 月 16 日，欧盟数据保护委员会（EDPB）发布《关于数据跨境传输认证机制的第 07/2022 号指南》（Guidelines 07/2022 on certification as a tool for transfers），征求公众意见。GDPR 第 46（2）（f）条引入了经批准的认证机制，作为在没有充分性协议的情况下将个人数据传输到第三国的新工具。指南旨在进

一步阐明此传输工具的实际使用。

指南就如何在实践中使用该工具以及在将个人数据从欧洲经济区传输到第三国时如何帮助维持高水平的数据保护提供指导。具体地，指南由四个部分组成，每个部分都聚焦于认证作为传输工具的具体方面，包括：（1）目的、范围和所涉及的不同参与者；（2）认证机构落实认证要求的指南；（3）用于证明存在适当传输保障措施的特定认证标准；（4）具有约束力和执行力的承诺。

14. 欧盟 EDPB 就《关于确定控制者或处理者主要监管机构的第 8/2022 号指南》征求公众意见

10 月 21 日，欧盟数据保护委员会（EDPB）就《关于确定控制者或处理者主要监管机构的第 8/2022 号指南》（Guidelines 8/2022 on identifying a controller or processor’s lead supervisory authority）征求公众意见。此次更新和公共咨询的内容集中于 29-34 段以及附件的第 2 点 d 项，即有关联合数据控制者或处理者主要监管机构的内容。

指南明确联合控制者（joint controllers）在确定其各自责任时，除考虑 GDPR 第 26 条规定的内容外，还应当注意各项任务的执行主体、各自的责任义务、数据主体与监管机构之间的联系等。需要注意的是，主要机构（main establishment）是与单一控制者关联的概念，每个控制者都能够建立自己的主要机构，但不能扩充到联合控制者的范围。

指南附录部分第 2 条 d 项将联合控制者设立范围由“EU（欧盟）”修改为“EEA（欧洲经济区）”，并规定在 EEA 成立的联合控制者的主要监管机构为中央政府所在的国家监管机构。

15. 英国数据跨境流动标准合同条款正式生效

3 月 21 日，英国信息专员办公室（ICO）发布的《国际数据传输协议》（IDTA）和《欧盟 2021 年标准合同条款附录（英国附录）》正式生效。

《国际数据传输协议》（IDTA）可以作为一个独立的协议来执行，以配合主要的商业合同，确保数据传输符合英国数据保护立法。同时，鉴于许多在国际上经营的组织已经有了欧盟标准合同条款。《欧盟 2021 年标准合同条款附录（英

国附录）》允许同时遵守英国数据保护法律和欧盟-GDPR 的公司确保国际数据转移，不需要执行一个全新的、独立的机制。

英国组织必须在 2024 年 3 月 21 日之前完全执行英国的 SCC，并在此期限内用这些新条款更新现有合同。对于现有合同公司有以下三种选择：（1）继续使用旧的欧盟合同条款；（2）执行新的 IDTA；或（3）在执行欧盟合同条款同时执行新的英国附录。对于 2022 年 9 月 21 日或之后签订的合同，组织必须使用新的英国 SCC，这意味着完全执行 IDTA 或执行英国附录和欧盟 SCC。

16. 英国发布《数据共享治理框架》

5 月 23 日，隶属于英国内阁办公室的中央数字和数据办公室发布《数据共享治理框架》（Data Sharing Governance Framework），为促进公共部门数据共享提供指导。

该框架的目标对象是数据和技术领域的高级领导者，包括：（1）负责为政府组织或部门制定战略和方向的高级领导，包括那些没有特定数据职位的人；（2）数据管理专家；（3）数据共享从业者，即从事数据提供或数据采集工作的人；（4）数据请求者，即定期或偶尔需要访问政府其他部门的数据，但不像数据共享从业者那样专业的人。框架主要侧重于解决公共部门数据共享的非技术障碍，围绕公共部门数据制定明确和共同的治理标准，制定五项原则，其中包括建立数据共享问责制、实现轻松的数据共享、最大化所持有数据的价值以及提高数据的可发现性和互操作性。

17. 英国与韩国就跨境数据传输达成数据充分性原则协议

7 月 5 日，韩国和英国就跨境数据传输达成《数据充分性原则协议》（Data adequacy agreement in principle between the UK and Republic of Korea）。这一原则性协议是英国退出欧盟以来的首个独立数据充分性协议，允许在两国间不受限制地进行数据传输和共享。

协议旨在促进两国之间可信赖的数据使用和交换，使英国组织能够不受限制地将数据安全地传输到韩国，允许企业在更少限制和无合同保障的情况下共享数据。两国进一步同意就各自数据框架和立法改进开展合作，包括对英国国家数

据战略和英国《通用数据保护条例》（UK GDPR）的拟议改革，以及韩国《个人信息保护法》（PIPA）的拟议修正案。

18. 英国 ICO 发布三年战略计划《ICO25-以信息赋能公民权利》

7 月 14 日，英国信息专员办公室（ICO）公布 2022-2025 年战略计划《ICO25-以信息赋能公民权利》（ICO25--Empowering you through information），涉及生物识别、算法公平等举措。

该计划是一项三年战略，列出了 ICO 的监管方法和优先事项。ICO 承诺保护最弱势群体的信息权利，包括儿童隐私监管、AI 歧视、福利系统中的算法使用以及掠夺性营销电话（predatory marketing calls）的影响。计划包含四个战略目标：保护和赋予公民权利；赋能负责任的创新经济增长；促进开放、透明和问责；不断发展 ICO 的文化和能力。

19. 英国 ICO 发布更新后的《使用约束性公司规则作为数据传输机制的指南》

7 月 26 日消息，英国信息专员办公室（ICO）发布更新后的《使用约束性公司规则作为数据传输机制的指南》（Guide to Binding Corporate Rules）。

ICO 将约束性公司规则（BCR）视为“黄金标准”转移机制，使用 BCR 表明公司致力于实施适当的保护措施。此次更新是 ICO 在认识到 BCR 申请人可能同时寻求欧盟和英国的 BCR，并且两个司法管辖区的有关 BCR 的要求重叠，BCR 申请人需要为准备相关材料而耗费时间后做出的，旨在简化英国 BCR 的审批流程。

20. 法国国家信息与自由委员会发布《个人登录令牌或令牌访问指南》

9 月 8 日，法国国家信息与自由委员会（CNIL）发布《个人登录令牌或令牌访问指南》（Les jetons individuels de connexion ou token access），对数字令牌身份验证的用途进行评估，分析其带来的安全挑战，并提出最佳实践建议。CNIL 警告，以链接形式制成的访问令牌可能会带来安全风险，因为该令牌可以允许使用者持续访问互联网上的个人数据，如果访问令牌由第三方获取并使用，则可能导致个人数据、用户账户或在线个人空间的完整性或机密性受到损害。同时，如果没有双因素身份验证，单用户远程登录令牌还会导致“额

外的安全性风险”。

为此，CNIL 提出以下建议：（1）记录令牌创建和使用情况；（2）明确令牌的有效期；（3）生成不包含个人数据或变量的身份验证链接；（4）若令牌允许访问个人数据，则强制实施新的身份验证；（5）根据预期目的限制访问次数，例如单次或临时使用；（6）在出现可疑密集型请求时，临时或永久删除对所请求资源的访问权限。

21. 新加坡 PDPC、IMDA 发布《数据保护基本要素计划》

4 月 4 日,新加坡个人数据保护委员会(PDPC)和信息通信媒体发展局(IMDA)推出《数据保护要素计划》（Data Protection Essentials（DPE）programme），旨在帮助中小型企业（SME）获得基本水平的数据保护和安全实践，以保护客户个人数据和在数据泄露的情况下快速恢复。

根据 DPE，SME 需满足以下条件：（1）在新加坡注册和经营；（2）拥有至少 30%的当地股权；（3）集团年销售额不超过每年 1 亿新元，或集团雇员人数不超过 200 人。实施 DPE 将通过以下方式使 SME 受益：（1）新成立或收集和使用个人数据的 SME 可以采用加密和备份安全解决方案；（2）更密集地收集和使用个人数据的 SME 可以获得在 IMDA 注册的服务提供商提供的一站式专业服务，帮助 SME 建立基本的数据保护和安全能力。实施 DPE，将会在 IMDA 的网站上列出并授予 DPE 标志，以彰显 SME 为实施基本数据保护和安全实践所做的努力。如果发生 PDPA 规定的数据泄露事件，PDPC 可能会将企业实施 DPE 视为采取了安全保护措施。

22. 新加坡 PDPC 发布《在安全应用中负责任地使用生物特征数据的指南》

5 月 17 日，新加坡个人数据保护委员会（PDPC）发布《在安全应用中负责任地使用生物特征数据的指南》（Guide on the Responsible Use of Biometric Data in Security Applications），帮助管理公司、建筑/场所所有者和安全服务公司等组织，负责任地使用安全摄像头和生物识别系统，保护收集、使用或披露的个人生物识别数据。指南包括以下三个部分：关键术语定义；负责地收集、使用和披露生物特征数据的最佳实践；PDPA 义务如何适用于生物识别数据。

23. 新加坡 PDPC 发布《区块链设计个人数据保护注意事项指南》

7 月 18 日，新加坡个人数据保护委员会（PDPC）发布《区块链设计个人数据保护注意事项指南》（Guide on Personal Data Protection Considerations for Blockchain Design），通过澄清在部署区块链应用程序时应如何遵守《个人数据保护法》（PDPA），帮助组织采用区块链，以确保对客户个人数据进行更负责任的管理。指南适用于以下主体：（1）管理、配置和运营区块链的网络和联盟，即区块链运营商；（2）在区块链上设计、部署和维护应用程序的服务商，即应用服务提供商；（3）使用区块链的申请者，即参与组织。

指南正文由两部分组成：第一部分介绍了指南制定的目标和背景，并对区块链及区块链可能会产生的个人数据保护风险和注意事项进行介绍；第二部分区分“非许可链”（permissionless blockchain）和“许可链（permissioned blockchain）”两种不同类型的区块链，详细介绍应如何设计区块链应用，以符合 PDPA 要求。指南指出：（1）除非获得个人关于公开披露其个人数据的同意，否则企业不应将个人数据存储在“非许可链”上；（2）企业应采取技术管理等措施，确保“许可链”上的个人数据安全，如对“许可链”上的个人数据进行加密或匿名化处理；（3）企业应同时将个人数据存储在可通过传统权限控制措施进行管理的链外环境中，进一步降低个人数据保护风险。指南附件“为区块链制定数据保护管理计划”详细列举了当区块链应用程序涉及个人数据时，企业应当采取的具体措施。

24. 越南颁布法令详细说明《网络安全法》数据本地化要求

8 月 15 日，越南政府发布《第 53/2022/ND-CP 号法令》（Nghị định 53/2022/NĐ-CP hướng dẫn Luật An ninh mạng），详细说明越南《网络安全法》的一些条款，法令已于 2022 年 10 月 1 日生效。

越南《网络安全法》已经起草、修订并等待实施多年，如果没有这项法令，当地监管机构无法全面执行《网络安全法》要求，特别是该法第 26 条（i）数据本地化“特定类型数据应在越南存储，例如用户数据或个人数据”和（ii）设立当地办事处“在越南设立分公司或代表处”。法令规定，外国公司必须在越南境内存储用户数据并设立当地办事处。用户数据包括帐户名、信用卡信息、电子邮

件和 IP 地址、服务使用时间、最近登录记录、注册的电话号码、朋友和用户在线互动的群组等。数据应至少保存 24 个月，用于刑事调查目的的系统日志应保存至少 12 个月。根据公安部的指示，公司有 12 个月的时间来建立本地数据存储和本地办事处。

25. 中国香港私隐公署发布《跨境资料转移指引：建议合约条文范本》

5 月 12 日，香港个人资料私隐专员公署（私隐公署）发布《跨境资料转移指引：建议合约条文范本》，分别提供两种不同的跨境资料转移的情况应用，即（i）由一名资料使用者转移予另一名资料使用者；（ii）由一名资料使用者转移予一名资料处理者。

此外，建议条文范本中列举的一般条款及细则，适用于一香港机构将个人资料转移至另一境外机构；或同一香港资料使用者控制的两个香港境外机构之间的个人资料转移。

个人资料私隐专员钟丽玲表示：即使个人资料被转移至香港境外，关键的是持份者仍须肩负起保障资料当事人个人资料私隐的责任。建议条文范本提供了实际的框架，有利于个人资料从香港转移至境外地方，使机构能订立清晰的协议，在符合《个人资料（私隐）条例》规定及良好数据道德标准的前提下转移资料。

26. 香港个人资料私隐专员公署就《数据出境安全评估办法》生效发布提醒

9 月 1 日，香港个人资料私隐专员公署就《数据出境安全评估办法》生效发布提醒。私隐专员公署提醒香港企业，尤其是在内地开展业务的香港企业或机构，例如银行、保险公司和证券公司等，如符合办法所订明的情形，可能须按有关规定向国家网信部门申报数据出境安全评估。

个人资料私隐专员（私隐专员）钟丽玲指出：在办法实施前已经开展的数据出境活动，如不符合办法的规定，亦须在办法实施起计 6 个月内，即 2023 年 2 月 28 日前，完成整改。有关企业或机构应尽早了解办法的规定及评估办法对其数据出境活动的影响，作出适时的跟进和（如有需要）寻求专业意见，以符合办法的相关要求。

27. 全国信安标委发布《信息安全技术 重要数据识别指南》（征求意见稿）

1 月 13 日，全国信安标委发布《信息安全技术 重要数据识别指南（征求意见稿）》，给出识别重要数据的基本原则、考虑因素以及重要数据描述格式。

征求意见稿明确识别重要数据应遵循的六项原则，分别是聚焦安全影响、突出保护重点、衔接既有规定、综合考虑风险、定量定性结合、动态识别复评。具体来说，征求意见稿要求从国家安全、经济运行、社会稳定、公共健康和安全等角度识别重要数据，只对组织自身而言重要或敏感的数据不属于重要数据，如企业的内部管理相关数据。应通过对数据分级，明确安全保护重点，使一般数据充分流动，重要数据在满足安全保护要求前提下有序流动，释放数据价值。

3 月 16 日，根据主管部门的要求和之前收集的意见，标准编制组对标准作了较大改动，并更名为《信息安全技术 重要数据识别规则（征求意见稿）》。新的识别规则将重要数据定义为特定领域、特定群体、特定区域或达到一定精度和规模的数据，一旦被泄露或篡改、损毁，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全。

28. 工信部再次公开征求对《工业和信息化领域数据安全管理办法（试行）》（征求意见稿）的意见

2 月 10 日，工信部再次公开征求对《工业和信息化领域数据安全管理办法（试行）》（征求意见稿）的意见。此次发布的征求意见稿对数据定义、监管机构、重要数据和核心数据目录备案、主体责任、数据出境等诸多条款进行调整。

工业和信息化领域数据处理者责任方面，征求意见稿明确其对数据处理活动负安全主体责任，对各类数据实行分级防护，不同级别数据同时被处理且难以分别采取保护措施的，应当按照其中级别最高的要求实施保护，确保数据持续处于有效保护和合法利用的状态。应当将本单位重要数据和核心数据目录向地方工业和信息化主管部门（工业领域）或通信管理局（电信领域）或无线电管理机构（无线电领域）备案。

征求意见稿增加核心数据跨主体处理、日志留存条款，要求跨主体提供、转移、委托处理核心数据的，应当评估安全风险，采取必要的安全保护措施，并经由地方工业和信息化主管部门（工业领域）或通信管理局（电信领域）或无线

电管理机构（无线电领域）报工信部。工信部按照有关规定进行审查。

29. 工信部发布《车联网网络安全和数据安全标准体系建设指南》

2 月 25 日，工信部发布《车联网网络安全和数据安全标准体系建设指南》，聚焦车联网终端与设施网络安全、网联通信安全、数据安全、应用服务安全、安全保障与支撑等重点领域，着力增加基础通用、共性技术、试验方法、典型应用等产业急需标准的有效供给，覆盖车联网网络安全、数据安全的关键领域和关键环节。

其中，数据安全标准主要规范智能网联汽车、车联网平台、车载应用服务等数据安全和个人信息保护要求，包括通用要求、分类分级、出境安全、个人信息保护、应用数据安全等 5 类标准。通用要求标准主要规范车联网可采集和处理的数据类型、范围、质量、颗粒度等，包括数据最小化采集、数据安全存储、数据加密传输、数据安全共享等标准。

30. 科技部发布《人类遗传资源管理常见问题解答》

3 月 2 日，科技部中国人类遗传资源管理办公室发布《人类遗传资源管理常见问题解答》。

针对数据统计公司如需接收人类遗传资源信息是否需要进行信息备份和备案的问题，解答回应是“合作各方之外的外方单位如需接收人类遗传资源信息，需要进行信息备份和备案”。针对实时出境的数据信息应如何进行备份和备案的问题，解答回应是“如涉及基因数据信息，应将拟出境数据信息类型、合计例数、单位/规格等进行数据备份，并预估整个项目的数据量进行数据备案，备案通过后定期进行数据备份，如果实际备份的数据量预计超过备案数据量时，需要进行备案变更；如不涉及基因数据信息，不需要进行信息备份和备案”。

31. 科技部发布《人类遗传资源管理条例实施细则（征求意见稿）》

3 月 21 日，科技部社会发展科技司发布《人类遗传资源管理条例实施细则（征求意见稿）》。征求意见稿明确，采集、保藏、利用、对外提供我国人类遗传资源，应当遵守本实施细则。人类遗传资源包括人类遗传资源材料和人类遗传

资源信息。其中，人类遗传资源信息是指利用人类遗传资源材料产生的人类基因、基因组数据等信息资料。

征求意见稿规定重要人类遗传资源目录管理、登记和主动申报要求。科技部在全国性人类遗传资源调查等基础上，组织开展重要遗传家系和特定地区人类遗传资源研究，逐步建立清单目录，适时修订完善。征求意见稿建立人类遗传资源材料出境许可、人类遗传资源信息对外提供备案和安全审查制度，规定将人类遗传资源信息向境外组织、个人及其设立或者实际控制的机构提供或者开放使用可能影响我国公众健康、国家安全和社会公共利益的，应当通过科技部组织的安全审查。

32. 国家发改委发布公告，对“数据基础制度观点”征集意见

3 月 21 日，国家发展改革委创新和高技术发展司发布公告，就“数据基础制度观点”征集意见。公告同期发布关于构建数据基础制度的总体思路、数据产权、流通交易、收益分配、安全治理等制度规则方面的若干观点，希望社会各界就此提出意见建议。

数据要素流通交易制度方面，建议进一步完善和规范数据流通规则，构建在使用中流通、场内场外相结合的交易制度体系。建议围绕数据要素流通交易需要，培育一批数据服务商和第三方专业服务机构，壮大数据产业。数据要素安全治理制度方面，建议构建有效市场和有为政府相结合的数据要素治理格局，构建政府、企业、社会多方协同治理模式。建议充分发挥政府有序引导和规范发展的作用，守住安全底线，明确监管红线，打造安全可信、包容创新、公平开放的数据要素市场环境。建议坚持“宽进严管”原则，明确企业主体责任和义务，牢固树立企业的责任意识和自律意识。

6 月 16 日，国家发改委在例行发布会上宣布已形成数据要素基础性制度文件初稿。

33. 中共中央、国务院发布《关于加快建设全国统一大市场的意见》

3 月 25 日，中共中央、国务院发布《关于加快建设全国统一大市场的意见》，旨在从全局和战略高度加快建设全国统一大市场。

意见要求，加快培育数据要素市场，建立健全数据安全、权利保护、跨境传输管理、交易流通、开放共享、安全认证等基础制度和标准规范，深入开展数据资源调查，推动数据资源开发利用。意见要求，强化标准验证、实施、监督，健全现代流通、大数据、AI、区块链、第五代移动通信（5G）、物联网、储能等领域标准体系。深入开展 AI 社会实验，推动制定智能社会治理相关标准。推动统一智能家居、安防等领域标准，探索建立智能设备标识制度。加快制定面部识别、指静脉、虹膜等智能化识别系统的全国统一标准和安全规范。

34. 国家市场监督管理总局、国家互联网信息办公室发布《关于开展数据安全管理认证工作的公告》

6 月 5 日，国家市场监督管理总局、国家互联网信息办公室发布《关于开展数据安全管理认证工作的公告》，决定开展数据安全管理认证工作，鼓励网络运营者通过认证方式规范网络数据处理活动，加强网络数据安全保护。从事数据安全管理认证活动的认证机构应当依法设立，并按照《数据安全管理认证实施规则》实施认证。

公告同步发布《数据安全管理认证实施规则》，规定对网络运营者开展网络数据收集、存储、使用、加工、传输、提供、公开等处理活动进行认证的基本原则和要求。《数据安全管理认证实施规则》明确数据安全管理认证的认证模式为技术验证+现场审核+获证后监督。认证机构根据认证委托资料、技术验证报告、现场审核报告和其他相关资料信息进行综合评价，作出认证决定。对符合认证要求的，颁发认证证书；对暂不符合认证要求的，可要求认证委托人限期整改，整改后仍不符合的，以书面形式通知认证委托人终止认证。

35. 习近平主持召开中央全面深化改革委员会第二十六次会议强调：加快构建数据基础制度

6 月 22 日，中共中央总书记、国家主席、中央军委主席、中央全面深化改革委员会主任习近平主持召开中央全面深化改革委员会第二十六次会议，审议通过《关于构建数据基础制度更好发挥数据要素作用的意见》等文件。

习近平在主持会议时强调，数据基础制度建设事关国家发展和安全大局，

要维护国家数据安全，保护个人信息和商业秘密，促进数据高效流通使用、赋能实体经济，统筹推进数据产权、流通交易、收益分配、安全治理，加快构建数据基础制度体系。

会议指出，数据作为新型生产要素，是数字化、网络化、智能化的基础，已快速融入生产、分配、流通、消费和社会服务管理等各个环节，深刻改变着生产方式、生活方式和社会治理方式。我国具有数据规模和数据应用优势，我们推动出台数据安全法、个人信息保护法等法律法规，积极探索推进数据要素市场化，加快构建以数据为关键要素的数字经济，取得了积极进展。要建立数据产权制度，推进公共数据、企业数据、个人数据分类分级确权授权使用，建立数据资源持有权、数据加工使用权、数据产品经营权等分置的产权运行机制，健全数据要素权益保护制度。要建立合规高效的数据要素流通和交易制度，完善数据全流程合规和监管规则体系，建设规范的数据交易市场。要完善数据要素市场化配置机制，更好发挥政府在数据要素收益分配中的引导调节作用，建立体现效率、促进公平的数据要素收益分配制度。要把安全贯穿数据治理全过程，守住安全底线，明确监管红线，加强重点领域执法司法，把必须管住的坚决管到位。要构建政府、企业、社会多方协同治理模式，强化分行业监管和跨行业协同监管，压实企业数据安全责任。

36. 国家互联网信息办公室公布《数据出境安全评估办法》

7 月 7 日，国家互联网信息办公室发布《数据出境安全评估办法》，自 2022 年 9 月 1 日起施行。办法规定数据出境安全评估的范围、条件和程序，为数据出境安全评估工作提供具体指引。

办法规定应当申报数据出境安全评估的情形，包括数据处理者向境外提供重要数据、关键信息基础设施运营者和处理 100 万人以上个人信息的数据处理者向境外提供个人信息、自上年 1 月 1 日起累计向境外提供 10 万人个人信息或者 1 万人敏感个人信息的数据处理者向境外提供个人信息以及国家网信部门规定的其他需要申报数据出境安全评估的情形。

办法提出数据出境安全评估的具体要求，规定数据处理者在申报数据出境安全评估前应当开展数据出境风险自评估并明确重点评估事项。数据处理者在与

境外接收方订立的法律文件中应明确约定数据安全保护责任义务，在数据出境安全评估有效期内发生影响数据出境安全的情形应当重新申报评估。此外，还明确了数据出境安全评估程序、监督管理制度、法律责任以及合规整改要求等。

37. 国家互联网信息办公室发布《数据出境安全评估申报指南（第一版）》

8 月 31 日，国家互联网信息办公室发布《数据出境安全评估申报指南（第一版）》，对数据出境安全评估申报方式、申报流程、申报材料等具体要求作出说明。数据处理者因业务需要确需向境外提供数据，符合数据出境安全评估适用情形的，应当根据《数据出境安全评估办法》规定，按照申报指南申报数据出境安全评估。

38. 中国气象局印发《气象数据开放共享实施细则（试行）》

9 月，中国气象局印发《气象数据开放共享实施细则（试行）》。实施细则指出气象数据开放共享应当遵循依法依规原则，以确保国家安全和数据安全为前提，保护数据提供者的合法权益，充分考虑用户实际需求，注重数据服务效益，分类分级开放共享。要充分发挥气象部门的技术优势，优先采用提供产品数据和服务等方式，依据数据使用用途和具体应用场景，通过气象数据服务资源平台充分保障各类用户的气象数据需求。

实施细则提出，对于原始数据和数据产品，应提供经过严格质量控制评估并经过业务准入的数据，确保数据质量；对于预报产品和服务产品，应优先提供经过业务准入实时更新的业务数据，确保服务时效。

39. 民航局印发《关于民航大数据建设发展的指导意见》

10 月 13 日，民航局发布《关于民航大数据建设发展的指导意见》，旨在进一步加强民航大数据发展的顶层设计，指导行业更好地开展民航大数据建设工作。

指导意见明确民航大数据建设的总体框架，即“三个导向，六个方向，六个靶向”。“三个导向”是指进一步明确机构职责，健全体制机制，增强一体化数据整合能力，更好地把民航大数据“管起来”“用起来”“活起来”。“六

个方向”是指从数据管理维度实现数据的数字化、标准化，从数据使用维度实现数据的资源化、资产化，从数据流通维度实现数据的要素化、市场化。“六个靶向”是指一体推进工作组织体系、法规标准体系、数据资源体系、数据要素体系、基础设施体系、数据安全体系建设。

指导意见阐明民航大数据建设的6大主要任务和14个方面具体工作任务，要求加强法规体系建设、构建数据标准体系、提升数据管理水平、加强数据质量管理、推进数据要素流通、加强民航数据网络建设、强化安全管理责任、提升安全保障能力等。

40. 国务院办公厅印发《全国一体化政务大数据体系建设指南》

10 月 28 日，国务院办公厅印发《全国一体化政务大数据体系建设指南》，旨在充分发挥政务数据在提升政府履职能力、支撑数字政府建设以及推进国家治理体系和治理能力现代化中的重要作用。

安全保障方面，指南认为政务数据安全保障能力亟需强化。亟需建立完善与政务数据安全配套的制度。数据全生命周期的安全管理机制不健全，数据安全技术防护能力亟待加强。缺乏专业化的数据安全运营团队，数据安全管理的规范化水平有待提升，在制度规范、技术防护、运行管理三个层面尚未形成数据安全保障的有机整体。

对此，指南将“安全保障一体化”作为主要任务之一。以“数据”为安全保障的核心要素，强化安全主体责任，健全保障机制，完善数据安全防护和监测手段，加强数据流转全流程管理，形成制度规范、技术防护和运行管理三位一体的全国一体化政务大数据安全保障体系。充分利用电子认证，数据加密存储、传输和应用手段，防止数据篡改，推进数据脱敏使用，加强重要数据保护，加强个人隐私、商业秘密信息保护，严格管控数据访问行为，实现过程全记录和精细化权限管理。

41. 天津市发布《天津市数据交易管理暂行办法》

1 月 25 日，天津市互联网信息办公室发布《天津市数据交易管理暂行办法》，自发布之日起施行，有效期两年。办法共八章四十三条，涉及交易主体、交易对

象、交易行为、交易平台、交易安全、监督管理等环节。

其中，交易主体包括数据供方、数据需方和数据交易服务机构。办法要求数据交易服务机构开展业务应当将数据交易服务平台部署在我国境内；定期开展安全测评、风险评估，以云服务方式建设数据交易服务平台的，应当通过国家有关机构组织的云计算服务安全评估。交易安全方面，办法要求数据交易服务机构应当对拟交易数据建立分类制度，落实有关部门对不同类别数据提出的安全要求。数据交易服务机构应当对拟交易数据建立分级保护机制，根据数据的不同级别，为数据供需双方提供不同强度的安全保护技术支持措施。

42. 山东省发布《山东省公共数据开放办法》

1 月 31 日，山东省政府发布《山东省公共数据开放办法》，自 2022 年 4 月 1 日起施行。办法进一步拓展公共数据适用范围，明确国家机关，法律法规授权的具有管理公共事务职能的组织，具有公共服务职能的企业事业单位，人民团体等在依法履行公共管理职责、提供公共服务过程中，收集和产生的各类数据均属于公共数据，应纳入公共数据开放办法管理。与其他地方现有公共数据开放立法相比，办法的适用范围更全面。

关于重点和优先开放数据范围，办法有针对性地提出：重点和优先开放与数字经济、公共服务、公共安全、社会治理、民生保障等领域密切相关的市场监管、卫生健康、自然资源、生态环境、就业、教育、交通、气象等数据，以及行政许可、行政处罚、企业公共信用信息等数据。同时，办法遵循“需求导向”原则，重点和优先开放的数据范围应当征求社会公众、行业组织、企业、行业主管部门的意见，切实满足公民、法人和其他组织开发利用公共数据的需求。在开发利用促进措施及数据安全保护等方面，办法也结合实际作出规定。

43. 重庆市发布《重庆市数据条例》

3 月 30 日，重庆市第五届人民代表大会常务委员会第三十三次会议通过《重庆市数据条例》，自 2022 年 7 月 1 日起施行。条例共八章六十条，分为总则、数据处理和安全、数据资源、数据要素市场、法律责任等内容。

条例明确处理涉及个人信息的数据应当遵循合法、正当、必要原则和其他

相关规则，提出自然人、法人和非法人组织违反与市数据主管部门签订的开放利用协议，超出约定使用范围使用公共数据，逾期未改正的或者造成严重后果的，处1万元以上10万元以下的罚款。数据安全方面，条例建立健全数据处理规则和数据安全体系，明确开展数据处理活动的禁止性行为和数据安全保护义务。条例规定建立数据安全责任制，明确数据处理者是数据安全责任主体，同时存在多个数据处理者的，分别承担各自安全责任。

44. 广东省发布《广州市数字经济促进条例》

4月6日，广州市人大常委会发布《广州市数字经济促进条例》，自2022年6月1日起施行。条例共十一章八十九条，以推动数字产业化和产业数字化发展为核心，加强数字基础设施建设，推进数据资源价值化，努力提升城市治理数字化水平，致力构建数字经济全要素发展制度体系，为广州建设成为具有全球影响力的数字经济引领型城市提供法治保障。

条例推行首席数据官、数据经纪人等创新制度，建立健全部门协同、市区联动、政企合作的数据治理体制机制，探索推行首席数据官等数据管理创新制度，探索建立数据交易平台、场所以及数据入场规范、数据经纪人管理等配套制度。

45. 黑龙江省发布《黑龙江省促进大数据发展应用条例》

5月13日，黑龙江省十三届人大常委会第三十三次会议通过《黑龙江省促进大数据发展应用条例》，自2022年7月1日起施行。条例共八章七十条，涉及数据资源、数据要素市场、发展应用、安全保护等内容。

条例规定自然人、法人和非法人组织对其合法处理数据形成的数据产品和服务享有法律、行政法规及本条例规定的财产权益，依法自主使用，进行处分。公共管理和服务机构应当在确保国家安全、公共安全和保护个人隐私、商业秘密的前提下，在法律、法规允许范围内最大限度开放公共数据。安全方面，条例要求省和设区的市级政务数据主管部门应当建设公共数据灾备体系。鼓励采集非公共数据的自然人、法人和非法人组织建立重要系统和核心数据的灾备机制，定期开展数据恢复性测试。

46. 江西省发布《江西省“十四五”数字经济发展规划》

5 月 25 日，江西省人民政府发布《江西省“十四五”数字经济发展规划》。规划要求坚持促进发展和监管规范并重，更好把充分发挥市场决定性作用和更好发挥政府作用有机结合起来，构建经济社会各主体多元参与、协同联动的数字经济发展新机制，建立健全适应数字经济发展的市场监管、宏观调节、政策法规体系，牢牢守住安全底线。

安全方面，规划要求强化协同治理和监管机制、增强政府数字化治理能力、完善多元共治新格局、健全网络安全保障体系、强化数据安全保护。具体来说，规划要求进一步明确平台企业主体责任和义务；贯彻《网络安全法》《密码法》，落实等级保护、安全测评、电子认证、应急管理、国产密码应用等制度；全面贯彻落实《数据安全法》《个人信息保护法》，建立健全数据安全相关管理制度；制定重要数据具体目录，加强数据分类分级保护。

47. 河北省发布《河北省数字经济促进条例》

5 月 27 日，河北省十三届人大常委会第三十次会议审议通过《河北省数字经济促进条例》，自 2022 年 7 月 1 日起施行。条例共九章八十一条，主要围绕数字基础设施建设、数据资源开发利用、数字产业化、产业数字化、数字化治理、京津冀数字经济协同发展、保障和监督等方面作出规范。

条例指出，数据资源开发利用应当遵循依法规范、促进流通、合理使用、保障安全的原则，加强数据资源全生命周期管理，提高数据要素质量，培育发展数据要素市场，激发数据要素潜能。

48. 辽宁省发布《辽宁省大数据发展条例》

5 月 31 日，辽宁省十三届人大常委会第三十四次会议表决通过《辽宁省大数据发展条例》，自 2022 年 8 月 1 日正式施行。条例共九章五十四条，是规范全省大数据发展的首部地方性法规。

为解决数据要素市场发育不充分问题，条例设置“数据要素市场”专章，明确市场主体在数据采集、加工、使用、交易等基本权益方面的保障性规定；同时，对数据交易和竞争行为以“负面清单”方式划定禁区，就交易市场配套制度

建设予以规定，并对违法交易、侵害其他市场主体合法权益等行为设置处罚条款。安全方面，条例设置“数据安全”专章，规定实行数据安全责任制和分类分级保护制度，明确责任确定原则，搭建数据安全管理体制，并就全社会各主体建立落实数据安全保护制度、强化数据存储管理和应急处置等予以明确。

49. 上海发布《上海市数字经济发展“十四五”规划》

7 月 12 日，上海市人民政府办公厅发布《上海市数字经济发展“十四五”规划》，提出“十四五”时期，数字经济核心竞争力不断提升、数字经济企业活跃度显著提高、数字新赛道新动能持续壮大、数据要素市场体系基本建立四大发展目标。

培育数据新要素方面，规划围绕数据产品与服务、数字内容、数字贸易、数字设计、数字安全展开。规划要求，释放城市海量数据价值，统筹推进数据产业各环节布局，激发数据要素乘数效应，健全数据要素产业生态。完善数据流通交易服务体系，大力培育数据经纪、数据合规性评审、数据审计、数据资产评估、数据交易撮合、争议仲裁等专业中介服务机构。发展支持企业整体数字化转型的规划咨询、检测认证、安全培训等高端定制安全服务，培育事前预防、事中防护、事后补偿的全周期安全保险服务。保障措施方面，规划要求完善数据治理。落实《上海市数据条例》，加快出台市公共数据授权运营管理办法等配套文件，试点开展公共数据授权运营服务。出台上海数据要素市场制度体系建设相关政策，促进数据要素市场流通。

