学科动态专题报道

2022 年第 3 期

总第（69）期

网络安全专题

主办者：图书馆学科服务部

2022.03

为传播科学知识，促进业界交流，特编辑《学科动态专题报道》，仅供个人学习、研究使用。

前 言

网络安全是指在运行的网络服务过程中，能够抵御意外风险或者恶意侵入，维护网络系统的软硬件设施，保障系统数据完整性和秘密性，保证网络系统的稳定、连续的安全运行。网络安全作为数字经济发展的压舱石，在护航实体经济转型、促进共同富裕、保障国家安全方面发挥着不可或缺的重要作用。在我国，网络安全早已被上升至国家战略的高度。在今年的政府工作报告中，“强化网络安全、数据安全和个人信息保护”被列为 2022 年重点工作之一。

本报道通过前期调研国内外相关研究，并与我校深耕网络安全领域教师交流的基础上，特将国内外有关“网络安全”的资讯、报告和发展动态等进行系统梳理，为广大科研人员提供研究参考资料。

本期学科动态主要分以下专栏：

《法规指引》专栏的信息主要来源于我国关于网络安全的法律法规。

《海外资讯》专栏的信息主要来源于国外新闻网站、政府网站有关网络安全方面的最新报道。

《国内资讯·聚焦两会》专栏信息主要来自于 2022 年两会期间关于网络安全的代表提案。

《国内分析报告》板块主要选取中国信息通信研究院、中国网络安全产业联盟、工业和信息化部人才交流中心等机构中有关网络安全的分析报告。

《国际分析报告》板块主要选取世界经济论坛、国际电信联盟等国际组织以及普华永道有关网络安全的分析报告。

《国家社科基金项目统计分析》版块主要对国家社科基金项目中网络安全相关立项进行统计和分析，以便了解网络安全领域课题研究动态。

《知识可视化分析》板块运用文献计量工具 Citespace，对目前网络安全研究的发文趋势、研究热点及我校研究热点、作者合作、研究机构进行分析，以帮助科研人员快速了解该领域的研究发展现状和热点。

《资源获取门户网站》主要汇总网络安全领域相关信息和资料的免费获取网站及公众号。

《馆内图书》将我馆现有网络安全相关图书进行展示。

目 录

【法规指引】.....1
《中华人民共和国网络安全法》.....1
《关键信息基础设施安全保护条例》.....2
【海外资讯】.....4
美国参议院通过新的网络安全法案《加强美国网络安全法》.....4
新加坡将建立国家量子安全网络，保障基础设施网络安全.....4
英国在即将出台的《网络安全法案》中增加新刑事犯罪内容.....6
北约网络安全中心成功测试抗量子计算机攻击的安全网络.....7
【国内资讯·聚焦两会】.....9
全国政协委员肖新光：加强 IT 供应链网络安全能力.....9
李宗胜代表:深入开展未成年人网络安全保护公益诉讼.....10
全国政协委员周鸿祎：建议将网络安全升级为数字安全.....11
全国政协常委张亚忠：医卫行业网络安全存在隐患 应加强管理13
【国内分析报告】.....16
中国网络安全产业白皮书.....16
5G 网络安全标准化白皮书（2021）.....18
中国网络安全产业分析报告（2021）.....20
网络安全产业人才发展报告（2021）.....21
【国际分析报告】.....24
2022 年全球网络安全展望.....24
全球网络安全指数.....26

2021 年全球网络信任调查报告.....28
【国家社科基金项目统计分析】.....30
“网络安全”国家社科基金项目统计.....30
“网络安全”国家社科基金项目分析.....32
【知识可视化分析】.....35
模块一：年度发文趋势.....35
模块二：研究热点分析.....35
模块三：作者合作分析.....39
模块四：机构分析.....40
【资源获取门户】.....41
【馆内图书】.....43

【法规指引】

《中华人民共和国网络安全法》

《中华人民共和国网络安全法》由中华人民共和国第十二届全国人民代表大会常务委员会第二十四次会议于 2016 年 11 月 7 日通过，自 2017 年 6 月 1 日起施行。

这是我国第一部全面规范网络空间安全管理方面问题的基础性法律，是我国网络空间法治建设的重要里程碑。进一步明确了政府各部门的职责权限，完善了网络安全监管体制；强化了网络运行安全，重点保护关键信息基础设施；完善了网络安全义务和责任，加大了违法惩处力度；将监测预警与应急处置措施制度化、法制化。该法将近年来一些成熟的好做法制度化，并为将来可能的制度创新做了原则性规定，为网络安全工作提供切实法律保障。

《网络安全法》的出台具有里程碑式的意义。它是全面落实党的十八大和十八届三中、四中、五中、六中全会相关决策部署的重大举措，是我国第一部网络安全的专门性综合性立法，提出了应对网络安全挑战这一全球性问题的中国方案。此次立法进程的迅速推进，显示了党和国家对网络安全问题的高度重视，是我国网络安全法治建设的一个重大战略契机。网络安全有法可依，信息安全行业将由合规性驱动过渡到合规性和强制性驱动并重。

《中华人民共和国网络安全法》包括七章：

第一章 总则

第二章 网络安全支持与促进

第三章 网络运行安全

第四章 网络信息安全

第五章 监测预警与应急处置

第六章 法律责任

第七章 附则

法规全文请查看链接：http://www.cac.gov.cn/2016-11/07/c_1119867116.htm

《关键信息基础设施安全保护条例》

国务院总理李克强签署国务院令，公布《关键信息基础设施安全保护条例》（以下简称《条例》），自 2021 年 9 月 1 日起施行。

党中央、国务院高度重视关键信息基础设施安全保护工作。关键信息基础设施是经济社会运行的神经中枢，是网络安全的重中之重。当前，关键信息基础设施面临的安全形势严峻，网络攻击威胁事件频发。制定出台《条例》，建立专门保护制度，明确各方责任，提出保障促进措施，有利于进一步健全关键信息基础设施安全保护法律制度体系。

一是明确关键信息基础设施范围和保护工作原则目标。《条例》明确，重点行业和领域重要网络设施、信息系统属于关键信息基础设施，国家对关键信息基础设施实行重点保护，采取措施，监测、防御、处置来源于境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治违法犯罪活动。保护工作应当坚持综合协调、分工负责、依法保护，强化和落实关键信息基础设施运营者主体责任，充分发挥政府及社会各方面的作用，共同保护关键信息基础设施安全。

二是明确了监督管理体制。《条例》规定，在国家网信部门统筹协调下，国务院公安部门负责指导监督关键信息基础设施安全保护工作。国务院电信主管部门和其他有关部门依照《条例》和有关法律、行政法规的规定，在各自职责范围内负责关键信息基础设施安全保护和监督管理工作。省级人民政府有关部门依据各自职责对关键信息基础设施实施安全保护和监督管理。

三是完善了关键信息基础设施认定机制。《条例》明确了认定工作的组织方式和认定程序，依照行业认定规则，国家汇总并动态调整关键信息基础设施认定结果，确保重要网络设施、信息系统纳入保护范围。

四是明确运营者责任义务。《条例》对关键信息基础设施运营者落实网络安全责任、建立健全网络安全保护制度、设置专门安全管理机构、开展安全监测和风险评估、报告网络安全事件或网络安全威胁、规范网络产品和服务采购活动等作了规定。

五是明确了保障和促进措施。《条例》对制定行业安全保护规划、建立信息共享机制、建立健全监测预警制度、明确网络安全事件应急处置要求、组织安全

检查检测、提供技术支持和协助等作了规定。

六是明确了法律责任。《条例》对关键信息基础设施运营者未履行安全保护主体责任、有关主管部门以及工作人员未能依法依规履行职责等情况，明确了处罚、处分、追究刑事责任等处理措施。对实施非法侵入、干扰、破坏关键信息基础设施，危害其安全活动的组织和个人，依法予以处罚。

