网络安全技术发展方向与趋势研究

孙倩文，闫　寒，陈羽凡，李　端，刘芷君
（国家工业信息安全发展研究中心，北京 100040）

摘　要：随着新一代信息技术与经济社会发展各领域深度融合，网络安全形势日益严峻，网络安全技术在维护国家安全、支撑产业转型、服务社会发展、保护公众利益等方面的重要作用愈加凸显。本文开展了面向2035年的网络安全技术预见，综合运用愿景分析、需求分析、前沿分析、相关研究成果分析等方法，总结凝练密码技术、数据安全、内容安全等7个子领域的60项网络安全领域关键技术，通过两轮德尔菲调查筛选出10项网络安全领域优先技术方向。面向全球网络安全技术发展新态势新趋势和我国经济社会发展新要求，提出了加快推动我国网络安全技术发展的建议。

关键词：网络安全，技术预见，德尔菲调查，关键技术

1. 引言

没有网络安全就没有国家安全，网络安全技术为维护国家网络安全提供了重要的技术基础，为支撑经济社会发展构建坚实的安全屏障。党的十九届五中全会明确了我国“十四五”期间发展的战略任务和2035年远景目标，强调要统筹发展和安全，全面加强网络安全保障体系和能力建设，对网络安全技术和防护能力提出了新的更高要求。技术预见作为一种战略规划工具，在世界各国的科技政策制定中发挥了重要作用[1]，开展网络安全技术预见通过分析研判网络安全领域发展态势和走向，提出网络安全技术优先方向，能够为网络安全领域技术和产业发展提供路径指引，为网络安全领域相关战略政策制定提供研究支撑。

近年来，各国将网络安全作为国家安全战略的优先方向加大资源投入和力量部署。网络安全在维护国家安全、支撑产业转型、促进社会发展、保障公众利益等方面的重要作用愈加凸显。

从维护国家安全看，网络空间正在成为大国竞争博弈的新场域，极限施压、技术脱钩、技术民族主义等趋势对于信息技术产业链、供应链的负面影响上升，网络空间“巴尔干化”日益显现。未来随着5G、物联网等技术落地普及，基于万物感知、万物互联的智慧社会对于网络安全防御技

作者简介：孙倩文，女，硕士，工程师，国家工业信息安全发展研究中心信息政策所主任，研究方向为数据安全、网络安全技术产业研究。

闫　寒，男，硕士，工程师，国家工业信息安全发展研究中心信息政策所，研究方向为网络安全战略、网络空间治理研究。* 通讯作者。

陈羽凡，女，硕士，工程师，国家工业信息安全发展研究中心信息政策所，研究方向为网络安全产业研究。

李　端，男，硕士，工程师，国家工业信息安全发展研究中心信息政策所，研究方向为数据安全、工业互联网安全研究。

刘芷君，女，硕士，工程师，国家工业信息安全发展研究中心信息政策所，研究方向为供应链安全、网络安全战略研究。

基金项目：中国科协创新战略研究院科研项目“网络安全技术发展方向与趋势研究”（项目编号：2019ys1-1-2-4）。

术能力的综合性、及时性的要求更高，网络安全技术为维护国家安全提供重要的技术手段。

从支撑产业数字化转型看，当前产业转型升级的现实需求引导网络互联互通，实现跨行业跨领域连接、海量数据采集汇聚，同时网络威胁也能直达生产一线，有效应对工业信息安全风险已经成为支撑产业转型升级的重要保障。亟须加强网络安全技术研发的前瞻性布局，提升网络安全防护能力。

从维护社会稳定看，信息化手段在城市建设和政务服务中的加快推广，城市治理和公共服务的泛在化、融合化、智能化水平日益提升。可以预见，各项城市公共服务和电子政务服务对于网络安全防护的需求与日俱增，构建体系化安全保障能力是必然趋势。