50. 海南省发布《海南省政府数字化转型总体方案（2022—2025）》

7 月 25 日，海南省人民政府办公厅发布《海南省政府数字化转型总体方案（2022—2025）》。

方案要求提升数据安全防护能力。贯彻落实《保密法》《数据安全法》《个人信息保护法》《网络安全法》《民法典》等相关法律法规。落实数据安全主体责任，明确安全责任边界。方案要求建立安全有序便利的数据流动管理制度。制定实施公共数据分类分级管理指南、公共数据开放安全评估办法。建设公共数据安全监管体系，强化公共数据开发利用和全生命周期安全管理，加强海量数据汇

聚后的安全属性研判、预警分析和技术处理。试点建设跨境数据流动监管体系，建立区域性跨境数据流动规则和白名单机制。试点开展数据跨境流动安全评估，建立数据跨境流通和交易风险评估等制度。探索利用区块链、探针等技术，实现数据共享全程留痕可监测，确保数据使用全生命周期可溯源。

51. 广东省发布《广东省企业首席数据官建设指南》

8 月 24 日,广东省工业和信息化厅发布《广东省企业首席数据官建设指南》，涉及建设原则、建设内容、保障措施等三部分内容。

指南鼓励具备条件的企业设立首席数据官（CDO），按照“企业主导、政府推动、价值优先、多方协同”的建设原则组织实施。CDO 应设置在企业决策层，是企业对数据资产的使用管理和安全全面负责的高层管理人员。CDO 应当开展数据治理、数据安全等工作任务，贯彻执行国家数据等方面的法律、法规和政策，建立企业数据资产安全保障制度和分类分级安全管理制度,组织制定并实施企业数据安全防护方案,提升数据全生命周期安全防护能力,定期组织数据安全评估，组织基于供应链的数据安全监测，提高企业数据风险管控能力，确保企业数据隐私与安全等。

52. 江苏、北京等省市推动数据出境安全评估工作落地实施

(1) 江苏省发布《江苏省数据出境安全评估申报工作指引（第一版）》

9 月 1 日，江苏省互联网信息办公室发布《江苏省数据出境安全评估申报工作指引（第一版）》，对数据、重要数据、个人信息、敏感个人信息、数据处理等概念进行界定，对适用范围、申报方式、申报流程等予以规定，并公布联系电话和报送具体地址。

(2) 北京设立数据出境安全评估申报咨询电话

9 月 1 日，为规范有序开展申报工作，北京市互联网信息办公室设立数据出境安全评估申报咨询电话：010-67676912（工作日上午 9：30-11：30，下午 14：00-17：00）。

(3) 天津市互联网信息办公室开通数据出境安全评估申报咨询电话

9 月 2 日，天津市互联网信息办公室正式开通数据出境安全评估申报咨询

电话：022-88355322（工作日上午 9:30-11:30，下午 14:00-17:00）。

(4) 河北省网信办开通数据出境安全评估申报咨询电话

9 月 3 日,河北省互联网信息办公室设立数据出境安全评估申报咨询电话：0311-87909716（工作日上午 9:30-11:30，下午 14:00-17:00），联系人：李慧冬、姚文昱，邮箱：jscs@caheb.gov.cn，地址：河北省石家庄市桥西区维明南大街 79 号 321 室，邮编：050051。

(5) 黑龙江设立数据出境安全评估申报咨询电话

9 月 8 日，黑龙江省互联网信息办公室发布通知表示开始受理数据受理者申报数据出境安全评估，并公布咨询电话：0451-58685723（工作日上午 9：30-11：30，下午 14：00-17：00）。

(6) 浙江省互联网信息办公室开通数据出境安全评估申报通道

9 月 8 日，浙江省互联网信息办公室正式开通数据出境安全评估咨询和申报通道，接收数据处理者提交的书面申报材料及附带材料电子版。通过电话方式咨询数据出境安全评估申报事宜，需明确告知来电单位主体信息。咨询时间：工作日 9：30-11：30，15：00-17：00；咨询电话：0571-81051250；电子邮箱：data_sec.zjwxb@zj.gov.cn；报送地址：浙江省杭州市西湖区省府路 29 号。

(7) 上海发布关于接受数据出境安全评估申报咨询的通知

9 月 9 日，上海市互联网信息办公室发布关于接受数据出境安全评估申报咨询的通知，明确咨询范围为注册地为上海的数据处理者。咨询时间：工作日上午 9:00-11:00，下午 14:00-17:00；联系电话：64743030-2711。

(8) 内蒙古自治区开通数据出境安全评估申报通道

9 月 15 日，内蒙古自治区互联网信息办公室正式开通数据出境安全评估咨询和申报通道，接收数据处理者提交的书面申报材料及附带材料电子版。咨询电话：0471-4821277（工作日上午 9：00-12：00，下午 14：30-17：00）。电子邮箱：sj_nmgwxb@nmww.gov.cn。报送地址：内蒙古自治区呼和浩特市赛罕区银河南街 8 号

(9) 重庆市互联网信息办公室开通数据出境安全评估咨询和申报通道

9 月 22 日，重庆市互联网信息办公室正式开通数据出境安全评估咨询和申报通道，接收数据处理者提交的数据出境安全评估申报材料。通过电话方式

咨询数据出境安全评估申报事宜，需明确告知来电单位主体信息。咨询时间：工作日 9:00—18:00。咨询电话：023-63151805。报送地址：重庆市渝北区青竹东路 6 号北楼重庆市互联网信息办公室。

(10) 贵州省互联网信息办公室开通数据出境安全评估申报通道

9 月 30 日，贵州省互联网信息办公室设立数据出境安全评估申报咨询电话：0851-82995001（工作日上午 9:30-11:30，下午 2:00-5:00），联系人：刘文静，邮箱：gzcert@cert.org.cn，地址：贵州省贵阳市云岩区宝山北路 39 号，邮编：550001。注册地为贵州的数据处理者向境外提供数据，应当通过贵州省网信办向国家网信办申报数据出境安全评估，申报方式为送达书面申报材料并附带材料电子版。

（11）福建省互联网信息办公室开通数据出境安全评估申报通道

10 月 14 日，福建省互联网信息办公室发布消息，根据《数据出境安全评估办法》和《数据出境安全评估申报指南（第一版）》要求，注册地为福建的数据处理者向境外提供数据，应当通过福建省委网信办向国家网信办申报数据出境安全评估，申报方式为送达书面申报材料并附带材料电子版。为指导和帮助数据处理者规范、有序申报数据出境安全评估，福建省互联网信息办公室开通数据出境安全评估申报通道。

（12）山东省互联网信息办公室开通数据出境安全评估申报通道

10 月 26 日，根据《数据出境安全评估办法》和国家互联网信息办公室发布的《数据出境安全评估申报指南（第一版）》要求，山东省向境外提供在境内运营中收集和产生的重要数据和个人信息的组织或个人，应当通过省网信办向国家网信办申报数据出境安全评估，申报方式为送达书面申报材料并附带材料电子版。

为指导和帮助数据处理者规范、有序申报数据出境安全评估，省网信办开通数据出境安全评估申报通道。咨询电话：18853135773，0531-51773249、81913920（工作日上午 9:30-11:30，下午 14:00-17:00，来电咨询请明确告知申报主体基本信息）报送地址：山东省济南市市中区经十路 20637 号文博写字楼 217 室（山东省互联网信息办公室）。邮编：250001

53. 河南省人民政府办公厅发布《河南省大数据产业发展行动计划（2022—2025年）》

9月15日，河南省人民政府办公厅发布《河南省大数据产业发展行动计划（2022—2025年）》。行动计划要求完善数据安全保障体系，包括实施数据安全“铸盾”行动，开展数据资源分类分级管理试点工作，加强数据应用、数据流转、数据共享、数据隐私、数据交易等环节监管等。明确加强隐私计算、数据脱敏、密码、区块链等技术和产品的研发应用。

54. 陕西省人大常委会通过《陕西省大数据条例》

9月29日，陕西省第十三届人民代表大会常务委员会第三十六次会议通过《陕西省大数据条例》。条例共八章八十一条，涉及基础设施、数据资源、开发应用、产业发展、安全保障、法律责任等内容。

条例规定，政务部门应当按照一数一源、一源多用的要求，在政务数据目录内收集数据，并及时对政务数据资源进行更新和维护，确保数据收集的准确性、完整性、时效性、安全性，实现政务数据的一次收集、共享使用；可以通过共享方式获得政务数据的，不得通过其他方式重复收集。县级以上人民政府及其有关部门根据应急处置工作需要，可以收集自然人、法人和非法人组织的相关数据，处理数据应当依照法律、法规有关规定进行，不得用于与应急处置工作无关的事项。

安全保障方面，条例规定，网信部门会同大数据主管部门按照国家数据分类分级保护制度，确定本行政区域的重要数据具体目录，对列入目录的数据进行重点保护。政务部门负责管理政府信息化建设过程中收集、产生的数据，不得将数据管理权向企业转移。政务部门应当要求参与政府信息化建设、维护的企业、事业单位按照有关法律、行政法规的规定和合同约定履行数据安全保护义务，对涉及的敏感个人信息等，依法采取脱敏、加密保护等措施。企业、事业单位不得擅自留存、使用、泄露或者向他人提供获取的政务数据，不得擅自将数据用于商业用途或者向境外提供。数据收集、持有、管理、使用等负有数据安全责任的单位和个人向境外提供数据的，应当依法进行数据出境安全评估和审查。

（六）个人信息保护

1. 美国NIST发布《信息系统和组织安全、隐私控制评估指南》

1月25日，美国国家标准与技术研究院（NIST）发布《信息系统和组织安全、隐私控制评估指南》（Assessing Security and Privacy Controls in Information Systems and Organizations），用于对系统和组织内使用的安全和隐私控制进行评估。

指南为评估程序提供一个足够灵活的评估框架和初始起点，以满足不同组织需求，同时在进行控制评估时协调一致。指南强调提高用户网络安全意识、启用具有成本效益的安全评估程序和隐私控制、为高管创建可靠的安全信息等措施的重要性。

2. 美国NIST发布新版《实施<健康保险可携带性和责任法>安全规则：网络安全资源指南》

7月21日，美国国家标准与技术研究院（NIST）更新医疗保健网络安全指南，新出版物草案命名为第2版SP 800-66《实施<健康保险可携带性和责任法>安全规则：网络安全资源指南》（Implementing the Health Insurance Portability and Accountability Act（HIPAA）Security Rule: A Cybersecurity Resource Guide），旨在帮助组织遵守《健康保险可携带性和责任法》（HIPAA）的安全规则，维护个人健康信息的机密性、完整性和可用性。修订后的指南更具可操作性，医疗机构可用于改善其网络安全并遵守安全规则。

第二版指南仅对之前版本的结构进行轻微调整，对内容进行更新而非“大修”，更加强调对受保护的电子健康信息（ePHI）的风险评估和管理。因此，这次修订是为了指导卫生保健组织改进其ePHI风险管理。

3. 美国《数据隐私和保护法案》提交众议院委员会

6月23日，《美国数据隐私和保护法案》（the American Data Privacy and Protection Act，简称ADPPA）提交众议院委员会。

ADPPA是首份获得两党、两院支持的美国综合隐私立法草案，旨在：（1）

建立强有力的国家框架，保护消费者数据隐私和安全；（2）为公民提供广泛的保护，防止其数据被歧视性地使用；（3）要求数据处理者在前端尽量减少需要收集、处理和传输的个人数据，以便将消费者数据的使用限制在特定产品和服务的合理、必要、相称的限制范围内；（4）要求数据处理者遵守特定实践相关的忠实义务，同时确保消费者不必为隐私付费；（5）要求法律适用的实体允许消费者关闭有针对性的广告；（6）为儿童和未成年人提供更强的数据保护；（7）整个互联网生态系统中建立平等监管；（8）促进创新，为初创企业和小企业提供成长和竞争的机会。

4. 美国犹他州正式通过《犹他州消费者隐私法》

3 月 24 日，美国犹他州州长签署《犹他州消费者隐私法》（Utah Consumer Privacy Act，简称 UCPA），自 2023 年 12 月 31 日生效。犹他州成为美国第四个颁布全面消费者隐私立法的州。

UCPA 适用于以下控制者或处理者：（1）在本州开展业务，或生产针对本州居民的产品或服务；（2）年收入达到或超过 25，000，000 美元；并且（3）满足以下一个或多个门槛：在一个日历年内，控制或处理 10 万或更多消费者的个人数据；或该实体 50%以上的总收入来自个人数据的销售，并控制或处理 25，000 名或更多消费者的个人数据。

UCPA 规定了四项消费者权利和六项控制者义务。其中，消费者权利分别是访问权、删除权、数据可携权、消费者选择不接受某些处理的权利。六项控制者义务分别是：（1）透明度。要求控制者向消费者提供合理清晰的隐私通知；（2）儿童个人数据特殊规定。处理已知未满 13 岁的消费者个人数据的控制者必须获得可核实的父母同意，并按照《儿童在线隐私保护法》进行处理；（3）安全。控制者必须建立、实施和维护合理的行政、技术和物理数据安全措施，保护个人数据保密性和完整性；（4）非歧视性。如果消费者选择退出定向广告，或者如果该提议与消费者自愿参与善意的忠诚度计划有关，控制者可以提供不同的价格、费率、水平、质量或对商品或服务的选择；（5）回应消费者要求。除非有例外情况，控制者有义务在 45 天内对消费者的请求作出回应；（6）数据处理合同。处理者代表控制者进行的处理活动必须受到合同的约束。

UCPA 没有规定私人诉权，州检察总长拥有独家执法权。UCPA 责成消费者保护司管理“一个接受消费者投诉的系统”，并授权该司调查所指控的违法行为。如果该司司长有“合理的理由相信存在实质性的（违规）证据”，则需要将其提交给检察总长。检察总长若决定对移交事项采取行动，该办公室必须向控制者或处理者提供书面通知。控制者和处理者有 30 天的时间来纠正违规行为，并向检察总长提供一份“明确的书面声明，说明违规行为已被纠正，不会再发生被纠正的违规行为”。如果控制者或处理者未能纠正违规行为，或在提供书面声明后继续违规，总检察长可启动执法行动并进行处罚，即实际损失和每项违规行为最高 7500 美元的罚款。

5. 美国康涅狄格州正式通过《康涅狄格州数据隐私法》

5 月 10 日，美国康涅狄格州州长签署参议院第 6 号法案，即《康涅狄格州数据隐私法》（Connecticut Data Privacy Act），自 2023 年 7 月 1 日生效。康涅狄格州成为继加州、弗吉尼亚州、科罗拉多州和犹他州之后，美国第五个通过综合性消费者隐私法的州。

该法适用于：（1）在康涅狄格州开展业务，或生产针对康涅狄格州居民的产品或服务；（2）在上一个日历年，控制或处理至少 100,000 名消费者的个人数据，不包括仅为完成支付交易而控制或处理的个人数据；或控制或处理至少 25,000 名消费者的个人数据，并且其总收入的 25%以上来自出售个人数据。

根据该法，消费者享有五项主要权利，分别是（1）访问权。消费者有权“确认控制者是否正在处理消费者的个人数据，并访问此类个人数据”；（2）纠正权。消费者有权“在考虑到个人数据的性质和处理消费者个人数据的目的的情况下，纠正消费者个人数据中的不准确之处”；（3）删除权。消费者有权“删除由消费者提供的或获得的关于消费者的个人数据”；（4）数据可移植性。在行使其访问权时，消费者有权“以便携、在技术上可行的范围内、易于使用的格式，获取由控制者处理的消费者个人数据的副本。该格式使消费者能够不受阻碍地通过自动化方式将数据传输给另一个控制者，前提是不应要求该控制者透露任何商业秘密”；（5）选择退出权。消费者有权“出于以下目的，选择拒绝处理个人数据”：有针对性的广告；出售个人数据；或为促进出台有关消费者的法律或类

似的重大影响，完全自动决定而进行的特征分析。

6. 美国加州正式通过《加州适龄设计规范法》

9 月 16 日，美国加州州长签署第 2273 号议会法—《加州适龄设计规范法》（The California Age-Appropriate Design Code Act）。这是美国第一部要求青少年可能使用的在线服务商为 18 岁以下用户提供广泛保障措施的州级法规。尽管遭到科技行业的反对，但加州立法机构还是在 8 月底一致通过了该法。

该法适用于 18 岁以下用户可能使用的诸多数字产品，包括社交网络、游戏平台、联网玩具、语音助手和智能学习工具等。该法限制应用程序收集 18 岁以下用户的数据，并要求在线服务在默认情况下为儿童和青少年开启“最高隐私设置”。该法强制在线服务主动采取安全措施，在设计产品和功能之初就考虑年轻用户的最佳利益，例如在用户访问其平台之前验证用户的实际年龄。

此外，该法的影响还可能超出加州范围，促使许多服务机构在全美进行变革。不过，许多行业团体反对这项立法，称其范围太广，条款过于含糊，不利于实施。代表许多美国大型科技公司的行业组织 TechNet 已经向加州立法者施压，要求他们将该法中“儿童”的定义缩小到 16 岁以下，而不是 18 岁以下。该机构还声称，许多面向普通受众的在线服务也可能会被儿童访问，这将使大量网站和应用程序受到该法的限制。多位公民自由专家认为，这项措施也可能对成年人产生不利后果。为了迫使网站以不同的方式对待青少年和儿童，面向普通受众的在线服务可能会建立侵入性年龄验证系统，要求所有用户向公司提供敏感个人信息。这也将使儿童（和其他所有人）受到更多监视，并让匿名使用在线服务成为不可能。以上行为可能侵害受宪法保护的言论自由权及网站、平台和应用程序的编辑权，违反宪法第一修正案。

据悉，该法将于 2024 年 6 月生效，尚不清楚科技公司是否会改变法案的具体内容和实施规范。

7. 加州隐私保护局发布 CCPA 拟议法规草案的最新修订情况

10 月 17 日，美国加州隐私保护局（CPPA）发布《2018 年加州消费者隐私法》（CCPA）拟议法规草案的修订版，以回应此前收到的数百条公众意见。

修改后的拟议法规共72页，调整了数据最小化、获取同意的要求、数据收集通知、处理消费者请求、限制使用/披露敏感个人信息的权利、对第三方的要求等内容。修改后的拟议法规为企业收集、使用、保留或共享消费者个人信息提出额外要求。收集或处理个人信息的目的必须与“消费者的合理期望”相一致。消费者的合理期望必须基于：（1）消费者与企业之间的关系；（2）企业寻求收集或处理的个人信息类型、性质和数量；（3）个人信息的来源和业务的收集或处理方法；（4）向消费者披露有关收集或处理消费者个人信息的目的的具体性、明确性和突出性；（5）消费者认为服务提供商、承包商、第三方或其他实体是否明显参与收集或处理个人信息的程度。修改后的拟议法仍保留“不成比例的努力”条款，即如果履行响应访问、删除、更正请求等义务会导致不成比例的努力，将会限制此类义务的履行。

8. 欧盟EDPB发布《关于向俄罗斯联邦传输个人数据的第02/2022号声明》

7月12日，欧盟数据保护委员会（EDPB）发布《关于向俄罗斯联邦传输个人数据的第02/2022号声明》（Statement 02/2022 on personal data transfers to the Russian Federation），对欧盟成员国向俄罗斯传输数据的行为作出进一步规制。

声明指出，在没有欧盟委员会根据GDPR第45条作出适当决定的情况下，只有控制者或处理者提供了适当的保障措施，并且数据主体享有可强制执行的权利和有效的法律补救措施的条件下，数据出口商才有可能将个人数据传输至第三国。如果没有根据第45（3）条作出充分性决定，或根据第46条采取适当的保障措施，个人数据向第三国的传输应仅在第49条“特殊情形下的克减”规定的条件下发生。

俄罗斯没有从欧盟委员会取得充分性认定。因此，向俄罗斯传输个人数据必须使用GDPR第五章中规定的其他传输规则之一。考虑到这一点，EDPB指出，当个人数据被传输到俄罗斯时，在GDPR规制下的数据出口商，应评估和确定数据传输的法律基础与GDPR第五章中所提及的规则（如标准合同条款或约束性公司规则），以确保保障措施的恰当应用。

此外，根据欧洲法院Schrems II裁决与EDPB关于补充措施的建议，数据

出口商还应评估，在利害关系转移的背景下，俄罗斯有效的法律和实践中是否存在任何内容可能会影响保障措施的有效性。如果存在这种情况，数据出口商应确定并采取必要的补充措施，以确保数据主体获得与欧洲经济区（EEA）内基本同等水平的保护。如果这种评估导致不能或不再确保合规的结果，并且无法确定补充措施，数据出口商必须停止数据传输。

9. 欧盟 EDPB 就《关于 GDPR 个人数据泄露通知的第 9/2022 号指南》征求公众意见

10 月 18 日，欧盟数据保护委员会（EDPB）就《关于 GDPR 个人数据泄露通知的第 9/2022 号指南》（Guidelines 09/2022 on personal data breach notification under GDPR）征求公众意见。此次意见征集主要针对指南第 73 段的内容，并将于 2022 年 11 月 29 日截止。

根据 GDPR 的规定，个人数据泄露必须通知主管数据监督机构，并在符合特定情况下，通知受到泄露影响的数据主体。指南解释了 GDPR 强制性数据泄露通知和沟通要求，以及数据控制者和处理者为履行这些义务可以采取的步骤和措施，还举例说明了各种具体类型的违规行为应当如何进行通知。

指南进一步明确对于非欧盟机构发生个人数据泄露时的通知要求。未在欧盟设立的数据控制者仍可能受到 GDPR 第 3（2）和第 3（3）条的约束，此时如果控制者出现数据泄露，仍需遵守 GDPR 第 33 条和第 34 条的规定履行通知义务。GDPR 第 27 条还要求数据控制者和处理者在欧盟中指定一名代表。指南第 73 段规定仅有成员国代表的出席不会触发一站式服务制度（the one-stop- shop system），需要将数据泄露通知受数据影响主体所在成员国的每一个监管机构，通知程序应当按照控制者向其代表的授权进行。在确定控制者或者处理者的主要监管机构时应当参照《关于确定控制者或处理者主要监管机构的指南》有关要求。

10. 英国 ICO 发布《匿名化、假名化及隐私增强技术指南（草案）》

9 月 7 日，英国信息专员办公室（ICO）发布《匿名化、假名化及隐私增强技术指南（草案）》（Draft anonymisation, pseudonymisation and privacy enhancing technologies guidance）。

隐私增强技术（PETs）是指通过最小化个人数据使用、最大化数据安全、提升个人自主权来实现基本数据保护原则的技术。草案共分为两部分，分别介绍PETs如何有助于数据保护合规和实践中常见的PETs类型。草案承认PETs有助于实现“通过设计和默认方法的数据保护”，并协助组织遵守数据处理的最小化原则，但也指出PETs不是满足数据保护合规义务的“灵丹妙药”，数据处理仍然需要合法、公平和透明。

11. 挪威DPA发布《有关共享和处理儿童个人数据和同意的指南》

4月25日，挪威数据保护机构（DPA）更新《有关共享和处理儿童个人数据和同意的指南》（Samtykke fra mindreårige）。

指南规定儿童只有在年满18岁时才能单独同意共享和处理自己的个人数据。在此之前，父母或负有父母责任的人必须代表孩子同意。然而，儿童有权随着年龄的增长而增加自决和共同决定权，因此，父母在代表子女达成协议之前应与子女本人核实。在特定情况下，18岁以下的儿童如果能够给予知情和自愿的同意，可以自己表示同意，但必须根据儿童的成熟程度以及所提供的信息是否适应儿童的年龄和理解其同意内容的能力来评估这一点。

12. 爱尔兰DPC发布三份儿童数据保护权利指南

5月25日，爱尔兰数据保护委员会（DPC）发布三份儿童数据保护及GDPR下儿童权利的简短指南。这些指南主要针对13岁及以上的儿童，因为这个年龄的儿童可以开始自己注册多种形式的社交媒体。

三份指南分别是：（1）《个人信息和数据保护—是什么？》（Your Personal Information and Data protection--What’s it all About？），向儿童和青少年介绍个人数据和数据保护理念，以及为什么他们了解这些信息很重要；（2）《数据保护权》（My data protection rights），向儿童介绍不同的数据保护权利以及如何使用它；（3）《保持在线数据安全的重要提示》（Top tips for keeping your data safe online），包含15条有用的提示，可帮助儿童（实际上是每个人）在上网时保护个人数据安全。

13. 安道尔《关于个人数据保护的第 29/2021 号法》生效

5 月 17 日，安道尔数据保护局宣布《关于个人数据保护的第 29/2021 号法》（Act 29/2021 on Personal Data Protection）正式生效。该法于 2021 年 10 月 28 日正式通过。

该法旨在根据 GDPR，更新个人、私人实体和安道尔公共行政部门处理个人数据的相关法规。该法还包括与 GDPR 一致的适用于个人数据处理的原则，如合法性、公平性、透明度、目的限制、数据最小化和准确性。具体而言，该法还规定了数据主体的一些权利，如更正权、访问权、数据可携带权，以及有关设计和默认数据保护的条款。

14. 新加坡 PDPC 发布《基础匿名化指南》

3 月 31 日，新加坡个人数据保护委员会（PDPC）发布《基础匿名化指南》（Guide to Basic Anonymisation），为企业数据匿名化与去标识化提供指引。

指南概述了基本的数据匿名化与去标识化概念，并提出数据匿名化的五个步骤：（1）识别数据。将所控制数据划分为直接标识符、间接标识符与目标变量，如对员工数据而言，姓名为直接标识符，性别为间接标识符，雇佣类型为目标变量；（2）对数据进行去标识化。删除数据中的所有直接标识符，或为直接标识符分配唯一假名，以假名替换直接标识符；（3）应用匿名化技术。对数据中的间接标识符应用匿名化技术，可采用技术如删除数据行、删除数据属性、将数据值中的某些字符替换为“*”、降低数据颗粒度（如将“26 岁”替换为“25-30 岁”）、偏转数据、增加干扰因素修改原数据等；（4）评估匿名化效果。评估、计算匿名数据面临重识别的风险，并重复第三步与第四步，直到达到最佳数据匿名化效果；（5）管理数据重识别与披露风险。采取数据加密、访问权限控制等技术、流程控制措施与签署数据处理协议等第三方管理措施，管理数据使用中的重识别与披露风险。

15. 新加坡《个人数据保护法》执行修正案生效

10 月 1 日，新加坡《个人数据保护法》（PDPA）执行修正案生效。根据该修正案，个人数据保护委员会（PDPC）的权力得到加强，可以接受自愿承诺作为

其执行制度的一部分。此外，对于本地年营业额超过1000万新元的组织，可能施加的罚款上限从先前固定的100万新元增加到该组织在新加坡年营业额的10%。

16. 日本PPC发布《<个人信息保护法>合规要点》

2月18日，日本个人信息保护委员会（PPC）发布《<个人信息保护法>合规要点》（改正個人情報保護法対応チェックポイント），以帮助中小企业应对《个人信息保护法》修订实施带来的合规压力。

要点包括：（1）如果发生泄露等可能损害个人权益的情况，经营者有义务向PPC报告并通知个人信息主体；（2）如向外国第三方提供个人信息，应当加强向个人信息主体披露该第三方处理个人信息的相关情况；（3）原则上应当公布所采取的安全管理措施。如涉及在国外处理个人信息，有必要在了解国外个人信息保护制度后采取安全管理措施；（4）在6个月内删除的短期保存数据同样受到披露要求的约束。个人亦有权要求披露经营者向第三方提供和接收个人信息的记录，披露方式由个人选择。此外，还扩大了停止利用与删除个人信息请求权的范围；（5）禁止以不正当方式使用个人信息，如向涉嫌从事非法行为的企业提供个人信息；（6）在向第三方提供时，如果该信息对于提供方而言不属于个人信息，但提供方预期接收方可能将其作为个人信息，则该信息的对外提供也应当征得本人的同意。个人关联信息包括通过终端标识符收集的网站浏览历史、商品购买历史、位置信息等（这些信息中，能够识别特定个人的属于个人信息，不属于个人关联信息）。

17. 日本经济产业省与总务省发布新版《企业隐私治理指南ver1.2》

2月18日，日本经济产业省与总务省发布新版《企业隐私治理指南ver1.2》（DX時代における企業のプライバシーガバナンスガイドブックver1.2）。指南面向企业经营者，明确今后应采取的必要条件以及组织体制。由于隐私问题不仅由企业来解决，指南还针对隐私问题相关的社会关系，如与消费者之间的互动交流提出要求。

2020年8月，经济产业省与总务省发布指南ver1.0。2021年7月制定发布

指南 ver1.1，强化案例指引。

18. 日本新修订的《个人信息保护法》正式施行

4 月 1 日，日本新修订的《个人信息保护法》（個人情報保護法）正式施行。新修订的《个人信息保护法》要点包括：

（1）增强用户权利。2015 年旧版《个人信息保护法》规定，用户可在数据处理者违反法律规定将其个人信息提供给第三方时，要求数据处理者停止该数据提供行为。新法增加第三十条第五款，规定当数据处理者失去使用保存中的个人信息的必要性时，或者存储的可识别用户的个人信息发生本法规定的安全事件，或可能损害用户权利或正当利益时，用户均可要求数据处理者停止提供该等数据。

（2）加重数据处理者义务。如用户依据上述第三十条第五款提出要求停止使用数据的，数据处理者应在一定条件下立即予以停止；数据处理者不得以有可能助长、诱发违法或不正当行为的方式使用个人信息；在一定条件下，数据处理者发生包括数据泄露、灭失、毁损在内的其他 PPC 规定的涉及数据安全保障的事件，很有可能对个人权利和利益造成损害的，应按照 PPC 规则，将事态报告给 PPC。同时规定，在一定条件下信息处理者还应将发生的事态通知用户。

（3）新增假名化信息加工条款，规定假名加工数据处理者的义务。主要包括：1）在假名加工阶段，假名加工的数据处理者应为删除信息等安全管理事项采取相应的措施；2）假名加工处理不可超出目的范围；丧失必要性后应及时删除个人信息；3）以及不得为识别本人而将该假名加工信息与其他信息相对照等；4）原则上假名加工的数据处理者不可将假名加工信息提供给第三方。

（4）扩大域外适用范围。依照旧法规定，日本域外的主体对涉及向日本国内用户提供物品或服务的个人信息进行数据处理的，PPC 仅能对域外对象进行指导建议等不具有强制力的措施。新法扩大对域外主体可采取措施的范围，规定 PPC 可向该等域外主体要求提供报告、命令、实地检查等强制权利。

19. 以色列政府修订《隐私保护法》

1 月 5 日，以色列政府提出第 14 号修正案(הפרטיות הגנת חוק הצעת (מס תיקון'

14), התשפ"ב-2022），对《隐私保护法》（PPA）进行重大修订。议会通过后，该法案将是自 1996 年以来最大和最全面的更新。

修正案将更新关键术语的定义，使 PPL 与《欧盟通用数据保护条例》（GDPR）保持一致。拟修改的定义包括：（1）数据——数据的定义将被修改包括“任何类型的潜在可识别信息”；（2）具有特殊敏感性的数据——法案将引入一个敏感个人数据类别，包括个人政治观点、犯罪记录、地理位置、生物特征和消费习惯等信息；（3）数据库所有者、持有者和管理者——此定义将与 GDPR 中的规定保持一致。修正案要求组织任命一名信息安全官员（DPO），这是以色列第一次将 DPO 义务纳入法律。修正案还引入几项新的实质性限制：（1）禁止控制者或处理者重新调整数据用途或允许第三方这样做；（2）禁止未经控制者授权，使用数据库中的数据；（3）禁止管理或使用数据库，如果其中包含的数据是以违反 PPA 或其他法律的方式收集的。

刑事制裁方面，修正案列出了一系列刑事犯罪和相应的制裁措施，其中不仅包括罚款，还包括长达五年的监禁。例如以欺诈意图从个人处收集数据，包括在隐私通知中进行虚假陈述的行为，最高可被判处三年监禁。控制者或处理者超出数据收集目的，使用数据或允许他人使用数据的行为，可处五年以下监禁。未经授权使用或访问数据库中的数据，最高可被判处三年监禁。

20. 巴西国民议会颁布《第 115 号宪法修正案》

2 月 10 日，巴西国民议会颁布《第 115 号宪法修正案》（Emenda Constitucional 115），将个人数据保护列入基本宪法权利与保障，并规定联邦在该问题上的专属立法权。修正案规定可识别个人身份的任何数据（如全名、自然人税号），或与其他信息交叉后可识别个人身份的数据均为个人数据。

2021 年 10 月，参议院批准该修正案，授权政府根据《通用数据保护法》进行个人数据保护与处理活动监管，并为国家数据保护局提供宪法支撑。巴西联邦最高法院（STF）已承认个人数据保护是一项基本权利。

21. 泰国《个人数据保护法》正式生效

6 月 1 日，2019 年发布的泰国《个人数据保护法》（PDPA）在因疫情原因

被推迟两年后正式生效。

PDPA 是泰国制定的第一部有关数据保护的立法，适用于直接在泰国或总部在国外但在泰国参与控制和处理商品、服务及消费者行为数据的组织。其确立了数据收集、使用和披露的合法性基础，规定了敏感个人数据的收集使用规则、数据控制者和处理者义务以及数据主体基本权利。违反 PDPA 的个人或实体可能遭受刑事或行政处罚。刑事处罚包括最高 100 万泰铢的罚款和/或最高一年的监禁，行政处罚包括最高 500 万泰铢的罚款和高达实际损失金额两倍的惩罚性赔偿。

22. 菲律宾就针对侵犯数据隐私的行为发布《行政罚款指引》

8 月 8 日，菲律宾国家隐私委员会（NPC）针对个人信息控制者（PIC）和个人信息处理者（PIP）的数据隐私侵权行为发布《行政罚款指引》（GUIDELINES ON ADMINISTRATIVE FINES）。

指引规定，NPC 将根据违法行为情节构成严重或重大，分别处以违法行为人年总收入的 0.5%至 3%和 0.25%至 2%的行政罚款。对于以下违规行为，PIC 或 PIP 将被处以不低于 5 万比索但不超过 20 万比索的行政罚款：（1）未注册 PIC、数据处理系统或自动决策信息的真实身份或联系方式；（2）未能提供有关 PIC 的身份或联系方式、数据处理系统或自动决策信息的最新信息。

如果不遵守 NPC 或其正式授权官员的任何命令、决议或决定，将导致在对原始违规行为处以罚款的基础上加处以不超过五万比索的行政罚款。如果 PIC 或 PIP 运营未超过一年，则计算行政罚款的基础将是该实体在违规时的总收入总额。如果 PIC 或 PIP 拒绝支付罚款，可能会被下达停止令、委员会根据《数据隐私法》第 7 条授权以及根据法院规则启动的其他程序或救济。

23. 菲律宾国家隐私委员会发布《关于提交个人数据泄露通知和年度安全事件报告的声明》

10 月 14 日，菲律宾国家隐私委员会（NPC）发布《关于提交个人数据泄露通知和年度安全事件报告的公告》（Announcement regarding the submission of Personal Data Breach Notifications（PDBN） and Annual Security Incident Reports（ASIR））。公告指出，所有个人数据泄露通知和年度安全事件报告均