《关键信息基础设施安全保护条例》包括六章：

第一章　总则

第二章　关键信息基础设施认定

第三章　运营者责任义务

第四章　保障和促进

第五章　法律责任

第六章　附则

法规全文请查看链接：

http://www.cac.gov.cn/2021-08/17/c_1630785976988160.htm

【海外资讯】

美国参议院通过新的网络安全法案《加强美国网络安全法》

刘程 编译 苑艺 校对

2022 年 3 月 1 日，美国参议院通过《加强美国网络安全法》(Strengthening American Cybersecurity Act)，旨在加强美国关键基础设施所有者的网络安全。

该法由《网络事件报告法案》(CIRA)、《联邦信息安全现代化法案》(FISMA)和《联邦安全云改进和就业法案》(FSCIJA)三项网络安全法案措施组成。

新的法案规定，遭网络安全事件的实体必须在 24 小时内向美国网络安全和基础设施安全局 (CISA)发出关于勒索支付的警报，且必须在 72 小时内向 CISA 上报受攻击事件。此外，受影响的组织必须保留相关数据，如果出现大量新的或不同的信息，或者如果涵盖的实体在提交网络安全事件报告后支付了赎金，则需及时共享对以前提交的网络安全事件报告的更新。

FISMA 集成了更有效的网络安全实践，FSCIJA 旨在加速部署云计算产品和服务，并大力推动采用安全云能力、创建工作并减少对遗留信息技术依赖。

新的网络安全法案现在已经得到参议院的批准，在正式签署成为法律之前还需要获得众议院的通过。

美国参议员罗伯·波特曼（ Rob Portman ）在 2021 年 9 月指出，“随着网络勒索攻击不断增加，联邦政府必须要能够迅速协调应对，并追究这些不良行为者的责任。该法案将增加对日常发生在我们国家的网络攻击的可见性，并启用完整的政府响应、缓解并提醒关键基础设施相关人员和其他人注意正在发生以及即将发生的攻击。”

编译自：

https://thehackernews.com/2022/03/us-senate-passes-cybersecurity-bill-to.html

新加坡将建立国家量子安全网络，保障基础设施网络安全

张福学 编译 苑艺 校对

新加坡量子工程计划（QEP）将展开全国性的量子安全通信技术试验，该技

术有望为关键基础设施和处理敏感数据的公司提供强大的网络安全保障。该项目由新加坡国家研究基金会（NRF）支持，由 15 名私人和政府合作者共同展开。

网络安全是当今数字社会的基石。众所周知，由于量子计算机在某些任务的处理能力可能比传统计算机强大数百万倍，保护着数十亿比特数据的公钥加密未来极易受到量子计算机的攻击。虽然如今的量子计算机还不足以破解加密，但随着技术进步，解决网络安全威胁的呼声变得更加迫切。

量子安全通信技术旨在通过专门的硬件和新的密码算法对抗量子计算的威胁。它们可以保护政府通信系统、能源网等关键基础设施，以及为在医疗、金融等领域内处理敏感数据的公司提供安全保障。

新加坡的国家量子安全网络（NQSN）还将部署商业技术，与政府机构和私营企业开展试验，对安全系统进行深入评估，并制定指导方针以支持企业采用此类技术。

“新加坡可以利用其在量子科学、光学和网络安全工程方面的传统，成为一家值得信赖的全球量子网络技术和服务供应商。在国家量子安全网络中，我们将把量子创新引入已部署的光学网络，与行业合作伙伴一起研究量子网络的可靠性和适应性等运行问题。”来自新加坡国立大学电气与计算机工程系和量子技术中心的 NQSN 首席助理研究员 Charles Lim 说。他将与另外三位项目负责人合作实现这一目标。量子工程计划由新加坡国立大学主导，将在三年内获得 850 万新元资金支持。合作者将为项目带来专业知识、设备和具体用例。

智慧国家及数码经济(NRF)部门主任 Ling Keok Tong 指出，“新的国家量子安全网络旨在利用先进的量子技术和解决方案加强关键基础设施的网络安全，同时也可以成为公私合作的强大平台。这标志着技术转化的优越性，也是 RIE2025 计划的关键举措之一，该计划将推动新加坡向可靠的数字创新中心持续转型。”

信息通信媒体发展局（IMDA）集群总监（BizTech Group）翁振辉说，“随着我们探索量子计算和网络技术的进步，国家量子安全网络向前迈出重要的一步。IMDA 将继续推动前沿技术的发展，以构建新加坡的数字未来。我们将与 NRF、NUS 以及我们的行业和研究合作伙伴一起研究如何在新加坡广泛的光纤网络基础设施上运营和实施量子密钥分发网络。”

联合研究团队预计在一年内完成第一批节点。同时，他们将建立一个量子安

全实验室，开始高级量子安全漏洞研究和安全设计。他们还将与潜在用户进行研讨会，以更好地了解他们的需求，提高对新技术的认识。

编译自：

https://thequantuminsider.com/2022/02/20/singapore-to-build-national-quantum-safe-network-to-protect-critical-infrastructure/

英国在即将出台的《网络安全法案》中增加新刑事犯罪内容

谭朔金 编译 苑艺 校对

英国政府公布了加强其网络安全法案的计划，其中包括设立新的刑事犯罪。

这项立法于 2021 年 5 月首次起草，将对用户上传内容或在线交流社交媒体网站和其他服务施加新的规定，以删除和限制非法和有害内容的传播，包括儿童性虐待、恐怖材料和自杀内容。

英国通信监管机构 Ofcom 将负责追究这些公司的责任，并有权对未能履行其义务的公司处以高达 1800 万英镑或全球年营业额 10%的罚款，以较高者为准。

数字部长纳丁·多里斯（Nadine Dorries）近期宣布，与滥用和攻击性在线通信有关的三项新罪行将被纳入该法案。此前，法律委员会进行了一次审查，得出的结论是，这一领域的现行法律没有跟上智能手机和社交媒体的发展步伐。

新的罪行包括:

“真正具有威胁性”的通信犯罪，发送或张贴信息以传达严重伤害的威胁。这将打击网上威胁强奸、杀人和实施身体暴力或给人们造成严重经济损失的行为。这是专门为保护公众人物而设计的，如议员、名人或足球运动员等。

一种基于伤害的通信犯罪，用于捕获在没有合理理由的情况下发送造成伤害的通信。这种罪行基于有意地对受害者造成心理伤害，并考虑通信发送的背景。希望这将更好地解决针对妇女和女孩的辱骂信息，这些信息在单独考虑时可能危害不够明显。它还旨在避免将无意造成伤害的通信定为刑事犯罪，如成人之间的自愿信息。

当一个人发送他们知道是虚假的信息，意图造成巨大的情感、心理或身体伤害时，即构成犯罪。这将涵盖故意发送给他人造成伤害的虚假通信，如恶作剧炸弹威胁，而不是人们不知道自己发送的是虚假的或真正相信是真实的错误信息。

这些罪行将被判处不同的最高刑罚，包括因威胁性通信而被判处最高五年的监禁。

刑法专员彭尼·刘易斯（Penney Lewis）教授解释说:“刑法应该针对那些明确打算造成伤害的人，同时允许人们善意地分享有争议的想法。我们的建议创造了一个更加细致的刑事犯罪集，更好地保护真正有害通信的受害者，以及更好地保护言论自由。”

此外，社交媒体公司将被赋予新的职责，以更快地删除其网站上最有害的非法内容和犯罪活动。这些犯罪内容包括色情、仇恨犯罪、欺诈、出售非法毒品或武器、鼓励自杀、人口走私、恐怖主义和性剥削。对于这些类型的内容，社交媒体网站必须采取主动措施，防止用户查看它们。在线平台的高管如果不遵守这些新规定，最终可能会入狱。