从保障人民利益看，信息高度实时共享释放个人信息保护需求，用户个人信息泄露和非法利用等风险正在增加，“网络谣言”“假新闻”“信息造假”等网络违法犯罪行为层出不穷，个性化算法推荐、深度伪造等技术门槛降低，严重侵害了广大人民群众切身利益。目前，监管能力对于网络犯罪违法行动的震慑能力有待增强，亟需提升“以技术管技术”的手段支撑。

因此，基于经济社会数字化转型需求及其可能带来的网络安全风险挑战，分析研究网络安全技术发展趋势具有重要战略和现实意义。本文面向2035年网络安全技术发展趋势，采用愿景分析、需求分析、文献计量等方法，总结了涵盖7个类别60项网络安全领域关键技术方向，组织开展了两轮德尔菲问卷调查，提炼了网络安全领域关键技术方向，并有针对性地提出了加快网络安全技术发展的建议。

2. 国内外网络安全相关技术预见研究进展

近年来，数据安全、隐私保护、网络治理等网络安全议题愈发引起各方高度重视，各国相继开展的信息技术领域的技术预见活动都将网络安全相关技术方向作为重点研究领域之一。

国外相关技术预见研究将网络安全技术作为重点技术方向。2019年11月1日，日本科技学术政策研究所发布了《第11次科技预测调查综合报告》，报告将信息通信技术分析和服务领域列为重要性较高的五大领域之一，其他重点领域为健康医疗和生命科学领域、材料器件和生产工序领域、城市土木建筑和交通领域、宇宙地球海洋等基础科学领域。2017年1月，英国发布第三版《技术与创新的未来2017》报告。提出电池、面向互联网的量子安全、算法与机器学习、机器人与自动系统等四项技术，是未来发展的技术创新趋势。其中，面向互联网的量子安全是重点关注方向之一。报告认为，下一代的光子学可通过量子效应，为数字网络提供更稳定的在线安全性。2016年4月，美国陆军发布了《2016-2045年新兴科技趋势》预测报告，将网络安全技术作为24项值得关注的新兴技术之一，其中用户身份鉴定技术、自我进化型网络、下一代解密技术是网络安全技术最具代表性的发展方向。

我国信息技术领域也开展了对网络安全关键技术的研究，《中国工程科技2035发展战略》筛选了信息与电子领域中关系全局和长远发展的战略领域及优先方向，网络空间安全技术是其中重要的子领域，主要技术方向包括：大规模网络攻击的机理和过程分析技术、网络虚拟身份管理技术、信息内容的理解和研判技术、新一代密码技术、新材料环境下的网络传输安全防御技术等[2]。在《全球工程前沿报告》中，信息与电子工程领域Top10工程开发前沿涉及网络安全技术包括“网络安全中的身份认证与访问控制”[3]；在机械与运载工程领域将“车联网信息安全与隐私保护”列为工程研究前沿热点技术之一；信息与电子工程领域工程开发前沿将“物联网安全检测技术”列入

Top10开发热点之一[4]。

3. 网络安全技术预见方法及过程

本次网络安全技术预见在充分吸收国内相关研究的经验和成果的基础上，以经济社会发展对于网络安全技术的需求分析为研究背景，以文献计量分析为手段支撑，以德尔菲法和专家研讨为核心，识别和遴选网络安全领域关键技术。

（1）文献分析

选取中国计算机学会推荐的网络和信息安全领域高水平会议论文（A、B、C三类），通过Scopus数据库检索下载，时间跨度为2015年至2019年，获取9073篇论文，以论文的标题、摘要、关键词字段作为分析数据，作为基础研究热点及前沿的分析挖掘基础。综合运用无监督聚类方法、复杂网络方法和突发词检测算法展开深度挖掘分析，具体而言，基于Python语言，利用NLTK包对文本数据进行预处理，利用TFIDF方法对文本进行向量化表示，采用K-means++算法对数据进行聚类，对各个聚类簇进行解读和研判，形成网络安全领域的研究热点。此外，基于复杂网络结构洞理论，展开研究前沿分析和挖掘，最后利用链路预测算法识别潜在基础研究前沿。