应通过数据泄露通知管理系统（DBNMS）在线平台提交，通过电子邮件、个人档案、普通邮件、持牌快递服务以及任何其他实物提交方式提交的材料将视为无效。此外，国家隐私委员会就如何使用 DBMNS 系统提供视频指引，包括如何创建数据库帐户、如何提交个人数据更新报告、如何提交申请等。

24. 印尼国会审议通过《个人数据保护法》

9 月 20 日，印尼国会全体会议审议通过《个人数据保护法》（Rancangan Undang-Undang Pelindungan Data Pribadi，简称 PDP 法）。这是印尼颁布的首部全面的数据保护立法。受该法约束的组织将有两年时间遵守该法要求。

该法自 2016 年提出以来经过详细讨论和审议，最终通过的法律共 16 章 76 条，比最初提交的草案增加 4 条。该法对个人数据类型、数据主体权利、数据处理者和控制者义务以及处理个人数据主体的义务、法律责任等作出规定。

该法要求处理印尼公民个人数据的实体（无论是公共实体还是私人实体）确保其系统中的数据得到保护。个人权利方面部分条款借鉴 GDPR 规定，例如数据可携权以及同意撤回权的规定。

该法授权印尼总统设立一个监督机构，对违反该法的实体处以高达实体年收入 2%的罚款，泄露个人数据的公司资产也可能被没收或拍卖。对于个人的刑事处罚，非法收集或使用他人个人资料的数据处理者，可能面临最高五年监禁。非法泄露他人数据的监禁最高为四年；为谋取利益而伪造个人数据的个人，则可能被判入狱长达六年。根据该法，印尼公民将能够对侵犯其个人数据权利的行为要求赔偿。

25. 俄罗斯三读通过《关于个人数据保护的修正案》

7 月 6 日，俄罗斯国家杜马宣布三读通过第 101234-8 号法案《关于个人数据保护的修正案》（по вопросам защиты прав субъектов персональных данных），提出针对公民个人数据的额外保护措施。

修正案要求个人数据运营商立即向授权机构报告所有网络攻击和泄露事件，运营商有义务在发现事件后 24 小时内通知联邦通信、信息技术和大众传媒

监督局 Roskomnadzor。事件报告将分两个阶段进行：24 小时内报告对受影响数据的描述，3 天内报告内部检查结果。

修正案要求，运营商必须告知当局将个人数据转移到国外的目的，在某些情况下，这种转移可能会受到限制。修正案禁止运营商在公民未授权提供个人数据（包括生物特征数据）时拒绝向其提供服务，即使在必要时也是如此。修正案还对未成年人的生物特征个人数据的处理进行了限制。

8 月 11 日，俄罗斯联邦通信、信息技术和大众传媒监督局（Roskomnadzor）领导的公共委员会修订近期通过的《联邦个人数据法》，重点讨论了该法案的变化及其在数字服务背景下保护主体的权利，加强对用户的保护以及对强调数据运营商的泄密责任。修正案部分内容将于 9 月 1 日生效，本次修订的主要内容包括：

（1）从 2022 年 9 月 1 日起，运营商需要向 Roskomnadzor 报告用户信息泄露事件。运营商可以在 24 小时内报告，说明被泄露数据并指明联系人；或者在三天内报告内部检查结果和导致泄露的人员。

（2）从 2023 年 3 月 1 日起，运营商必须在开始数据跨境传输之前通知 Roskomnadzor，通知内容包括数据转移的对象、目的和具体信息。对于已经进行跨境传输的运营商，该义务立即生效。

（3）针对个人数据的处理，限制在以合同为目的。个人享有对其数据的控制权，包括是否同意接收处理信息、删除或销毁数据以及向第三方传输数据。

（4）向个人提供关于法律依据、处理数据的目的、数据转移过程和缘由、数据构成和接收来源的详尽信息的时限。从 9 月 1 日起，对此类请求的答复期限不得超过 10 个工作日，但如果有充分理由，该期限可再延长 5 个工作日。

26. 加拿大隐私专员办公室发布《确保加拿大数字身份生态系统隐私和透明度》

10 月 24 日，加拿大隐私专员办公室（Office of the Privacy Commissioner of Canada）发布《确保加拿大数字身份生态系统隐私和透明度》（Ensuring the Right to Privacy and Transparency in the Digital Identity Ecosystem in Canada）。文件指出，数字身份是数字社会的基本要素，也是公共服务现代化的基础。但数字身份生态系统的发展也会带来很多无法接受的后果，比如超出

必要、合理的范围收集个人信息，歧视风险增加，身份盗窃、欺诈等事件频发等。因此，联邦、省和地区的隐私专员致力于确保数字身份生态系统能负责任地设计和运行。

在数字身份生态系统中，文件要求，早期设计、开发、更新阶段就应当进行隐私影响评估；系统设计、功能和信息流对隐私的影响应当对系统的所有用户透明；不得创建中央数据库；数字识别不得用于可匿名提供给个人的信息或服务，适当情况下系统应当支持匿名和假名服务；在数字身份识别过程中应当坚持个人信息最小化原则，只收集、使用、披露或保留必要的信息。个人权利与救济方面，文件要求，个人能自愿参与数字身份生态系统；服务之间的信息交换应当以个人明确和知情同意为前提；个人对其信息有控制权；当发生侵权事件时，有权向具有足够资源和权力的独立机构请求赔偿。政府部门应当公开数字身份系统的目的、哪些个人信息将被使用、以及将被谁以何种方式使用；必要时通过现有隐私法加强数字治理；建立明确的责任机制，包括为监管机构提供权力和资源，并对不遵守规定施加适当的惩罚等。

27. 香港私隐专员公署发布《资讯及通讯科技的保安措施指引》

8 月 30 日，香港私隐专员公署发布《资讯及通讯科技的保安措施指引》，为资料使用者建议相关的资料保安措施，以协助遵从《个人资料（私隐）条例》（第 486 章）的规定。

指引建议：（1）采取资料管治和机构性措施，包括委任合适的领导人员负责资料保安，及提供足够的培训予工作人员；（2）在启用新系统和新应用程式前，以及在启用后定期进行资料保安风险评估；（3）建议一系列的技术上及操作上的保安措施；（4）资料使用者须采取合约规范方法或其他方法，以防止转移至资料处理者的个人资料在未获准许或意外的情况下被查阅、处理、删除、丧失或使用；（5）资料保安事故发生后采取补救措施，从而减轻对机构及受影响人士可能造成的伤害；（6）定期监察、评估及改善资料保安政策的遵从情况；（7）使用云端服务、自携装置，及便携式储存装置所应采取的资料保安措施。

28. 全国信安标委发布《网络安全标准实践指南—个人信息跨境处理活动安全认证规范》

6 月 24 日，全国信安标委发布《网络安全标准实践指南—个人信息跨境处理活动安全认证规范》。

指南依据有关政策法规要求，为落实《个人信息保护法》、建立个人信息保护认证制度提供认证依据。申请个人信息保护认证的个人信息处理者应当符合 GB/T 35273《信息安全技术 个人信息安全规范》的要求；对于开展跨境处理活动的个人信息处理者，还必须符合本指南的要求。指南从基本原则、个人信息处理者和境外接收方在跨境处理活动中应遵循的要求、个人信息主体权益保障等方面提出要求，为认证机构实施个人信息保护认证提供跨境处理活动认证依据，也为个人信息处理者规范个人信息跨境处理活动提供参考。

29. 国家互联网信息办公室发布《个人信息出境标准合同规定（征求意见稿）》

6 月 30 日，国家互联网信息办公室发布《个人信息出境标准合同规定（征求意见稿）》，同步发布《个人信息出境标准合同》。

征求意见稿共十三条，规定个人信息处理者依据《个人信息保护法》第三十八条第一款第（三）项，与境外接收方订立合同向中华人民共和国境外提供个人信息的，应当按照本规定签订个人信息出境标准合同。

征求意见稿规定，依据标准合同开展个人信息出境活动，应坚持自主缔约与备案管理相结合，防范个人信息出境安全风险，保障个人信息依法有序自由流动。个人信息处理者同时符合下列情形的，可以通过签订标准合同的方式向境外提供个人信息：（1）非关键信息基础设施运营者；（2）处理个人信息不满 100 万人的；（3）自上年 1 月 1 日起累计向境外提供未达到 10 万人个人信息的；（4）自上年 1 月 1 日起累计向境外提供未达到 1 万人敏感个人信息的。

30. 上海市发布《关于进一步促进和保障城市运行“一网统管”建设的决定》

5 月 24 日，上海市十五届人大常委会第四十次会议表决通过《关于进一步促进和保障城市运行“一网统管”建设的决定》。

决定规定，本市运用治理数字化功能，在疫情防控期间，实行个人疫情防

控信息核验措施（即“场所码”或“数字哨兵”等核验措施），核验个人健康信息。信息核验中采集、处理个人疫情防控信息应当遵守个人信息保护相关法律、法规的规定，采集的个人信息仅用于疫情防控需要，任何单位和个人不得泄露。“一网统管”建设相关部门和单位应当按照有关法律法规和安全技术标准，建立健全风险评估、安全审查、日常监控、应急处置等机制，严格落实网络安全等级保护制度，加强数据分类分级保护，依法履行个人信息保护义务。

（七）网络信息内容治理

1. 美国国防部发布《将社交媒体用于公共事务目的的官方用途》

8 月 15 日，美国国防部发布第 DODI 5400.17 号国防部指令《将社交媒体用于公共事务目的的官方用途》（Official Use of Social Media for Public Affairs Purposes）。

国防部首席信息官此前发布 DODI 8170.01《在线信息管理和电子消息》，为安全和适当地使用社交媒体提供政策指导。本次发布的指令则是该部门第一个针对社交媒体用于公共事务的全部门指导，除了详细说明国防部领导层在社交媒体实践中的作用和职责外，还为在官方社交媒体平台上生成及发布内容的部门人员提供指导。具体来说，该政策涉及国防部内部使用社交媒体的原则、关于社交媒体账户记录管理程序的指导，以及确保个人社交媒体账户不被歪曲或误解为官方账号等内容。

2. 美国加州通过《社交媒体平台：服务条款法》，要求提高社交媒体透明度

9 月 13 日，美国加州州长签署第 587 号议会法—《社交媒体平台：服务条款法》（AB-587 Social media companies: terms of service），要求提高社交媒体透明度，社交媒体平台应“在其平台上公开披露有关仇恨言论、错误信息、骚扰和极端主义的内容审核政策，并报告有关政策执行情况的数据”，以保护加州人免受在线传播的仇恨和虚假信息的影响。

该法要求 Facebook、Twitter 和 Instagram 等社交媒体平台在网上公布其服务条款并每年向州检察长提交两次报告。服务条款中应当规定平台上允许的

用户活动类型与可能受到约束的用户活动类型，以及平台可能采取的约束措施，如删帖和暂停账户。具体而言，半年度报告将公开披露平台关于仇恨言论、虚假信息、极端主义、骚扰和外国政治干预的内容审核政策，以及平台如何以及何时执行这些政策的关键指标和数据。如果平台违反这些规定中的任何一项，将受到民事处罚、罚款或司法部长/城市检察官的诉讼。

该法提出者表示，这是首例旨在打击极端主义的社交媒体透明立法。但这些透明度措施与其他几个提案类似，包括目前在德克萨斯州和佛罗里达州受阻的两项法律的部分内容。该法预计将从 2024 年 1 月开始生效，除非被阻止或受到严重挑战。

3. 《欧盟处理恐怖主义内容在线传播条例》生效

6 月 7 日，《欧盟处理恐怖主义内容在线传播条例》（EU Regulation on Addressing the Dissemination of Terrorist Content Online）生效并开始实施。条例提供了一个法律框架，以确保托管服务提供商在一小时内删除网上的恐怖主义内容。这一规定所包含的义务和保障措施将遏制恐怖分子在网上传播涉恐信息。与此同时，条例将加强删除网上恐怖主义内容措施的可追责性和透明性。

条例建立以下几项规则：（1）一小时规则：网络平台接到成员国当局发出的删除命令后，必须在一小时内删除恐怖主义内容；（2）强制要求网络平台在接触到恐怖主义内容时采取措施；（3）删除命令必须对该材料所包含的内容被认定为恐怖主义的原因进行正当解释；（4）规定强有力的保障措施，以确保网络平台充分尊重个人基本权利，如言论自由和知情权；（5）成员国有权对不遵守条例的行为进行制裁，并决定惩罚的级别。惩罚的级别应与侵权行为的性质成比例；（6）网络平台透明度义务，要求国家当局每年报告被删除的恐怖主义内容的数量、投诉和申诉的结果，以及对网络平台实施处罚的数量和类型。

条例重点规定以下内容：（1）托管服务提供商应履行合理且适当的注意义务，以解决通过其服务向公众传播恐怖主义内容的问题，并在必要时迅速删除或阻止对此类内容的访问；（2）成员国可以根据联合国法律并采取适当的措施以保障基本权利，尤其是在开放和民主社会下的言论自由和知情权，以查明并确保服务提供商立即删除恐怖主义内容，并促进成员国主管当局、服务提供商以及欧

洲刑警组织之间开展适当地合作。

4. 欧盟委员会发布《2022 年虚假信息实践守则》

6 月 16 日,欧盟委员会发布更新版的《2022 年虚假信息实践守则》(The 2022 Code of Practice on Disinformation）。

新守则包含 44 项承诺和 128 项具体措施，主要包括以下方面：（1）扩大守则参与者，使其不仅适用于大平台，还涉及各种不同的参与者，在减少虚假信息传播方面共同发挥作用；（2）确保虚假信息提供者不会从广告收入中受益，减少传播虚假信息的经济激励；（3）覆盖新的信息操纵行为，例如虚假账户、机器人或恶意深度伪造；（4）为用户提供更好的工具来识别、理解和标记虚假信息；（5）在欧盟成员国中扩大事实核查，同时确保事实核查人员的工作得到公平回报；（6）通过更好的打标签和明确赞助商等信息，确保用户可以轻松识别政治广告，确保政治广告透明；（7）通过提供更好的平台数据访问能力支持研究人员；（8）通过建立强有力的监控框架、要求平台定期报告守则履行情况，评估平台影响力。守则签署方将有 6 个月的时间来执行其已签署的承诺和措施，在 2023 年初将向委员会提供第一份实施报告；（9）建立透明度中心和工作组，以轻松、透明地概述本守则的实施情况，使守则能够适应未来并符合制定目的。

34 家平台签署了该守则，覆盖主要在线平台，包括 Meta、Google、Twitter、TikTok 和微软，以及各方参与者，如小型或专业平台、在线广告行业、广告技术公司、事实核查机构、民间机构等。

5. 欧盟《数字服务法》生效

11 月 16 日，欧盟《数字服务法》（Digital Services Act，简称 DSA）正式生效。

DSA 侧重从内容及形式等方面规范数字企业提供的服务,以更好地保护欧盟消费者。DSA 规定，在欧盟经营的大型门户网站和社交媒体公司必须加强对非法内容的审查和用户数据的保护,及时删除非法和有害的在线内容,包括仇恨言论、虚假信息和假货交易信息等。DSA 将拥有超过 4500 万用户的平台认定为“超大型在线平台（VLOPs）或超大型搜索引擎（VLOSEs）”，进一步强化此类主体义

务，包括对其服务在线风险进行年度评估。DSA 规定，违反 DSA 的企业可被处以全球营业额 6%的罚款，在屡次严重违规的情况下，还可被禁止在欧盟单一市场内运营。

DSA 生效后，在线平台将有 3 个月的时间（截止 2023 年 2 月 17 日）报告其网站上的最终活跃用户数量。根据这些用户数量，委员会将评估平台是否属于 VLOPs 或 VLOSEs。被认定为 VLOPs 或 VLOSEs 的，平台将有 4 个月的时间落实 DSA 规定的义务，包括进行并向委员会提供第一次年度风险评估报告。

6. 俄罗斯发布修正案，严惩故意公开传播俄罗斯武装部队虚假信息行为

3 月 4 日，俄罗斯总统普京正式签署《俄罗斯联邦刑法典及俄罗斯联邦刑事诉讼法典第 31 条和 151 条修正案》（О внесении изменений в Уголовный кодекс Российской Федерации и статьи ），自公布之日起生效。修正案包括刑法典补充内容、条文编排技术性调整、生效时间共 3 条，核心体现于刑法典补充内容：

（1）在现行《俄罗斯联邦刑法典》中新增第 207.3 条，引入“故意公开发布俄罗斯联邦武装部队相关虚假信息”的刑罚。根据该条规定，以报告来源可靠为幌子公开传播包含俄罗斯联邦武装部队数据的虚假信息的行为，构成犯罪。根据是否有特殊情节、危害后果严重程度，该条设置了三档不同处罚。一般情节的，将面临最低档处罚，即 70 万至 150 万卢布，或与行为人 1 年至 18 个月收入相当数额的罚款，或 1 年以下劳教、3 年以下强制劳动或监禁。利用职务便利，或有组织的团体，或出于政治、意识形态、种族、民族或宗教仇恨或敌意等公开传播上述信息的，将面临 300 万至 500 万卢布或与行为人 3 至 5 年收入相当数额的罚款，或 5 年以下的强制劳动并剥夺 5 年以下担任某些职位或从事某些活动的权利，或处以 5 年至 10 年的监禁并剥夺 5 年内担任某些职务或从事某些活动的权利。上述行为造成严重后果的，将面临 10 至 15 年监禁，并剥夺 5 年以下担任某些职位或从事某些活动的权利。

（2）在现行《俄罗斯联邦刑法典》中新增第 280.4 条，引入“以保护俄罗斯联邦及其公民的利益、维护国际和平与安全为名诋毁俄罗斯武装力量的公开行动”的刑罚。根据该条规定，一年内因以保护俄罗斯联邦及其公民的利益、维护

国际和平与安全为名诋毁俄罗斯武装力量公开行动，包括公开呼吁防止使用俄罗斯联邦武装力量，被追究行政责任后再犯的，构成犯罪，将面临 10 万至 30 万卢布或与行为人 1 至 2 年收入相当数额的罚款，或 3 年以下的强制劳动、拘留 4 至 6 个月、3 年以下的监禁并被剥夺担任某些职务或从事某些活动的权利。上述行为过失导致导致公民健康、财产损害，或公民死亡，或大规模违反公共秩序或公共安全，或干扰生活配套设施、交通或社会基础设施、信贷机构、能源、工业或通讯设施的运作或使其停止运作的，将面临 30 万至 100 万卢布或与行为人 3 至 5 年收入相当数额的罚款，或 5 年以下监禁并剥夺期内担任某些职务或从事某些活动的权利。

（3）在现行《俄罗斯联邦刑法典》中新增第 284.2 条，引入“呼吁对俄罗斯联邦、俄罗斯联邦公民或俄罗斯法人采取限制措施”的刑罚。根据该条规定，一年内因呼吁外国、州、联盟或跨国组织对俄罗斯联邦实施或延长政治或经济制裁，对俄罗斯公民或法人实体采取限制性措施，被追究行政责任后再犯的，构成犯罪。将面临 50 万卢布以下，或与行为人 3 年收入相当数额以下的罚款，或 3 年以下监禁，或 3 年以下强制劳动，或 6 个月拘留，或 3 年以下监禁并处 20 万卢布以下或与行为人 1 年收入相当数额以下的罚款。

7. 俄罗斯发布修正案：故意公开传播俄海外国家机构相关谣言的人将承担刑事责任

3 月 26 日，俄罗斯总统普京签署 No.9712-8 号联邦法《关于修改<俄罗斯联邦刑法典>和<俄罗斯联邦刑事诉讼法典>第 150 和 151 条的修正案》与 No. 9732-8 号联邦法《关于<俄罗斯联邦行政违法法典>第 8.32 条和 20.3.3 条的修正案》，规定制造俄罗斯海外国家机构相关谣言的人将承担刑事责任，量刑与制造俄武装力量相关谣言的人相同。此外，将对诋毁俄海外机构工作人员的人进行行政罚款。

No.9712-8 号联邦法规定，以冒充可靠消息的方式故意公开传播“俄罗斯联邦国家机构在俄罗斯联邦境外行使权力”相关虚假信息的，构成犯罪。具体裁量标准如下：（1）以保护俄罗斯联邦及其公民的利益、维护国际和平与安全为名，故意传播虚假信息的，将被处以 70 万至 150 万卢布罚金或 3 年以内有期徒刑；（2）利用职务便利，或团伙犯罪，或人为制造指控证据，或出于雇佣动机，或

出于政治、意识形态、种族、民族或宗教仇恨或敌意，故意传播虚假信息的，将被处以300万至500万卢布罚金或5年至10年有期徒刑。此外，旨在诋毁俄罗斯联邦国家机构在俄罗斯联邦境外行使权力的公共行为，构成犯罪的，将被处以10万至30万卢布罚金，或3年以内有期徒刑。若行为造成危害后果的，将被处以5年以内有期徒刑。

No.9732-8号联邦法规定，旨在诋毁俄罗斯联邦国家机构在俄罗斯联邦境外行使权力的公共行为的，如不触犯刑法条例，将对涉事公民处以3万至5万卢布罚款，对涉事官员处以10万至20万卢布罚款，对于涉事法人处以30万至50万卢布罚款。

8. 土耳其议会批准第7418号法《<新闻法（修正案）>和部分法律》

10月13日，土耳其议会批准第7418号法《<新闻法（修正案）>和部分法律》(BASIN KANUNU İLE BAZI KANUNLARDA DEĞİŞİKLİK YAPILMASINA DAİR KANUN)，加强土耳其社交媒体虚假信息管控并明确相应刑事责任。

该法第29条规定，在《土耳其刑法典》中引入“禁止公开传播误导性信息”条款，凡公开传播有关国家内部和外部安全、公共秩序和大众健康的不实信息，引起公众焦虑、恐惧或恐慌的，应处以一年以上三年以下有期徒刑。

9. 乌干达总统签署《计算机滥用（修正案）法》

10月13日，乌干达总统约韦里·穆塞韦尼签署《计算机滥用（修正案）法》（Comptter Misuse（Amendment）Bill，2022），正式将该国的一系列数字活动定为刑事犯罪。该法最初由2022年7月19日引入，9月8日获得议会通过。

修正案禁止以下行为：（1）使用社交媒体发布、分发或共享法律禁止发布的内容；（2）使用伪装、虚假身份信息；（3）与在线骚扰有关的活动；（4）利用网络编写、发送或共享可能嘲笑、贬低他人、部落、宗教或性别的信息。

该修正案备受舆论批评，被视为用作压制言论自由的工具，乌干达信息和通信技术部常务秘书曾表示反对该修正案。目前尚不清楚何时开始执法。

10. 国家互联网信息办公室发布《互联网信息服务深度合成管理规定（征求意见稿）》

1 月 28 日，国家互联网信息办公室发布《互联网信息服务深度合成管理规定（征求意见稿）》。

征求意见稿强调，深度合成服务提供者应当落实信息安全主体责任，建立健全算法机制机理审核、用户注册、信息内容管理、数据安全和个人信息保护、未成年人保护、从业人员教育培训等管理制度，具有与新技术新应用发展相适应的安全可控的技术保障措施。深度合成服务提供者应当加强深度合成信息内容管理，采取技术或者人工方式对深度合成服务使用者的输入数据和合成结果进行审核；建立健全用于识别违法和不良深度合成信息内容的特征库，完善入库标准、规则和程序；对违法和不良信息依法采取相应处置措施，并对相关深度合成服务使用者依法依约采取警示、限制功能、暂停服务、关闭账号等处置措施。

11. 国家互联网信息办公室发布修订后的《移动互联网应用程序信息服务管理规定》

6 月 14 日，国家互联网信息办公室发布新修订的《移动互联网应用程序信息服务管理规定》，自 2022 年 8 月 1 日起施行。

《移动互联网应用程序信息服务管理规定》自 2016 年 8 月 1 日施行以来，对于维护网络信息内容生态，保护公民、法人和其他组织的合法权益发挥了积极作用。但随着移动应用程序快速发展、广泛应用，新情况新问题不断出现，需要适应形势发展进行修订完善。新规定共 27 条，包括信息内容主体责任、真实身份信息认证、分类管理、行业自律、社会监督及行政管理等条款。

新规定要求应用程序提供者和应用程序分发平台应履行信息内容管理主体责任，建立健全信息内容安全管理、信息内容生态治理、数据安全和个人信息保护、未成年人保护等管理制度，确保网络安全，维护良好网络生态。应用程序提供者和应用程序分发平台应当按照要求，切实履行责任和义务，依照相关法律法规加强自身管理，主动接受社会监督，不断促进应用程序信息服务健康有序发展。

12. 国家互联网信息办公室发布《互联网用户账号信息管理规定》

6 月 27 日，国家互联网信息办公室发布《互联网用户账号信息管理规定》，自 2022 年 8 月 1 日起施行。

规定要求互联网信息服务提供者为互联网用户提供信息发布、即时通讯等服务的，应当进行真实身份信息认证；应当对互联网用户在注册时提交的和使用中拟变更的账号信息进行核验；应当在账号信息页面展示合理范围内的互联网用户账号的互联网协议地址归属地信息，便于公众为公共利益实施监督。互联网信息服务提供者应对履行账号信息管理主体责任，配备与服务规模相适应的专业人员和技术能力；建立健全并严格落实真实身份信息认证、账号信息核验、信息内容安全、生态治理、应急处置、个人信息保护等管理制度；建立健全互联网用户账号信用管理体系。

13. 国家互联网信息办公室发布《互联网弹窗信息推送服务管理规定（征求意见稿）》

9 月 9 日，国家互联网信息办公室、工信部、国家市场监督管理总局联合发布《互联网弹窗信息推送服务管理规定》，自 2022 年 9 月 30 日起施行。规定立足当前实际，紧盯弹窗新闻信息推送、弹窗信息内容导向、弹窗广告等重点环节，着力解决利用弹窗违规推送新闻信息、弹窗广告标识不明显、广告无法一键关闭、恶意炒作娱乐八卦、推送频次过多过滥、推送信息内容比例不合理、诱导用户点击实施流量造假等问题。

14. 国家互联网信息办公室发布《互联网跟帖评论服务管理规定（修订草案征求意见稿）》

11 月 16 日，国家互联网信息办公室发布新修订的《互联网跟帖评论服务管理规定》，自 2022 年 12 月 15 日起施行。新规定共 16 条，重点明确了跟帖评论服务提供者跟帖评论管理责任、跟帖评论服务使用者和公众账号生产运营者应当遵守的有关要求等内容。

（八）网络犯罪防治

1. 美国正式通过《优化网络犯罪度量法》

5月5日，美国总统拜登签署《优化网络犯罪度量法》（Better Cybercrime Metrics Act），旨在提升网络犯罪数据可见性、提高网络犯罪打击效率。总体来看，该法从网络犯罪分类、网络犯罪报告、全国犯罪被害调查、网络犯罪指标研究四大维度出发，综合改善联邦政府“追踪、衡量、分析、起诉网络犯罪的方式”，帮助执法机构更好识别网络安全威胁、防范勒索攻击、起诉网络犯罪案件。

该法要点包括：（1）司法部与国家科学院签订协议，共同制定可供执法部门使用的网络犯罪分类方法；（2）建立网络犯罪专门类别，确保国家突发事件报告系统（或任何后续系统）包含来自联邦、州和地方官员的网络犯罪报告；（3）调查网络犯罪被害情况，将网络犯罪相关问题纳入全国犯罪被害调查范畴；（4）评估当前网络犯罪报告机制有效性，剖析所报告的网络犯罪数据与其他类型犯罪数据之间的差异。

2. 美国签署《<网络犯罪公约>关于加强电子证据合作和披露的第二附加议定书》

5月12日，美国司法部代表美国政府签署《<网络犯罪公约>关于加强电子证据合作和披露的第二附加议定书》（Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence），这是一项旨在保护公民免受网络犯罪侵害并追究网络犯罪分子责任的多边条约。

《第二附加议定书》回应了国家之间以及国家与私营部门之间开展更多、更有效合作的需求，澄清了“服务提供商”能够直接向其他国家的主管当局提供其掌握的数据情况。该条约提供了加强合作和电子证据披露的方法，例如与服务提供商和注册商的直接合作、获取用户信息和流量数据的有效手段、紧急情况下的立即合作或联合调查等。

3. 美国司法部修订依据《计算机欺诈和滥用法》提起违规指控的政策，将不对“白帽黑客”追究责任

5 月 19 日，美国司法部宣布修订依据《计算机欺诈和滥用法》（CFAA）提起违规指控的政策，将不对“白帽黑客”追究责任。

司法部首次阐明 CFAA 不应被用来针对“白帽黑客”。司法部的新备忘录澄清了“诚信安全研究”不会被起诉的含义：“诚信安全研究”指仅为诚信测试、调查和/或纠正安全缺陷或弱点的目的而访问计算机，而该等活动的进行方式旨在避免对个人或公众造成任何伤害，以及从该活动中获得的信息主要用于促进被访问计算机所属的设备、机器或在线服务类别的安全性，或用于使用这些设备、机器或在线服务的人的安全性。它还指出，任何为勒索目的进行的“研究”都不能算作善意。

4. 美司法部发布《2022 年-2026 年战略计划》

7 月 1 日，美国司法部（DoJ）发布《2022 年-2026 年战略计划》（FYs 2022-2026 Strategic Plan），将提升网络安全和打击勒索攻击作为“保护美国国家安全”的战略目标。

提升网络安全方面，DOJ 做出以下承诺：打击所有类型网络攻击团体，包括单独行动者、跨国犯罪集团、“民族国家”和恐怖分子支持的团体；破坏并拆除网络攻击者使用的网络基础设施；没收网络攻击所得财产等。打击勒索攻击方面，DOJ 表示将提高案件处理效率，提升其在 72 小时内对勒索攻击做出反应的能力；将 DOJ 采取扣押或没收手段的勒索攻击结案数量增加 10%。

5. 欧盟 EDPB 就《<网络犯罪公约>关于加强合作和披露电子证据的第二项附加议定书》表明立场

2 月 22 日，欧盟数据保护委员（EDPB）会发布公开信，就《<网络犯罪公约>关于加强合作和披露电子证据的第二项附加议定书》表明立场。EDPB 认为，根据议定书向第三国传输的个人数据保护水平必须基本上等同于欧盟保护水平。EDPB 欢迎议定书中包含的保障措施，例如关于个人信息保护监督的规定。然而，EDPB 感到遗憾的是议定书作为一般性规则，不能保证免费向个人提供访问信息。

6. 《欧洲刑警组织条例》修正案生效

6 月 28 日，《欧洲刑警组织条例》修正案，即《欧洲议会和理事会 2022 年 6 月 8 日第 2022/991 号条例（EU），关于修订第 2016/794 号条例（EU），强化欧洲刑警组织与私人合作、为支持刑事调查的个人数据处理能力以及在研究和创新中的作用》（REGULATION （EU）2022/991 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol’s cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol’s role in research and innovation）正式生效。修正案主要作出以下修正：

（1）支持刑事调查。修正案规定，只要是为了支持特定的正在进行的犯罪调查，欧洲刑警组织（Europol）能够在不明确数据主体类别（DSC）的情况下处理个人数据。这是因为在处理大型复杂数据集时，只有在提取和分析相关信息后才能识别出 DSC。

（2）研究与创新。Europol 将支持欧盟成员国使用新兴技术、探索新方法并开发通用技术解决方案——包括在 AI 领域。其中，研究方向之一是为研发目的而处理个人数据的行为给予明确的法律依据，但处理个人数据时应当采取严格的数据保护措施。

（3）与私营主体合作。私营主体持有越来越多的可能与刑事调查相关的数据。修正案规定，Europol 将能够直接从私营主体处接收（receive）数据。修订案还特别规定了在处理网络危机或打击儿童性虐待材料在线传播时，Europol 应如何与私营主体合作。

（4）申根信息系统。Europol 将支持欧盟成员国处理由第三国或国际组织传输的数据，并建议成员国在申根信息系统中上传安全警报。

（5）自主调查。Europol 的执行主任可以提议对仅涉及一个成员国但影响欧盟政策所涵盖的共同利益的特定犯罪进行国家调查。是否遵守这一提议由成员国当局决定。

（6）基本权利官。在 Europol 现有的独立数据保护官（DPO）之外，修正案还引入了一个独立的基本权利官（FRO）职位。

（7）欧盟数据保护专员公署（EDPS）。自 2017 年 5 月 1 日起，EDPS 承担

了监督 Europol 个人数据处理行为的职责。修正案进一步强化 EDPS 的监督职能。

6 月 27 日，修正案生效的前一天，EDPS 发布消息称，修正案削弱了数据保护的基本权利，并不能确保对 Europol 的适当监督。EDPS 认为，修正案允许 Europol 在特定情况下处理大型数据集，导致该机构处理和存储的个人数据量大幅增加，但权力扩大的同时并没有建立强有力的数据保护措施，从而有效监督该机构的新权力。为此，EDPS 表示将与 Europol 管理委员会进行正式磋商。

7. 澳大利亚发布《2022 年打击网络犯罪国家计划》

3 月 21 日，澳大利亚发布《2022 年打击网络犯罪国家计划》（National Plan to Combat Cybercrime 2022），旨在为澳大利亚提供一个安全、公正和繁荣的网络世界。计划主要围绕预防与保护，调查、打击与起诉，以及恢复三方面展开。

预防与保护方面采取的具体行动包括：（1）将澳大利亚营造成网络罪犯的敌对环境，确保他们不会从针对澳大利亚的攻击中获利；（2）支持发挥行业领导力，预防网络犯罪威胁，并考虑如何通过设计理念加强产品和服务的安全性；（3）利用学术界和前沿研发，应对快速变化的威胁环境；（4）建立公民网络安全自信，改善网络安全习惯，保护自己免受网络犯罪威胁；（5）与国际伙伴合作，加强对网络犯罪威胁的全球应对，包括通过强有力的国际框架，确保执法机构拥有调查和起诉网络犯罪的机制和电子证据，同时尊重人权和法治；（6）适当唤回（calling out）愿意支持或为网络罪犯提供避风港的人。

调查、打击与起诉方面采取的具体行动包括：（1）加强联邦、州和地区执法机构、检察机构和其他政府机构之间的协调；（2）继续加强公共和私营部门之间的伙伴关系；（3）支持执法部门获取外国司法管辖区的电子证据，这些网络罪犯通常在海外活动；（4）确保执法能力对技术、数字服务和平台的快速发展做出反应；（5）利用政府在未来几年所做的投资，提高应对恶意网络威胁的能力；（6）确保澳大利亚的网络犯罪立法保持世界领先地位；（7）加强网络犯罪数据收集、报告和情报。

恢复方面采取的具体行动包括：（1）继续与执法部门和私营部门合作，在受害者中建立关于如何获取恢复资源和如何报告事件的意识，尽可能简化获取；（2）执法部门和行业之间继续努力阻止非法和欺诈性支付；（3）审查事件后反

馈机制，确保受害者的反馈尽可能有效；（4）继续支持专门从事事故后支持服务的组织。

同日，内政部宣布启动一个耗资 8900 万澳元的网络犯罪中心，支持网络犯罪打击工作，防止网络犯罪分子欺骗、窃取和欺骗澳大利亚公民。

8. 澳大利亚《2022 年电信服务提供商（客户身份验证）判定规则》生效

6 月 30 日，澳大利亚《2022 年电信服务提供商（客户身份验证）判定规则》（Telecommunications Service Provider(Customer Identity Authentication) Determination 2022）生效。规则要求：