英国数字、文化、媒体和体育部大臣娜丁·多里斯评论道:“本届政府表示将立法让英国成为世界上最安全的网络之地，同时保障言论自由，这正是我们将要做的。我们世界领先的法案将保护儿童免受在线虐待和伤害，保护最弱势群体免受有害内容的影响，并确保恐怖分子在网上没有藏身之地。我们正在听取议员、慈善机构和活动家的意见，他们希望我们加强立法，今天的变化意味着我们将能够利用法律的全部力量来打击那些利用互联网作为武器来破坏人们生活的人，并且这样做得更快、更有效。”

编译自:

https://www.infosecurity-magazine.com/news/uk-offenses-online-safety-bill/

北约网络安全中心成功测试抗量子计算机攻击的安全网络

刘程 编译　苑艺 校对

北约网络安全中心（NCSC）使用英国 Post-Quantum 公司提供的虚拟专用网络（VPN）成功测试运行了安全通信流，并表示这是能够抵御量子计算机攻击的安全网络。北约网络安全中心由北约通信和信息局（NCI Agency）运营，全天候保护北约网络安全。

Post-Quantum 公司提供了不同的算法来确保网络安全性，即使在面对使用量子计算的攻击者时也是如此。VPN 可以使用这些算法来保护通信安全，确保只

有正确的接收者才能读取数据。人们在传统的办公环境之外工作时，这种软件可以保护远程连接，并可用于确保运营环境中组织之间的安全通信。

北约网络安全中心首席科学家康拉德·沃纳（Konrad Wrona）说：“在量子时代，确保北约的通信安全对于我们在不担心被拦截的情况下有效运作的能力至关重要。随着‘现在获取，未来解密’的威胁迫在眉睫，这是一项越来越重要的能力，以防止当前和未来可能出现的威胁。”

Post-Quantum 是一种“混合后量子 VPN”，它结合了新的后量子和传统加密算法。由于世界需要多年时间才能完全迁移到能保证量子安全的未来，因此我们将这些新算法与更好理解的传统加密结合起来以确保互操作性更为现实。后量子解决方案是向互联网工程任务组（IETF）提出的开放标准化方案。

Post-Quantum 首席执行官 Andersen Cheng 表示，“超过十年的深度研发意味着我们有能力设计出真实世界的量子安全解决方案。与北约合作的这个项目是世界向量子安全生态系统过渡的重要里程碑，组织现在就采取行动是明智的”。

编译自:

https://www.ncia.nato.int/about-us/newsroom/nato-cyber-security-centre-experiments-with-secure-network-capable-of-withstanding-attack-by-quantum-computers.html

【国内资讯·聚焦两会】

随着信息技术的飞速发展，网络安全问题越来越复杂多样，受到社会各界强烈关注。在今年的政府工作报告中，“强化网络安全、数据安全和个人信息保护”被列为 2022 年重点工作之一。两会期间，多份提案涉及网络安全相关问题，代表委员们从不同角度就如何进一步做好网络安全工作，积极建言献策。

全国政协委员肖新光：加强 IT 供应链网络安全能力

IT 供应链环节复杂、暴露面多，上游环节被攻击者利用会引发雪崩效应造成不可估量的影响。近几年，网络攻击者通过入侵软硬件产品供应商，实现对下游政企应用场景的连锁突破，已经成为常态化攻击方式。为此，在今年全国两会上，全国政协委员、哈尔滨安天科技股份有限公司董事长肖新光提出了《关于加强 IT 供应链网络安全能力的提案》。

在肖新光看来，IT 供应链网络安全能力面临三个挑战。一是软件研发场景防护能力普遍薄弱。二是整体软件行业代码安全工程能力较差。三是政企用户侧供应链管理工作缺失网络安全维度。“在我国加速推进数字化转型和数字中国建设的背景下，上述问题如不能得到有效重视和积极应对，将对我国关键信息基础设施安全带来重大风险隐患。”

肖新光建议相关部门设立专项，研究推动软硬件研发场景安全防护工作。制定对应标准规范体系，覆盖开发环境、生产环境安全防护、软件强制签名要求与签发环境安全要求、软件分发升级环境安全规范等。通过建立试点示范项目、安全投入加计扣除等机制，引导基础软硬件、共性软件、政企场景工具软件等相关研发企业机构，重视网络安全工作，加大安全防护力度。

肖新光建议相关部门出台支持软件研发企业全面启动代码安全工程的专项政策和引导措施。跟进技术发展趋势，推动 SecDevOps 等先进方法成为软件安全开发的通用实践，实现安全、快速、持续的软件开发能力。设立专项支持安全引擎等安全中间件开发，鼓励研发企业与安全企业强强联合，通过产品嵌入安全中间件等方式，实现 IT 产品安全防护能力的出厂预置。

肖新光建议主管部门组织专项普查，全面分析关基和政企场景的软件工具应

用分布、来源、可控性等因素，形成完整图谱，掌握问题隐患。相关部门组织专项，研究制定关基场景全生命周期的供应链安全管理工作的系列标准规范、实践指南、考核办法、测试测评标准，以及制定供应商准入机制、成熟度评价标准的安全指南。

链接地址：http://www.rmzxb.com.cn/c/2022-03-08/3069529.shtm

李宗胜代表:深入开展未成年人网络安全保护公益诉讼

全国人大代表、辽宁安行律师事务所创始合伙人李宗胜十分关注未成年人合法权益保护问题，经过深入调研，他向十三届全国人大五次会议提交了关于深入开展未成年人网络安全保护公益诉讼的建议。

修订后的未成年人保护法第 106 条规定：“未成年人合法权益受到侵犯，相关组织和个人未代为提起诉讼的，人民检察院可以督促、支持其提起诉讼；涉及公共利益的，人民检察院有权提起公益诉讼。”

“这一规定通过在单行法增设公益诉讼条款的方式，解决了未成年人检察公益诉讼实践探索中上位法授权不足的问题。”李宗胜说。

调研中，李宗胜发现，近两年来，检察机关未成年人网络安全保护公益诉讼工作扎实推进， 但网络传播速度快、取证难及未成年人有自愿沉迷网络的行为等，均导致未成年人网络安全保护公益诉讼存在一定难度。

为此，李宗胜建议，除未成年人个人信息保护公益诉讼外，持续加强未成年人敏感信息的公益诉讼，特别是针对一些单位和部门安置的能够采集或诱惑未成年人同意采集敏感信息的，要关口前移，通过检察建议等形式，及时防患于未然。

“不仅要重视未成年人个人信息保护，还应深度保护未成年人面临的多重网络安全风险，诸如网络性侵、网络诈骗、网络暴力与欺凌、违法不良信息泛滥、隐私与个人信息泄露等。”李宗胜认为，上述网络安全风险面向不特定的未成年人群体，而未成年人及其监护人很可能缺乏维护自身权益的意识和能力。互联网治理涉及复杂的行政监管，网络平台和服务提供者往往拥有巨大的技术和商业资源。因此，应加大检察机关与公安、教育等部门协调配合力度，使检察机关通过提起相关公益诉讼，行使未成年人网络保护的法律监督职能。

李宗胜还建议，培养和储备一批既了解未成年人心理又懂得网络和公益诉讼

的检察官队伍，并及时梳理相关指导案例，引导全社会关注未成年人网络安全，保障未成年人健康成长。

链接地址：

https://baijiahao.baidu.com/s?id=1726683862122343360&wfr=spider&for=pc

全国政协委员周鸿祎：建议将网络安全升级为数字安全

全国政协委员、360 集团创始人周鸿祎在认真学习第十三届全国委员会常务委员会工作报告后表示：“政协工作报告强调要围绕中心任务议政建言，加快启动新的国家科技重大专项。我作为科技企业的委员，深感责任重大。当前中国正处于第二个百年奋斗目标的关键时刻，科技企业一定要始终坚持党的全面领导，秉承科技报国的理念，发挥‘上山下海’精神：“勇攀科技高山，积极参与国家重大科技专项，帮助国家解决‘急难关卡’技术难题，成为国家战略科技力量；积极下数字化蓝海，产业数字化是推动中国高质量发展的新引擎，各级政府和传统产业将成为数字化的主角。科技企业要积极为传统产业转型数字化赋能，用云计算、 大数据、人工智能等帮助他们优化业务流程、改造商业模式、升级产业结构。同时，要统筹发展与安全，为建设数字中国筑牢数字安全屏障。”