（2）德尔菲调查

基于网络安全关键技术清单，组织开展了网络安全关键技术专家调查，调查问卷设置集中于技术本身的重要性、技术应用的重要性、技术实现时间预测、技术基础与竞争力，以及技术发展制约因素等五个方面，旨在获取专家对于备选技术判断。在第一轮专家调查结束后，结合分析结果以及专家反馈的具体修改意见，对技术清单进行修订完善。一是根据专家的领域侧重，特别是针对一些小众、细分技术领域，扩大了调查问卷的发放范围，对专家勾选“不熟悉”较多的技术项，有针对性地邀请相关细分领域专家参加问卷调查。二是结合第一轮结果，针对部分技术的产业化的成熟度较高的现象，删除或者进一步聚焦特定技术方向，将重复接近的技术项进行合并。三是针对技术名称表达不够清晰的情况，不断调整细化技术方向的表述和内涵界定，充分体现技术的重要性和前瞻性。结合上述原则，根据第一轮调查中专家提出的部分技术项目，调整平衡不同技术的覆盖面和颗粒度，合并交叉重复的技术方向，形成第二轮技术清单。

德尔菲调查专家方面，46%的专家来自高校，36%的专家来自研究机构，其余专家来自政府部门和企业。从专家反馈看，对于所有填报的技术项，选择“熟悉”“一般”“不熟悉”的专家分别达到34%、52%、14%。总体来看，专家回函具有一定的专业性，统计分析结果具有较高的参考价值。

4. 技术预见结果分析

此次技术预见面向来自相关政府部门、高校、科研院所、企业的专家开展了两轮问卷调查，搜集了专家对于技术清单中技术项的全面评价，得到了技术方向的研发水平和实现时间、技术发展瓶颈及制约因素、领先国家情况等相关结果。

（1）关键技术清单遴选

网络安全技术清单的制定按照“网络安全领域—子领域—技术项”的分步骤分层次进行研究的收敛聚焦，通过专家研讨，凝练提出了7个子领域的划分方案（表1），技术清单在前期研究分析基础上，既考虑到我国经济社会数字化转型对于网络安全的现实需求，同时结合国际上技术前沿发展方向，重点关注网络安全领域潜在颠覆性及具有重大应用潜力的技术方向。并参考调查专家的反馈意见，对子领域的划分有所调整修正。

（2）技术预计实现时间

从实验室实现时间来看，多数技术集中于2021~2025年期间实现，约占91.9%，有8.1%的

表1　网络安全技术子领域及关键技术

序号	技术子领域	技术项
1	密码技术	零信任网络访问安全；基于零知识证明的身份认证；电子签名技术；匿名与隐私保护技术；量子加密技术；差分隐私及应用；同态加密技术
2	数据安全	云环境下的数据存储安全技术；数据防泄漏技术；侧信道分析技术；网络虚拟身份管理技术；基于生物识别的身份认证；大数据威胁情报分析技术；数据溯源
3	系统安全	端点检测及响应技术；多层级端点防护技术；端点准入防御；网络测绘技术；面向移动终端的安全技术；IPv6安全技术；多重安全网关技术；特征码提取与识别；云访问安全代理技术；边缘智能网络安全技术；入侵检测与防御技术
4	内容安全	信息内容的理解和研判技术；互联网舆情管理技术；视图像内容安全技术；网络安全审计与防护技术；行为监测与分析技术；网络可视化技术；网络资源管理技术
5	应用安全	应用访问控制技术；工业控制系统的安全防护技术；Web应用安全风险评估及防护技术；移动应用安全检测技术；可信计算技术；网络取证技术
6	网络攻防	态势感知网络防御；网络安全主动防御技术；动态网络安全防御技术；拟态防御技术；信息渗透与对抗技术；网络攻击追踪溯源技术；大规模网络攻击的机理和过程分析技术；基于机器学习的攻击预测/检测；边缘计算环境下网络安全防御体系；分布式拒绝服务攻击防御；漏洞分析及评估
7	新一代信息技术安全	5G与6G安全技术；软件定义网络安全技术；基于区块链的网络安全防御技术；基于量子的互联网安全技术；云访问安全代理技术；工业互联网安全技术；车联网网络安全防护技术；面向人工智能应用的网络安全防护；空天网络安全；金融网络安全；认知网络安全保障技术