（1）阅读并理解本规则。电信服务提供商有责任了解并遵守本规则规定的义务。如果有外包商，电信服务提供商有责任确保外包商遵守本规则。

（2）识别客户高风险交易。具体包括 SIM 卡交换、从后付费到预付费服务的转移、所有权变更、向帐户添加额外的电话服务、为海外客户激活服务、购买额外的手机、限制国际移动设备标识符或永久设备标识符。除列出的这些交易类型外，电信服务提供商可以根据自身业务范围识别更多的高风险交易类型。

（3）对高风险交易实施多因素身份验证（MFA）。MFA 至少需要 2 重身份验证，例如帐户用户名和密码，以及发送到客户手机号或经过验证的移动应用程序的唯一验证码或安全链接。

（4）向客户提供有关身份验证过程的详细信息。在 MFA 流程中使用唯一验证码或安全链接时，必须包含以下内容，以向客户提示风险：1）他们的电信服务已开始进行高风险交易；2）不要共享唯一验证码或安全链接；3）如果客户没有发起该高风险交易，客户可以做什么。

（5）识别并保护风险客户。开发系统以识别面临欺诈风险的客户并为其提供欺诈缓解保护，例如当客户提出账户更改要求时向他们发送通知、标记他们的帐户以表明高风险性、使用特定渠道完成 MFA、暂停部分交易、仅向其授权代表发送通知等。这些欺诈缓解保护也必须提供给认为自己面临欺诈风险的客户。

（6）客户提醒。应让客户知道 MFA 将用于所有高风险交易，还要让客户知晓应向电信服务提供商和银行报告可疑行为。

（7）保留记录至少 1 年以证明合规性。

9. 危地马拉国会通过《预防和保护网络犯罪法》

8月4日，危地马拉共和国国会全体会议宣布批准第39-2022号法《预防和保护网络犯罪法》（Ley de Prevención y Protección contra la Ciberdelincuencia），旨在保护危地马拉人的个人数据，并将网络犯罪定为刑事犯罪。该法要求建立计算机事件技术响应机构安全中心，采取行动防范针对数据或计算机系统的攻击，规范公共部门与私营组织之间的关系与合作。

该法第8条规定“非法访问罪”：故意非法访问全部或部分计算机系统，且违反安全措施进行访问，或以获取计算机数据或其他犯罪意图为目的进行访问的，构成非法访问罪，处三至五年有期徒刑，并处罚款；第13条规定“计算机伪造罪”：未经授权故意增加、更改、捕捉、删除存储在计算机系统中的数据的，构成计算机伪造罪，处三至七年有期徒刑，并处罚款。

10. 银保监发布《关于防范以“元宇宙”名义进行非法集资的风险提示》

2月18日，银保监处置非法集资部际联席会议办公室发布《关于防范以“元宇宙”名义进行非法集资的风险提示》。公告指出，近期，一些不法分子蹭热点，以“元宇宙投资项目”“元宇宙区块链游戏”“元宇宙房地产”“元宇宙虚拟币”等名目吸收资金，涉嫌非法集资、诈骗等违法犯罪活动。上述活动打着“元宇宙”旗号，具有较大诱惑力、较强欺骗性，参与者易遭受财产损失。

11. 中共中央办公厅、国务院办公厅发布《关于加强打击治理电信网络诈骗违法犯罪工作的意见》

4月18日，中共中央办公厅、国务院办公厅发布《关于加强打击治理电信网络诈骗违法犯罪工作的意见》，对加强打击治理电信网络诈骗违法犯罪工作作出安排部署。

意见要求，要依法严厉打击电信网络诈骗违法犯罪。坚持依法从严惩处，形成打击合力，提升打击效能；坚持全链条纵深打击，依法打击电信网络诈骗以及上下游关联违法犯罪；进一步强化法律支撑，为实现全链条打击、一体化治理提供法治保障。要加强行业监管源头治理。建立健全行业安全评估和准入制度；加强金融行业监管，及时发现、管控新型洗钱通道；加强电信行业监管，严格落

实电话用户实名制；加强互联网行业监管；完善责任追究制度，建立健全行业主管部门、企业、用户三级责任制；建立健全信用惩戒制度，将电信网络诈骗及关联违法犯罪人员纳入严重失信主体名单。意见还要求，要强化属地管控综合治理，加强犯罪源头地综合整治。

12. 最高人民检察院发布《关于加强刑事检察与公益诉讼检察衔接协作严厉打击电信网络犯罪加强个人信息司法保护的通知》

6 月 21 日，最高人民检察院发布《关于加强刑事检察与公益诉讼检察衔接协作严厉打击电信网络犯罪加强个人信息司法保护的通知》。

通知要求，深入开展依法打击行业“内鬼”泄露公民个人信息违法犯罪工作，积极配合“清朗”系列专项行动，探索积累常态化监督办案的典型经验。聚焦重点行业、重点领域、重点群体开展监督办案，包括处理大规模个人信息特别是个人敏感信息，容易产生个人信息泄露风险的重点行业；金融、电信、互联网、就业招聘行业中容易产生电信网络诈骗违法犯罪风险的重点领域；容易受到电信网络诈骗违法犯罪侵害的老年人、在校学生、未成年人等重点群体。在严厉打击刑事犯罪的同时，充分发挥公益诉讼检察职能，依法追究违法主体的民事责任，督促行政机关履职尽责，增强惩治预防效能。针对电信网络诈骗违法犯罪和个人信息公益损害呈现跨行政区划的特点，进一步加强大数据赋能，探索通过罪名、领域、行业等关键词自动抓取和智能算法技术，改革案件线索产出的供给侧，打破业务条线之间的数据壁垒。

13. 两高一部联合发布《关于办理信息网络犯罪案件适用刑事诉讼程序若干问题的意见》

8 月 30 日，最高人民法院、最高人民检察院、公安部联合发布《关于办理信息网络犯罪案件适用刑事诉讼程序若干问题的意见》。

意见主要内容包括：（1）进一步规范信息网络犯罪案件的管辖。意见明确信息网络犯罪案件的犯罪地包括用于实施犯罪行为的网络服务使用的服务器所在地，网络服务提供者所在地，被侵害的信息网络系统及其管理者所在地，犯罪过程中犯罪嫌疑人、被害人或者其他涉案人员使用的信息网络系统所在

地，被害人被侵害时所在地以及被害人财产遭受损失地等；（2）进一步规范信息网络犯罪案件的取证；（3）进一步规范信息网络犯罪案件的证据审查；（4）进一步规范信息网络犯罪案件涉案财物处理。

14. 我国正式通过《反电信网络诈骗法》

9 月 2 日，第十三届全国人大常委会第三十六次会议表决通过《反电信网络诈骗法》，自 2022 年 12 月 1 日起施行。该法共七章五十条，包括总则、电信治理、金融治理、互联网治理、综合措施、法律责任等内容。

作为一部“小切口”的专门立法，该法在总结反诈工作经验基础上，着力加强预防性法律制度构建，加强协同联动工作机制建设，加大对违法犯罪人员的处罚，推动形成全链条反诈、全行业阻诈、全社会防诈的打防管控格局。

（九）新技术新应用发展与安全

1. 美国白宫发布《推动美国政府向网络安全零信任原则迈进备忘录》

1 月 26 日，美国白宫发布《推动美国政府向网络安全零信任原则迈进备忘录》（Moving the U.S. Government Toward Zero Trust Cybersecurity Principles），旨在落实 2021 年 5 月发布的第 14028 号行政令，要求联邦政府能在未来两年内逐步采用“零信任”安全架构，以抵御现有威胁并增强整个联邦层面的网络防御能力。

备忘录提出制定联邦政府零信任架构战略，要求各级机构在 2024 财年结束之前达成各项既定网络安全标准与目标。零信任战略中的核心要素包括通过强大的多因素身份验证机制、改进网络钓鱼防御水平、整合各机构身份系统、加密进出流量、将内网环境视为不受信环境，同时加强应用程序安全以更好地保护数据等内容。

在这项新战略中，备忘录还提出以下几项具体展望：（1）联邦政府雇员应拥有由机构负责管理的账户，供他们访问日常工作中需要接触的一切信息，同时可靠地保护雇员免受针对性、复杂网络钓鱼攻击的影响；（2）联邦政府雇员使用的工作设备将受到持续跟踪与监控，而且在授予内部资源访问权限时，也应考

虑到设备的具体安全状况；（3）各代理系统间相互隔离，往来于不同系统及同一系统内部的网络流量应经过可靠加密；（4）业务应用程序应经过内部与外部测试，保证可通过互联网安全交付给雇员；（5）联邦政府各安全团队及数据团队应合作规划数据类别与安全规则，实现对敏感信息的自动检测，阻断一切未经授权的访问活动。

2. 美国白宫发布《确保数字资产负责任发展的行政令》

3 月 9 日，美国总统拜登签署《确保数字资产负责任发展的行政令》（Executive Order on Ensuring Responsible Development of Digital Assets），指示联邦机构采用全面政府手段研究加密货币带来的潜在风险，在此基础上利用数字资产及其基础技术的潜在利益，并考虑创建美国央行数字货币。这是美国历史上第一份针对数字资产领域采取全面措施的行政令，包括政策、目标、协调、定义等十个章节。

行政令指出数字资产为金融网络相关犯罪活动提供便利，金融活动中越来越多地使用数字资产增加洗钱、恐怖主义和扩散融资、欺诈和盗窃计划以及腐败等犯罪的风险。这些非法活动凸显了对数字资产的使用进行持续审查的必要性。

3. 美国白宫发布《关于加强国家量子倡议咨询委员会的行政命令》

5 月 4 日，美国白宫发布《关于加强国家量子倡议咨询委员会的行政命令》（Executive Order on Enhancing the National Quantum Initiative Advisory Committee），将通过加强国家量子倡议咨询委员会来进一步推动实现美总统对促进尖端科学技术突破的承诺。

为确保《国家量子倡议法》（NQI）计划和国家从不同的专家组和利益相关者处获得证据、数据和观点，特成立国家量子倡议咨询委员会。根据 NQI 法，委员会应就国家量子计划向总统、国家科学技术委员会（NSTC）量子信息科学小组委员会（SCQIS）和 NSTC 量子科学的经济和安全影响小组委员会（ESIX）提供建议。行政令中，美国政府希望通过进一步推动总统促进尖端科学技术突破的承诺来促进量子信息科学的进步。行政令将咨询委员会直接置于白宫的权力之下，确保总统、国会、联邦部门和机构以及公众获得最新、最准确和最具相关性的信息，

推动美国决策的发展，提升技术优势。

4. 美国白宫发布《关于促进美国在量子计算领域领导地位的同时降低易受攻击的密码系统风险的国家安全备忘录》

5月4日，美国白宫发布《关于促进美国在量子计算领域领导地位的同时降低易受攻击的密码系统风险的国家安全备忘录》(National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems），概述了本届政府与量子计算相关的政策和举措。备忘录确定了保持国家在量子信息科学（QIS）方面的竞争优势所需的关键步骤，同时降低量子计算机对国家网络、经济和国家安全的风险。备忘录具体内容包括：

（1）政策。为了平衡量子计算上的竞争机会与潜在风险，本届政府的政策是：1）通过持续投资、合作伙伴以及平衡的技术促进和保护，保持美国在QIS中的领导地位；2）通过及时、有效地将国家密码系统迁移到可对抗量子密码的系统，以减轻密码分析破解专用量子计算机（CRQCs）的威胁。同时，备忘录指出，随着量子计算技术及其风险的成熟，未来可能需要更多的政策指导和指令。

（2）提升美国领导地位。美国奉行“全政府参与、全社会参与”战略，从而更好地利用QIS的经济和科学效益以及后量子密码提供的安全增强措施。这一战略将需要对QIS研发采取协调、积极的方法，扩大教育和劳动力计划，并专注于发展和加强与工业界、学术界、盟友和志同道合的国家的合作关系。

（3）降低加密风险。任何现有使用公共标准公钥加密算法的系统或计划过渡到这种加密算法的系统，都可能容易受到来自量子计算机的攻击。为了降低这种风险，美国必须优先考虑，如何及时和公平地将现有通行的加密算法系统升级到后量子密码，目标是到2035年尽可能多地减轻量子风险。目前，NIST和国家安全局正在制定后量子密码技术标准，预计第一套标准将于2024年公开发布。

（4）保护美国技术。美国政府必须努力保护相关的量子研发和知识产权。尽管保护机制会有所不同，但可能包括反情报措施、有针对性的出口管制，以及对工业界和学术界开展的有关网络犯罪和知识产权盗窃威胁的教育活动。备忘录明确美国应确保美国开发的量子技术免受对手盗用。联邦执法机构和其他相关机

构应酌情调查和起诉参与窃取量子商业机密或违反美国出口管制法律的行为人。为支持保护敏感信息的工作，联邦执法机构应与负责开发和推广量子技术的机构交换相关威胁信息。

5. 美国NIST发布《规划零信任架构：联邦管理者的规划指南》

5月6日，美国国家标准与技术研究院（NIST）发布《规划零信任架构：联邦管理者的规划指南》（Planning for a Zero Trust Architecture：A Planning Guide for Federal Administrators）。

指南将“零信任”定义为在规划和实施企业架构时使用的一组网络安全原则，这些原则适用于端点、服务和数据流。指南指出，零信任不是单一的技术解决方案，而是整体的网络安全战略和操作实践。零信任是企业网络安全的整体方法，需要管理人员、IT人员和一般企业用户的支持。指南为正在向零信任架构迁移的管理员和操作人员介绍了NIST风险管理框架（RMF）的概念，还提供了一个整体的过程来管理系统和组织的网络安全和隐私风险。

6. 美国国防部发布《负责任的人工智能战略及实现途径》

6月22日，美国国防部发布《负责任的人工智能战略及实现途径》（U.S. Department of Defense Responsible Artificial Intelligence Strategy and Implementation Pathway），指导国防部制定实施AI基本原则的战略，及如何利用AI的框架。

文件要求：（1）调整管理结构和流程，持续监督国防部AI使用；（2）系统操作员需达到标准水平的技术熟练程度，以创建可信的AI系统和AI赋能系统；（3）考虑AI采购风险，并使AI开发速度满足国防部需求；（4）使用需求验证程序，确保AI能力与作战需求保持一致，同时解决相关的AI风险；（5）通过国内和国际合作促进对设计、开发、部署和使用负责任AI的共同理解；（6）确保所有国防部AI人员理解实施AI的技术、开发过程和操作方法。

7. 美国CISA发布第二版《云安全技术参考架构指南》

6月23日，美国网络安全和基础设施安全局（CISA）发布第二版《云安全

技术参考架构指南》（Cloud Security Technical Reference Architecture），通过解释共享服务、云安全状态管理等内容来指导机构安全迁移到云。指南侧重于更安全地使用公共云，提高联邦政府识别、检测、保护、响应和从网络事件中恢复的能力。CISA 指出，虽然指南是为联邦机构制定的，但可供所有迁移到云环境的组织使用，这些组织应采用其中的做法来最有效地管理组织风险。

8. 美国加州发布行政令，促进区块链和加密货币使用和监管

5 月 4 日,美国加州州长签署《N-9-22 号行政令》(Executive Order N-9-22)，为加强和规范该州的加密货币行业奠定基础。行政令的目标是“为在区块链中运营的公司创造一个透明和统一的商业环境”，以平衡消费者的利益和风险。加州此举使其成为美国首个启动官方措施研究如何监管数字货币的州。

行政令呼吁加州州长商业和经济发展办公室（GO-Biz）与该州的金融保护和创新部（DFPI）以及商业、消费者服务和住房局（BCSH）合作，共同负责设计“潜在的区块链应用程序和风险投资”，其中可能包括“私营部门、学术界和社区的应用程序”。它还命令 DFPI 制定加密货币的监管方法，创建消费者保护措施，并制作教育手册，让加州居民了解与加密货币相关的风险和收益。

9. 美国 NSA 发布《商业性国家安全算法组件 2.0》

9 月 7 日，美国国家安全局（NSA）发布《商业性国家安全算法组件 2.0》（Commercial National Security Algorithm Suite 2.0/CNSA 2.0），旨在帮助美国政府及其他运维或研制国家安全系统（National Security Systems）的利益相关方应对量子计算时代的密码安全挑战。

NSA 表示，将密码系统升级至可抵抗量子计算机破解的水平，需要美国政府、国家安全系统所有者及运营者、相关产业的通力合作。NSA 希望该文件的发布能帮助各相关方更高效地就向后量子密码系统迁移。该文件推荐：① 软件及固件签名使用 SP 800-208 文件中确定的 Leighton-Micali Signature（LMS）和 Xtended Merkle Signature Scheme（XMSS）密码算法；② 对称密钥密码算法使用美国联邦信息处理标准（FIPS）PUB 197 和 PUB 180-4 确定的 AES（256 位密钥）、SHA（384 或 512 位密钥）算法；③ 通用抗量子计算机破

解的公钥密码算法推荐新的CRYSTALS-Kyber和CRYSTALS-Dilithium算法。

NSA提出：即日起开始升级软件及固件签名算法，到2025年实现所有新软件和新固件使用推荐的密码算法进行签名，到2030年所有软件和固件均使用新标准密码算法进行签名；Web浏览器/服务器和云服务应在2025年前开始支持推荐的密码算法，至2030年全面使用新标准密码算法；虚拟私有网络、路由器等传统网络设备应在2026年前开始支持推荐的密码算法，至2030年全面使用新标准密码算法；操作系统应在2027年前开始支持推荐的密码算法，至2033年全面使用新标准密码算法；其他定制应用及老旧系统应在2033年前完成升级或退出使用。

10. 美国白宫发布《人工智能权利法案蓝图：让自动化系统服务于美国人民》

10月4日，美国白宫科技政策办公室发布《人工智能权利法案蓝图：让自动化系统服务于美国人民》（Blueprint for an AI Bill of Rights: Making Automated Systems Work for the AMERICAN People）。

该文件包含五项原则，以指导自动化系统的设计、使用和部署。每项原则都附有一本手册，详细介绍了如何落实这些原则。五项原则分别是：（1）安全有效的系统。自动化系统应在不同社区、利益相关者和领域专家的咨询下开发，并应进行部署前测试、风险识别和缓解；（2）算法歧视保护。自动化系统的设计者、开发人员和部署者应采取积极主动和持续的措施，以公平的方式设计系统，保护个人和社区免受算法歧视；（3）数据隐私。敏感数据应享有特殊保护，并应避免不受控制的监视；（4）通知和解释。自动化系统的设计者、开发人员和部署者应提供文档，清楚地描述自动化在整个系统中的作用，并对结果进行解释；（5）考虑和回退。个人应能够在适当情况下选择退出自动化系统，转而选择人性化的替代方案。

11. 美国正式通过《人工智能培训法》

10月17日，美国总统拜登签署《人工智能培训法》（AI Training Act），要求白宫管理和预算办公室（OMB）为执行机构的采购人员制定并提供AI培训计划，以了解AI相关的能力与风险。培训计划将提供与AI系统技术特征相关

概念，提供减轻AI风险的方法，并讨论未来AI趋势，包括对国家安全和创新有影响的趋势。根据该法案，OMB必须至少每两年更新一次AI培训计划，并对参与者的情况进行衡量，还应接收并考虑培训计划参与者的反馈和其他见解。

12. 美国和瑞士发表《关于加强量子信息科学技术合作的联合声明》

10月19日，美国和瑞士发表《关于加强量子信息科学技术合作的联合声明》（Joint Statement of the United States of America and Switzerland on Cooperation in Quantum Information Science and Technology）。

声明确定了两国的量子研究伙伴关系，将促进两国在量子计算、量子网络和量子传感等领域的研究与应用。声明指出，两国将利用双边科技合作机制和多边合作框架，寻求新的实施途径，促进量子信息科学技术（QIST）合作研发工作。通过让包括行业联盟、领先的研究者、政策制定者和业务安全利益相关者在内的利益相关者参与进来，为QIST研发建立值得信赖的市场和供应链。利用定期的多边机会讨论具有国际重要性的QIST问题和各自的政策问题。

13. 欧洲议会通过《关于数字时代人工智能的决议》

5月3日，欧洲议会通过《关于数字时代人工智能的决议》（European Parliament resolution of 3 May 2022 on artificial intelligence in a digital age），旨在促使欧盟成为AI全球标准的制定者。

决议指出欧盟不应总是将AI作为一种技术进行监管，监管干预的程度应与AI系统的特定使用相关的风险类型成正比。欧盟在全球AI竞争中的地位应通过监管方式、市场形势、投资等措施确立。决议指出，欧洲成为全球领导者的路线图包括：（1）有利的监管环境：建立立法、治理和执法、AI的法律框架；（2）完善的数字单一市场：国家AI战略、打破市场壁垒、实现公平竞争等；（3）数字绿色基础设施：连接性和算力、可持续性；（4）卓越生态：人才和研究；（5）信任生态系统：电子政府、电子医疗；（6）产业战略：战略规划与投资，对中小企业与初创企业的支持与鼓励；（7）安全：AI与执法、网络安全、网络防御、AI的军事应用保障。

14. 英国国防部发布《国防人工智能战略》

6 月 15 日，英国国防部发布《国防人工智能战略》（Defence Artificial Intelligence Strategy），旨在使国防部成为世界上最有效、最高效、最可信且最具影响力的国防机构。

战略将促进国防领域采用 AI 实现决策优势、提高效率、解锁新能力、增强整体力量。战略目标包括：（1）将国防部转变为一个“做好 AI 准备”的机构。提高人员技能，实现数字、数据和技术“赋能者”的现代化；（2）以最快的速度和规模采用/利用 AI。利用近期和长期的机会，进行系统性实验，开展国际合作；（3）加强英国国防与安全的 AI 生态系统。消除商业壁垒，激励与商业界开展合作；（4）塑造全球 AI 发展。支持负责任的全球 AI 发展，促进安全与稳定。

15. 欧盟委员会提出《人工智能责任指令的提案》

9 月 28 日，欧盟委员会提出《欧洲议会和欧盟委员会关于使非合同性民事责任规则适应人工智能指令（人工智能责任指令）的提案》（Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on adapting non-contractual civil liability rules to artificial intelligence （AI Liability Directive）），首次提出有针对性地协调各国 AI 的责任规则，使 AI 相关损害的受害者更容易获得赔偿。

提案旨在解决 AI 产品和服务及欧盟 27 个国家法规不一的相关问题。提案规定，如果个人或公司受到机器人、无人机和配有 AI 的软件或服务的伤害，包括物理伤害和数据安全泄露等，将更容易起诉索赔。受害者可就 AI 技术的提供者、开发者或用户的过失或疏忽对其生命、财产、健康和隐私造成的损害，或就使用 AI 的招聘过程中的歧视寻求赔偿。提案借由因果关系推定减轻受害者举证责任。受害者只需要证明制造商或用户未能遵守某些要求造成了伤害，然后在诉讼中证明与其 AI 技术的关系。根据获取证据的权利条款，受害者可要求法院命令公司和供应商提供有关高风险 AI 系统的信息，以识别责任人和造成损害的 AI 错误。

16. 英国 DCMS 发布两项人工智能政策文件

7 月 18 日，英国数字、文化、媒体和体育部（DCMS）发布两项人工智能文件《国家人工智能战略——人工智能行动计划》（National AI Strategy - AI Action Plan）与《建立一种支持创新的人工智能监管方法》（Establishing a pro-innovation approach to regulating AI），旨在就 AI 未来监管提出建议。

《国家人工智能战略——人工智能行动计划》概述了英国各政府部门推进《国家人工智能战略》，巩固 AI 领导者地位应采取的措施，并提出三大要点：（1）投资和规划 AI 生态系统的长期需求，以维持英国作为 AI 超级大国的领导地位；（2）支持向 AI 经济转型，并确保 AI 惠及所有部门和地区；（3）确保英国获得 AI 技术的国家和国际治理权，鼓励创新与投资，维护基本价值观。

《建立一种支持创新的人工智能监管方法》强调监管的合比例性，并基于 AI 的特征提出了一个促进创新的监管框架。文件提出两个与监管有关的 AI 的核心特征：一是技术的“适应性”，二是技术的“自主性”，前者关涉解释 AI 的行为或逻辑，后者则关涉行为责任的分配。在此基础上，文件提出 AI 监管框架，包括四个方面：（1）应用场景。AI 是一种动态、通用的技术，其产生的风险主要取决于其应用的场景。不同的监管机构应根据特定场景下 AI 对个人、群体或企业的影响采取各异的监管对策；（2）支持创新和基于风险。监管者应关注有证据表明存在真实且较高风险，而非低风险或假设存在风险的应用，以免为创新设置不必要障碍；（3）体系性。应建立针对 AI 核心特征的跨部门监管原则，监管体系应简单、清晰、可预测且稳定；（4）合比例性。

17. 德国《自动驾驶条例》生效

7 月 1 日，德国《关于规范具有自动和无人驾驶功能的机动车运营的条例以及〈道路交通法〉修订案》（Verordnung zur Regelung des Betriebs von Kraftfahrzeugen mit automatisierter und autonomer Fahrfunktion und zur Änderung straßenverkehrsrechtlicher Vorschriften），简称《自动驾驶条例》（Verordnung zum Autonomen Fahren）正式生效。

2017 年 6 月，德国颁布世界上第一部自动驾驶法《道路交通法第八修正案》，明确规定自动驾驶系统接管驾驶任务的情景，以及驾驶员在自动驾驶阶段的权利

和义务。2021 年 7 月，德国颁布世界上第一部允许无人驾驶机动车上路的立法《自动驾驶法》，首次提出技术监督员概念，并对参与自动驾驶车辆运营各方责任和义务做出规定。

为落实《自动驾驶法》中关于 L4 级及以上具有无人驾驶功能的机动车运营的相关要求，此次出台的《条例》主要包含以下事项：（1）规定无人驾驶汽车运营许可证的申请和审查程序；（2）规定无人驾驶汽车公共运营区域的要求和审批程序；（3）增加机动车行驶证的补充规定；（4）细化参与无人驾驶汽车运营各方（车主、技术监督员、制造商）的义务；（5）补充新的测试规定；（6）明确违法行为；（7）对无人驾驶汽车的结构、质量和设备提出技术要求。

18. 法国数据保护局发布《面向人工智能的 GDPR 合规指南》

4 月 5 日，法国数据保护局发布《面向人工智能的 GDPR 合规指南》（AI：comment être en conformité avec le GDPR）。

指南要点包括：（1）定义使用目的。在项目设计中首先明确 AI 技术的适用目的,如明确基于机器学习的 AI 模型在学习阶段(即开发和训练 AI 模型阶段）与生产阶段独立的个人数据处理目的；（2）明确法律基础。在 GDPR 提供的 6 类处理个人数据的法律基础中明确所适用的法律基础。需特别注意，为“科学研究”处理个人数据并非法定的法律基础之一；（3）构建数据库。为涉及的个人数据创建数据库，数据库的构成包括专为数据库建立（以用于算法验证等）目的收集的数据；重复利用已经为其他目的所收集的数据。就后一种情形，需充分评估其合法性；（4）最小化数据。严格遵循 GDPR 第 9 条要求，确保收集和使用的个人数据最小化。建议采取的措施包括明确并清晰区分 AI 模型训练和运行所必须的数据类型、批判性地评估所需的数据类型与数量、应用数据假名化技术或数据过滤/混淆机制、建立并保留数据处理日志、评估数据处理风险、采用访问控制管理以确保数据安全等；（5）防范与 AI 模型相关的风险。避免基于非法收集的数据训练 AI 模型。同时，尽管根据个人数据训练的 AI 模型不必然包含个人数据，但仍需注意避免 AI 模型遭受攻击导致数据泄露。

19. 澳大利亚联邦政府发布《2021 年国家研究基础设施路线图》

4 月 7 日，澳大利亚联邦政府发布《2021 年国家研究基础设施路线图》（2021 National Research Infrastructure Roadmap），建议制定国家数字研究基础设施（NDRI）战略。

路线图就 NDRI 战略提出以下建议：提供充分利用数据所需的计算资源、数字工具、数据治理框架和专业知识，以协调、整合和支持跨领域研究；为解决数字技能、数据收集、数据标准以及数据分析和可视化等问题指明方向；简化对数据的访问，并满足研究人员的计算、存储和分析需求；围绕高性能计算、百亿亿次计算、量子计算、大数据以及商业和非商业云服务等未来挑战做好规划和准备。

在发布路线图的同时，联邦政府也将 AI 和量子计算作为全球科技外交基金下的四个优先研究和合作领域之一，以推动澳大利亚与美国、英国、日本、法国和西班牙等国在这些领域的合作。需要指出的是，在 2021 年底公布的联邦政府关键技术蓝图中，澳大利亚已将量子技术确定为 63 个关键技术领域之一，并正在制定本国的国家量子战略。

20. 俄罗斯杜马引入《关于俄罗斯联邦监管数字金融资产流通和实用数字权利的立法修正案》

6 月 7 日，俄罗斯杜马引入第 138674-8 号法案《关于俄罗斯联邦监管数字金融资产流通和实用数字权利的立法修正案》。

法案强调，电子平台运营商为国家支付系统主体，拥有在符合金融标准要求下使用电子平台进行交易的权利。法案要求，用户应创建名义账号使用电子平台，禁止平台向用户提供资金以增加名义账户记录余额，禁止平台向用户收取账户利息。法案设立一项禁令，禁止将数字金融资产的转让、接收作为一种支付手段，禁止将数字资产用作对转让的商品、完成的工作、提供的服务或其他可能被视为支付的方法的“反准备金”（Counter Provision）。法案提出平台合规评估要求，规定俄罗斯中央银行对本法落实情况实施监督。

21. 俄罗斯发布法案，禁止在俄罗斯使用数字资产作为支付方式

7 月 14 日，俄罗斯总统普京签署第 138674-8 号法案《修改俄罗斯联邦某些

立法和暂停联邦法<关于银行和银行活动>第5.1条某些规定》（О внесении изменений в отдельные законодательные акты Российской Федерации и о приостановлении действия отдельных положений статьи 5.1 Федерального закона «О банках и банковской деятельности»），禁止使用加密货币和NFT等数字资产支付商品和服务费用。法案将在10天后生效。该法规定，禁止转让或接受数字金融资产作为转让货物、执行工程、提供服务的对价，以及以任何其他方式允许人们通过数字金融资产对货物（工程、服务）进行支付，除非联邦法律另有规定。

22. 巴基斯坦信息技术和通信部发布《云优先政策》

2月18日，巴基斯坦信息技术和通信部（MoITT）发布最终版《云优先政策》（PAKISTAN Cloud First Policy）。

鉴于政府部门维护数据会导致大量的财政支出，并且在数据管理方面可能存在困难，该政策将为所有公共部门开发一个通用平台，提供集体云服务，以保护其官方数据并使其易于管理。该政策获得批准后，联邦部委和部门的数据中心将转移到“中央云”。该政策还要求建立一个由MoITT部长担任主席的云办公室，负责监督云服务提供商的认证、质量、安全和部门IT事务。云办公室将授权云服务提供商提供所需的能力和设备。

政策通过后,MoITT已着手在该部建立云办公室。云办公室将执行以下职责：（1）基于国际标准，为云服务提供商建立分类、认证、注册和合规框架；（2）根据既定基准执行或寻求云服务提供商的合规性；（3）在公共服务实体中推广云文化和采用云服务；（4）如果有正当理由偏离/豁免云政策，提供基于时间的无异议证书（NOC）；（5）执行云优先投资；（6）支持各省在辖区内实行云优先政策。

23. 中非共和国通过立法，将比特币作为法定支付工具

4月26日，中非共和国总统办公厅发表声明表示，中非共和国国民议会全

票通过一项立法，建立有关加密货币监管的法律框架，并将比特币定为中非共和国法定支付工具。

24. 全球科技贸易协会 ITI 发布《实现人工智能系统透明度的政策原则》

9 月 15 日，全球信息技术产业委员会（ITI）发布《实现人工智能系统透明度的政策原则》（Policy Principles for Enabling Transparency of AI Systems），旨在为决策者提供了一个明确的指南，以了解并提高 AI 系统的透明度。ITI 强调，AI 系统的透明度理所当然地应当成为美国和全球决策者的首要关注点。法规必须有效地降低用户风险，同时保持 AI 技术的创新。

ITI 建议：（1）考虑透明度要求的最终目标是什么；（2）考虑透明度要求的目标受众，以及这些要求将适用于 AI 系统生命周期的哪一环节；（3）考虑上述要求时，应基于风险的透明度方法；（4）在法规或政策中明确“透明度”的含义；（5）考虑有不同的方法来提高透明度和信任度；（6）考虑在立法中纳入旨在要求向用户提供足够信息以了解可能对其基本权利产生负面影响的规定，并向用户提供审查或质疑此类决策的能力；（7）确保透明度规则不要求公司泄露敏感 IP 或源代码，或以其他方式泄露敏感个人数据；（8）利用自愿国际标准，尽可能保持各种 AI 透明度要求的互操作性；（9）有关披露的规定应灵活，避免具体信息或技术细节；（10）只有 AI 系统的实际部署者才应负责披露。

25. 香港政府发表《有关虚拟资产在港发展的政策宣言》

10 月 31 日，香港政府发表《有关虚拟资产在港发展的政策宣言》，阐明政府为在香港发展具有活力的虚拟资产行业和生态系统而订定的政策立场和方针。宣言表示，香港对全球从事虚拟资产业务的创新人员抱持开放和兼容的态度。政府正与金融监管机构缔造便利的环境，以促进香港虚拟资产行业得以可持续和负责任地发展。政府会适时订出所需规限，按照国际标准缓减实际和潜在风险，让虚拟资产创新能够在香港以可持续方式蓬勃发展。

宣言指出，香港认为透过一致、明确和清晰的全监管框架，有助于奠定稳固的基础，以迎接由全球虚拟资产急速发展所带来的金融创新和科技发展。在

加紧筹备新虚拟资产服务提供者发牌制度的同时，政府也乐意联系全球虚拟资产业界，邀请有关交易所在香港开拓商机。政府和监管机构正研究推出下列试验计划，以测试虚拟资产带来的技术效益，并尝试把有关技术进一步应用于金融市场。这些试验计划包括为2022年香港金融科技周发行非同质化代币(NFT)、绿色债券代币化及数码港元。

26. 中国八部门发布《关于加强网络预约出租汽车行业事前事中事后全链条联合监管有关工作的通知》

2月7日，交通运输部、工信部、公安部等八部门联合发布《关于加强网络预约出租汽车行业事前事中事后全链条联合监管有关工作的通知》。

通知要求各地联合监管机制建立健全日常工作制度，制定落实风险监测研判、定期报告、重大情况通报反馈、重大事项联合督办等工作制度，加强部门间信息通报和沟通共享。通知明确网约车平台公司存在危害网络安全、数据安全，侵害用户个人信息权益等违法违规行为的，可开展事前事中事后全链条联合监管。根据违法法规行为情节，可对网约车平台公司采取暂停区域内经营服务、暂停发布或下架移动互联网应用程序、停止互联网服务、停止联网或停机整顿等处置措施。