当前，发展数字经济、建设数字中国已上升为国家战略。然而，数字化的程度越高，安全挑战也就越大。以此为背景，本次两会，周鸿祎委员以直面新问题、应对新挑战为核心，着眼于解决当下最迫切的安全问题，将携多份提案上会，内容聚焦数字安全、智能网联汽车安全、开源软件安全以及中小微企业安全等。

网络安全升级为数字安全，筑牢数字安全屏障

2021 年，360 接到并处理 4000 多起勒索攻击事件，累计捕获境外 47 个国家黑客组织，监测到 4200 多次攻击，涉及 2 万余个攻击目标。这一数据说明网络安全已升级为数字安全，数字化的安全威胁超越虚拟世界，延伸到了现实世界，传统的网络安全已无法涵盖复杂的数字安全挑战。”全国政协委员、360 集团创始人周鸿祎在 2022 年全国两会上表示。

为此，今年两会周鸿祎委员带来了《网络安全升级为数字安全，筑牢数字安全屏障的建议》提案，分别瞄准产业数字化新场景、新型数字技术和应用场景和打造城市级数字空间安全基础设施和应急体系三个方向提出打造数字安全体系

的建议。

建立“数字空间碰撞测试”机制，护航智能汽车产业发展

近年来，智能网联汽车发展迅猛，车联网作为数字化新场景，面临巨大的安全挑战。据 360 车联网安全实验室统计，国内 25 家车企的 53 款在售智能网联汽车中，360 公司共计发现漏洞 1600 余个，其中，云端漏洞 1000 余个，可导致攻击者远程批量控制该品牌所有的智能网联汽车；车端漏洞 600 余个，可导致近距离非接触式控制汽车，如开关车门、启动引擎等。

为此，周鸿祎建立智能网联汽车“数字空间碰撞测试”机制和相关标准，保障汽车出厂安全和持续检测。同时，他还建议规范汽车安全漏洞的上报行为，不得恶意炒作和违规披露，汽车行业尽快打造一套以安全大脑为核心的智能网联汽车行业态势感知体系，建立汽车安全监管长效机制。以此，来帮助监管部门和车企实现汽车安全实时全程“可见、可控、可管”，确保上路的智能网联汽车始终处于良好的安全状态。

加强开源代码的系统性漏洞挖掘 建立开源软件的全生命周期安全管理

2021 年 12 月 10 日，Apache 基金会开源项目的 Log4j2 组件被发现存在远程代码执行漏洞，该漏洞被业内称为“核弹级”漏洞。周鸿祎表示，在 Log4j2 漏洞曝出之前，开源软件漏洞便已存在大量漏洞，只不过此漏洞的爆发引起了外界的普遍关注。周鸿祎对开源软件依然持积极看法，并十分提倡开源精神，认为这是新时代的“集中力量办大事”，没有开源软件也就没有中国互联网的今天。

然而，从安全的角度，开源软件很容易成为他国对我进行网络渗透攻击的渠道。周鸿祎提案建议开展对开源代码的系统性漏洞挖掘，构建开源代码的安全风险评估机制，明确软件企业承担起开源软件的全生命周期安全管理，建立软件企业安全责任制，并积极参与国际开源社区，促进国际开源软件的漏洞挖掘。

帮扶中小企业数字化转型，数字安全“一个都不能少”

作为中国经济的“毛细血管”，中小企业贡献了 50%以上的税收，60%以上的 GDP，70%以上的技术创新，80%以上的城镇劳动就业，90%以上的企业数量。推动中小企业发展数字化转型，对我国就业稳定、经济增长及产业转型意义重大。然而，中小企业深受“不会转、不敢转、不能转”的困扰。

不仅数字化转型困难，中小企业普遍缺乏数字安全能力。随着万物互联时代

的到来，中小企业的安全缺口不仅危及自身，还有可能成为攻击的跳板，对大型企业、单位，乃至国家安全造成伤害。为此，周鸿祎建议提高中小微企业数字安全能力，出台专项政策规范明确中小微企业应具备的数字安全能力要求。同时，他建议借鉴免费杀毒的模式，鼓励大型安全企业向中小微企业提供轻量化免费安全服务，以保障中小微企业数字安全不掉队。

在举国发展数字化的今天，作为安全行业的委员，周鸿祎今年两会提案有望引发更多政府机构和企业对数字安全的重视，共同投入，夯实数字化的底座，为数字文明时代保驾护航。

链接地址：

https://baijiahao.baidu.com/s?id=1726366325703736727&wfr=spider&for=pc

全国政协常委张亚忠：医卫行业网络安全存在隐患 应加强管理

近年来，我国医卫行业信息化全面发展，在线挂号、线上问诊、电子病历等数字化场景应用广泛。老百姓就医便捷，医院运转效率也得到提高。与此同时，大量数据汇入医卫系统，医疗信息数据中涉及大量患者个人隐私（真实身份、电话、家庭地址、疾病信息、检查信息等），如何保障老百姓就诊信息安全，避免隐私外泄风险？

十三届全国政协常委，九三学社中央常委、河南省委主委，河南省政协副主席张亚忠表示，“当前，我国医卫行业网络信息安全形势较为严峻，有些医卫单位的内网却存在‘僵木蠕’互联网病毒”。

网络安全隐患较多

据了解，医疗数据因隐私性强、可利用价值高、来源广泛，容易成为黑客重点攻击目标。仅从媒体公开报道即可看到，因医卫信息安全问题导致的泄露事件多次发生，小到医护人员转卖患者信息牟利，大到第三方公司利用外包服务便利，窃取患者医疗数据。2017 年杭州某公司在承接疾病预防控制部门网站信息化建设时，非法下载接种疫苗儿童及家长信息 370 余万条，曾造成恶劣社会影响。

张亚忠委员认为，“由于我国医卫行业信息安全工作起步较晚，整体风险较高且防护能力较低，网络信息安全形势较为严峻。主要存在三个问题：一是医信

系统存在安全隐患；二是安全管理建设不足，没有真正施行《网络安全法》要求的'三同步'建设原则；三是网络安全专业人才稀缺。”

数据显示，通过对我国医卫行业相关单位开展调研发现，部分单位应用服务端口在没有任何安全措施的情况下、直接暴露在公共互联网，有些单位正常工作受到“僵木蠕”网络病毒干扰，有些单位官方网站存在被篡改的安全隐患，甚至有单位网站已被篡改却不自知。

张亚忠指出，“有些医院的医疗信息系统（HIS）、电子病历系统（EMRS）缺少有效安全措施和审查机制，系统账号随意借用、一号多用、使用简单密码等情况导致核心业务数据存在盗用风险，医院内外网缺乏可靠的技术隔离措施、系统接口与合作单位及公共网络未经安全规划直接互联导致网络攻击、重要业务数据泄密风险加剧。”

对此，张亚忠建议“完善安全防控体系”：

一是完善医卫行业网络信息安全相关政策法规和标准规范。建立符合医卫行业特色的安全体系架构，制定具备行业特性的安全标准，出台医卫行业网络信息系统设计、实施和运维规范。

二是加强健康医疗数字身份管理。建设全国统一标识的医疗卫生人员和医疗卫生机构可信医学数字身份、电子实名认证、数据访问控制信息系统，推进医卫数据可信体系建设。

三是建立服务管理留痕可溯、诊疗数据安全运行、多方协作参与的健康医疗管理新模式。指导医卫行业相关单位设置网络信息安全管理专门机构和岗位，明确职责任务。

网络安全管理建设不足

张亚忠指出，“有些医卫单位投资网络信息安全建设时缺乏统筹、规划和审计，单纯注重硬件设备建设，且购买、招标、利用、分配全过程缺少严格审计。对信息安全的建设投入和宣传教育重视不足，安全管理机制不健全，忽视安全设备和专业人员的管理使用效能，发生安全事故无法高效启动安全措施，追踪溯源避免损失扩大。”