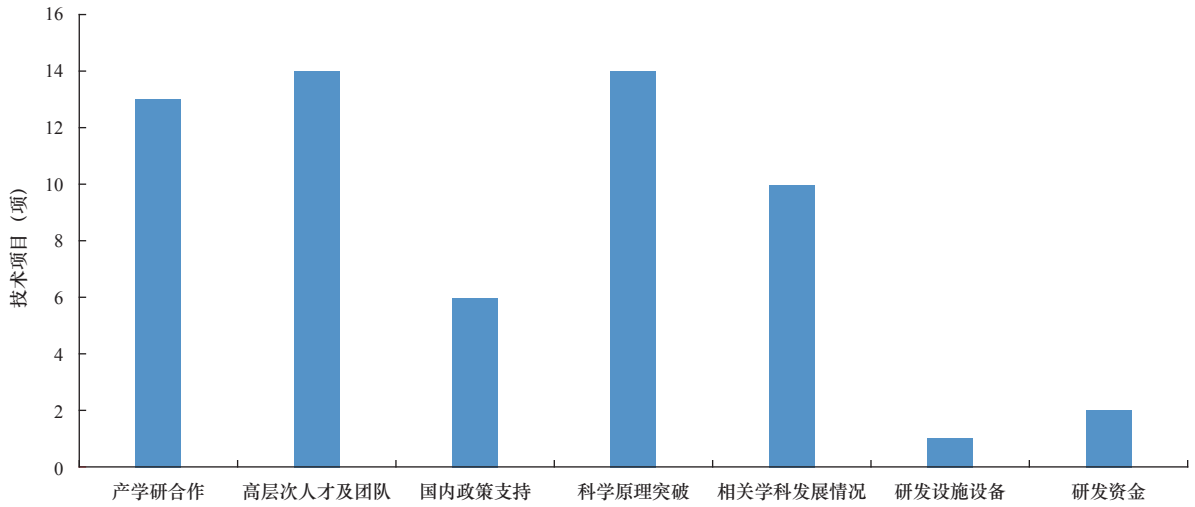

图4　实验室技术研发的制约因素

技术预计实现时间在2026~2030年。从社会推广时间来看，技术清单中技术实现时间仍集中于2021~2025年，预计在此区间内实现的技术约占72.6%，有25.8%的技术预计实现时间在2026~2030年，另有1.6%的技术预期于2031~2035年实现。

（3）技术发展制约因素

在技术研发的制约因素方面，科学原理突破、高层次人才及团队是限制网络安全技术发展主要制约因素，产学研合作、相关学科发展情况等因素的制约影响较强。在应用推广普及方面，