27. 中国五部门发布《关于进一步加强新能源汽车企业安全体系建设的指导意见》

3月29日，工信部、公安部、交通运输部、应急管理部与国家市场监督管理总局联合发布《关于进一步加强新能源汽车企业安全体系建设的指导意见》。

意见强调加强网络安全防护、数据安全保护、个人信息安全防护。企业要依法落实关键信息基础设施安全保护、网络安全等级保护、车联网卡实名登记、汽车产品安全漏洞管理等要求。对车辆网络安全状态进行监测，采取有效措施防范网络攻击、入侵等危害网络安全的行为。企业要切实履行数据安全保护义务，建立健全全流程数据安全管理制度，采取相应的技术措施和其他必要措施，保障数据安全。企业要按照法律、行政法规的有关规定进行数据收集、存储、使用、加工、传输、提供、公开等处理活动，以及数据出境安全管理。企业要按照《个

人信息保护法》以及相关法律法规的规定处理个人信息，制定内部管理和操作规程，对个人信息实行分类管理，并采取相应的加密、去标识化等安全技术措施，防止未经授权的访问以及个人信息泄露、篡改、丢失。

28. 最高人民法院发布《关于加强区块链司法应用的意见》

5 月 25 日，最高人民法院发布《关于加强区块链司法应用的意见》。意见明确人民法院区块链平台建设要求，要求充分运用区块链数据防篡改技术，进一步提升司法公信力；充分发挥区块链优化业务流程的重要作用，不断提高司法效率；充分挖掘区块链互通联动巨大潜力，增强司法协同能力；充分利用区块链联盟互认可信的价值属性，服务经济社会治理。

安全方面，意见要求以安全可信为前提，着力提升上链数据和智能合约的准确可控水平，确保数据安全，保护个人信息，推动形成区块链在司法领域稳中求进、有序发展、安全可靠的应用生态。各级人民法院要健全事前审核和测试评估机制，确保上链数据真实性、准确性、合规性以及链上链下数据一致性，确保智能合约的合法性、有效性、安全性和可靠性。

29. 六部门发布《关于加快场景创新以人工智能高水平应用促进经济高质量发展的指导意见》

8 月 12 日，科技部、教育部等六部门联合发布《关于加快场景创新以人工智能高水平应用促进经济高质量发展的指导意见》。指导意见要求坚持企业主导、创新引领、开放融合、协同治理的基本原则，提出场景创新成为 AI 技术升级、产业增长的新路径，场景创新成果持续涌现，推动新一代 AI 发展上水平的发展目标。

具体来说，指导意见要求加强 AI 场景创新要素供给，集聚 AI 场景数据资源。推动城市和行业的 AI“数据底座”建设和开放，采用区块链、隐私计算等新技术，在确保数据安全的前提下，为 AI 典型应用场景提供数据开放服务。加强“数据底座”的安全保护，对个人信息、商业秘密、行业重要数据等依法予以保护。

30. 上海发布《上海市政务云管理暂行办法》

4 月 6 日，上海市人民政府办公厅发布《上海市政务云管理暂行办法》。办法共七章三十五条，涉及规划建设、能力建设、资源管理、运行维护和安全保障、效能评估等内容。

办法指出政务云，是指依托非涉密电子政务网络，为等保三级及以下的非涉密信息系统提供计算资源、存储资源、服务支撑、安全保障等共性资源的信息基础设施，由市级政务云（含政务云专有域）和区级政务云组成。

政务云的安全管理遵循“谁建设谁负责，谁运营谁负责，谁管理谁负责，谁使用谁负责”的原则。政务云运行管理单位负责政务云平台安全管理，明确政务云安全技术和安全能力的要求和标准，监测、防御、处置各类安全风险和威胁，保护政务云免受攻击、侵入、干扰和破坏。使用单位负责本单位云上信息系统安全管理，在信息系统正式上线前协调开展安全资源申请、安全自查、检测评估、安全加固等工作，做好信息系统的网络安全等级保护，签订上云安全承诺书；在信息系统运行期间持续做好网络安全等级保护复测、数据安全保护等安全保障工作。政务云服务商负责建立健全安全保护工作制度，提供安全可信的产品和服务，做好政务云的安全监测和防御工作，定期开展网络安全等级保护测评与密码应用安全性评估，保障政务云安全稳定运行。政务云主管部门、政务云运行管理单位和使用单位应当严格落实国家网络安全和商用密码应用要求，采取安全管理措施，并与政务云同步规划、同步建设、同步运行网络安全体系与密码保障体系。

31. 上海发布两项行动方案，促进“元宇宙”和智能终端产业发展

6 月 24 日，上海市人民政府办公厅发布《上海市培育“元宇宙”新赛道行动方案（2022—2025 年）》和《上海市促进智能终端产业高质量发展行动方案（2022—2025 年）》。

《上海市培育“元宇宙”新赛道行动方案（2022—2025 年）》明确尊重规律、分步推进，集成创新、联动发展，价值引领、效果导向等基本原则，提出四项主要任务和八大重点工程。方案要求加强未来网络、云边计算、智能交互终端及数字基础设施的内生安全，保障海量数据的存储、传输和使用。强化“元宇宙”

领域法治建设，在数字成瘾、内容安全、个人隐私等方面推动研究相关法律法规。加强市场监管，夯实“元宇宙”数字空间平台主体责任。

《上海市促进智能终端产业高质量发展行动方案（2022—2025 年）》明确以品牌塑造强动能、以体系构建优动能、以创新引领新动能、以市场牵引主动能四项基本原则，提出七项主要任务。方案要求完善全市智能网联汽车公共数据平台，统筹建立一体化安全管理体系和安全态势监测系统。推动智能网联汽车功能安全、网络数据安全等评估能力和测试场地建设，探索数据跨境传输。加强智能终端产品全生命周期管理，持续推动提升系统安全、网络安全、数据安全能力，切实保障用户隐私。

32. 深圳发布《深圳经济特区智能网联汽车管理条例》

6 月 23 日，深圳市第七届人民代表大会常务委员会第十次会议通过《深圳经济特区智能网联汽车管理条例》。作为我国首部规范智能网联汽车管理的法规，条例共九章六十四条，涉及道路测试和示范应用、准入和登记、使用管理、车路协同基础设施、网络安全和数据保护、交通违法和事故处理等内容。

条例专门设置“网络安全和数据保护”一章，对智能网联汽车涉及的网络安全和数据保护问题进行规范：（1）规定市网信部门统筹协调全市智能网联汽车的网络安全风险监督管理工作；（2）规定市网信部门应当统筹协调、督促指导相关政府部门制定智能网联汽车网络安全事件应急预案；（3）规定智能网联汽车相关企业应当依法取得网络关键设备和网络安全专用产品的安全检测认证，依法制定网络安全事件应急预案；（4）规定智能网联汽车相关企业应当依照国家相关规定，制定数据安全管理制度和隐私保护方案，并将存储数据的服务器设在中国境内。未经批准，不得向境外传输、转移相关数据信息；（5）规定禁止利用智能网联汽车非法收集、处理、利用个人信息、与本车辆行驶和交通安全无关的信息和涉及国家安全的信息。

33.《浦东新区人工智能企业数据安全和算法合规指引（试行）》发布

9月3日，上海市浦东新区检察院与浦东新区工商联、人工智能行业指导部门、行业协会以及专业机构共同编制的《浦东新区人工智能企业数据安全和算法合规指引（试行）》首次发布，并从发布之日起试行。

指引涉及企业数据合规组织机构建设、数据安全制度建设、数据全生命周期安全管理、算法合规制度建设、数据合规评估体系等内容，适用于浦东新区AI企业，以及其他从事数据收集、处理和算法研发应用的相关企业。

指引具有三方面特色：（1）首次将算法合规纳入到数据合规体系，进一步完善数据合规管理体系。对AI企业的算法公开、算法评估、反垄断和反不正当竞争、自动化决防范算法歧视等方面均作出规定。提倡企业应强化责任意识，对算法应用产生的结果负主体责任，提供算法推荐服务具有舆论属性或社会动员能力的应当进行互联网信息服务算法备案；（2）进一步扩大数据保护范围。以往的数据合规指引往往侧重个人信息保护，指引则将保护范围由公民个人信息拓展到其他领域的重要信息与核心信息，更为注重数据合规的完整性；（3）创新性地引入数据合规的评价体系。通过外部评估与自评估两种方式相结合，帮助AI企业更好地发现数据合规管理中存在的问题，从而预防数据合规风险。

此外,指引还提倡数据处理者应当确保数据全生命周期内持续处于有效保护和合法利用的状态，保障数据免遭泄露、窃取、篡改、毁损、丢失、非法使用，并针对每个环节提出具体指引建议。

34.上海发布《上海市加快智能网联汽车创新发展实施方案》

9月5日，上海市人民政府办公厅发布《上海市加快智能网联汽车创新发展实施方案》。实施方案要求构建国内领先的智能网联汽车测试评价体系，完善网络及数据安全、软件升级等测试和评价技术。完善智能网联汽车系统验证及应用服务，构建“可兼容、可移植、可维护”的软件功能安全测评和信息安全测试验证平台。理顺智能网联汽车测试和数据采集管理机制。持续强化智能网联汽车信息安全能力评估、监督检查、违规事件处置、数据出境安全评估和地理位置信息安全监管。

35. 上海出台《上海市促进人工智能产业发展条例》

9 月 22 日，上海市十五届人大常委会第四十四次会议表决通过《上海市促进人工智能产业发展条例》，自 2022 年 10 月 1 日起施行。这是上海继《上海市数据条例》后的第二部数字经济领域地方性法规，将有力支撑城市全面数字化转型，助力建成具有国际影响力的人工智能“上海高地”。

条例共六章七十二条，根据国家有关标准和上海市实际，对 AI、AI 产业予以明确，并就管理体制机制等内容作出相关规定：（1）明确各级政府及相关部门在促进 AI 产业发展中的具体职责；（2）设立市人工智能战略咨询专家委员会，为产业发展中的重大战略、重大决策提供咨询意见；（3）要求人工智能行业协会及其他相关行业组织，促进产业协同，加强行业自律；（4）鼓励 AI 领域市场主体积极创新；（5）加强 AI 技术、产业等方面的合作，推动 AI 领域科普和宣传。

条例围绕增加 AI 创新的源头供给，促进开源共享，提升持续创新能力：（1）聚焦算力、算法、数据三大基本要素，加强算力基础设施规划，推进公共算力资源平台建设，保障中小企业获得普惠的公共算力；推动算法模型交易流通，加强对算法模型的保护；突出 AI 领域高质量数据集建设，扩大面向 AI 产业的公共数据供给范围；（2）强化科技创新。明确加强基础理论和关键共性技术的研发、鼓励跨学科交叉领域研究；推动相关国家实验室、重大科研平台等创新发展；推动 AI 领域大型科学仪器设施开放共享等。

36. 《厦门市元宇宙产业发展三年行动计划（2022-2024 年）》发布

3 月 23 日，厦门市工业和信息化局、厦门市大数据管理局印发《厦门市元宇宙产业发展三年行动计划（2022-2024 年）》。

行动计划围绕力争到 2024 年，元宇宙产业生态初具雏形，引入培育一批掌握关键技术、营收上亿元的元宇宙企业，元宇宙技术研发和应用推广取得明显进展，对政府治理、民生服务、产业转型升级的带动作用进一步增强的发展目标，提出五类十二项重点任务。监管治理方面，行动计划要求加强元宇宙应用规范和引导。根据《网络安全法》《数据安全法》《个人信息保护法》和《区块链信息服务管理规定》等相关条例，引导和推动元宇宙产品开发者和平台运

营者加强行业自律、落实主体责任。提升元宇宙数据治理能力。针对元宇宙发展遇到的价值伦理、虚拟空间管控等新问题，及时研究规范、精准合法治理。

（十）其他

1. 金砖国家领导人第十四次会晤达成《金砖国家数字经济伙伴关系框架》

6 月 27 日，金砖国家领导人第十四次会晤达成《金砖国家数字经济伙伴关系框架》，就深化金砖国家数字经济合作形成重要共识，开启金砖国家数字经济合作新进程。

作为金砖经贸领域第一份数字经济合作专门文件，框架纳入了数字认证、数据隐私和安全、网上争端解决等当前数字经济前沿领域，并同意就 AI 等新兴技术开展合作；针对金砖成员数字经济发展水平不同的现状，框架把弥合数字鸿沟作为重点之一，鼓励开展能力建设和政策实践分享，缩小数字基础设施、数字技术、数字服务和数字技能发展方面的差距；明确了数字经济的合作方向和重点领域，提出了提高港口数字化水平、鼓励数字基础设施投资、提升中小微企业能力等 17 条合作举措。金砖五国同意升级电子商务工作组为数字经济工作组，为推动落实数字经济合作作出重要的制度性安排。

2. 美国正式通过《2021 年联邦轮换网络劳动力计划法》

6 月 21 日，美国正式通过《2021 年联邦轮换网络劳动力计划法》（Federal Rotational Cyber Workforce Program Act of 2021）。

本法中参与轮换计划的“网络劳动力”职位是指根据《2015 年联邦网络安全劳动力评估法》确定的具有信息技术、网络安全或其他网络相关职能的职位。本法要求，人事管理办公室发布联邦轮换网络劳动力计划运营计划，提供详细说明各机构轮换网络职位中的员工政策、流程和程序。政府问责办公室必须通过评估各机构参与该计划的程度以及在该计划中服务员工的经验，来评估轮换网络劳动力计划的运作和有效性。

根据要求，运营计划至少应当包括以下内容：（1）确定参与轮换网络劳动力计划的机构；（2）建立程序；（3）明确员工系自愿参与；（4）如果员工的

雇佣机构负责人或员工的雇佣机构负责人的指定人批准员工参与，则员工有资格参与；（5）参加计划的员工，在服务期结束时有权返回所担任的职位，不会损失工资、资历或其他福利；（6）员工参加计划不得影响员工的正常职位。

3. 欧盟委员会发布《儿童和青少年的数字十年：为儿童打造更好互联网的新欧洲战略》

5 月 11 日，欧盟委员会通过《儿童和青少年的数字十年：为儿童打造更好互联网的新欧洲战略》（A Digital Decade for children and youth: the new European strategy for a better internet for kids，简称 BIK+），旨在改善适龄数字服务，补充和支持现有措施，以保护在线儿童，确保儿童都能在网上得到保护、授权和尊重。

战略以 2012 年《更好的儿童互联网欧洲战略》为基础，倡导提供符合儿童最大利益的可访问、适龄和信息丰富的在线内容和服务。战略提出三大支柱：（1）安全的数字体验，保护儿童免受有害和非法的在线内容、行为和风险的侵害，并通过安全、适龄的数字环境改善儿童福祉。为了让数字世界成为儿童和年轻人的安全场所，欧盟委员会将推动制定欧盟适龄设计规范，并要求在 2024 年前制定一项关于在线年龄验证的欧洲标准。战略还将探索如何使用计划中的欧洲数字身份钱包进行年龄验证，支持快速报告非法和有害内容。（2）数字赋权，使儿童获得必要的技能和能力，以在网上做出明智的选择，确保能够安全、负责任地上网。委员会将通过“更安全的互联网中心网络”为儿童、教师和家长组织媒体扫盲运动。（3）尊重儿童，让儿童在数字环境中有发言权，开展更多由儿童主导的活动，培养创新和创造性的安全数字体验。

4. 英国发布新的《英国数字战略》

6 月 13 日，英国发布新的《英国数字战略》（UK's Digital Strategy），旨在将跨部门的科技和数字政策整合到统一的路线图中，确保英国数字技术、基础设施和数据能够在未来几年内推动经济增长和创新。

自从英国政府在 2017 年推出第一个数字战略以来，英国的科技行业蓬勃发展，增长速度是整个经济的 2.5 倍。2021 年，每 11 天就有一家新的科技独角兽

公司诞生，比2017年的英国独角兽公司数量增加了一倍多。

战略将在这些实践的基础上，发展更具创新性、包容性和竞争力的数字经济。战略体现了英国政府在对持续推动数字增长至关重要的六个领域的雄心：（1）数字基础设施。推出世界一流的数字基础设施和灵活且有利于增长的监管制度，保护公民的同时鼓励投资和创新；（2）创新和知识产权。通过研发刺激创新，增长英国在未来技术方面的专业知识，包括AI、半导体和量子计算；（3）数字技能和人才。成立新的数字技能委员会（Digital Skills Council），加强科技人才发展；（4）为数字增长提供资金。鼓励包括养老基金在内的英国资本投资于英国的小型企业，并通过英国创新署和英国商业银行领导对创新的支持；（5）全国性的方法。帮助每个地区的企业采用最新的技术；（6）提升英国的国际地位。以自由和开放为中心，在国际数字贸易和技术治理系统方面进行合作。

5. 爱尔兰政府发布国家数字战略《利用数字—爱尔兰数字框架》

2月1月，爱尔兰政府发布新的国家数字战略《利用数字—爱尔兰数字框架》（Harnessing Digital－The Digital Ireland Framework），旨在推动爱尔兰经济和社会数字化转型。

战略要点包括：（1）促进网络连接性与融合性。稳步推进国家宽带计划、远程工作中心和宽带连接点；（2）提升全民数字素养与技能。通过学校、高等教育与终身学习，加强全民数字技能教育和培训，普及提升公民数字素养，让具备基本数字技能的成人比例在2030年达到80%；（3）推广包容性数字公共服务。加快推进包容性数字公共服务普及与使用；（4）提供企业数字化转型资助。通过提供资助与援助，助力中小企业把握数字化新机遇，让90%中小企业至2030年实现基本数字密度（Basic Digital Intensity），让云计算、AI和大数据领域企业普及率达到75%；（5）加大网络安全工作资金投入。加大国家网络安全中心建设投资，构建现代化、资源充足的网络安全监管框架。

6. 九部门发布《关于推动平台经济规范健康持续发展的若干意见》

1月20日，国家发展改革委等九部门发布《关于推动平台经济规范健康持续发展的若干意见》，从健全完善规则制度、提升监管能力和水平、优化发展环

境、增强创新发展能力、赋能经济转型发展等方面提出要求。

意见要求完善治理规则。完善数据安全法、个人信息保护法配套规则。细化平台企业数据处理规则。此外，健全制度规范。厘清平台责任边界，强化超大型互联网平台责任。建立平台合规管理制度，对平台合规形成有效的外部监督、评价体系。加大平台经济相关国家标准研制力度。完善跨境数据流动“分级分类+负面清单”监管制度，探索制定互联网信息服务算法安全制度。

意见要求探索数据和算法安全监管。切实贯彻收集、使用个人信息的合法、正当、必要原则，严厉打击平台企业超范围收集个人信息、超权限调用个人信息等违法行为。从严管控非必要采集数据行为，依法依规打击黑市数据交易、大数据杀熟等数据滥用行为。在严格保护算法等商业秘密的前提下，支持第三方机构开展算法评估，引导平台企业提升算法透明度与可解释性，促进算法公平。严肃查处利用算法进行信息内容造假、传播负面有害信息和低俗劣质内容、流量劫持以及虚假注册账号等违法违规行为。推动平台企业深入落实网络安全等级保护制度，探索开展数据安全风险态势监测通报，建立应急处置机制。国家机关在执法活动中应依法调取、使用个人信息，保护数据安全。

7. 中央网信办等四部门发布《2022 年提升全民数字素养与技能工作要点》

3 月 2 日，中央网信办、教育部、工信部、人力资源社会保障部联合发布《2022 年提升全民数字素养与技能工作要点》。工作要点部署八方面 29 项重点任务。八方面分别是加大优质数字资源供给、打造高品质数字生活、提升劳动者数字工作能力、促进全民终身数字学习、提高数字创新创业创造能力、筑牢数字安全保护屏障、加强数字社会文明建设，以及加强组织领导和整体推进。其中，安全保护方面要求增强网络安全、数据安全防护意识和能力，加强个人信息和隐私保护。

8. 国家互联网信息办公室就《未成年人网络保护条例（征求意见稿）》再次公开征求意见

3 月 14 日，国家互联网信息办公室就《未成年人网络保护条例（征求意见稿）》再次公开征求意见。征求意见稿共七章六十七条，涉及网络素养培育、网络信息内容规范、个人信息保护、网络沉迷防治等内容。

征求意见稿突出大平台责任，规定未成年人用户数量巨大、在未成年人群体具有显著影响力的重要互联网平台服务提供者，应当在互联网平台服务的设计、研发、运营等阶段，充分考虑未成年人身心健康发展特点，定期开展未成年人网络保护影响评估；按照国家规定建立健全未成年人网络保护合规制度体系，成立主要由外部成员组成的独立机构，对未成年人网络保护情况进行监督；遵循公开、公平、公正的原则，制定专门的平台规则，明确平台内产品或者服务提供者未成年人网络保护的义务，并以显著方式提示未成年人用户依法享有的网络保护权利和遭受网络侵害的救济途径等义务。

9. 中共中央办公厅、国务院办公厅联合发布《关于加强科技伦理治理的意见》

3 月 20 日，中共中央办公厅、国务院办公厅发布《关于加强科技伦理治理的意见》，涉及科技伦理原则、治理体制、治理制度保障、审查和监管、教育与宣传等内容。

意见强调，制定完善科技伦理规范和标准。制定生命科学、医学、AI 等重点领域的科技伦理规范、指南等，完善科技伦理相关标准，明确科技伦理要求，引导科技机构和科技人员合规开展科技活动。建立科技伦理审查和监管制度。明晰科技伦理审查和监管职责，完善科技伦理审查、风险处置、违规处理等规则流程。建立健全科技伦理（审查）委员会的设立标准、运行机制、登记制度、监管制度等，探索科技伦理（审查）委员会认证机制。提高科技伦理治理法治化水平。推动在科技创新的基础性立法中对科技伦理监管、违规查处等治理工作作出明确规定，在其他相关立法中落实科技伦理要求。“十四五”期间，重点加强生命科学、医学、AI 等领域的科技伦理立法研究，及时推动将重要的科技伦理规范上升为国家法律法规。对法律已有明确规定的坚持严格执法、违法必究。

10. 国家互联网信息办公室发布《网信部门行政执法程序规定（征求意见稿）》

9 月 8 日，国家互联网信息办公室发布《网信部门行政执法程序规定（征求意见稿）》。征求意见稿共五章五十六条，涉及管辖和适用、行政处罚的普通程序、执行与结案等内容。

征求意见稿规定设区的市级以下网信部门依职权管辖本行政区域内的网络

信息内容、网络安全、数据安全、个人信息保护等行政处罚案件。省、自治区、直辖市网信部门依职权管辖本行政区域内重大、复杂的网络信息内容、网络安全、数据安全、个人信息保护等行政处罚案件。国家网信部门依职权管辖应当由本部门实施行政处罚的案件及全国范围内重大、复杂的网络信息内容、网络安全、数据安全、个人信息保护等行政处罚案件。

征求意见稿规定网信部门办理个人信息保护案件可以采取查封、扣押等行政强制措施。采取或者解除查封、扣押措施，应当向网信部门主要负责人书面报告并经批准。情况紧急，需要当场采取查封、扣押措施的，执法人员应当在二十四小时内向网信部门主要负责人报告，并补办批准手续。网信部门主要负责人认为不应当采取查封、扣押措施的，应当立即解除。征求意见稿规定，当事人到期不缴纳罚款的，作出行政处罚决定的网信部门可以每日按罚款数额的百分之三加处罚款，加处罚款的数额不得超出罚款的数额。

11. 国务院国有资产监督管理委员会公布《中央企业合规管理办法》

9 月 16 日，国务院国有资产监督管理委员会公布《中央企业合规管理办法》。

办法要求，中央企业应当结合实际设立首席合规官，不新增领导岗位和职数，由总法律顾问兼任，对企业主要负责人负责，领导合规管理部门组织开展相关工作，指导所属单位加强合规管理。中央企业应当将合规审查作为必经程序嵌入经营管理流程，重大决策事项的合规审查意见应当由首席合规官签字，对决策事项的合规性提出明确意见。中央企业因违规行为引发重大法律纠纷案件、重大行政处罚、刑事案件，或者被国际组织制裁等重大合规风险事件，造成或者可能造成企业重大资产损失或者严重不良影响的，应当由首席合规官牵头，合规管理部门统筹协调，相关部门协同配合，及时采取措施妥善应对。

12. 民政部发布《民政部贯彻落实〈国务院关于加强数字政府建设的指导意见〉的实施方案》

9 月 28 日，民政部发布《民政部贯彻落实〈国务院关于加强数字政府建设的指导意见〉的实施方案》。方案围绕总体目标，明确构建协同高效的民政数

字化履职能力体系、科学规范的民政数字政府建设制度规则体系、民政数字政府全方位安全保障体系等五个方面十九项任务，并从加强组织领导、提升数字素养、强化分析评估三方面提出具体保障措施。

方案要求构建民政数字政府全方位安全保障体系。统筹做好民政数字政府建设安全和保密工作，落实主体责任和监督责任，加强督促指导和信息通报，形成跨地区、跨部门、跨层级的协同联动机制。建立数字政府安全责任落实和重大事件处置机制，加强对参与信息化建设、运营企业和人员的规范管理，确保政务系统和数据安全管理边界清晰、职责明确、责任落实。落实数据分类分级保护、风险评估等制度，加强数据全生命周期安全管理和技术防护，加大对涉及国家秘密、工作秘密、商业秘密、个人隐私和个人信息等数据的保护力度。加强关键信息基础设施安全保护和网络安全等级保护，定期开展网络安全、保密和密码应用检查。

13. 上海发布团体标准《网络安全保险服务规范》

9 月 28 日，上海银保监局指导上海市保险同业公会发布网络安全保险服务团体标准《网络安全保险服务规范》。标准对保险公司开展网络安全保险业务在承保、风控、理赔服务等各个环节制定统一标准要求，特别是针对承保前风险评估服务、承保中风险管控服务、事件发生后应急处置服务以及保险理赔服务明确要求。

上海银保监局表示，目前，网络安全保险的安全技术服务规范标准及服务能力评价标准也正在制定过程中，这两大配套标准将指导网络安全保险定点服务商开展相关安全服务支撑工作，并帮助相关方识别、评价各类网络安全保险服务供应商的能力。

三、回顾：2022 年全球网络安全研究分析报告盘点

（一）网络主权保障与国际合作

1. 北约 CCDCOE 发布《2030 年网络空间战略展望——全球观察和分析报告》

3 月 16 日，北约网络合作防御卓越中心（CCDCOE）发布《2030 年网络空间战略展望：全球观察和分析》（Cyberspace Strategic Outlook 2030：Horizon Scanning and Analysis）报告，从网络空间防御的背景、战略展望、态势分析到与全域联合作战的融合以及环境影响，完整分析 2030 年影响网络空间变革的驱动因素。

报告认为，到 2030 年影响网络空间的变革驱动因素包括：（1）网络空间域和相关作战环境。 2030 年最有可能发生的情况在很大程度上是当今全球权力动态的延续，中国和俄罗斯的军事现代化程度可能超过美国。鉴于网络空间作战与信息作战、电磁作战（EW）、信号情报（SIGINT）和空间作战相融合，并与其他域的作战活动相互影响，未来研究应考虑跨域作战的影响，以及引入新型漏洞和风险；（2）与网络空间相关的新兴和颠覆式技术。2020 年 3 月，北约将八项新兴和颠覆性技术指定为未来 20 年的主要关注对象，这些技术目前正处于发展的初期阶段或正在经历快速发展，包括数据、高超音速、生物技术和材料、AI、ML、深度神经网络、人机交互、数据分析/数据科学和量子技术等。这些技术的交互和组合将对网络空间领域产生深远影响；（3）网络空间变化的其他驱动因素。主要包括信息作战、国际法和规范、北约凝聚力和互操作性三方面。建议北约战略规划者必须考虑国家和国际法律框架将如何限制或促进进攻性网络空间行动。在未来十年的展望中，其很可能会达成范围更广的自愿性网络规范，以促进自由、开放、和平和安全的网络空间。

2. 美国国家情报总监办公室发布《美国情报界年度威胁评估报告》

3 月 8 日，美国国家情报总监办公室发布《美国情报界年度威胁评估报告》（Annual Threat Assessment of the U.S. Intelligence Community），重点关注未来一年美国面临的最直接、最严重的威胁。一方面，对中国、俄罗斯、伊

朗和朝鲜等国家，就区域和全球目标活动、网络技术以及对美国的不利影响等角度进行综合评估；另一方面，就新冠疫情、地区冲突等问题进行论述。

报告认为，中国仍将是美国技术竞争力的最大威胁，中国将继续深化与俄罗斯的外交、国防和技术合作，对美国形成挑战。俄罗斯仍将是美国的头号网络威胁，俄不断改进和运用其间谍、影响力和攻击能力，并将网络破坏视为影响其他国家决策的外交政策杠杆，以及威慑和军事工具。俄特别注重提高其针对美国以及盟国和伙伴国家的关键基础设施的能力，包括水下电缆和工业控制系统，因为破坏这些基础设施可以提高并展示其在危机期间破坏基础设施的能力。

3. 美国对外关系委员会发布《面对网络空间的现实：碎片化互联网的外交政策报告》

7 月 12 日，美国对外关系委员会（CFR）发布题为《面对网络空间的现实：碎片化互联网的外交政策》（Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet）的报告，提出美国应制定新的网络空间外交政策来应对互联网的新现实。

报告认为，全球互联网时代已经结束，当前的互联网更不自由、更加分散、更不安全。数字化程度的提高会增加脆弱性，网络犯罪已经构成国家安全风险，AI 和其他新技术将增加战略不稳定性，但大多数侵犯主权的网络攻击仍低于使用武力或武装攻击的门槛。美国不能将网络和信息作战视为两个独立的领域，且未能对攻击者施加足够的成本。起诉和制裁无助于阻止国家支持的黑客。美国需要制订新的战略和外交政策应对支离破碎且具有潜在危险的互联网。

报告提出网络外交政策的三大支柱和十六项具体建议：（1）美国应面对现实，围绕互联网的愿景巩固盟友的联盟，尽可能地保留一个可信、受保护的国际交流平台；（2）美国应对对手施加更有针对性的外交和经济压力，以及更具破坏性的网络行动；（3）美国应将数字竞争政策与国家安全战略体系更紧密地联系起来。

4. 新美国安全中心发布《重新连接：半导体与美国产业政策》报告

9 月 19 日，新美国安全中心（CNAS）发布《重新连接：半导体与美国产业

政策》（Rewire: Semiconductors and U.S. Industrial Policy）报告。报告探讨了当前半导体产业发展趋势以及全球产业政策发展史，为政策制定者提供建议。报告认为，当前美国政府应围绕半导体产业的四个主要目标制定政策：促进技术进步、确保半导体供应链安全、保持“卡脖子”以及减缓中国技术进步。

报告认为美国政府必须加强其在半导体产业领域的专业知识。在此基础上，政府有必要为半导体产业制定连贯的战略，可以在支持劳动力发展、资助技术研发方面发挥作用。此外，半导体产业的制造和组装能力过度集中在中国及其周边地区，这在发生地缘政治危机时会带来严重的中断风险，政府必须对此做好准备。

5. 美国 ITIF 发布《如何应对美国社交媒体上的政治宣传》报告

10 月 11 日，美国信息技术与创新基金会（ITIF）发布《如何应对美国社交媒体上的政治宣传》（How to Address Political Speech on Social Media in the United States）报告。报告指出，需要采取新的方法来应对美国社交媒体上的政治宣传危机：（1）美国政府应为七国集团建立国际论坛，在共同的民主价值观基础上为社交媒体制定内容管控准则；（2）美国政府应帮助平台对国家有害内容进行治理，例如可以资助识别来自对手国家虚假信息的学术研究；（3）国会应通过立法要求社交媒体平台披露其内容审核政策。然而内容审核存在合法性危机，有必要就内容审核准则达成国际共识，提供更多资源来解决虚假信息问题，提高内容审核透明度。技术方面，报告建议：（1）数据可移植性和互操作性要求。数据可移植性将允许用户导出他们的数据并在相互竞争的社交媒体平台之间转移。同时，互操作性将允许用户在不同社交媒体平台之间相互沟通；（2）公共资助。政府为平台提供资助以改善其算法。

6. 美国 CSIS 发布《切断中国通往人工智能之路——美国对人工智能和半导体的新出口管制标志着美中技术竞争的转变》

10 月 11 日，美国战略与国际问题研究中心（CSIS）发布《切断中国通往人工智能之路——美国对人工智能和半导体的新出口管制标志着美中技术竞争的转变》（Choking Off China’s Access to the Future of AI: New U.S. Export Controls on AI and Semiconductors Mark a Transformation of U.S. Technology

Competition with China）。报告以拜登政府新出台的全面对华出口管制政策为研究对象，从半导体技术供应链的角度，指出新管制政策意图从四个方面对中国进行制约。报告分析了政策背后拜登政府对于中美在半导体产业上的博弈、中美关系和AI的未来等三个关键问题的认识，最后着眼进一步提高新管制政策执行成效，报告指出了当前仍然存在的六方面挑战。报告认为，新管制政策彻底改变近几十年来的对华半导体政策，表明美国政府的干预达到前所未有的程度，目的是通过卡脖子彻底绞杀中国高科技产业。

新管制政策表明，美国正以空前规模运用其技术和地缘政治力量，将其在全球半导体供应链中占据主导的卡脖子技术武器化，这反映出拜登政府的三个关键认识：（1）中国愿意采取非常措施以逃避出口管制，摆脱对美国半导体供应链的依赖；（2）美国针对中国的目标是有限的，并不是意图迫使中国陷入经济衰退和通胀螺旋；（3）AI的发展潜力及其对国家安全的影响是真实可信的。

7. 美国CSIS发布《巨变——美国新的半导体出口管制及其对美国公司、盟友和创新生态的影响》

11月，美国战略与国际问题研究中心（CSIS）发布《巨变——美国新的半导体出口管制及其对美国公司、盟友和创新生态的影响》（A Seismic Shift——The New U.S. Semiconductor Export Controls and the Implications for U.S. Firms, Allies, and the Innovation Ecosystem）。报告指出，2022年10月，美国商务部工业与安全局宣布修改出口管制政策，旨在限制中国获得可用于军事领域的特定高端半导体器件、发展超级计算机、制造先进半导体器件的能力。新出口管制政策是美国近几十年来最广泛的出口管制行动，标志着传统策略发生根本性变化。

报告认为，新出口管制政策旨在遏制向中国转让设备、器件和专门知识，并确保无论中国投入多少资金，都无法实现与西方的技术平等。为实现这些目标，美国必须进行持续、多方面的“全政府”努力。美国对半导体的管制只是开始，美国正在考虑对其他一些关键技术制定新的出口规则。目前，美国政府可能装备不足、资源不足，对半导体产业及其错综复杂的全球供应链也知之甚少，因此情报界和国防界需要扩大招聘并与私营部门建立长期伙伴关系，以获取更多专业知

识，同时亟需吸引这方面的专业力量，制定必要的立法，建立新的体制结构，使新政策长期有效。

8. 美国布鲁金斯学会发布《美国半导体战略》报告

11 月 4 日,布鲁金斯学会发布《美国半导体战略》(A semiconductor strategy for the United States）。报告以“美国如何建立一个开放、长期、坚定、耐心、成功和全球性的政府战略”作为核心问题，表示深化美国目前的立场优势是解决这一问题的有效手段。报告建议政府的政策不仅要着眼于提高美国的制造能力，更要全面加强整个半导体行业，使其能够承受供应链冲击，推动技术转型，并赢得未来的行业控制点。