对此，张亚忠建议尽快“健全安全审查机制”，加强对医疗设备及商业化软件的安全审查和安全检测，制定设备远程运维监管制度。严格落实内外网络分离，

严格落实系统用户分级分类接入，改进安全感知、安全处置和安全审计等方面的数据防护能力，加强对第三方安全运维单位的监管。

网络安全专业人才稀缺

医卫行业网络安全是我国网络安全的重要组成部分，受到国家高度重视。党中央、国务院及医疗监管部门陆续出台相关政策法规，逐步完善行业网络安全体系。但传统医院体系里缺少网络安全人才，即使服务外包，也无法专业把控第三方公司所存在的安全风险。

张亚忠认为，应全力培养医卫系统内部的网络安全专家。“医院里多以医卫专业人员替代管理网络信息系统，其专业性、敏感性较低，对网络安全认知存在不足，易出现安全事故处置失当、人为加剧事故等情况。”

对此，张亚忠建议，“通过资质认证、教育培训、攻防演练等方式，提升医卫系统现行信息安全队伍的专业技能，全力培养行业安全专家。建立行业网络、信息系统及数据安全专控队伍，定期开展行业重要信息系统的安全测评、风险评估以及安全应急演练等工作。对于医疗专业人员定期开展信息安全宣传教育，有针对性的开展保护患者隐私、医疗数据安全、反钓鱼、反欺诈宣传，增强医务人员的网络信息安全意识和法制观念。”

今年两会，张亚忠已提交《关于加强医卫行业网络信息安全的提案》，他呼吁尽快“对症下药”完善安全防控体系、健全安全审查机制、强化专业队伍建设。让技术更好守护人民群众健康，保障医卫系统信息安全的全生命周期。

链接地址：

http://www.msweekly.com/show.html?id=135897

【国内分析报告】

中国网络安全产业白皮书

2022 年 1 月，中国信息通信研究院在工业和信息化部网络安全管理局指导下，基于网络安全产业发展和前沿技术应用研究成果，发布 2021 年《中国网络安全产业白皮书》。

报告所研究的网络安全产业，主要聚焦在政策、资本、生态环境等外部因素影响下，网络安全供需双方主体通过市场机制作用，进行一系列研发、生产、经营、采购等活动所形成的组织业态。为了构建清晰的研究脉络，报告首先对网络安全市场规模和结构总体情况进行概述，然后对国内外政策、技术产品体系、企业经营、资本赋能、产业生态等内外部因素的最新发展动态进行重点分析，多维度展现我国网络安全产业发展态势。希望为关注网络安全产业发展的政府机构、企事业单位以及相关组织和个人提供参考和帮助。

内容概览：

一、全球网络安全产业发展动态

(一)全球网络安全市场增速回落，结构分布稳中有变

(二)网络安全政策举措纵深推进，优化产业发展环境

(三)市场主体发展总体良好，新兴厂商优势凸显

(四)资本加持重点领域，融资并购出现两极分化

二、我国网络安全产业进展

(一)网络安全市场发展稳中向好，区域行业差异明显

(二)政策体系不断完善，推动产业发展迈向新阶段

(三)技术产品体系持续演进，为产业发展注入动能

(四)市场主体发展放缓，大型企业具备竞争优势

(五)资本赋能效应显现，投资主体进一步丰富

(六)生态建设持续优化，构筑高质量发展屏障

三、我国网络安全产业发展举措建议

(一)加速完善政策措施，筑牢网络安全坚实防线

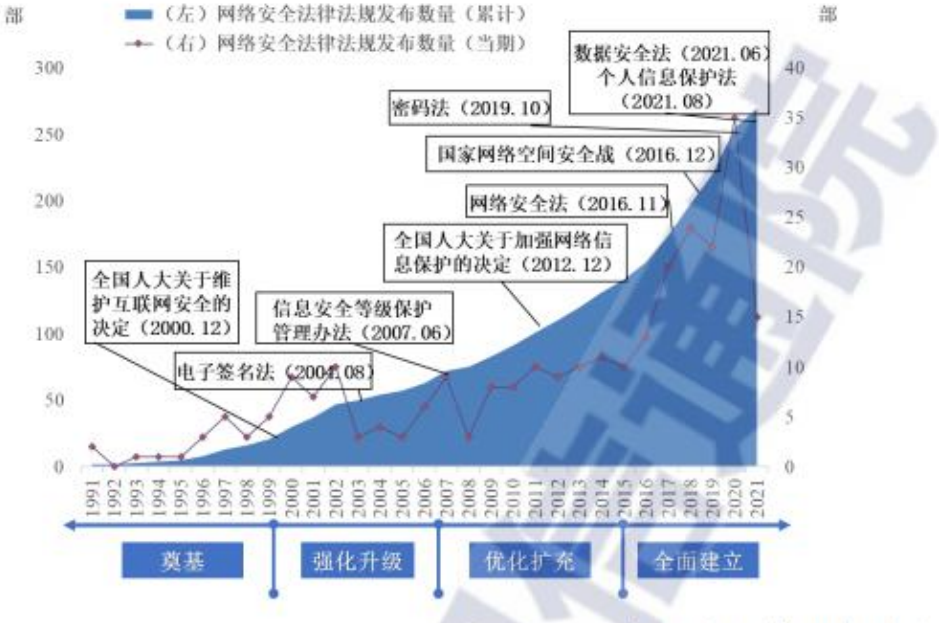
(二)持续强化技术创新,提升产业供给水平

(三)不断优化素质结构,完善人才梯队建设

(四)科学统筹要素资源,优化产业生态环境

来源：中国信息通信研究院

图 14 2015-2021 年我国网络安全产业规模增长情况



来源：中国信息通信研究院

图 20 我国网络安全法律法规数量变化趋势

附件：1.《中国网络安全产业白皮书》.pdf

链接地址：http://www.cww.net.cn/article?id=557143

5G 网络安全标准化白皮书（2021）

《5G 网络安全标准化白皮书》由中国移动通信集团有限公司,中国电子技术标准化研究院,中国信息通信研究院等 15 家企事业单位共同编制。

在全球范围内 5G 广泛商用、规模快速扩大的背景下,5G 网络安全问题也成为各方关注焦点。5G 网络安全包括终端安全、IT 化网络设施安全、通信网络安全、行业应用安全、数据安全、网络运维安全等多个方面。虽然 5G 较 4G 拥有更为完善的安全特性,但随着 5G 融合应用的不断深入,又将面临的新网络安全威胁与风险。为促进 5G 与相关产业的健康安全发展,切实发挥标准在网络安全工作中的基础性、规范性、引领性作用,有效指导和体系化推进相关重点标准研究制定工作,本白皮书在充分调研国内外5G网络安全发展情况的基础上,针对5G典型应用场景和关键环节,研究提出 5G 网络安全标准框架和下一步标准研制工作建议,为规范引导 5G 网络安全标准化工作提供参考。

报告结构如下:

第 1 章:介绍了本白皮书编写的背景

第 2 章:介绍了 5G 概念与应用场景、5G 关键技术与安全特性

第 3 章:介绍了国内外的 5G 网络安全法规与政策、5G 网络安全标准化现状

第 4 章:介绍 5G 网络安全风险,包括终端安全风险、IT 化网络设施安全风险、通信网络安全风险、行业应用安全风险、数据安全风险和网络运维安全风险

第 5 章:基于 5G 网络安全标准化需求,给出了 5G 网络安全标准框架

第 6 章:给出了 5G 网络安全标准化工作推进建议

第 7 章:给出了本白皮书所引用的参考文献

附录 A 介绍了国内外已发布及在研的相关标准

附录 B 介绍了 5G 网络安全标准应用实践案例

附录 C 给出了相关术语定义

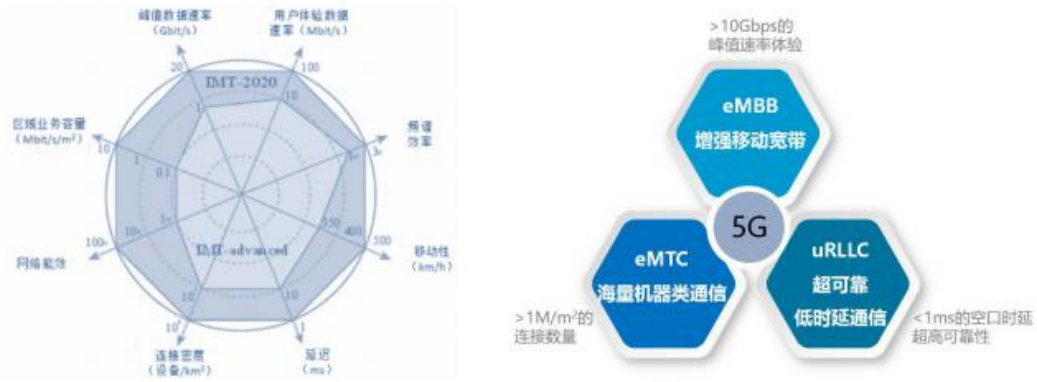


图1 ITU定义的5G关键指标和应用场景

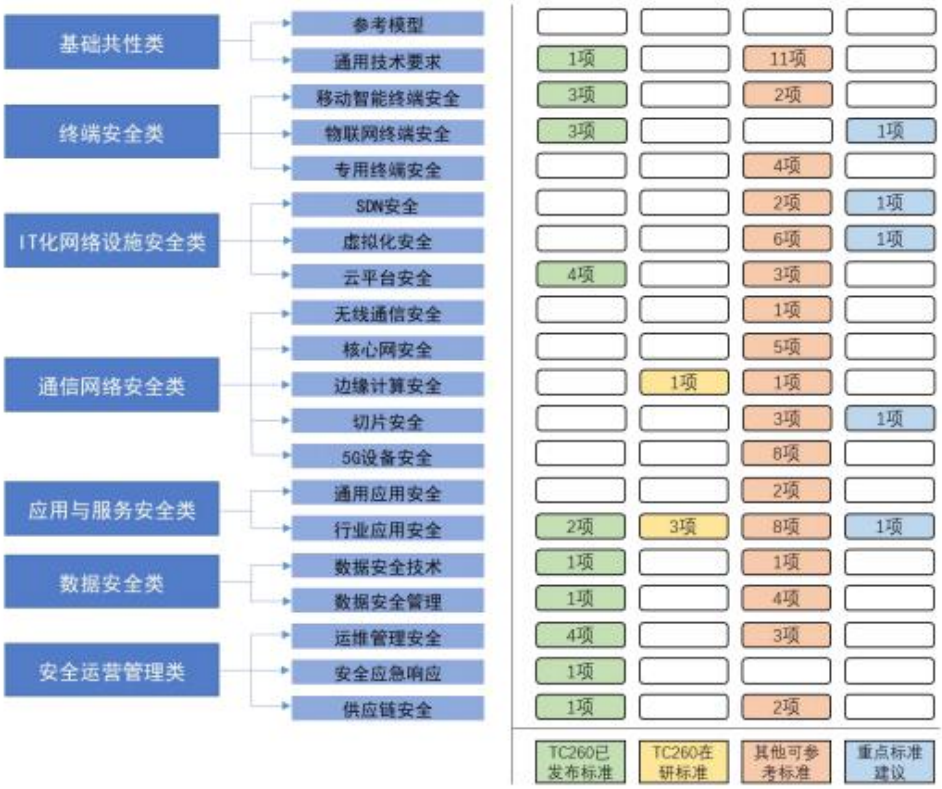


图 3 5G 网络安全标准架构

附件：2.《5G 网络安全标准化白皮书》.pdf

链接地址：https://www.tc260.org.cn/front/postDetail.html?id=20210512165851

中国网络安全产业分析报告（2021）

《中国网络安全产业分析报告（2021 年）》（以下简称“报告”）由中国网络安全产业联盟（CCIA）发布，由数说安全提供研究支持。

报告调研以具备网络安全产品、服务和解决方案销售收入的我国网络安全企业为目标研究对象，调研企业数量近 300 家，最终收集到近 200 家有效数据，覆盖了国内核心网络安全企业。

报告以真实调研数据为基础，客观分析得出我国网络安全产业发展最新情况，结合产业发展面临的新形势、新挑战、新机遇，对网络安全产业规模及增速、市场区域分布及增速、客户所属行业分布及增速、网络安全产品需求热度、企业竞争力与产业格局、资本市场、技术热点等内容进行了全面分析，最后对我国网络安全产业发展进行了展望。

内容概览：

一、 我国网络安全产业在“十四五”开局之年面临的新变化、新挑战、新机遇

二、 我国网络安全产业基本情况

三、 我国网络安全企业竞争力与产业格局

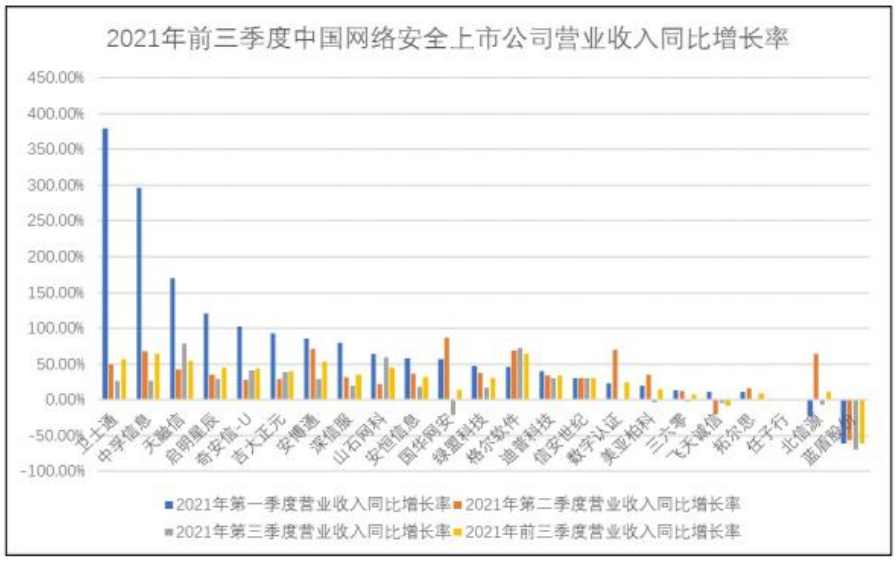
四、 我国网络安全资本市场分析

五、 我国网络安全产业技术热点分析

六、 我国网络安全产业发展展望

附录 A 2021 年前三季度中国网络安全上市公司营业收入

附录 B 2021 年 CCIA50 强、CCIA 成长之星、CCIA 潜力之星榜单



数据来源：巨潮资讯 20211031，数说安全、CCIA 整理

图 2 2021 年前三季度我国网络安全上市公司营业收入同比增长率

数据来源：数说安全、CCIA 根据公开资料整理

图 4 近四年中国网络安全行业集中度分析

附件：3.《中国网络安全产业分析报告（2021）》.pdf

链接地址：http://china-cia.org.cn/home/WorkDetail?id=61ca800a0200330f80e90e94

网络安全产业人才发展报告（2021）

《网络安全产业人才发展报告（2021）》由工业和信息化部人才交流中心、工业和信息化部网络安全产业发展中心、西北工业大学、西安电子科技大学、安恒信息和猎聘网联合编写，对梳理网络安全产业人才市场需求，激活网络安全产业未来人才发展动力，形成网络安全产业健康有序发展格局，具有重要的参考价