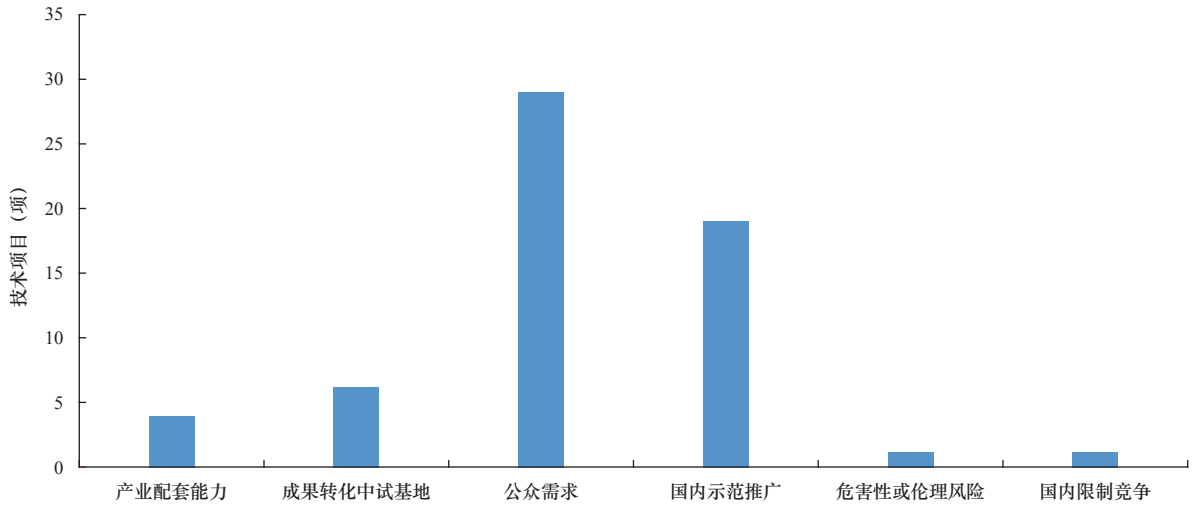

图5　社会应用推广中的制约因素分布

公众需求、国内示范推广对网络安全技术发展的影响较为突出。

（4）技术的领先国家和地区

从全球看，美国在网络安全技术的研究开发水平处于绝对领先的地位，此调查中所有技术美国研究开发水平居于世界第一位。从我国看，有4.8%的技术处于国际领先水平，包括互联网舆情管理技术、拟态防御技术、量子加密技术等，另有91.9%接近国际水平，3.3%落后于国际水平。

表2　网络安全关键技术方向

技术方向	技术子领域	实现时间		制约因素	
		实验室实现	社会推广	实验室制约因素	社会推广制约因素
网络攻击追踪溯源技术	数据安全	2023	2025	高层次人才及团队	国内示范推广
面对人工智能应用的网络安全技术	新一代信息技术安全	2024	2028	高层次人才及团队	国内示范推广
大数据威胁情报分析技术	数据安全	2023	2025	产学研合作	国内示范推广
云环境下的数据存储安全技术	应用安全	2024	2025	产学研合作	产业链配套
信息内容的理解和研判技术	内容安全	2024	2027	高层次人才及团队	公众需求
网络安全主动防御技术	网络攻防	2024	2024	产学研合作	公众需求
网络虚拟身份管理技术	数据安全	2024	2025	国家政策支持	国内示范推广
车联网网络安全防护技术	新一代信息技术安全	2024	2027	产学研合作	公众需求
可信计算技术	应用安全	2025	2028	研发资金	产业链配套
工业控制系统的安全防护技术	应用安全	2023	2024	产学研合作	产业链配套

5. 技术发展趋势及影响

经过专家研讨，综合考虑技术项目在实验室和应用推广的时间，同时也结合不同技术方向之间存在一定的关联性，遴选出网络安全领域需要优先发展的10项关键技术。

网络攻击追踪溯源技术。追踪攻击源的溯源技术针对攻击者的背景、目的、来源以及行为方式进行研究，详细分析网络攻击什么时候发生，为什么发生，攻击将达到什么效果，同时对整个攻击路径进行溯源、对攻击源进行画像等，以威慑潜在的网络攻击者。未来随着政府、企业等主体对于追踪溯源的重视程度提升，结合网络安全数据的积累，将能够通过自动化分析实现更高成熟度的网络攻击溯源。

面向人工智能应用的网络安全技术。人工智能在网络防护、信息审查、智能安防以及舆情监测等方面拥有广阔的应用前景。通过与专家合作，人工智能平台的网络攻击检测率达85%，准确率提高了2.92倍[5]。人工智能算法可以发现超出正常模式的不正常网络行为，并以此识别可疑用户和个人，这将为广大企业赋能，为远程办公、协同办公等应用提供有效防护。在此过程中，人工智能技术必须能够更适应网络安全防护的复杂困难场景，进一步提升技术应用的可行性和可操作性。

大数据威胁情报分析技术。大数据分析包括大数据采集、预处理、存储和管理、分析和挖掘、可视化呈现等一整套技术[6]。未来基于大数据的威胁情报分析技术通过结合威胁情报和攻击事件信息进行大数据挖掘分析，能够更好地解决海量威胁情报信息的采集、存储、对威胁情报进行各种汇聚关联并进行综合分析，洞悉网络安全态势，应对新型复杂的威胁及未知多变的风险[7]。