9. 欧盟发布《欧盟安全联盟战略》第四次进展报告

5 月 25 日，欧盟发布《欧盟委员会、欧洲议会和理事会关于<欧盟安全联盟战略>执行情况的第四次进展报告》(COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the Fourth Progress Report on the implementation of the EU Security Union Strategy）,对当前俄乌冲突国际环境下欧盟面临的安全威胁进行梳理。报告指出，尽管目前俄乌冲突在很大程度上仍然是通过常规手段推进，溢出效应有限，但也充分说明网络和关键基础设施领域面临的风险是真实存在的,进一步凸显落实现有立法及推动制定中立法的紧迫性。

10. 国家计算机病毒应急处理中心发布《“NOPEN”远控木马分析报告》

3 月 14 日，国家计算机病毒应急处理中心发布《“NOPEN”远控木马分析报告》，对名为“NOPEN”的木马工具进行攻击场景复现和技术分析。该木马工具针对 Unix/Linux 平台，可实现对目标的远程控制。根据“影子经纪人”泄露的 NSA 内部文件，该木马工具为美国国家安全局（NSA）开发的网络武器，是一款功能强大的综合型木马工具，也是 NSA 接入技术行动处（TAO）对外攻击窃密所使用的主战网络武器之一。

“NOPEN”主要用于文件窃取、系统提权、网络通信重定向以及查看目标设

备信息等，是 TAO 远程控制受害单位内部网络节点的主要工具。报告认为，“NOPEN”木马工具编码技术复杂、功能全面、隐蔽性强、适配多种处理器架构和操作系统，并且采用插件式结构，可以与其他网络武器或攻击工具进行交互和协作，是典型的用于网络间谍活动的武器工具。“NOPEN”支持多种植入运行方式，包括手动植入、工具植入、自动化植入等，其中最常见的植入方式是结合远程漏洞攻击自动化植入至目标系统中，以便规避各种安全防护机制。此外，TAO 还研发了一款名为 Packrat 的工具，可用于辅助植入“NOPEN”木马工具，其主要功能为对“NOPEN”木马工具进行压缩、编码、上传和启动。

11. 国家计算机病毒应急处理中心发布《西北工业大学遭美国 NSA 网络攻击事件调查报告（之一）》《美国 NSA 网络武器“饮茶”分析报告》《西北工业大学遭美国 NSA 网络攻击事件调查报告（之二）》

9 月，国家计算机病毒应急处理中心发布《西北工业大学遭美国 NSA 网络攻击事件调查报告（之一）》《美国 NSA 网络武器“饮茶”分析报告》《西北工业大学遭美国 NSA 网络攻击事件调查报告（之二）》，披露西北工业大学遭网络攻击事件调查结果。

2022 年 6 月 22 日，西北工业大学发布公开声明称该校遭受境外网络攻击。陕西省西安市公安局碑林分局随即发布警情通报，证实在西北工业大学的信息网络中发现了多款源于境外的木马样本，西安警方已对此正式立案调查。国家计算机病毒应急处理中心和 360 公司联合组成技术团队，全程参与此案技术分析工作。技术团队先后从西北工业大学的多个信息系统和上网终端中提取到多款木马样本，综合使用国内现有数据资源和分析手段，并得到欧洲、南亚部分国家合作伙伴的通力支持，全面还原相关攻击事件的总体概貌、技术特征、攻击武器、攻击路径和攻击源头，初步判明相关攻击活动源自美国国家安全局（NSA）“特定入侵行动办公室”（TAO）。

调查发现，TAO 近年里对中国国内的网络目标实施上万次的恶意网络攻击，控制数以万计的网络设备，窃取超过 140GB 的高价值数据。TAO 利用其网络攻击武器平台、“零日漏洞”及其控制的网络设备等，持续扩大网络攻击和范围。经技术分析与溯源，技术团队现已澄清 TAO 攻击活动中使用的网络攻击基础设施、

专用武器装备及技战术，还原攻击过程和被窃取的文件，掌握NSA及其下属TAO对中国信息网络实施网络攻击和数据窃密的相关证据，涉及在美国国内对中国直接发起网络攻击的人员13名，以及NSA通过掩护公司为构建网络攻击环境而与美国电信运营商签订的合同60余份，电子文件170余份。

报告指出，在针对西北工业大学的网络攻击中，TAO使用40余种不同的NSA专属网络攻击武器，持续对西北工业大学开展攻击窃密，窃取该校关键网络设备配置、网管数据、运维数据等核心技术数据。通过取证分析，技术团队累计发现攻击者在西北工业大学内部渗透的攻击链路多达1100余条、操作的指令序列90余个，并从被入侵的网络设备中定位了多份遭窃取的网络设备配置文件、遭嗅探的网络通信数据及口令、其它类型的日志和密钥文件以及其他与攻击活动相关的主要细节。TAO使用“饮茶”作为嗅探窃密工具，将其植入西北工业大学内部网络服务器，窃取SSH、TELNET、FTP、SCP等远程管理和远程文件传输服务的登录密码，从而获得内网中其他服务器的访问权限，实现内网横向移动，并向其他高价值服务器投送其他嗅探窃密类、持久化控制类和隐蔽消痕类网络武器，造成大规模、持续性敏感数据失窃。据分析，TAO利用相同的武器工具组合，“合法”控制了全球不少于80个国家的电信基础设施网络。

12. 卡巴斯基发布《2022年第一季度DDoS攻击数据》

4月25日，卡巴斯基发布《2022年第一季度DDoS攻击数据》（DDoS attacks in Q1 2022），显示自2月份以来，围绕俄乌争端导致的DDoS攻击达到空前规模，DDoS攻击数量突破历史最高水平。报告显示，与2021年第四季度相比，2022年第一季度的DDoS攻击增加46%，大部分攻击被用于针对俄罗斯。同时，DDoS攻击的持续时间也比去年要长，几乎是2021年末的80倍。

卡巴斯基安全专家表示，DDoS攻击的上升趋势在很大程度上受到地缘政治局势影响，非常不寻常的是DDoS攻击持续时间很长，持续数天甚至数周，表明攻击背后有政治因素推动。

13. 微软发布《乌克兰——俄罗斯在乌克兰网络攻击活动总览报告》

4月27日，微软公司发布《特别报告：乌克兰——俄罗斯在乌克兰网络攻

击活动总览》（Special Report：Ukraine——An overview of Russia’s cyberattack activity in Ukraine），详细介绍俄罗斯在战前及战争爆发后针对乌克兰开展的网络攻击活动，透析俄罗斯在针对乌克兰的“混合战争”中使用网络能力的范围、规模和方法。

报告称，早在2021年3月，与俄罗斯武装力量总参谋部情报总局、联邦对外情报局和联邦安全局相关的威胁行为体就开始为冲突做准备，并加强对乌克兰及其盟国的攻击活动。微软观察到，针对乌克兰的破坏性网络攻击接近40次，目标涉及数百个系统，至少有8个破坏性恶意软件系列被部署在乌克兰网络上。其中，32%的攻击直接针对乌克兰国家、地区和城市层面的政府机构，超过40%的攻击针对关键基础设施机构，针对后者的攻击可能对乌克兰政府、军队、经济和平民产生二阶负面影响。

报告还发现，俄罗斯网络攻击与军事行动密切相关，有时甚至直接与其同步，在针对乌克兰宣传机构、马里乌波尔等的打击行动中体现得尤为明显；俄罗斯网络攻击活动与俄乌局势及政治外交活动存在关联，战前已预先对乌克兰和北约成员国开展网络渗透活动为后续活动做准备，并在局势紧张时发起破坏性网络攻击，战争爆发后持续开展网络攻击以支持军队的战略和战术目标。

14. 微软发布《保卫乌克兰：网络战争的早期教训》

6月22日，微软公司发布新报告《保卫乌克兰：网络战争的早期教训》（Defending Ukraine: Early Lessons from the Cyber War），揭示有关俄罗斯网络活动的新信息，提供从所收集和分析数据中得出的一系列经验教训和结论，并呼吁采取协调和全面的战略来加强集体防御。

微软总裁兼副主席布拉德·史密斯在新报告的前言部分表示，俄乌战争反映出过去两个世纪其他重大冲突中出现的趋势，即各国使用最新技术发动战争，而战争本身加速了技术变革。俄罗斯的军事行动部分依赖于网络战略，该战略至少包括三项不同但互相协调活动，包括针对乌克兰境内的破坏性网络攻击、针对乌克兰境外的网络渗透和间谍活动以及针对世界各地民众的网络影响行动。网络空间的独特性决定俄乌战争所带来的网络威胁不会局限于乌克兰，这彰显出新的集体防御方法的必要性。

报告得出五方面的经验教训：（1）国家需具备将数字业务和数据资产跨境转移到其他国家的能力，从而能够在战争中维持民事和军事行动；（2）网络威胁情报和端点保护的最新进展帮助乌克兰抵御了高比例的破坏性俄罗斯网络攻击，体现出网络防御的相对优势；（3）俄罗斯情报机构加强针对乌克兰以外盟国的网络渗透和间谍活动，具体涉及政府、智库、人道主义组织、IT 公司以及能源和其他关键基础设施供应商等目标；（4）俄罗斯机构正在开展全球网络影响力行动以支持其战争活动，上述行动具有范围广泛、数量众多、目标精确、敏捷快速的特点，并重点针对俄罗斯、乌克兰、美国和欧洲、不结盟国家等四类受众开展各具特定目标的定向宣传；（5）俄乌战争体现出需要采取协调和全面的多边和多方利益攸关方战略，以加强对全方位网络破坏、间谍和影响行动的防御，应在“数字策略、公私合作、多边主义、言论自由”四项原则基础上提高集体应对能力，更好地检测、防御、破坏和阻止外国网络威胁。

15. 兰德发布《信息领域竞争：俄罗斯的信息对抗概念》报告

8 月 18 日，兰德公司发布《信息领域竞争：俄罗斯的信息对抗概念》（Rivalry in the Information Sphere：Russian Conceptions of Information Confrontation）。报告建议，美国情报界应研究俄罗斯的军事科学文献，以更好地了解俄罗斯在信息领域的活动和意图，并深入了解信息在俄罗斯军事战略中的作用以及俄罗斯如何看待美国的信息行动。美国军事情报部门还应审查公开的、公开来源的和非机密的俄语报告。美国军方应更密切地监视俄罗斯关于歪曲历史事实的言论，并将其作为信息对抗的新兴工具，特别是在东欧地区。美国应将乌克兰学术界也共同参与到研究中，以纳入乌克兰和其他国家的学术文献。报告指出，俄罗斯军事科学文献中详细讨论了信息对抗，但对如何定义该术语存在分歧，相关但有所区别的术语是信息影响（information influence）和信息战（information warfare）。俄罗斯的军事科学文献中经常将信息武器的战略影响等同于大规模杀伤性武器的战略影响。执行信息对抗的国家行为者包括军队和安全部门，非国家行为体也会为信息对抗提供支撑。曾经在战斗中发挥辅助作用的信息活动正在发展成为现代混合战争的核心。

对此，报告建议，美国情报界应研究俄罗斯的军事科学文献，以更好地了解

俄罗斯在信息领域的活动和意图，并深入了解信息在俄罗斯军事战略中的作用以及俄罗斯如何看待美国的信息行动。美国军事情报部门还应审查公开的、公开来源的和非机密的俄语报告。美国军方应更密切地监视俄罗斯关于歪曲历史事实的言论，并将其作为信息对抗的新兴工具，特别是在东欧地区。美国应将乌克兰学术界也共同参与到研究中，以纳入乌克兰和其他国家的学术文献。混合战争中的信息对抗，即如何将其作为软实力的工具，以及国际治理机制如何规范未来的信息对抗，需要进一步研究。

（二）网络安全管理

1. 美国 CISA 发布《公共安全陆地无线移动通信安全白皮书》

1 月 10 日，美国网络安全与基础设施安全局（CISA）发布《公共安全陆地无线移动通信安全白皮书》（Public Safety Land Mobile Radio Communications Security）。白皮书简明扼要地解释了通信安全的重要性、通信安全计划的基本要素，以及如何制定有效的策略来防止和减少未经授权的信息访问。白皮书定义通信安全（COMSEC）是一组用于保护敏感信息的集成策略、过程和技术。同时，白皮书是在不影响互操作性的情况下实施加密的最佳实践，指出加密是通信安全的关键组件。

2. 美国网络安全局发布《NSA2021 年度回顾报告》

2 月 3 日，美国国家安全局下设网络安全局（NSA Cybersecurity Directorate）发布《NSA2021 年度回顾报告》（2021 NSA Cybersecurity Year in Review）。报告中，网络安全局认为其在 2021 年取得的主要成果包括：（1）与中国、俄罗斯等对手展开网络空间战略竞争；（2）建立及加强外联合作关系；（3）防御针对美国军事网络的攻击并支持美军作战司令部的作战行动。

3. 美国 NIST 发布《基于网络安全风险的企业风险管理报告》

2 月 10 日，美国国家标准与技术研究院（NIST）发布 NISTIR 8286B《优先考虑网络安全风险的企业风险管理》报告（Prioritizing Cybersecurity Risk

for Enterprise Risk Management）。

本报告作为NIST机构间/内部报告NISTIR 8286《整合网络安全和企业风险管理》的补充性文件，是该系列文件中的第二个文件。该系列报告提供了更多有关企业应用网络安全风险信息的详细信息，描述了根据这些风险对企业的潜在影响，以确定每个风险的优先级。NISTIR 8286B还描述了如何将风险优先级和风险响应信息添加到网络安全风险登记册（CSRR），有关风险响应的选择和预计成本的信息将用于维护整个企业的网络安全风险综合研判。

4. 美国GAO发布《关于互联网架构是有弹性的，但联邦机构仍需应对风险的报告》

3月3日，美国政府问责局（GAO）发布《关于互联网架构是有弹性的，但联邦机构仍需应对风险的报告》（Cybersecurity: Internet Architecture is Considered Resilient, but Federal Agencies Continue to Address Risks）。

报告指出，尽管互联网具有弹性，但美国政府仍然需要应对风险。通信部门运营着多个独立网络，这些独立网络构成互联网基础。为了支持网络流量的交换，服务提供商使用许多组件来管理和控制核心基础设施要素，包括连接国内和国际网络的互联网交换点和海底电缆登陆站，由此就有意或无意造成的互联网面临各种网络和物理风险。报告认为，联邦政府应就这一问题采取以下措施：（1）指导关键基础设施保护和私营部门参与；（2）参与国际网络外交；（3）支持网络研发；（4）协调网络事件响应；（5）调查和起诉网络犯罪；（6）制定安全标准；（7）对美国通信网络部分进行监管；（8）解决与数据路由硬件和服务相关的供应链问题；（9）操作域名系统根区域服务器；（10）颁发登陆和运营海底电缆的许可证。

5. 美国HPH发布《医疗保健和公共卫生部门勒索软件趋势报告》

5月5日，美国卫生与公众服务部（HPH）发布《医疗保健和公共卫生部门勒索软件趋势报告》（Ransomware Trends in the HPH Sector）。

报告指出，2022年第一季度影响HPH行业的前5名RaaS组织分别是LockBit、Conti、SunCrypt、ALPHV/Blackcat和Hive。同时，勒索软件组织越来越多地在

勒索软件入侵期间利用合法的工具，如远程访问工具、加密工具、文件传输工具、开源软件等。出于经济动机和由国家资助的威胁行为者很可能会继续更新其战术、技术和程序，以成功实施攻击。合法工具可能会继续在勒索活动中被滥用或武器化。此外，报告提出 17 项防范措施，包括使用主机防火墙限制文件共享通信、使用网络签名的网络入侵检测和预防系统、对用户和特权帐户使用多因素身份验证、对敏感域进行网络分段等。

6. 美国商会发布《美国中间市场商业指数报告》

6 月 2 日，美国商会发布年度网络安全专题报告《美国中间市场商业指数》（RSM US middle market business index），认为尽管当前中间市场正在向着正确的方向发展，网络安全事件的报告数量也有所下降，但仍然需要高度关注网络安全风险。

报告指出，2021 年，大型企业的网络安全事件占据了大多数，这表明没有任何企业能够真正对网络安全事件“免疫”。中间市场，特别是那些脱离公共关注的中间市场，更容易成为网络犯罪分子的关注焦点，因为网络犯罪分子可以更为便利地通过中间市场中缺乏有效安全控制措施的中小企业寻找漏洞，实施网络攻击或破坏活动。2021 年中间市场报告的网络安全事件数量大幅度下降（只有 22%的中间市场企业报告发生了网络安全事件），这得益于有效的保护措施。但不可否认的是，中间市场企业对此仍然不能掉以轻心，未经授权的信息和信息系统访问仍然存在风险。尽管网络安全事件的报告数量有所下降，但报告指出，大部分中间市场企业仍然认为自身处于明显的风险环境中，72%的中间市场企业预测其会遭遇未经授权的数据或系统访问。

7. 美国 GAO 发布《网络保险：需要采取行动评估联邦政府对灾难性网络攻击的潜在反应报告》

6 月 21 日，美国政府问责局（GAO）发布题为《网络保险：需要采取行动评估联邦政府对灾难性网络攻击的潜在反应》（Cyber Insurance：Action Needed to Assess Potential Federal Response to Catastrophic Attacks）的报告，要求联邦政府评估是否需要提供联邦网络保险服务。

报告认为，鉴于以美国实体为目标的恶意网络行为者范围广泛且技能不断提高，网络事件数量正以惊人的速度上升。尽管联邦机构没有全面的网络安全事件清单，但几个关键的联邦和行业消息来源显示美国的网络攻击正在增加，网络攻击规模和成本在不断扩大。由于有不得不承担如此巨大损失的可能性，私人保险公司正在退出市场，将一些最高级别的网络攻击排除在保险单的覆盖范围之外。虽然通常仍涵盖数据泄露和勒索攻击，但报告发现“私人保险公司一直在采取措施限制系统性网络事件造成的潜在损失”，拒绝承担网络战行为或蓄意的基础设施攻击所造成的损失。根据美国财政部的说法，一些保险公司也一直在通过降低保单在网络攻击情况下支付的最高金额和/或增加保费来减轻风险，以保护自己免受损失。GAO 发现，有进一步证据表明，一些保险公司正在完全退出基础设施领域的保险，并认为受到攻击的风险太高。

8. 美国网络安全审查委员会发布《2021 年 12 月 Log4j 漏洞事件审查报告》

7 月 11 日，美国网络安全审查委员会（Cyber Safety Review Board）发布首份报告《2021 年 12 月 Log4j 漏洞事件审查报告》（Review of the December 2021 Log4j Event），指出 Log4j 漏洞已成为“流行病”，将在未来十年甚至更长时间持续引发风险。报告的最后部分提出了 19 条建议，具体包括应对 Log4j 漏洞产生的持续性影响、落实网络安全现有最佳实践、营造更好的软件生态系统、投资于未来的网络安全，以供各实体在 Log4j 漏洞威胁下采用。

报告耗时约五个月，共采访约 80 个组织，并与行业、外国政府及安全专家开展信息交流。委员会还与中国政府代表进行了沟通，因为最初发现并上报这个开源软件工具漏洞的正是阿里巴巴的工程师。

9. 大西洋理事会发布《龙之尾：坚持国际网络安全研究》

9 月 14 日，大西洋理事会发布《龙之尾：坚持国际网络安全研究》（Dragon tails: Preserving international cybersecurity research）。报告指出，由安全研究人员、黑客和漏洞猎手组成的国际社区中，成员通常会发现并披露关键漏洞，然而各国围绕漏洞披露的政策法律中往往未能将这些主体纳入考量。报告分析了一系列中国监管变化对漏洞披露的影响，并进一步指出，虽然国家法规在

某些情况下确实会影响漏洞研究，但影响程度可能比预期的小。因此，应当降低漏洞研究和披露的准入门槛，提升全球漏洞披露研究的健康程度。

10. 美国 CSIS 发布《勒索攻击中的艰难选择》报告

9 月 28 日，美国战略与国际研究中心（CSIS）发布《勒索攻击中的艰难选择》（Hard Choices in a Ransomware Attack）报告。报告站在受害者角度，全面展现出其在遭遇勒索攻击、事件响应、与恶意行为者沟通、决定是否支付赎金等方面的无力感。报告认为，实体在应对勒索攻击时取决于在攻击发生之前做出的决定，鼓励政府和行业为勒索攻击防御提出建议。

11. 欧盟两部门联合发布《提高组织网络安全弹性报告》

2 月 14 日，欧盟网络安全局（ENISA）和 CERT-EU 发布《联合出版物——提高组织网络安全弹性报告》（Joint Publication——Boosting your Organisation’s Cyber Resilience），主要面向决策者（包括 IT 和一般管理人员）、安全官员（如 CISO）、支持组织风险管理的实体。

报告通过系统一致的方式提高欧洲的整体网络弹性，指导组织应根据其特定的业务需求确定行动优先级。具体的最佳实践包括：（1）对可远程访问的服务部署多因素身份验证；（2）鼓励用户在应用程序支持的情况下（例如在社交媒体上）使用多因素身份验证；（3）确保所有软件都是最新的；（4）严格控制第三方对组织内部网络和系统的访问；（5）在将关键负载转移到云之前，应特别注意强化组织的云环境；（6）查看组织的数据备份策略；（7）更改所有默认凭据并禁用不支持多因素身份验证或使用弱身份验证的协议；（8）在做出访问决策时，采用适当的网络分段和限制来限制访问并利用附加属性；（9）进行定期培训，以确保 IT 和系统管理员对组织的安全政策和相关程序有充分的了解；（10）定期组织网络意识活动，以培训组织的用户了解常见的网络钓鱼技术及网络钓鱼攻击的影响等。

12. 欧盟 ENISA 发布《欧盟协同漏洞披露政策报告》

4 月 13 日，欧盟网络安全局（ENISA）发布《欧盟协同漏洞披露政策》

（Coordinated Vulnerability Disclosure Policies in the EU）报告。报告全面概述欧盟成员国和美国、日本、中国协同漏洞披露（CVD）的现状和主要措施，概述欧盟在实施CVD政策时面临的各种挑战并提出具体建议。

报告认为，欧盟实施CVD政策需要应对来自法律、经济等方面的挑战。各国在制定CVD政策时，需要评估以下方面的挑战在多大程度上将造成政策制定和实施的阻碍：（1）法律障碍。安全研究人员面临着重大的法律风险；（2）利益攸关方之间缺乏合作；（3）政府对漏洞利用的模棱两可；（4）市场激励有限；（5）财政和人力资源挑战。报告给出的主要建议包括：（1）修订刑法和网络犯罪指令，为参与漏洞发现的安全研究人员提供法律保护；（2）在为安全研究人员建立法律保护之前，明确定义区分“道德黑客”和“黑帽”活动的具体标准；（3）通过国家或欧洲漏洞赏金计划，或通过促进和开展网络安全培训，为安全研究人员制定积极参与CVD研究的激励措施。

具体来说，国家刑法应对安全研究人员提供免责的可能性，成员国可以修订其刑法，为参与发现漏洞的研究人员创造法律确定性和必要的“安全港”，同时也承认“道德黑客”的行为。修订“网络犯罪指令”，以便为参与发现漏洞的安全研究人员提供法律确定性，并允许界定各成员国的共同规则和程序，以便在欧洲建立一个协调的漏洞披露共同程序。

13. 欧盟ENISA发布《2021年电信安全事件报告》《2021年可信服务安全事件报告》

7月27日，欧盟网络安全局（ENISA）发布《2021年电信安全事件报告》（Telecom Security Incidents 2021)和《2021年可信服务安全事件报告》(Trust Services Security Incidents 2021）。

《2021年电信安全事件报告》提供了2021年重大电信安全事件信息，指出成员国在2021年报告的168起电信安全事件中，7%是由系统故障造成，90%是由人为错误造成的。《2021年可信服务安全事件报告》概述了2021年通报的违规事件，分析了统计数据、根本原因和趋势，指出通报的事件正在稳步增加。其中，47%的事件是由系统故障造成的，而由恶意行为造成的事件增加了20%。

14. 欧盟ENISA发布《勒索攻击威胁态势报告》

7月29日，欧盟网络安全局（ENISA）发布《勒索攻击威胁态势报告》（ENISA Threat Landscape for Ransomware Attacks）。

报告分析了2021年5月至2022年6月报告期内欧盟、英国和美国共发生的623起勒索攻击事件。数据来自政府和安全公司的报告、媒体、经过验证的博客，以及来自暗网的部分资源。报告指出，2021年5月至2022年6月期间，勒索软件威胁参与者每月窃取大约10 TB的数据，58.2%的被盗数据包括员工个人数据。94.2%的事件不清楚受害组织是否支付了赎金。据统计，当受害组织与攻击者协商失败时，攻击者通常会在他们的网页上公开数据，有37.88%的受害组织遭遇此种情况。因此，报告认为，其余62.12%的组织要么与攻击者达成协议，要么找到了另外的解决方案。

15. 欧盟ENISA发布《2022年网络安全威胁全景报告》

11月，欧盟网络安全局（ENISA）发布第十版《2022年网络安全威胁全景报告》（ENISA Threat Landscape 2022），对年度网络安全状况进行总结。报告指出在大多数网络事件中，事件所产生的影响仍是“未知的”，因为受害者不清楚影响其组织的程度或类型，或者出于对声誉产生连带影响的担忧而不愿意披露这类信息。缺乏来自目标组织的可靠数据，使得报告很难全面了解情况。

报告指出，在报告期间，勒索软件和针对可用性的威胁仍排在第一位。组织越是提高其防御和网络安全计划的成熟度，攻击者的成本也会随之提高，进而促使他们开发和/或购买零日漏洞。自2021年以来，黑客技术即服务的商业模式越来越受欢迎。同时，数据泄露事件逐年增加。勒索软件集团在供应链攻击和针对管理服务提供商（MSP）的攻击中表现出越来越强的能力。勒索软件集团会采取“退休”和品牌重塑的方法来避免执法和制裁。此外，网络钓鱼再次成为初始访问的最常见载体。网络钓鱼的复杂性、用户疲劳和有针对性的、基于环境的网络钓鱼导致了这种增长。地缘政治继续对网络行动产生重大影响，破坏性攻击是国家行为者行动的重要组成部分。

16. 欧洲 ENISA 发布《2022 年网络威胁态势》

11 月 3 日，欧洲网络与信息安全局（ENISA）发布《2022 年网络威胁态势》（ENISA Threat Landscape 2022）。报告指出，2021 年 7 月至 2022 年 7 月间，由于每月有超过 10TB 的数据被盗，因此勒索软件仍然是报告期内的主要威胁之一，网络钓鱼成为此类攻击最常见的初始载体。同时，受地缘政治局势，特别是俄罗斯入侵乌克兰影响，在报告期内改变了全球网络领域的游戏规则。虽然威胁数量也在增加，但出现了更广泛的传播媒介，例如利用零日漏洞和 AI 支持的虚假信息和深度伪造，导致攻击的危害程度和波及范围更加广泛，具有更大的破坏性影响。

17. 英国政府发布《2022 年网络安全激励和监管审查报告》

1 月 19 日，英国政府发布《2022 年网络安全激励和监管审查报告》（2022 cyber security incentives and regulation review），指出英国组织目前没有足够的强有力措施来成功抵御迅速增加的网络攻击风险。

报告指出，提高经济社会的网络弹性是抵御网络攻击的第一道防线。2016 年以来，政府在应对网络威胁和提高英国社会和经济的复原力方面取得重大进展。但当前更广泛的业务框架尚未有效激发整个业务所需的治理和问责制。为此，政府需要更加主动地干预。报告指出，未来英国政府将在以下四个关键政策领域采取行动：（1）基石：就网络风险管理和推广可信服务提供建议和指导；（2）能力：支持能够提供建议和指导的熟练专业人员；（3）市场激励：与市场参与者合作，为组织投资网络安全措施创造激励机制；（4）问责制：让组织对其网络风险的有效管理负责。其中，基石和能力侧重于政府如何为企业提供工具、支持和技能，市场激励和问责制关注的是从市场驱动或监管角度刺激网络安全实践。

18. 英国 DCMS 发布《2022 年英国劳动力市场的网络安全技能报告》

5 月 3 日，英国数字、文化、媒体和体育部（DCMS）发布题为《2022 年英国劳动力市场的网络安全技能》（Cyber security skills in the UK labour market 2022）的报告。报告针对英国网络安全劳动力现状，探讨当前英国网络安全技能

差距（缺乏适当技能的人）和技能短缺（缺乏从事网络安全工作的人）情况。

报告主要结论包括：（1）在整体经济中，基本技术领域的技能差距仍很常见。与此同时，事件管理相关技能差距也在增加；（2）虽然网络安全企业也在持续应对技术技能差距问题，但求职者缺乏技能在今年已成为一个更为严重的问题；（3）随着对网络技能需求的增加，网络雇主和求职者了解培训需求、能够识别高质量的外部培训比以往任何时候都更重要；（4）证据表明，网络部门雇佣越来越多的职业初学者，劳动力多样性得到改善。未来几年数据将有助于证实这两种趋势；（5）网络雇主和网络团队将继续受疫情影响。

19. 瑞士国家网络安全中心发布《NCSC 半年度报告》

5 月 5 日，瑞士国家网络安全中心（NCSC）发布《NCSC 半年度报告》（NCSC semi-annual report），披露 2021 年下半年在瑞士和国际上最重要的网络事件。

报告指出，报告期内，国家网络安全委员会共收到网络事件报告 11,480 件，其中大部分涉及各类欺诈行为。特别是，据称由执法机构发送的电子邮件经常被举报。其他报告涉及预付款欺诈、投资欺诈、首席执行官欺诈和分类广告欺诈。在一些欺诈行为者中出现了采用更精细、定制化方法的趋势，他们会为受害者工作很长一段时间，以便在实际试图欺骗他们之前建立信任。2021 年下半年，还出现了多起勒索攻击。软件组件漏洞方面，报告指出，诸如库或开源代码之类的现有组件通常用于软件开发。但是，这些也可能存在漏洞。如果发现此类漏洞，则必须在所有集成了该漏洞的组件的产品中进行修复。

20. 德国 BSI 发布《2022 年德国 IT 安全状况报告》

10 月 25 日，德国联邦信息安全办公室（BSI）发布《2022 年德国 IT 安全状况》（Die Lage der IT-Sicherheit in Deutschland 2022）报告，指出在 2021 年 6 月至 2022 年 5 月的报告期内，本已紧张的局势继续恶化。报告指出，高威胁水平的原因是网络犯罪领域的持续活动、俄罗斯袭击乌克兰背景下的网络攻击以及在许多情况下 IT 产品和软件的安全水平不足。软件或硬件产品中的每个漏洞都是攻击者的潜在门户，并危及管理、企业和社会中的信息安全。2021 年，软件产品中注册了超过 20，000 个漏洞，较上一年相比增长 10%。

21. 日本NISC发布《2021年度网络安全报告》

6月17日，日本国家网络安全事件准备和战略中心（NISC）发布《网络安全2022（2021年度报告，2022年度计划）》（サイバーセキュリティ2022（2021年度年次報告・2022年度年次計画））。报告阐述了网络空间的近期变化、因形势变化而产生的政策问题，以及实现“自由、公平和安全的网络空间”的措施。报告着眼于加强包括重要基础设施在内的网络安全，还建议加强中小型企业网络安全，确保供应链可持续性。

22. 巴西联邦审计法院发布《联邦公共管理局的高风险清单报告》

7月，巴西联邦审计法院（TCU）发布《联邦公共管理局的高风险清单》（Lista de alto risco na Administração Pública Federal）报告，显示巴西绝大多数联邦政府组织面临网络攻击高风险，可能影响政府服务质量和公共政策效力。

报告列举了最近发生的重大网络安全事件，其中针对卫生部的网络攻击导致2019年新冠肺炎疫苗接种数据丢失，以及针对高等法院的攻击，被称为“从规模和复杂性来看，是针对巴西公共机构最严重的网络攻击”。报告指出，参与调查的组织中，74.6%的组织没有正式批准的备份政策，71%将系统托管在自己的服务器上且没有针对其主系统的特定备份计划。60.2%的组织没有将数据备份保存在至少一个不可远程访问的目的地，这就带来了备份文件本身可能最终被攻击者或恶意软件实施破坏、删除和/或加密的风险。66%采取了备份措施的联邦政府机构没有使用加密，超过80%的组织处于IT业务连续性能力建设的早期阶段。针对上述缺陷，报告指出必须采取基本措施，确保在发生安全事件时业务流程和服务提供的连续性，包括“实施一般政策和连续性计划，以及维持有效的内部控制。”

23. 中国互联网络信息中心发布第50次《中国互联网络发展状况统计报告》

8月31日，中国互联网络信息中心（CNNIC）发布第50次《中国互联网络发展状况统计报告》。《报告》显示，截至2022年6月，我国网民规模为10.51亿，互联网普及率达74.4%。

互联网安全状况方面，报告发现，2022年上半年，中国电信、中国移动和中国联通总计监测发现DDoS攻击316,542起，较2021年同期（368,374起）下

降 14.1%。工业和信息化部网络安全威胁和漏洞信息共享平台总计接报网络安全事件 15,654 件，较 2021 年同期（49,605 件）下降 68.4%。

24. 中国信息安全测评中心发布《2022 上半年网络安全漏洞态势观察报告》

9 月 2 日，由中国信息安全测评中心牵头编写的《2022 上半年网络安全漏洞态势观察》报告发布。报告围绕漏洞数量变化趋势、漏洞危害、漏洞利用、漏洞管控等内容，把握总体形势，分析关键漏洞现实威胁，并在漏洞管控与综合治理、感知与预警、供应链安全与开源治理等方面提出对策建议。

报告指出，2022 年上半年，网络安全漏洞形势依旧严峻，高危漏洞数量不断增长，漏洞利用渐趋隐蔽，融合叠加风险攀升，在野漏洞利用成为重大网络安全热点事件的风险点以及国家级 APT 活动的新手段。美欧国家从漏洞发现收集、修复消控、协同披露、出口管制等层面加大管控力度。对策建议方面，报告认为多措并举加强漏洞安全防范与保障成为当务之急。一是进一步强化国家级网络安全漏洞综合治理能力，加强漏洞管控统筹协调，提升漏洞资源共享共治水平；二是建设国家级漏洞感知与预警机制，提升漏洞发现与处置能力；三是积极推进 ICT 供应链安全治理，完善符合我国情的开源生态。

25. 医疗物联网安全公司发布《2022 年医疗保健行业互联设备不安全性报告》

8 月 3 日，医疗物联网安全公司 Cynerio 与 Ponemon Study 共同发布《2022 年医疗保健行业互联设备不安全性报告》（Insecurity of Connected Devices in HealthCare 2022 Report）。报告研究了网络攻击对医疗保健设施以及物联网和联网医疗设备产生的影响，报告的数据基于来自美国各地医院和医疗保健系统领导职位的 517 名医疗保健专家的数据。

56%的受访者表示他们的组织在过去 24 个月中经历了一次或多次涉及物联网/物联网设备（IoT/IoMT 设备）的网络攻击，在同一时间范围内平均发生 12.5 次攻击。报告称，45%的受访者认为这些攻击对患者护理产生了不利影响，其中 53%报告了导致死亡率增加的不利影响。此外，过去 24 个月至少经历过一次网络攻击的 56%的受访者中，82%在该时间范围内平均经历了四次或更多次攻击。勒索攻击的发生率大致相当，43%经历过攻击，76%平均遭受过三次或更多次攻击。