值和指导意义。

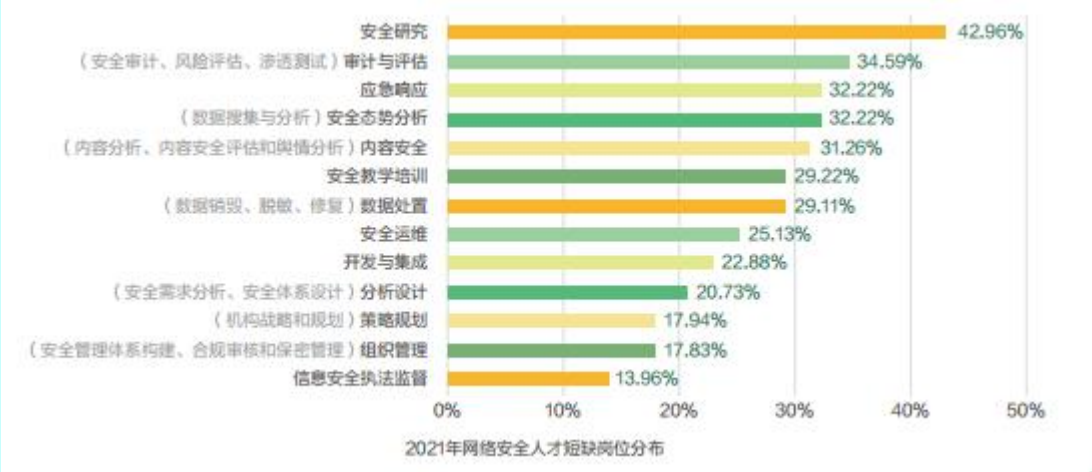
报告基于国内外网络安全人才培养过程中的知识体系建设，从网络安全产业人才的市场特征、人才需求、院校供给、社会供给及发展建议等五个维度进行展开，深挖网络安全人才的发展特点，有针对性地反映网络安全产业人才供需现状，为其培养相关方提供启发和借鉴。

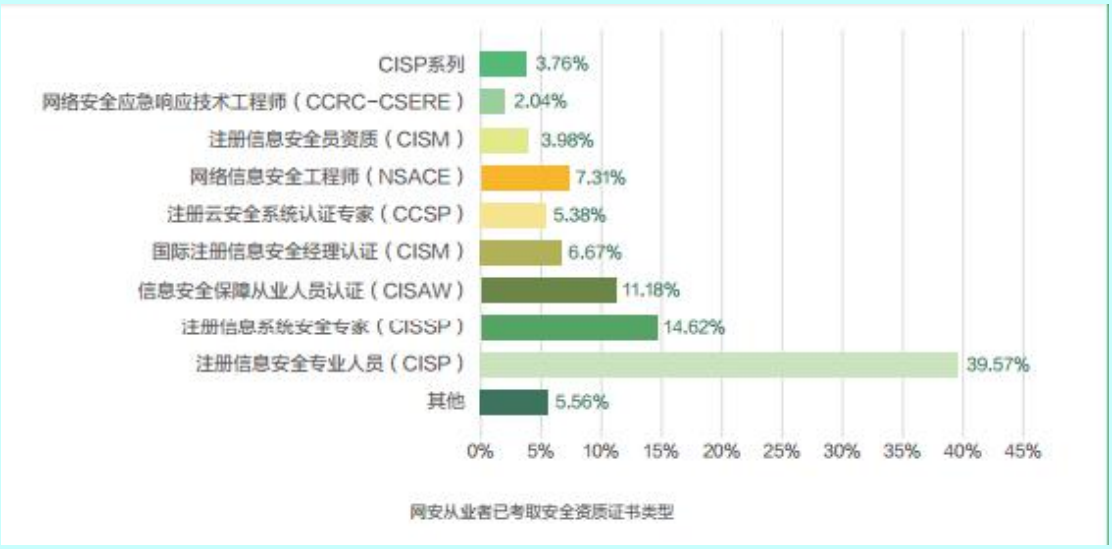
报告显示，今年以来相关专业人才需求呈现高速增加趋势，需求总量较去年增长 39.87%，网络安全在各行业的渗透率全面提高，在人才需求结构中的重要性显著上升。

内容概览：

1. 网络安全产业人才的发展概况
2. 网络安全产业人才的市场特征
3. 网络安全产业人才的需求分析
4. 网络安全产业人才的在校供给分析
5. 网络安全产业人才的在岗供给分析
6. 网络安全产业人才的发展建议

2019-2021年网络安全人才最高学历分布





附件：4.《2021 网络安全产业人才发展报告》.pdf

链接地址：https://www.miitec.cn/home/index/detail?id=2661

【国际分析报告】

2022 年全球网络安全展望

本报告是世界经济论坛（World Economic Forum）联合埃森哲公司一起针对2021年的全球网络安全状况做的调查研究报告,调查对象是来自20个国家的120位全球网络领导者。报告确定了目前的趋势并分析了近期的网络安全挑战。随着人们在新冠肺炎疫情期间加速转向远程工作,再加上最近备受关注的网络攻击问题，组织和国家的关键决策者越发将网络安全放在首位。

报告最后得出结论：

随着数字化进程推进和新技术的引入，网络风险将不可避免的持续加大。

AI、机器人技术、量子计算、物联网、云计算、区块链和远程工作和学习模型等前沿技术在推动数字世界发展的同时，也会带来潜在的网络风险和漏洞。

量子计算可能会打破目前大多数企业、数字基础设施和计算机所依赖的加密技术。

48%的受访者表示自动化和机器学习将在短期内带来网络安全领域最大的变革。

组织领导层要基于各种业务场景，构建网络安全的防御和容灾能力。除了网络安全之外，网络弹性的相关问题也是重中之重。

内容概览：

1.调查详解：

新常态下，网络入侵越来越频繁和复杂

从网络安全到网络弹性过渡

2.安全与业务的不同视角：

网络问题优先级

商业决策支持

网络安全人才

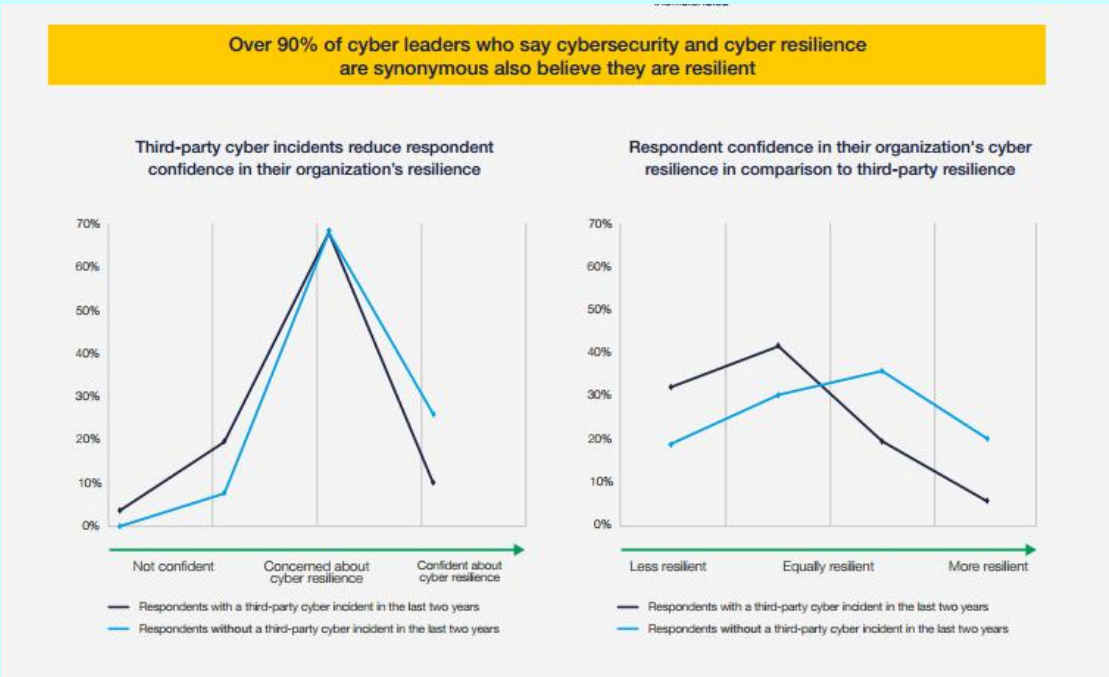
3.保护组织的生态系统：

生态系统脆弱性

复原力的重要性

通过透明度和信任获得成功

4.结论



附件：1.《2022 年全球网络安全展望》.pdf

链接地址：hhttps://cn.weforum.org/reports/global-cybersecurity-outlook-2022

全球网络安全指数

国际电信联盟（ITU）2021 年 6 月 29 日发布第 4 版《全球网络安全指数》调查报告，该报告是国际电信联盟隔年施行的一项衡量各国网络安全能力水平的研究项目，作为比较和分析各国网络安全能力使用，由法律、技术、组织、力量与合作 5 个项目构成，国际电信联盟以各国对各项问题提交的答复和证明资料为基础进行评价。