云环境下的数据存储安全技术。数据中心承载着所有业务实现过程中数据的存储、计算和处理，云安全已经成为数据安全防护的主战场[8]。但随着混合云、私有云的发展，云边界、云上资产及应用，虚拟化放大了传统信息系统环境下安全域的规模，增加了网络安全防护难度和强度。目前有潜力的技术包括零信任策略、联邦学习、隐私计算等方向，在数据安全合规愈发严格的情况下，新的技术方向能够为各方协同应用提供保障，释放数据价值，为网络用户提供更多创新应用。

信息内容的理解和研判技术。传统的文本过滤技术已经不能适应新安全要求，大数据技术辅助网络挖掘和机器学习可执行广度的自动化分析和快速挖掘舆情信息，通过采集、过滤、记录网络上所有的网络数据报文，实时监测网络上的流量信息，发现可疑的内容和目标，并对可疑内容和目标进行记录、报警和阻断。信息内容理解和研判技术将为识别网络虚假新闻、维护数字知识产权、打击网络犯罪行为提供重要的技术手段，促进更多高质量的网络内容传播和推广，营造风朗气清的网络空间。

网络安全主动防御技术。主动网络安全防御是解决网络系统中未知威胁与入侵攻击的新途径，在动态的网络安全技术体系架构中，可根据全局网络安全状态、实战化安全运营要求等，构建主动防御模式，应对已知攻击、未知风险。数据挖掘分析中，溯源定位、策略动态下发、事件自动化响应处置显得尤为重要，主动防御以高效率、弹性资源利用等优势，成为网络安全防御技术研究领域的重点方向。

网络虚拟身份管理技术。网络虚拟身份管理是使网络空间中的个人、组织、服务和设备等对象由权威源建立和认证对应的数字身份，使各方可以相互信赖，其中需要综合使用身份验证、数据保护等技术。未来有望突破十亿级用户的网络虚拟身份高效管理技术，并在全国全面推广，实现与各类网络应用的高度集成[10]。网络虚拟身份管理技术实现并在电子商务、公共服务、社交网络等领域的应用将能够避免用户在不同网络及移

动网络应用时的行为数据被追踪和汇聚，为保护公民个人身份信息提供有力保障。

车联网网络安全防护技术。车联网已经成为未来智慧交通的重要应用场景，同时其带来的网络安全问题引起广泛关注，自动驾驶性能提升带来软件代码的激增，其中软件缺陷中很大一部分是可以被利用的漏洞，这些程序漏洞可能导致软件系统的完整性受损。车联网安全防护需要结合车联网业务场景，采用多种防护技术协同联动[9]，未来面向车联网具体应用场景的网络安全技术，将通过实时感知、及时反馈的安全防护方案，为自动驾驶落地提供安全保障。

可信计算技术。可信计算基于芯片的硬件安全机制，主动检测和抵御可能的攻击。相对于传统的杀毒软件、防火墙等被动防御方式，可信计算不仅可以在攻击发生后进行报警和查杀，还可以在攻击发生之前就进行主动防御，能够更系统更全面地抵御恶意攻击。未来可信计算将需完善可信计算产品体系，从技术、标准、产业链等方面全力推动，建立网络空间免疫生态体系。

工业控制系统的安全防护技术。工业控制系统的网络安全防护与互联网有很大区别，很多联网工业设备设计之初未考虑到网络安全设计，工业生产的可靠性、连续性要求较高，导致针对特定工业控制设备的定期更新升级通常很困难。随着工业互联网加快应用，未来主要的技术发展方向有：威胁情报通过构建攻击知识库，使得针对网络威胁的响应更快；态势感知技术面向运营技术，对各种工控数据进行全面深入的安全智能分析；纵深防御通过设置多层重叠的安全防护系统，加强整体安全能力。