报告称，勒索攻击导致医院越来越多地将赎金支付视为快速恢复的可行选择，其中47%的遭受攻击的人需要支付赎金。32%的赎金在250,000美元至500,000美元之间。同时，没有支付赎金的人最常将其行为归因于有效的备份策略（53%）和公司政策（49%）。报告还发现患者数据仍然很有价值，43%的受访者在过去24个月中至少遭受过一次数据泄露。其中，65%在该时间段内平均遭受五次或更多次数据泄露，其中88%的时间涉及IoT/IoMT设备。对于参与研究的组织而言，最大数据泄露的平均总成本估计为1300万美元。

26. 解决方案提供商Kroll发布《2022年第二季度威胁形势：勒索软件回归，医疗保健行业遭受打击报告》

8月11日，解决方案提供商Kroll发布报告《2022年第二季度威胁形势：勒索软件回归，医疗保健行业遭受打击》（Q2 2022 Threat Landscape: Ransomware Returns, Healthcare Hit）。报告显示，勒索软件助长了对医疗保健行业的网络攻击，因为本季度的攻击增加，再次成为最大威胁，紧随其后的是电子邮件泄露。与今年第一季度相比，目标医疗机构的数量增加了90%，因为越来越多的勒索软件使用远程服务进行初始访问，影响网络安全。

报告显示，影响医疗保健行业的常见威胁事件类型包括勒索软件（33%）、未经授权的访问（28%）和电子邮件泄露（28%）。在勒索软件案例中，常见的是双重勒索策略，网络钓鱼是影响医疗保健行业的常见初始访问方法。报告称，虽然攻击者继续利用漏洞和网络钓鱼计划来部署勒索软件，但在第二季度，勒索软件最有可能通过外部远程服务侵入。报告观察到，本季度用于初始访问的远程桌面协议（RDP）和虚拟专用网络（VPN）等外部远程服务增加700%。基于此，报告呼吁医疗机构密切关注远程服务安全，并建议在这些系统上实施多因素身份验证，保持远程服务无法从Internet访问；维护定期修补、测试和漏洞扫描计划，特别是针对VPN和RDP服务中的安全漏洞。

27. 奇安信等发布《2022医疗卫生行业网络安全分析报告》

8月18日，由奇安信行业安全研究中心联合补天漏洞响应平台、奇安信安全托管团队、奇安信安服团队、安全内参共同撰写的《2022医疗卫生行业网络

安全分析报告》正式发布。《报告》内容涉及医疗卫生行业网站2100个，应急响应事件84起，及百余起医疗卫生行业网络安全运营风险事件。

报告显示，从整体来看，补天平台2021年共收录全国医疗卫生行业相关网站的安全漏洞2568个。其中，高危漏洞占比为38.4%。从漏洞的技术类型来看，信息泄露漏洞最多，占比为21.7%，其次是命令执行漏洞，占比为21.0%，弱口令漏洞，占比为13.4%。但医疗卫生行业网络安全建设水平在近年来得到快速提升。以补天平台收录的医疗卫生行业网站漏洞为例，网站漏洞修复率高达98.9%，显著高于平均水平97.8%，在所有行业中排名居前。同时，针对行业应急响应事件的分析也显示，96.4%的事件是医疗卫生行业机构自主发现的，这一水平也较前些年有显著提升。

报告提到，从2021年发生的安全事件攻击类型来看，恶意程序、漏洞利用仍然排名靠前，占比分别为46.4%和29.8%，是医疗卫生行业网络当前所面临的最主要的网络安全风险。在2021年的医疗卫生行业的网络安全应急响应事件中，还有16.7%并非是由网络攻击事件触发的。这些事件绝大多数都是机构内部运营故障、操作失误或管理疏失所造成的。网络安全问题会影响业务开展，而业务问题也同样会触发网络安全事件。

28. 安全公司Trellix发布《XDR：重新定义网络安全的未来——关于SecOps面临的主要挑战及应对的新调查报告》

9月28日，安全公司Trellix发布《XDR：重新定义网络安全的未来——关于SecOps面临的主要挑战及应对的新调查》（XDR：Redefining the future of cybersecurity——New survey highlights key SecOps challenges and how to overcome them）报告，显示安全运营（SecOps）团队每天都在努力应对数十起网络安全事件。

报告对来自15个市场的规模超过500人的组织的9000名安全决策者进行调查。调查发现，SecOps团队平均每天必须管理51起事件，36%的受访者声称他们每天要处理50到200起事件。约一半（46%）同意他们“被永无止境的网络攻击所淹没”这一表述。报告称，部分问题在于安全、检测和响应系统的孤立性质。大约60%的受访者认为，产品集成度差意味着团队无法高效工作，而三分之一

（34%）的受访者承认他们存在盲点。因此，60%的受访者承认他们无法跟上安全威胁的快速发展步伐。绝大多数（84%）受访者估计，他们的组织在过去一年因安全漏洞损失了高达10%的收入。中型企业（收入50至1亿美元）平均损失8%的收入，而营业额为100亿至250亿美元的大型企业则为5%。这可能意味着由于SecOps不足，每年都会浪费数亿美元。

（三）关键信息基础设施保护

1. 美国GAO发布《关键基础设施保护：机构网络安全评估指南落实情况报告》

2月9日，美国政府问责局（GAO）发布《关键基础设施保护：机构网络安全评估指南落实情况》（Critical Infrastructure Protection: Agencies Need to Assess Adoption of Cybersecurity Guidance）报告。

报告指出，尽管NIST《关键基础设施网络安全改进框架》已经实施，但负责关键基础设施管理工作的各联邦部门一直未就安全改进效果开展量化评估。16大关键基础设施领域中，仅3个评估了该框架的采用情况，分别是国防工业基地、政府设施及自来水/废水处理系统，多数表现滞后。GAO建议相关部门抓紧推进该项工作。有联邦机构表示，持续的疫情和勒索攻击影响了对该工作的资源投入。

2. 美国GAO发布《关键基础设施保护：CISA应改进优先级设置、利益相关者参与和威胁信息共享报告》

3月1日，美国政府问责局（GAO）发布《关键基础设施保护：CISA应改进优先级设置、利益相关者参与和威胁信息共享报告》（Critical Infrastructure Protection：CISA Should Improve Priority Setting，Stakeholder Involvement, and Threat Information Sharing）。

报告指出，关键基础设施风险已经从极端天气事件转变为更多的物理和网络攻击。大部分关键基础设施由私营部门拥有和运营，因此要想确保关键基础设施安全，联邦政府与私营部门以及州、地方等合作至关重要，而网络安全和基础设施安全局（CISA）是负责监督美国关键基础设施保护的主要联邦机构。对此，GAO建议CISA采取以下行动：（1）改进其确定关键基础设施优先事项的流程，以更

好地反映现实威胁；（2）寻求尚未提供关键基础设施最新信息的州意见；（3）让利益相关者参与国家关键职能框架的制定；（4）记录国家关键职能框架的目标和战略；（5）加强网络安全服务协调工作；（6）分享特定地区的威胁信息。

3. 美国 CRS 发布《关键基础设施安全和弹性：应对俄罗斯和其他国家网络威胁报告》

3 月 16 日，美国国会研究服务部（CRS）发布《关键基础设施安全和弹性：应对俄罗斯和其他国家网络威胁》（Critical Infrastructure Security and Resilience: Countering Russian and Other Nation-State Cyber Threats）报告。

报告指出国土安全部是负责关键基础设施安全和弹性的主要联邦机构。在联邦一级，关键基础设施行业是在总统政策指令的主持下组织起来的，这些指令指派 DHS 通过网络安全和基础设施安全局（CISA）推动、领导跨关键基础设施部门的自愿公私伙伴关系。由于国家的大部分关键基础设施由私营部门拥有和运营，实施联邦网络安全举措以应对民族国家和其他威胁通常取决于私营部门实体参与关键基础设施安全和弹性的意愿和能力。对于以利益为导向的行业，这关系到相关的弹性投资和快速报告网络事件，即使是那些可能造成声誉、法律或监管后果的事件。同样，易受攻击系统的所有者和运营商可能不得不承担大量的前期业务成本以提高安全性。鉴于此类系统的互连性，不符合关键基础设施法定定义的系统所有者和运营商仍可能遭受系统性风险攻击。

4. 美国 GAO 发布《关键基础设施保护：国土安全部迫切需要采取行动更好地保护国家的关键基础设施报告》

4 月 6 日，美国政府问责局（GAO）发布《关键基础设施保护：国土安全部迫切需要采取行动更好地保护国家关键基础设施》（Critical Infrastructure Protection: DHS Actions Urgently Needed to Better Protect the Nation's Critical Infrastructure）报告。报告认为，为了提高关键基础设施安全性，DHS 需要采取的关键行动包括：（1）加强联邦政府在保护关键基础设施网络安全方面的作用。推动完成 CISA 转型，包括最终确定该机构的基本任务职能和完

成劳动力规划活动；（2）改进优先级设置工作。因此，GAO 向 DHS 提出 11 项建议，DHS 已经表示打算在 2022 年底之前实施这些建议。

改进优先级设置工作方面，报告指出，目前通过国家关键基础设施优先计划，CISA 会确定一份系统和资产清单，这些系统和资产如果被破坏或中断，将导致国家或地区灾难性影响。CISA 需要每年更新并确定列表优先级。然而，GAO 认为该优先计划几乎没有用。例如利益相关者质疑用于将关键基础设施添加到优先计划列表中的标准是否具有相关性。2019 年，CISA 发布了一组 55 项政府和私营部门的国家关键职能，这些职能被认为对国家的安全、经济、公共卫生和安全至关重要。然而，GAO 采访的大多数联邦和非联邦关键基础设施利益相关者报告说，他们通常不参与、不知道或不了解框架的关键功能目标。

5. 欧盟两部门发布《铁路分区和管道报告》

2 月 28 日，欧盟网络安全局（ENISA）与欧洲铁路信息共享和分析中心（ISAC）共同发布《铁路分区和管道报告》（ZONING AND CONDUITS FOR RAILWAYS），旨在为铁路系统建设网络安全区和管道提供指导。

报告指出，要想实现网络安全战略在所有利益相关者之间共享并高效实现，首先应当确定并商定一个可能危及铁路应用的通用网络安全威胁列表，并就威胁达成一致意见，否则威胁的差异将导致低估风险和缺乏控制措施的实施。对于威胁形势应每年至少更新一次（或根据合同要求），对于排除在考虑范围之外的威胁应当提供相应理由。为每个区域制定网络安全要求规范，并依据公司特定政策、标准和相关法规，根据一般网络安全要求对其进行审查，并由铁路资产部批准。

6. 安全公司 Cynerio 发布《研究报告：2022 年医疗物联网设备安全状况》

1 月 19 日，安全公司 Cynerio 发布《研究报告：2022 年医疗物联网设备安全状况》（Research Report: The State of Healthcare IoT Device Security 2022）。

报告调查分析了全球 300 多家医院和医疗机构的 1000 多万台医疗设备，发现 53%的联网医疗设备含有已知漏洞，三分之一的床旁医疗设备存在重大风险。如果遭到黑客攻击，这些医疗设备的服务可用性、数据机密性会受到影响，甚至

患者安全都会受到威胁。所有医疗设备中，占医院物联网设备38%的输液（IV）泵是漏洞重灾区，73%的输液泵都存在某种漏洞。输液泵一旦被攻击者侵入，就会直接危及患者。之所以存在这些漏洞，部分原因在于一些相对简单的问题，比如程序老旧。报告发现，大多数物联网设备运行的Windows版本都较老，具体讲就是早于Windows 10。此外，整个部门共用同样的默认密码也是常见的风险，21%的设备都使用的是默认密码。

7. 安全公司Claroty发布《2021年全球工业网络安全态势：应对中断的韧性》

2月，安全公司Claroty发布《2021年全球工业网络安全态势：应对中断的韧性》（The Global State of Industrial Cybersecurity 2021: Resilience Amid Disruption）报告。报告对全球1100名关键基础设施领域工作的信息技术和运营技术专业人士进行调查，探讨他们如何应对2021年的重大挑战、网络韧性以及安排优先级事项。

调查显示，80%的受访者曾经遭受勒索攻击，其中47%表示其OT/工业控制系统环境受到影响。超过60%支付了赎金，超过一半（52%）支付了500，000美元或更多。超过90%的人向股东和/或当局披露了这一事件，69%认为及时报告应是强制性的。此外，大多数受访者估计其运营停机每小时的收入损失等于或大于支出。即使在支付赎金的人中，仍有28%在支付后一周或更长时间里遭受重大影响。调查结果表明，尽管支付赎金有众所周知的缺点，但对于大多数受害组织来说，替代方案（由于长时间的运营停机造成的收入损失）成本太高，难以承受。

（四）供应链安全

1. 美国两部门发布《美国IT行业关键供应链评估报告》

2月23日，美国商务部和国土安全部发布《美国IT行业关键供应链评估报告》（Assessment of the Critical Supply Chains Supporting the U.S. Information and Communications Technology Industry）。该报告是在拜登总统指示下，为落实第14017号行政令《保障美国供应链安全》，美国商务部和国土安全部在评估特定硬件产业和软件产品的供应链状况后形成的评估结论。

报告从五个方面给出美国IT行业关键供应链所面临的主要风险,分别是ICT制造业、ICT软件行业、ICT劳动力、影响ICT产业基础的交叉供应链问题、ICT产业基础供应链的外部风险。报告指出，美国在许多产品类别的ICT发展和创新方面继续处于领先地位,但是印刷电路板和显示器等产品的生产与电子组装越来越集中于中国。开源软件的普遍使用与其易被利用的特性给软件供应链安全带来风险。ICT供应链的复杂性导致许多原始设备制造商将固件开发外包给第三方供应商，而供应商编程和网络安全标准的不透明性也带来隐患。对此，报告提出提升供应链韧性的多项对策，包括振兴美国ICT制造业，构建安全、透明、具有韧性的供应链，加强公私合作和国际合作，投资未来ICT技术，加强ICT人才培养，深入开展ICT产业基础研究，确保可持续性仍是ICT发展的基石。

2. ISACA发布《供应链安全差距：2022年全球研究报告》

6月21日，国际信息系统审计协会ISACA发布《供应链安全差距：2022年全球研究报告》(Supply Chain Security Gaps: A 2022 Global Research Report)。

报告收录了逾1300名IT专业人士对供应链的看法。受访者主要关注以下五种主要的供应链风险：勒索软件（73%）、供应商不良信息安全实践（66%）、软件安全漏洞（65%）、第三方数据存储（61%）、对信息系统、软件代码或IP具有物理或虚拟访问权限的第三方服务提供商或厂商（55%）。

25%的受访者证实所在组织在过去一年中供应链遭到攻击。30%的受访者表示自己组织的领导对供应链风险缺乏足够了解。只有44%的受访者表示对自己组织的供应链安全很有信心，44%对整个供应链的访问控制很有信心。受访者对未来前景也不乐观——53%的受访者预计供应链问题未来半年内解决不了，甚至可能恶化。谈及应对措施时，84%的受访者表示组织的供应链管理有待提升。近五分之一的受访者表示在评估供应商时没有考虑网络安全和隐私。此外，39%的受访者没有与供应商制定网络安全事件响应计划，60%的受访者没有与供应商协调实施供应链安全事件响应计划。近一半的受访者（49%）表示自己的组织没有对供应链进行漏洞扫描和渗透测试。

（五）数据利用与安全保障

1. OECD 发布《跨境数据流动：评估主要政策和举措报告》

10 月 12 日，经合组织（OECD）发布报告《跨境数据流动：评估主要政策与举措报告》（Cross-border Data Flows: Taking Stock of Key Policies and Initiatives）。报告总结七国集团成员国参与的有助于促进可信跨境数据流动的现有协议、进程和倡议，以期为七国集团未来在这一领域的努力提供参考。

报告总结归纳两大单边政策：一是“开放保障措施”，即主要依赖转让实体，以确保所涉及的公共政策目标的持续保护，而对如何满足这些要求没有一般的规定；二是“预先授权的保障措施”，其特点通常是公共部门预先更多地参与，以确保可信的数据传输，如由公共部门单方面将接受国列入白名单，要求在合同中加入公共部门预先批准的特定条款等。报告还总结政府间正在进行的一系列措施，以推进合作进程，实现可信的跨境数据流动。主要包括七国集团和二十国集团在信任数据自由流动和跨境数据流动领域的讨论、制定标准的努力以及促进多边组织对话的研究，区域伙伴之间订立有约束力的协定以及各种优惠性质的贸易协定。

2. 大西洋理事会发布《数据鸿沟：新兴技术及其利益相关者如何影响第四次工业革命》报告

10 月 5 日，大西洋理事会发布《数据鸿沟：新兴技术及其利益相关者如何影响第四次工业革命》（The data divide: How emerging technology and its stakeholders can influence the fourth industrial revolution）。报告针对日益严重的数据鸿沟并提出相关政策建议，认为随着第四次工业革命的发展，联网设备增多，将会推动每天生成、存储和分析大约 2.5 万亿字节的数据。只有优化数据处理、监测和评估主要利益相关者的政策和计划，以及出于社会利益的目的协调公私伙伴关系，才能缩小数据鸿沟。报告强调，私营企业、政府和民间社会组织作为三类利益相关者需要共同努力，通过共享数据、减少数据收集偏见、创建新的数据治理结构等方式缩小数据鸿沟。

3. 美国 CRS 发布《欧盟-美国数据隐私框架：背景、实施和下一步报告》

10 月 24 日，美国国会研究服务局（CRS）发布《欧盟-美国数据隐私框架：背景、实施和下一步》（The EU-U.S. Data Privacy Framework：Background, Implementation, and Next Steps）报告，对美国和欧盟之间数据隐私框架变革的背景、美国实施该框架的步骤以及涉及国会利益的问题进行解释说明。

报告指出，拜登发布的《关于加强美国信号情报活动保障措施的行政令》，试图解决欧盟法院对美“隐私保护”的批评：即美国的监控没有足够的数据保护保障措施，也没有为个人数据被非法获取的非美国人提供足够的法律补救措施。报告认为，行政令和新的数据隐私框架可能会引发几个潜在问题。其中一个问题可能是总统有权在未来撤销行政令，行政令的撤销可能会使欧盟公民失去行政令的保障措施和追索权，撤销行政令可能会威胁到新的数据隐私框架的可行性。国会可以尝试通过立法来提供这些保障措施。另一个单独却相关的问题是欧洲法院可能会认定行政令中规定的保障措施不足以缓解对美国监视的担忧。如果欧洲法院认定美国根据 FISA 第 702 条授权的监视不符合 GDPR，即使存在行政令的保障措施，确保欧美数据流动的合法性仍可能需要修订 FISA。FISA 第 702 条计划于 2023 年底到期。

4. 大西洋理事会发布《实践中的数字主权：欧盟推动塑造新的全球经济》报告

11 月 2 日，大西洋理事会发布《实践中的数字主权：欧盟推动塑造新的全球经济》（Digital sovereignty in practice: The EU’s push to shape the new global economy）。报告确定了欧盟数字主权的三个要素，即加大对支持欧盟内部技术发展的承诺，努力制定管理数据和数字环境的全球规范以及对欧盟市场的非欧盟参与者采取更多限制。报告强调，制定规则方面，欧盟应推动欧洲技术创新，争夺全球规则制定权，将自身的标准发展为国际“黄金”标准从而增强全球影响力。国际合作方面，报告强调民主国家有必要建立数字联盟以应对日益增长的威胁。通过专注于欧洲经济数字化和技术投资，欧盟希望弥补目前的不足，并与美国和中国等数字强国进行更有力的竞争。

5. 欧盟EINSA发布《数据保护工程报告》

1月27日，欧盟网络安全局（EINSA）发布《数据保护工程：从理论到实践》（Data Protection Engineering: From Theory to Practice）报告，结合最新实践，介绍了相关技术在数据保护领域的运用。

报告认为，技术发展给数据保护带来新的威胁和挑战，GDPR的数据保护原则在实施方面可能面临挑战，需要定义新的行为者和责任，并将技术作为有力的保障措施之一。保障措施必须将技术和组织措施相结合，挑战在于选择、实施和配置适当的技术和组织措施，将GDPR原则转化为有形的要求。数据保护工程能够支持适当的技术和组织措施的选择、部署和配置。报告认为，监管机构（如数据保护机构和欧盟数据保护委员会)应在欧盟范围内形成数据保护工程的最佳实践，并通过公开文件进行推广；研究界应在监管机构的政策指导和资金支持下，继续探索部署能够支持数据保护原则实施的安全技术;监管机构和欧盟委员会应根据GDPR推动建立相关认证计划，以确保数据通过适当工程措施得到保护。

6. 欧盟EDPS、EDPB发布《2021年度报告》

4月20日，欧洲数据保护专员公署（EDPS）发布《2021年度报告》（Annual Report 2021）。报告概述了EDPS监管活动，尤其是在个人数据国际传输、新冠肆虐下的数据保护、对自由、安全和司法领域的持续监督、欧洲新数字治理体系的搭建等七方面的工作情况。报告指出，欧盟法院作出Schrems II判决后，EDPS开始推动Schrems II战略，旨在确保并监督欧盟机构遵守Schrems II判决中有关向欧盟和欧洲经济区之外的地区（特别是向美国）传输个人数据的要求。作为EDPS Schrems II战略的一部分，2021年5月，因亚马逊和微软提供的云计算服务涉及向美国传输个人数据，EDPS启动针对亚马逊和微软的两项隐私调查，以帮助欧盟机构在与服务提供商的谈判中保证数据保护的合规性。此外，2021年，EDPS还发布了一系列关于向欧盟和欧洲经济区之外地区传输个人数据的决议。

5月12日，欧盟数据保护委员会（EDPB）发布2021年度报告《增强数据保护的深度和广度》（Enhancing the depth and breadth of data protection），详细概述了EDPB在2021年开展的工作。报告强调，在过去一年里，EDPB继续重点关注个人数据的国际传输，还通过了关于其他国际传输工具（如行为准则）

的指导文件，并与 EDPS 一起就欧盟委员会发布的一套新的标准合同条款通过了联合意见。数字政策也是 EDPB 的重点工作之一，EDPB 和 EDPS 就数据治理法案和 AI 法案草案通过联合意见。报告强调 2022 年目标包括就合法利益作为法律依据和执法当局使用面部识别等各种主题的指导工作，EDPB 还将继续努力优化合作和执法。

7. 欧盟委员会发布《关于数据保护执法指令（LED）评估和审查的首份报告》

7 月 25 日，欧盟委员会发布《关于数据保护执法指令（LED）评估和审查的首份报告》（First report on application and functioning of the Data Protection Law Enforcement Directive（EU）2016/680（LED）。报告审查了 LED 所要求的第三国和国际组织个人数据转移规则的应用情况及经验教训，还概述了成员国将 LED 纳入本国法律的情况，以及未来方向。报告指出，LED 是保障个人数据基本权利的欧盟框架的三大支柱之一，另外两个支柱是 GDPR 和《欧盟各类官方机构个人数据处理条例》（EUDPR）。

8. 爱尔兰公民自由委员会发布《关于美国和欧洲实时竞价系统数据传播报告》

5 月 16 日，爱尔兰公民自由委员会（ICCL）发布《关于美国和欧洲实时竞价系统数据传播报告》（Report on the Scale of Real-Time Bidding Data Broadcasts in the U.S. and Europe）。

何为实时竞价系统（简称 RTB）？公开资料显示，RTB 是一种利用第三方技术，在数以百万计的网站上针对每一个用户展示行为进行评估以及出价的竞价技术。可理解为让广告商通过浏览记录和地理位置信息来锁定潜在用户并针对目标广告位进行出价的过程，目的是为了实现精准营销。报告显示，谷歌、微软等公司使用 RTB 系统实时追踪并分享用户的网络浏览记录和地理位置信息给广告商。在美国每天分享上述用户信息 2940 亿次，平均每人被曝光 747 次；在欧洲每天分享 1970 亿次，平均每人被曝光 376 次，并且“没有任何办法可以控制这些数据的用途”。报告推测，美国网络用户的网络浏览记录和位置信息每年被追踪和共享 107 万亿次，欧洲每年为 71 万亿次，并称这些用户数据会被发送至全球各地的公司。报告强调上述数据都十分保守，因为此次调查仅统计了在线广告生态

系统的“巨头”之一谷歌，并未关注脸书和亚马逊。

9. 国家互联网信息办公室发布《数字中国发展报告（2021 年）》

7 月 23 日，国家互联网信息办公室发布《数字中国发展报告（2021 年）》，介绍数字中国建设取得的显著成就，作出 2022 年数字中国建设展望。

报告指出，党的十九大以来数字中国建设取得显著成就。具体包括：（1）建成全球规模最大、技术领先的网络基础设施；（2）数据资源价值加快释放。2017 年到 2021 年，我国数据产量从 2.3ZB 增长至 6.6ZB，全球占比 9.9%，位居世界第二；（3）数字技术创新能力快速提升；（4）数字经济发展规模全球领先。2017 年到 2021 年，我国数字经济规模从 27.2 万亿增至 45.5 万亿元，总量稳居世界第二；（5）数字政府治理服务效能显著增强；（6）数字社会服务更加普惠便捷；（7）数字化发展治理取得明显成效。

展望方面，报告认为应：（1）加强数字技术自主创新，实现高水平自立自强；（2）夯实数字基础设施根基，打通信息“大动脉”；（3）做强做优做大数字经济，释放高质量发展动力；（4）提高数字政府建设水平，增强管理服务效能；（5）推动数字文化繁荣发展，共筑美好精神家园；（6）加快数字社会建设步伐，共享普惠包容的数字生活；（7）推进数字生态文明建设，促进人与自然和谐发展；（8）推进数据资源高效利用，加快激发数据要素活力；（9）完善数字安全和治理体系，营造健康安全的发展环境；（10）加强数字领域国际合作交流，携手构建网络空间命运共同体。

10. 国务院发布《关于数字经济发展情况的报告》

10 月 28 日，国务院《关于数字经济发展情况的报告》提请十三届全国人大常委会第三十七次会议审议。

报告明确，十年来，我国数字经济取得了举世瞩目的发展成就，总体规模连续多年位居世界第二，对经济社会发展的引领支撑作用日益凸显。与此同时，我国数字经济还存在大而不强、快而不优等问题。要充分发挥我国社会主义制度优势、新型举国体制优势、超大规模市场优势，强化目标导向和问题导向，牢牢抓住数字技术发展主动权，把握新一轮科技革命和产业变革发展先机，大力发展数

字经济。报告提出，以数据为关键要素，以推动数字技术与实体经济深度融合为主线，以协同推进数字产业化和产业数字化、赋能传统产业转型升级为重点，以加强数字基础设施建设为基础，以完善数字经济治理体系为保障，不断做强做优做大我国数字经济。

报告从八个方面提出下一步工作安排，包括集中力量推进关键核心技术攻关，牢牢掌握数字经济发展自主权；适度超前部署数字基础设施建设，筑牢数字经济发展根基；大力推动数字产业创新发展，打造具有国际竞争力的产业体系；加快深化产业数字化转型，释放数字对经济发展的放大、叠加、倍增作用；持续提升数字公共服务水平，不断满足人民美好生活需要；不断完善数字经济治理体系，推动数字经济规范健康持续发展；全面加强网络安全和数据安全保护，筑牢数字安全屏障；积极参与数字经济国际合作，推动构建网络空间命运共同体。

11. 广东数字政府研究院等发布《广东省数据要素市场化配置改革理论研究报告》

10 月 26 日，《广东省数据要素市场化配置改革理论研究报告》正式发布，是全国首份以“数据要素市场化配置改革理论框架”为研究主题的研究报告。

报告由五个章节组成，分别描述当前我国数据要素市场化配置改革的形势与挑战，剖析制约我国数据要素市场功能有效发挥的主要矛盾；从数据要素治理、数据要素资源配置和市场结构等视角进行理论分析，论证广东两级数据要素市场结构的合理性，构建广东数据要素市场化配置改革理论框架；从构建数据要素市场治理体系、提升数据要素市场治理能力、促进经济社会全面数字化发展、打造全国数据要素市场化配置改革先行区等方面，提出促进广东数据要素市场化配置改革发展的政策建议。

12. Verizon 发布《数据泄露调查报告》

5 月 23 日，美国移动通信运营商 Verizon 发布《数据泄露调查报告》（Data Breach Investigations Report）。

报告审查了 23，896 起安全事件，显示勒索软件在 2022 年同比增长 13%，增幅超过过去五年的总和。报告表示，经济利益仍然是攻击的主要动机，其次是

间谍活动。网络攻击（尤其是勒索软件）的增加是由于连接设备的持续爆炸和多个行业的广泛数字化。虽然大流行导致勒索攻击增加，但在新常态下不作为或延迟更新技术和基础设施，使组织更加脆弱，勒索软件即服务的出现和加密货币的采用也可能是促成因素。该研究还显示，数据泄露的四个关键途径是未经授权的凭据、网络钓鱼、漏洞利用和僵尸网络。有组织犯罪也继续成为网络安全领域的一股普遍力量。大约五分之四的违规行为可归因于有组织犯罪，来源于外部行为者的安全事件是内部行为者的四倍。地缘政治紧张局势的加剧也推动了与民族国家相关的网络攻击的复杂性、知名度和意识的提高。

13. IBM 发布《2022 年数据泄露成本报告》

7 月，IBM 公司发布名为《2022 年数据泄露》（Cost of a Data Breach Report 2022）的研究报告。报告主要研究了 2021 年 3 月至 2022 年 3 月期间受数据泄露影响的 550 家组织，这些事件分布在 17 个国家和地区，涉及 17 个不同行业。

通过对受数据泄露影响的组织中的个人进行的 3600 多次访谈，报告发现，83%的被调查组织曾经历过一次以上数据泄露；60%的企业数据泄露导致转嫁给客户的价格上涨；79%的关键基础设施组织没有部署零信任架构；19%的数据泄露是由于与合作伙伴的关联；45%的数据泄露事件基于云环境。报告发现，组织在不同数据泄露事件中的成本与组织对数据泄露的即时和长期响应措施直接相关。

报告建议组织采取以下措施：（1）采用零信任安全模型，防止对敏感数据未经授权的访问；（2）在云环境中通过数据加密和完全同态加密保护敏感信息；（3）投资 SOAR（安全编排自动化和响应技术）和 XDR（可拓展威胁检测与响应技术）帮助缩短检测和响应时间；（4）使用有助于保护和监控端点和远程员工的工具；（5）采取并测试应急处置措施，提高网络弹性。

14. 中国中小企业协会联合 360 天枢智库发布《2022 中小微企业数字安全报告》

7 月 30 日，2022 全球数字经济大会数字安全峰会暨第十届互联网安全大会（ISC 2022）举行，会上发布《2022 中小微企业数字安全报告》。

报告显示，我国有超过九成（92.3%）中小微企业面临非常严峻的数字安全威胁。在受访的 142 家国内中小微企业中，85.3%遇到过数字安全问题，近 77.4%

的中小微企业反馈其自身不能有效处置数字安全问题。根据报告，81%的受访者认为其领导的中小微企业会在现在或不久的将来遭到黑客攻击，对未来防御网络攻击持悲观态度；而认为不会遭到黑客攻击的仅占 19%。

勒索攻击、网络钓鱼和恶意软件已成为全球中小微企业最具威胁的数字攻击。据统计，28%的美国中小微企业认为供应链攻击已成为主要威胁之一。我国 76.9%的中小微企业受访者认为未来因合作方发生网络安全事件会引发其自身安全风险增加，并且有 12.8%的受访者经历过因合作方所引起的网络攻击和数据泄露事件。超一半受访者表示会把安全风险评估做为交易与否的主要决定因素。

至于网络攻击可能带来的后果，报告显示，由于担心被取消相应认证资格或失去客户机会，36%的受访中小微企业最担心“不符合合规要求”；其次有 34.7%的受访者担心遭到黑客组织数字攻击而导致其业务中断；另外，分别有 33.3%和 28%的受访者担心重要信息丢失和敏感数据泄露，13.3%担心资金损失。

中小微企业数字安全能力普遍不足的重要原因之一是资金缺乏。报告显示，60%的受访者在数字安全方面的年投入不超过 10 万元，12%的受访者表示尽管认同数字安全的重要性，但是没有数字安全预算；20%的受访者表示能接受的数字安全投入不能超过十万。

（六）个人信息保护

1. 联合国发布《数字时代的隐私权》报告

9 月 16 日，联合国发布《数字时代的隐私权》（The right to privacy in the digital age）报告，重点关注国家保护和促进隐私权相关的三个关键领域。

首先，普遍性滥用侵入性黑客工具。报告详细介绍了诸如 Pegasus 软件之类的监控工具如何将大多数智能手机变成“24 小时监控设备”，称“虽然据称被部署用于打击恐怖主义和犯罪，但此类间谍软件工具经常被用于非法原因，包括压制批评或反对意见以及表达这些意见的人”。报告指出，针对个人通信设备的黑客行为构成了对隐私权的严重干扰，并且可能与侵犯一系列其他权利有关，对数字通信设备的入侵不但威胁到用户的访问记录、搜索、浏览历史，还可能深入了解遭受黑客攻击的个人的思维模式及其宗教、政治观点和信仰，从而干扰自由的意见和想法。

其次，加密限制。加密是数字空间中隐私和人权的关键推动因素，对于保障权利至关重要，加密为面临在线监视、骚扰和暴力的特殊威胁的个人提供重要保护，防止非自愿披露信息。但这一因素正在受到破坏，报告呼吁各国不要干涉加密技术并鼓励企业努力实现解决方案，以保护数字交易和通信的机密性，包括加密、假名化和匿名措施。

最后，公共场所监控。报告对越来越多的公共场所监视提出警告。据统计2021 年，全球使用的监控摄像头将超过 10 亿个。除了国家运行的监控系统外，一些公司还制作了私人使用的监控工具，具有向有关部门报告事件甚至允许他们直接访问其数据流的专用功能。这极大地扩展了受监控的公共空间，同时削弱透明度、监督和问责制。报告强调，各国应将公共监视措施限制在“绝对必要和相称”的范围内，重点关注特定地点和时间。数据的存储时间应同样受到限制，此外还应当限制在公共场所使用生物特征识别系统。

2. 美国 GAO 发布《隐私：专业领导者可以改善隐私保护项目并应对挑战报告》

9 月 22 日，美国政府问责局（GAO）发布《隐私：专业领导者可以改善隐私保护项目并应对挑战》（Privacy：Dedicated Leadership Can Improve Programs and Address Challenges）报告。

报告对《首席财务官法》所覆盖的 24 个机构进行审查，发现各机构在实施隐私保护项目的主要做法各不相同。许多机构没有将隐私完全纳入其风险管理战略，没有为隐私官员提供包含个人身份信息的系统授权，也没有制定隐私持续监测战略。报告发现，24 个机构都指定了一名高级官员负责隐私。然而，大多数官员并不把隐私保护作为他们的主要责任。他们有许多其他的职责，例如管理 IT 和信息安全。其他官员不太可能把大部分时间花在隐私问题上，机构通常将隐私项目操作方面的任务委托给级别较低的官员，这使负责隐私的高级机构官员在与其他高级机构领导讨论时，不太可能将注意力集中在隐私问题上。报告建议国会考虑立法，为目前缺乏隐私官员的机构指定一名专门的高级隐私官员。GAO 提出 62 项建议，包括全面建立隐私保护计划、建立与其他机构职能之间的协调政策和程序，并将隐私保护纳入风险管理活动。

3. 美国NIST发布《2021年网络安全和隐私年度报告》

10月1日，美国国家标准与技术研究院（NIST）发布《2021年网络安全和隐私年度报告》（2021 Cybersecurity and Privacy Annual Report）。

报告涵盖密码标准、网络安全测量、教育和人力资源、身份和访问管理、隐私工程、风险管理、可信网络、可信平台8个关键领域。密码方面，NIST持续推进加密技术，包括更新FIPS出版物《加密模块的安全要求》（Security Requirements for Cryptographic Modules）；风险管理方面，报告强调保护受控非密信息、系统工程和网络弹性、供应链和移动技术等方面的工作；NIST还介绍在后量子密码学、供应链安全、零信任以及控制系统网络安全等领域的研究和应用。

4. 挪威隐私保护局发布《2021年个人数据安全事件报告》

4月4日，挪威隐私保护局（IMY）发布《2021年个人数据安全事件报告》，指出与其他部门相比，医疗服务机构报告的由IT攻击引起的个人数据安全事件比例大幅提升。报告指出，由于卫生服务在很大程度上涉及处理敏感个人数据，因此个人数据安全事件可能会对数据主体造成重大损害。因此，认真对待IT攻击风险非常重要。个人数据事件发生的最常见诱因是人为因素，包括不正确地发送信件、电子邮件或短信。人为因素导致的大量数据安全事故凸显以组织措施补充技术安全措施的重要性，例如通过持续培训提高员工的数据安全知识与意识。

5. 挪威数据保护当局发布《老板看到你了吗？监控员工的数字活动调查报告》

9月1日，挪威数据保护当局（Datatilsynet）发布针对员工监控工具的调查报告—《老板看到你了吗？监控员工的数字活动》（Sjefen ser deg? Overvåking og kontroll av arbeidstakeres digitale aktiviteter）。

报告主题是监控员工的数字活动，重点研究三大问题：（1）数字化工作场所有哪些监控措施和系统；（2）专门设计用于监控员工的软件如何运作；（3）员工在应对数字监测和控制方面有哪些经验。报告显示，雇主有能力收集员工数字活动中产生的大量信息；一半以上的员工对雇主收集其个人信息没有充分了解；员工监控软件可能侵犯员工隐私；越来越多的员工表示其对网站的访问正受

到雇主监控。此外，报告特别关注远程办公场景下的员工监控措施，表示远程办公的推广应用将导致雇主在更大程度上使用数字工具来跟进和协调未在工作场所办公的员工，这将给员工个人隐私保护带来极大挑战。

6. 香港个人资料私隐专员公署发布《社交媒体私隐设定大检阅报告》

4 月 12 日，香港个人资料私隐专员公署在对香港十大最常使用的社交媒体，包括 Facebook、Facebook Messenger、Instagram、LINE、LinkedIn、Skype、Twitter、WeChat、WhatsApp 及 YouTube 进行检视后，发布《社交媒体私隐设定大检阅报告》。

私隐公署已经将报告送交各社交媒体营运者，并提出以下建议：（1）社交媒体营运者应持续采取贯彻私隐的设计，优化其服务，并向用户提供更多私隐相关功能，增加用户选择；（2）社交媒体应留意所收集的个人资料种类，避免收集超乎所提供服务所需要的资料；（3）社交媒体的私隐政策应清晰易明，用字不应含糊笼统。私隐公署认为采用分层式展示或以图片、表格或短片辅助说明有助增加私隐政策的易读性；（4）社交媒体不应将位置追踪功能预设为开启，应让用户因应其需要作出选择；（5）社交媒体应提供端对端加密及双重认证功能以加强保障用户个人资料；（6）社交媒体营运者亦应主动应对起底、数据撷取或其他非法行为，限制搜寻用户的方式。

7. 江苏省消保委发布《新能源汽车行业不公平格式条款调查报告》

5 月 19 日，江苏省消保委发布《新能源汽车行业不公平格式条款调查报告》。报告选取市场上具有一定知名度和影响力的新能源汽车品牌进行样本调查，收集比亚迪、长安、长城、广汽埃安、极狐、极氪、吉利、理想、奇瑞、上汽通用五菱、特斯拉、蔚来、威马、小鹏等 14 家新能源汽车企业 47 份协议后梳理形成。

报告共梳理出 10 个方面共 15 项不公平格式条款问题。其中，涉及个人信息保护方面的不公平格式条款包括以下三个方面：（1）收集个人信息不规范，消费者被要求必须概括同意；（2）个人信息使用不当，消费者个人信息保护缺位；（3）约定响应时间过长，难以满足消费者实际需要。

（七）网络犯罪防治

1. 美国司法部发布《关于如何加强国际执法合作，以侦查、调查和起诉与数字资产相关犯罪活动的报告》

6 月 6 日，美国司法部发布《关于如何加强国际执法合作，以侦查、调查和起诉与数字资产相关犯罪活动的报告》（How To Strengthen International Law Enforcement Cooperation For Detecting, Investigating, And Prosecuting Criminal Activity Related To Digital Assets）。

报告首先解释了数字资产交易区别于传统金融交易的特征，以及这些特征可能如何影响跨国调查，随后解释了美国执法机构和监管机构打击数字资产相关犯罪的几种方式。报告指出，在涉及打击非法使用数字资产的众多成功案例中，国际合作至关重要，但仍存在诸多挑战，例如应如何充分利用美国及其外国执法伙伴之间的司法互助，将滥用数字资产的犯罪分子绳之以法，扣押其犯罪所得，并向受害者提供赔偿方面等。报告提出了加强执法和改善国际合作的建议：（1）进一步提升与国际伙伴进行专业化调查的能力；（2）在各种国内和国际机构的调查中进行强有力的信息共享；（3）通过实施有助于降低司法套利风险的国际标准，促进美国和外国合作伙伴在数字资产领域进行更加统一的监管。

2. 美国司法部发布《全面网络审查》最终报告

7 月 20 日，美国司法部发布《全面网络审查》（Comprehensive Cyber Review）最终报告，强调司法部应与其合作伙伴和盟友加强合作，以及优先考虑预防工作的必要性。司法部于 2021 年 5 月启动了网络审查，以重新评估司法部在勒索攻击和供应链攻击增加情况下打击网络威胁的策略。

报告建议司法部可以“通过与合作伙伴和盟友更密切地合作来显著扩大自己的影响力”。根据这项建议，司法部将指定有史以来第一个网络运营国际联络员，他将与其他部门和欧洲盟友合作，加快实现针对网络犯罪分子的行动，包括指控、逮捕、引渡、资产扣押和拆除基础设施。此外，报告强调需要优先考虑预防工作，并更新司法部对自身系统的重大网络入侵的响应计划。

3. 美国司法部发布《执法部门在侦查、调查和起诉与数字资产相关的犯罪活动中的作用报告》

9 月 16 日，美国司法部发布《执法部门在侦查、调查和起诉与数字资产相关的犯罪活动中的作用》（The Role Of Law Enforcement In Detecting, Investigating, And Prosecuting Criminal Activity Related To Digital Assets）报告。

报告概述了犯罪分子利用数字资产开展违法犯罪活动的多种方式，主要包括三个类别：（1）将加密货币作为犯罪活动的支付手段或促进犯罪活动的方式；（2）使用数字资产作为隐藏非法金融活动的手段；（3）涉及或破坏数字资产生态系统的犯罪。报告探讨了去中心化金融等新技术给执法活动带来的挑战，并提出三大建议：将防止金融机构员工向嫌疑人提供情报的相关法律的适用范围拓展至虚拟资产服务提供商；加强将无证汇款业务经营定罪的法律；鉴于数字资产调查的复杂性，延长特定法律法规的时限。

（八）新技术新应用发展与安全

1. 世界经济论坛发布《量子计算现状：构建量子经济》报告

9 月 13 日，世界经济论坛发布《量子计算现状：构建量子经济》（State of Quantum Computing: Building a Quantum Economy）报告，全面介绍量子计算当前的发展情况，包括技术现状、应用领域、各国在量子产业中的战略与投入、构建量子生态系统及其未来发展潜力的关键因素。报告认为，新冠疫情期间，特别是在过去一年中，量子计算在技术开发和通过云的可访问性方面取得很大进展。量子计算已被世界主要经济体视为一项战略技术，有望带来重大的经济、环境和社会机遇，也将引入新的重大安全风险。

报告指出，当量子计算机达到可用水平时，可能会出现供应短缺。投资或与一家量子计算机开发公司合作则可以抢占先机。同时，量子计算开发者需要商业合作伙伴来引导技术发展，量化技术对行业的潜在影响，找到最有效的用例，同时帮助加速技术理解和开发。此外，除了关键应用领域，其他组织的网络安全可能受到量子计算的影响。应了解潜在量子计算攻击的暴露程度，并确定必要的保

护步骤。政府和企业需要采取进一步行动，推动更多的公私合作和竞争前合作，并就共同语言和性能标准达成共识，结合新的政策和法规，以确保合乎伦理和可靠的技术开发和使用。

2. 美国参议院发布《加密货币在勒索攻击、可用数据和国家安全问题中的使用报告》

5 月 24 日，美国参议院国土安全和政府事务委员会发布题为《加密货币在勒索攻击、可用数据和国家安全问题中的使用》（Use of Cryptocurrency in Ransomware Attacks, Available Data, and National Security Concerns）的报告。

报告介绍了对日益增长的勒索软件威胁进行的为期 10 个月的调查结果。报告引用 FBI 的数据显示，该机构已收到 3729 起勒索软件投诉，损失超过 4920 万美元。然而，即使是这些数字“也可能大大低估了实际数量以及相关损失。”报告认为，关于勒索攻击和赎金数据的报告和收集是分散且不完整的。这部分是由两个独立的联邦机构——网络安全和基础设施安全局（CISA）和 FBI 负责。虽然这些机构表示他们彼此共享数据，但“勒索软件事件响应公司质疑此类共享渠道对协助受害者的有效性。”

调查还强调加密货币，尤其是比特币，在勒索攻击中的作用越来越大，已成为一种近乎普遍的赎金支付形式。这些货币的去中心化性质使得执法部门难以识别和逮捕恶意行为者，尤其是外国团体。然而，FBI 追回了 Colonial Pipeline 支付的一半以上的赎金，表明“通过访问正确的信息，执法部门可以利用加密货币的独特功能以及其他调查技术来追踪网络犯罪分子并追回被盗资金。”

3. 美国大西洋理事会发布《缺失的钥匙：网络安全和央行数字货币的挑战报告》

6 月 15 日，美国大西洋理事会发布报告《缺失的钥匙：网络安全和央行数字货币的挑战》（Missing Key: The Challenge of Cybersecurity and Central Bank Digital Currency），探讨若美国发行央行数字货币（CBDC）可能对网络安全造成的影响，并提出应对措施。

报告显示，截至 2022 年 6 月，占全球 GDP95%的 105 个国家正在研究和探索

发行 CBDC。如果 CBDC 需要收集一个国家每个人的金融交易信息，那么该数据库将成为一个非常高价值的目标，可能引发网络安全风险。美国联邦储备委员会已将保护美元和国际金融体系视为国家安全的核心挑战，并开始论证发行 CBDC 的好处和风险。据此，大西洋理事会提出以下几项原则，以完善未来 CBDC 的立法和监管政策：（1）利用好现有风险管理和法规框架；（2）重视隐私以加强安全性；（3）发行前广泛测试、安全审计；（4）确立问责制等。

4. 布鲁金斯学会发布《人工智能合作落地：全球范围内的人工智能研发》

11 月 4 日，布鲁金斯学会发布《人工智能合作落地：全球范围内的人工智能研发》（AI cooperation on the ground: AI research and development on a global scale）。报告探讨了各国 AI 政策的异同、国际合作途径、研发、生态系统、标准制定等问题。通过分析当前 AI 的全球合作状况以及相关项目合作前景，报告建议政府和其他利益相关方优先考虑 AI 在气候变化监测和管理中的应用，以及加速隐私保护技术开发两个方面的国际合作。

5. 美国 ITIF 发布《全球监控义务提案对端到端加密的影响》

11 月 14 日，美国信息技术与创新基金会（ITIF）发布《全球监控义务提案对端到端加密的影响》(The Effect of International Proposals for Monitoring Obligations on End-to-End Encryption）。报告指出，2022 年，美国立法机构更新 EARNIT 草案、英国政府《在线安全法案》草案进入讨论、欧盟《制定防止和打击儿童性虐待规则》进入讨论。上述三项立法活动均针对保护儿童免受在线犯罪活动和性剥削，要求科技公司对在线服务和照片、私人消息和云文件等在线内容履行监控义务，这些义务将会迫使科技公司停用端到端加密（E2EE）。报告认为，相比于针对在线内容强加监督义务，政府应当将加密服务排除在监控义务之外、增加国家执法机构资源以起诉相关犯罪活动、强化科技公司的报告和协调义务以帮助执法机关及时追踪和起诉非法活动。

6. 卡托研究所发布《中央银行数字货币：评估风险和破除迷思》

11 月 18 日，卡托研究所发布《中央银行数字货币：评估风险和破除迷思》

（Central Bank Digital Currency: Assessing the Risks and Dispelling the Myths）。报告指出，中央银行数字货币或从根本上改变美国的金融体系。对中央银行数字货币的研究已经不再单纯地停留在学术层面，已广泛引起政治家、央行行长、科技行业甚至公众的关注。美国和相关政府官员正在积极致力于实施中央银行数字货币并加强政府对支付系统的控制，但这个想法不切实际，因为中央银行数字货币最终会篡夺私营部门并危及美国人的核心自由。报告认为，国会应明确禁止美联储和财政部以任何形式发行中央银行数字货币。

7. 欧盟 ENISA 发布《5G 网络安全标准报告》

3 月 16 日，欧盟网络安全局（ENISA）发布《5G 网络安全标准报告》（5G Cybersecurity Standards），重点从技术及组织角度介绍 5G 网络安全标准，并说明标准化对 5G 生态系统中缓解技术风险的价值。

报告搜集分析了 140 多份文件中的 150 项安全措施，得出如下结论：（1）现有标准、规范和准则都是通用的，相应调整后即可应用于 5G 技术和功能领域、生命周期过程；（2）5G 标准、规范和准则在更大程度上适用于电信部门；（3）5G 标准、规范和准则基本覆盖技术生命周期的“运行”阶段，其他阶段则需删减；（4）现有关于网络安全威胁和 IT 安全准则的知识库可用于基于应用程序编程接口（API）的 5G 云体系结构；（5）现有文献不适用于 5G 生态系统中“端到端”信任度和弹性，可能需要关于 5G 专用工具和关键绩效指标的指导方针，以确保 5G 保护的理解；（6）标准化差距上，只有治理和风险管理领域、人力资源安全方面存在适度差距，其他领域（业务管理、业务连续性管理和事件管理等）则存在较大差距。

8. 欧洲刑警组织发布《面对现实？执法和深度伪造的挑战报告》

4 月 26 日，欧洲刑警组织发布其首份深度伪造研究报告--《面对现实？执法和深度伪造的挑战》（Facing reality? Law enforcement and the challenge of deepfakes）。报告的调查结果基于广泛的案例研究和通过战略前瞻性活动与执法专家进行的深入探讨和磋商。报告认为，深度伪造（deepfake）在未来几年可能成为更大的风险。

报告详细概述了 Deepfakes 技术的犯罪用途，包括用于 CEO 欺诈、证据篡改和制作未经同意的色情制品等严重犯罪。Deepfakes 造成的威胁分为四大类：（1）社会层面——引发社会动荡和政治两极分化；（2）执法层面——伪造电子证据；（3）个人层面——骚扰、欺凌、非自愿色情和在线儿童剥削；和（4）传统网络安全层面——敲诈勒索、欺诈、操纵金融市场。报告详细阐述了执法部门在检测和防止恶意使用 Deepfakes 方面面临的挑战，表明执法部门、在线服务提供商和其他组织需要制定政策，研究错误信息检测和预防解决方案，政策制定者也需要适应不断变化的技术现实。报告认为避免采取 Deepfake 技术可能比试图检测 Deepfake 更有效。

9. 欧洲 EPRS 发布《数据治理和人工智能：可持续和公正的数据治理模式研究报告》

7 月 11 日，欧洲议会研究局（EPRS）发布题为《数据治理和人工智能：可持续和公正的数据治理模式》（Governing data and artificial intelligence for all: Models for sustainable and just data governance）的研究报告。报告关注 AI，旨在研究欧盟数据治理框架政策，并侧重于对欧盟数据治理战略进行总体评估和考虑。报告提出了四个良好的数据治理基准：维护和加强公共基础设施和公共产品、包容性、可竞争性和问责机制以及全球责任。

报告认为，在开发和使用方面，AI 并不是一个民主的技术类别。大规模开发和部署 AI 是一项特权，该特权主要由社会中最强大的参与者（无论是商业部门还是公共部门）获得。除非运用大量的资源来对抗它，否则它将继续依赖大规模的商业计算基础设施，将分析和干预数据的权力输送给那些拥有最多资源和能力的人。因此，报告讨论的核心问题是通过对 AI 系统及其所依赖的数据生态系统对数据所附权力进行分配，激励开发和部署数据系统的人进行良好的数据治理。总体而言，报告强调了社会团体集体意愿和决策的重要性，结合对公共价值的规范导向，提出 AI 和数据治理的重要考虑因素。

10. 欧盟 ENISA 发布《后量子密码：集成研究报告》

10 月 18 日，欧盟网络安全局（ENISA）发布报告《后量子密码：集成研究》

（Post-Quantum Cryptography - Integration study）。作为 2021 年 5 月《后量子密码：当前状态和量子缓解》研究的后续，报告探讨了新的加密协议并强调将后量子系统集成到现有协议中的必要性。

随着量子计算技术的发展，其密码分析能力可能会给设备和系统带来新的安全风险，导致目前使用的大多数加密方案变得不安全，并最终从根本上改变现有的威胁模型。为应对上述挑战，需要向量子安全加密过渡，报告提出以下技术建议：（1）为主要用例制定指南，以评估不同方法和系统的最佳适配应用场景；（2）新方案或现有方案的重大变化应考虑后量子密码（PQC），同时考虑 PQC 系统的集成需求；（3）在现有密码系统中添加可被转化为 PQC 的混合系统层，以方便后续工作。

11. 英国 DCMS 发布《企业联网设备的网络安全》报告

5 月 9 日，英国数字、文化、媒体和体育部（DCMS）发布题为《企业联网设备的网络安全》（Cyber security in enterprise connected devices）的报告。

“企业联网设备”是指由企业和组织使用的联网设备，如办公室打印机、办公室摄像头、门禁系统和房间预订系统等。这些联网设备在英国各地数千个组织日常运作中使用，可为恶意行为者攻击企业系统提供途径。联网设备不仅对个人用户和公司网络构成威胁，还可能对整体数字环境构成大规模战略风险。报告列出一些关键发现，包括：（1）企业联网设备在许多组织中得以部署、形成依赖，然而 IT 专业人士对此类设备的安全性有很大担忧；（2）在企业联网设备中经常发现安全漏洞，这些安全漏洞已将大量组织置于风险之中；（3）对于如何采取监控等保护措施使组织免受联网设备攻击，企业缺乏明确的规定。

12. 新加坡金融管理局发布《FEAT 原则评估方法》等五份白皮书

2 月 4 日，新加坡金融管理局（MAS）发布五份白皮书，分别是《Veritas 文件 3——FEAT 原则评估方法》（Veritas Document 3——FEAT Principles Assessment Methodology）、《Veritas 文件 3A——FEAT 公平原则评估方法》（Veritas Document 3A——FEAT Fairness Principles Assessment Methodology）、《Veritas 文件 3B——FEAT 伦理和问责制原则评估方法》（Veritas

Document 3B——FEAT Ethics and Accountability Principles Assessment Methodology）、《Veritas 文件 3C——FEAT 透明度原则评估方法》（Veritas Document 3C——FEAT Transparency Principles Assessment Methodology）、《Veritas 文件 4——FEAT 原则评估案例研究》（Veritas Document 4——FEAT Principles Assessment Case Studies），详细介绍了公平、伦理、问责制和透明度（FEAT）原则的评估方法，以指导金融机构负责任地使用 AI。白皮书由 MAS 领导的行业联盟 Veritas Consortium 发布，该联盟还发布了一个开源工具包帮助金融机构采用公平评估方法。

白皮书提供了：（1）供金融机构在其 AI 和数据分析（AIDA）软件开发生命周期中采用的综合 FEAT 清单；（2）增强的公平评估方法，使金融机构能够定义其 AIDA 系统的公平目标，识别个人的个人属性和任何无意的偏见；（3）一种新的伦理和责任评估方法，除了目前采用的定性做法外，其还为金融机构提供了一个框架，可以对伦理实践进行量化衡量；（4）新的透明度评估方法，可帮助金融机构确定是否需要以及需要多少内部/外部透明度来解释机器学习模型的预测结果。

13. Gartner 发布《供应链人工智能》报告

8 月 19 日，Gartner 发布《供应链人工智能》（Supply Chain AI）报告，认为供应链复杂性的提高增加了对 AI 的需求。报告指出，在供应链中，高级分析和大数据被视为最重要的新兴技术领域，受访者普遍认可在 2025 年 AI 将对该行业的自动化决策、交通运输、采购等环节产生重大影响。报告同时也关注到机器学习的成熟会导致人类知识领域不可避免的损失，为此供应链领导者试图通过数据素养培养、过程挖掘、众包等方式将人类领域知识与分析见解相结合，发挥人机优势以管理日益复杂的供应链。

四、前瞻：全球网络安全政策法律未来趋势研判

党的二十大报告指出，世界之变、时代之变、历史之变正以前所未有的方式展开。世界又一次站在历史的十字路口，何去何从取决于各国人民的抉择。三变之下，中国网络与数据安全法治如何变，未来怎么走，值得思考。未来五年，是我国全面建设社会主义现代化国家开局起步的关键时期。面对复杂多变的国际形势，面对我国社会主要矛盾转化后，经济社会高质量发展的现实需求，我们既要直面百年未有之挑战，也要抓住前所未有之机遇，准确认识和适应全球网络安全政策法律发展演变的基本趋势和特征变化，因势利导、顺势而为，答好网络安全的中国之问、世界之问、人民之问、时代之问。网络安全法治作为中国特色社会主义法治体系的重要组成部分，也是过去十年统筹推进国内法治和涉外法治的重要成果，在法治斗争中发挥了重要作用，在未来也将成为新征程高质量发展的重要法治保障。

（一）国家安全因素全面“注入”网络安全，国家成为网络安全的主要推手

当前，全球经济复苏疲软，网络空间不仅日益成为国际竞争与博弈的重要领域，更凸显其在安全领域中的极度敏感和脆弱性，各国通过不同目的、用意刻画网络空间的各个立面，传递其安全、利益和价值理念。一方面，利用监控软件进行监听监视，泛化国家安全概念、滥用出口管制措施，利用网络舆论造谣抹黑，肆意对他国进行网络渗透、网络攻击的事件屡见不鲜，网络成为个别国家建立网络霸权、维持所谓全球领导力的工具；另一方面，通过多边安全倡议、行动规约是包括中国在内更多国家在国际顶层秩序建设中的持续努力。国际竞争越来越体现为制度、规则、法律之争[2]。在北约新发布的《北约 2022 年战略概念》文件中，首次提及中国，称中国对北约的价值观和安全造成挑战，将保持对华建设性的接触。美国政府发布的新版《国家安全战略》将中国定位为“优先考虑的、唯一的全球竞争对手”，表示“未来十年是美国与中国竞争的决定性十年”。国际关系，尤其是大国关系正在深刻影响全球网络安全整体态势，包括网络安全政策法律制

[2] 习近平：坚持走中国特色社会主义法治道路 更好推进中国特色社会主义法治体系建设. 链接：http://www.gov.cn/xinwen/2022-02/15/content_5673681.htm?token=274d9611-02d9-4188-a527-85b49fe47761

定趋势。

作为负责任的大国，我国始终致力于为动荡变化的世界注入更多稳定性。在近期国家主席习近平同美国总统拜登举行的会晤中，表示“当前中美关系面临的局面不符合两国和两国人民根本利益，也不符合国际社会期待”，应采取切实行动，推动中美关系重返稳定发展轨道。我国正处于加快建设网络强国、数字中国的重要时期，应主动识变应变求变，对外展现负责任的大国担当，研究全球互联网治理规则、营造非歧视数字发展环境，推动构建网络空间命运共同体。把维护国家安全贯穿网络安全工作各方面，坚定维护国家主权、安全、发展利益，在国际博弈中清晰界定“国家安全”应有边界，反对国家安全的泛化和工具论；对内主动防范化解风险，提升应对各种重大风险的能力，推动实现中国式现代化。

可以预见，随着对网络空间虚拟性、风险传导等方面特点的深入理解和挖掘，未来一些国家仍将围绕网络空间安全肆意发挥，网络空间将成为大国间检验和测试其信息与网络技术、策略和风险模型的极限试验场。

（二）关键信息基础设施适当“聚焦”与供应链安全强势“扩张”成为网络安全并行不悖的两条主线

各国逐步认识到在大规模、国家级网络安全事件频发背景下，关键信息基础设施安全面临着日趋复杂多变的安全威胁，关键信息基础设施安全保护已经并将长期成为网络安全保障的重点工作。为突破监管瓶颈，各国关键信息基础设施安全规则随之加速推进。保护对象方面，欧盟 CER 指令提案和澳大利亚《2022 年安全立法修正案（关键基础设施保护）法》进一步量化了设施的粒度，将关键实体或关键基础设施中部分具有极端重要性的实体或资产单列出来，赋予更加严格的保护义务；从保护内容来看，侧重态势感知与事件报告。总体反映出关键基础设施保护过程中适当收缩、聚焦重点的特点。美国通过专门立法中的事件管理和报告时限的区分设计，事实上体现出对不同基础设施的重视程度。目前，我国在《关键信息基础设施安全保护条例》施行后，关键信息基础设施识别认定工作正在稳步开展，1960 号文和《信息安全技术 关键信息基础设施安全保护要求》意味着关键信息基础设施保护工作进入快进模式。如何全面建立并落实与关键信息基础设施“重中之重”地位相适应的安全保护制度，能够在面对外部冲击时确保持续稳定运行值得思考。在此过程中，应坚持问题导向，守住关键、保住要害、

精准发力，既避免关键信息基础设施范围过大，导致“重中之重”概念泛化；也要避免“大而广”的保护要求导致有限资源过于分散。

与此同时，“供应链安全”成为近年来信息技术领域，乃至全球经济发展中的高频词汇。SolarWinds 供应链攻击、Log4j 漏洞曝光等安全事件使得各国普遍意识到供应链安全产生的级联效应的危害性，开源软件、固件开发、网络产品软硬件集成的全球化也使得网络产品极易成为他国网络渗透、网络监听监视、网络窃密的重要工具，供应链安全与国家安全的关系日益密切。同时，世纪疫情、局部地区冲突、国际关系等均深刻影响着供应链的稳定性，过度依赖单一且脆弱的供应链将引发难以忽视的潜在风险，供应链的结构性风险日益凸显。如果说 SolarWinds 等供应链攻击事件引发的是短期内对于网络软硬件产品安全性的担忧，那么美国《2022 年芯片与科学法》以及接连不断的出口管制措施引发的是更为长远的对于产业链供应链升级转型的思考，而信息网络技术对航空、海运、能源等传统行业的影响则要求对其供应链的全链关注走得更远。因此，今后一段时期，供应链安全这一话题将强势“扩张”。建立供应链安全管理策略和准入机制、开展供应链安全风险评估等措施将在短期内提升供应链安全保障能力；长期来看，要求我国在供应链安全保障上也需要发挥能动，想未想之想，为以为之为，推动供应链转型升级，加快补齐短板、锻造长板，提高供应链韧性和安全水平，增强产业体系抗冲击能力，提升供应链现代化水平是最终目标。

（三）数据规则全面塑造，安全与发展的辩证在数字化进程中得到深刻诠释

进入数字时代，数字化转型是大势所趋，数字经济成为重组全球要素资源、重塑全球经济结构、改变全球竞争格局的关键力量。作为国家基础性战略资源，数据不仅是数字经济深化发展的核心引擎，其安全性更成为国家安全的重要组成部分。美国对外关系委员会曾表示“数据是地缘政治力量和竞争的来源，被视为经济和国家安全的核心。”

2022 年，全球数据安全保障规则持续细化，尤其是数据跨境流动秩序在加速构建。作为安全与发展平衡的试炼场，欧美推动的“跨大西洋数据流动框架”取得重要进展，美国白宫发布《关于加强美国信号情报活动保障的行政令》，为重塑欧美数据流动提供制度支撑。尽管跨大西洋数据流对于实现 7.1 万亿美元的

欧盟-美国经济发展至关重要[3]，但正如美国国会研究会在报告中担忧的那样，出于安全考虑，欧洲法院并不一定会认定美国行政令能够提供充分的保障措施。同时，欧盟、英国、韩国等国家和地区的标准合同条款、约束性公司规则、充分性认定、数据跨境传输认证机制等均在稳步推进；我国正式发布《数据出境安全评估办法》，在积极探索推进数据要素市场化的同时保障数据出境安全。上述差异化的立法要求是各国对于安全与发展的不同考量在立法中的映射。未来，安全与发展的辩证关系将随着全球数字化进程的推进得到更加深刻地诠释。进而言之，一方面像印度、新加坡在内的一些国家将通过降低安全需求以寻求数字经济的发展（当然有其安全构架的底线），另一方面则是如越南对《网络安全法》进行释义，要求“外国公司必须在越南境内存储用户数据并设立当地办事处”（同时又以各种实操层面措施缓解外商投资的焦虑）。各国在数据合法使用、数据交易和产业化、数据安全方面的立法将继续推进，并可能在数据基础制度体系、重要数据识别与保护方面取得突破。

（四）网络安全治理能力建设成为网络安全的屏障，网络安全法治的软实力与信息、网络的硬科技同等重要

我国网络立法的“四梁八柱”已基本构建，基本形成以宪法为根本，以法律、行政法规、部门规章和地方性法规规章为依托，以传统立法为基础，以网络内容建设与管理、信息化发展和网络安全等网络专门立法为主干的网络法律体系[4]。治理国家，制度是起根本性、全局性、长远性作用的。然而，没有有效的治理能力，再好的制度也难以发挥作用[5]。因此，在网络安全治理体系基本完善的背景下，提升国家网络安全治理能力成为当务之急。欧盟2022年通过或推进多项重磅法律，已成功影响并正在重塑美欧之间的经济和贸易秩序，达到了其单纯通过开放数据和小微发展无法企及的目标；而美国除了持续将政策法律作为影响他国决策的武器外，也在奋力推动信息网络技术和安全领域的专门立法，体现出其内外有别的两手考虑。对我国而言，初步建立的网络法律体系不是终点，一方面需

[3] FACT SHEET: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework. 链接：
https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/

[4] 国务院新闻办公室. 《携手构建网络空间命运共同体》白皮书

[5] 习近平关于国家治理体系和治理能力现代化的战略思考. 链接：
https://www.dswxyjy.org.cn/n1/2019/0821/c427794-31309149.html

要持续跟踪研判各国主要的政策立法进展，同时宣介和延展我国立法体系和价值理念在推动国际公平公正等秩序中的重大作用；另一方面还需要通过严格网络执法和网络司法、营造网络合规生态、提升网络安全普法宣传力度等途径，推动网络安全法律法规要求切实转化为国家与社会、组织与个人的网络安全保护能力，把我国制度优势更好转化为国家治理效能。

具体来说，在法治中国建设进程中，应持续推动监管机构、职能、权限、程序、责任法定化，推动网络与数据安全行政执法精准化、专业化，重视网络与数据安全行政执法裁量基准、程序性规定对一线执法人员的指引作用，全面推进严格规范公正文明执法。网络司法应更加科学，借助网络安全合规不起诉等制度的推广适用，为数字经济发展留下空间，营造良好的网络合规生态。鉴于政府部门、监管机构掌握着大量的重要数据和敏感信息，日益成为网络安全事件的目标，应通过借助社会化网络安全服务机构的测试、认证、监测等技术模式形成保障合力，秉承安全技术中立和划定监管边界等方式，丰富安全产业和业态。此外，在充分履行网络与数据安全监管职责的同时，政府部门、监管机构应积极推动落实作为网络运营者、数据处理者、个人信息处理者的主体责任，约束和规范自身网络行为与数据活动，避免成为薄弱环节，保障网络与数据安全。

与此同时，新技术新应用不断发展，在为未来安全治理提供工具性价值的同时，也对国家治理体系和治理能力现代化提出新的要求。在未来相当长的时期内，围绕新技术、新应用的既有规则解释、现实执法监管仍将持续展开，以缓解技术产生的立法滞后，甚至催生出新立法、新执法手段和新司法裁判。同时，面对新技术新应用、新风险新安全，同步甚至超前部署相应安全保障措施变得更为常见。元宇宙成为新赛道，国际刑警组织建立全球首个专为全球执法机构设计的元宇宙，帮助警察更好地学习管理虚拟空间。我国《上海市培育“元宇宙”新赛道行动方案（2022-2025 年）》《厦门市元宇宙产业发展三年行动计划（2022-2024 年）》在培育元宇宙新动能的同时，均将安全作为重要一环。再如量子通信与后量子密码的超前部署，既是量子信息的新一轮发展的两翼，也是筑牢安全的多层屏障。对于持续迭代升级的未来技术，坚持技术发展与安全的“同步”原则、在设计研发中植入安全基因、在部署应用中持续关注安全问题是应有之义。

公安部第三研究所网络安全法律研究中心简介

公安部第三研究所网络安全法律研究中心成立于 2016 年 2 月，是公安部第三研究所下设的专业法律研究机构。自成立以来，中心致力于开展前瞻性研究，切实践行理论研究与立法实践深度结合，跟踪研判国内外网络安全政策立法及事件动向，持续推动科研成果应用于网络安全相关立法活动，为政府相关部门提供法律动态研判和决策研究支撑等服务。

邮　箱：cslaw@gass.ac.cn

公众号：公安三所网络安全法律研究中心

360 集团法务中心法律研究简介

360 法律研究是隶属于 360 集团法务中心的高端智库。旨在依托 360 集团卓越的网络安全技术、多元化的产品形态和丰富的法律实践，围绕数字经济发展的前沿性问题，立足国家安全和行业发展，通过开放合作的研究平台，汇集各界智慧，协同解决互联网行业新型法律问题，为共建网络空间命运共同体提供战略支撑，理论保障和人才支持。

邮　箱：g-bp-law@360.cn

公众号：360 法律研究

信安未来简介

“信安未来”是公安部第三研究所自主研发的开放式交流和服务平台，以“共建安全生态 共享安全未来”为目标，集信息安全行业资讯、培训认证、安全产品和服务三大核心功能为一体。平台的“安查查”数据安全合规自查工具免费向全社会开放，后续还将提供资产测绘、互联网资产搜索、安全意识演练、安全测试等更多服务。

ISF 信安未来 INFO SEC FUTURE

共建安全生态　共享安全未来