6. 网络安全关键技术发展建议

2020年10月，党的十九届五中全会对我国“十四五”时期发展作出了全面部署，这些任务目标对网络安全和信息化领域技术发展提出了更高的要求。面向全球网络安全技术发展新趋势和我国经济社会发展新要求，网络安全技术发展应坚持“四个面向”，贯彻总体国家安全观，加强基础研究和前瞻部署，加快推动我国网络安全技术研发和应用达到世界先进水平。

（1）网络安全技术发展方面

注重大数据、人工智能、量子科技等领域的基础研究，加强前沿性技术在网络安全领域的创新应用。开展关键技术联合攻关，引导网络安全领域技术能力强、自主程度高的产学研力量加强协作，提升协同创新能力。面向国家网络安全攻防体系建设、网络安全态势感知体系、关键基础设施安全保护、新基建网络安全保障等方面关键性、综合性技术发展，加快网络安全产品服务的迭代创新和演进升级。加强网络安全学科建设，探索网络安全人才联合培养机制，支持通过引进优质师资资源、设立海外技术研发中心等形式，加强高水平人才培养，培育高层次人才团队。

（2）保障技术发展的政策方面

强化国家战略的引领作用，加强国家网络安全的战略部署和综合施策，研究制定技术路线图和时间表，发挥新型举国体制下的资源整合优势，推动跨学科、跨部门、跨领域联合创新、协同创新。加大网络安全网络安全试点示范的推广力度，推动网络安全产业集聚化、差异化发展。加快网络安全技术成果转化，加大关键信息基础设施网络安全投入，引导市场从满足合规需求为主向兼顾合规和能力建设转化。促进产业结构优化，形成不同层次、不同水平的安全产品和服务，更好地适应网络安全市场需求。发挥国家科技计划对创新型网络安全企业开展自主研发创新的引导作用，支持大型龙头企业牵头参与基础技术研发，支持企业、高校、科研机构等加强良性互动，建立自主产业生态。

责任编辑：李琦　校对：陈峰 李琦

参考文献

[1] 赵立新，梁帅.新形势下中国科协开展技术预见的实践与思考[J].今日科苑，2020(8):12-18.

[2] 中国工程科技2035发展战略研究项目组.《中国工程科技2035发展战略·信息与电子领域报告》[M].北京：科学出版社，2019.

[3] 全球工程前沿2018[EB/OL].（2018-12-07）[2020-5-6]. http://www.engineering.org.cn/PDF-EF/Engineering-Fronts-2018-Chinese-Version.pdf.

[4] 全球工程前沿2019[EB/OL].（2019-12-12）[2020-5-6]. http://www.engineering.org.cn/ch/con/Engineering-Fronts/archive.

[5] 周鸿祎.人工智能安全及应对思考[J].九三论坛，2019(6):35-39.

[6] 孙辉，罗双春，李余彪.大数据技术在信息网络威胁情报中的运用研究[J].网络与信息安全，2020(39):28-32.

[7] 劳晓燕，宋丹娃.基于大数据和威胁情报的网络攻击防御体系研究[J].信息安全研究，2019(5):383-387.

[8] 陈慧慧，夏文.“数字新基建”安全态势分析与技术应对[J].信息安全与通信保密，2020(10):17-22.

[9] 李玉峰，陆肖元，曹晨红，等.智能网联汽车网络安全浅析[J].电信科学，2020(04):36-54.

A research on the development direction and trend of cybersecurity technology

Sun Qian-wen, Yan Han*, Chen Yu-fan, Li Duan, Liu Zhi-jun

(China Industrial Control Systems Cyber Emergency Response Team, Beijing 100040, China)

Abstract: With the deep integration of the new generation of information technology and various fields of economic and social development, cyber-security situation is becoming increasingly severe. The significant roles of cyber-security technology in maintaining national security, supporting industrial digital transformation, serving social development, and protecting public interests have become more prominent. This paper carries out the cyber-security technology foresight for 2035, through scenario analysis and other methods, summarizes sixty kinds of technologies in seven sub-fields including cryptography technology, data security and content security. After two rounds of Delphi surveys, ten key technologies are selected, then the paper puts forward suggestions for accelerating these key technologies.

Key words: cyber-security; technology foresight; Delphi survey; key technology