报告显示，美国排名第 1、英国和沙特阿拉伯排名第 2、爱沙尼亚排名第 3、韩国、新加坡、西班牙排名第 4、俄罗斯、阿联酋、马来西亚排名第 5。

全球网络安全指数报告显示，许多国家颁布了新的网络安全立法和法规，以解决隐私、未经授权的访问和在线安全等领域的问题。它还强调需要建立战略和机制以增强能力，帮助政府和企业更好地准备和缓解日益增长的网络风险。现在，世界上超过一半的国家都有一个计算机事故响应小组（CIRT），近三分之二的国家都有某种形式的国家网络安全战略来指导它们的总体网络安全态势。

全球网络安全指数表明，网络安全确实是一个发展问题，因此我们需要通过促进知识、技能提升和能力建设来解决发达国家和发展中国家之间日益扩大的网络能力差距。我们要在发展中国家扎根并在数字基础设施、数字技能和资源方面增强能力，以此来缩小这一差距。

内容概览：

1.全球网络安全指数：背景

2.关键主题

法律措施：规划未来干预措施

技术措施：增加 CIRTs/CERTs 的部署

组织措施：调整战略

能力建设措施：发展网络安全能力

合作措施：应对集体网络安全行动

儿童在线保护

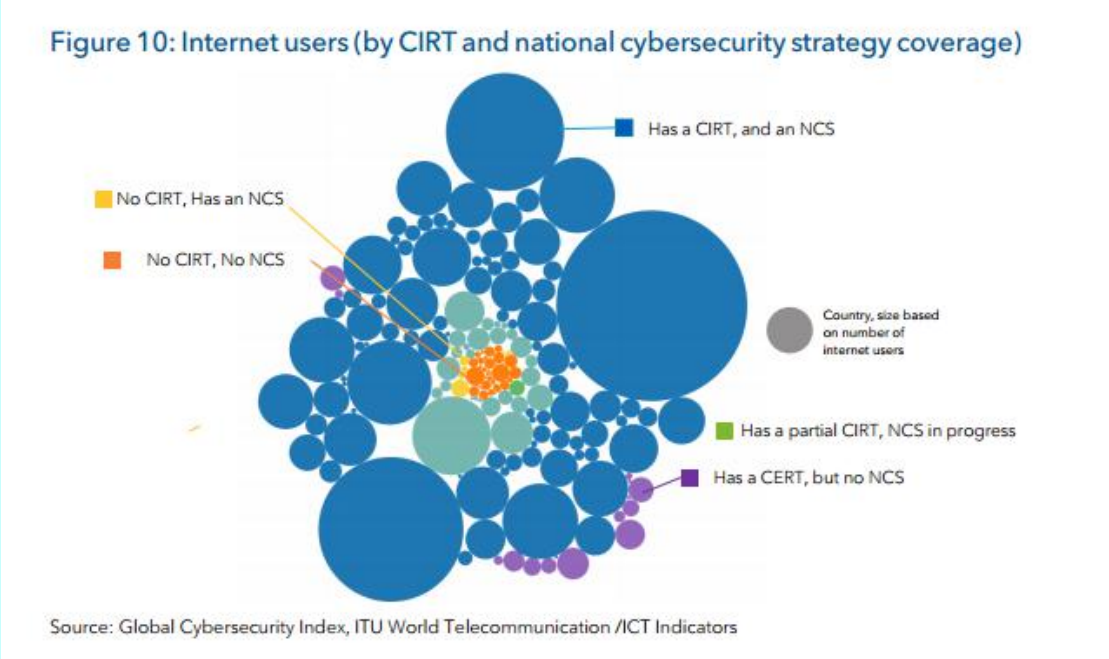
3.GCI 结果：得分和排名

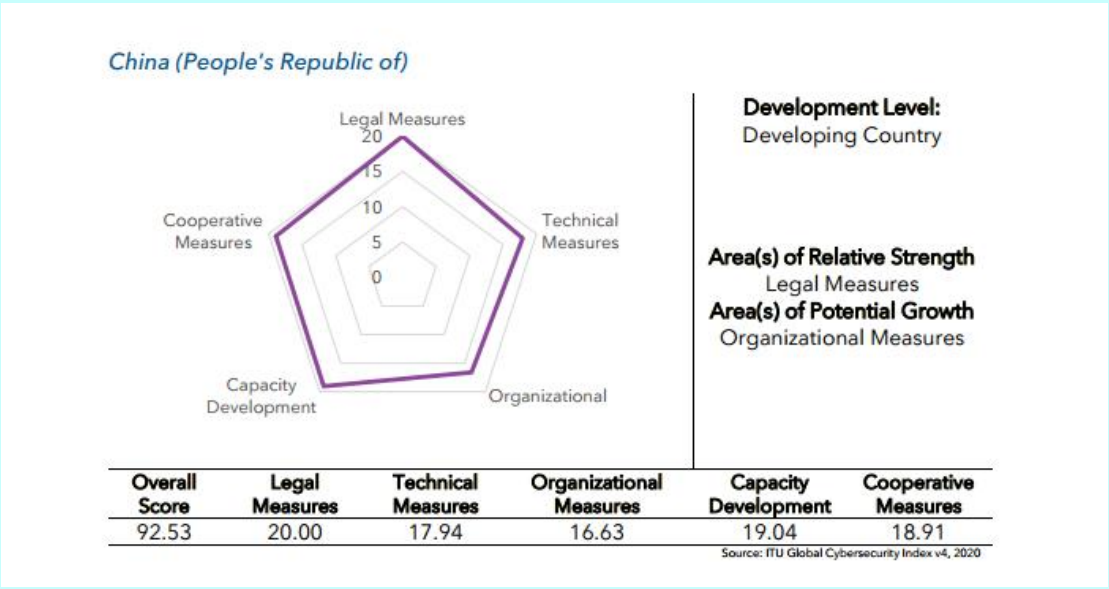
各国的全球得分和排名

地区得分和国家排名

4.2020 年全球网络安全指数：国家概况

（翻译：张福学　校对：苑艺）





附件：2.《全球网络安全指数》.pdf

链接地址 https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

2021 年全球网络信任调查报告

普华永道发布《2021 年全球网络信任调查报告》，分析了人们对网络安全的态度。这份报告基于对全球 3249 名企业和技术高管的采访。

报告显示：

1、重新设定网络战略，为新时代发展领导力

业务转型更加全面和迅速，40%的高管表示他们正在加速数字化。

首席信息安全官（CISO）正在向业务需求发展，40%的高管认为其需要 CISO 成为转型领导者（20%）或者成为运营领导者和战术大师（20%）。

2、重新思考网络预算，以获得更多的收益

55%的技术和安全主管计划增加他们的网络安全预算，到 2021 年，将有 51%的企业增加全职网络员工，尽管大多数（64%）的高管预计业务收入将下降。

超过半数的企业和技术/安全主管（55%）对网络支出与最重要风险保持一致方面缺乏信心。

3、全力投入，与攻击者平局

新技术颠覆网络犯罪问题。根据 CB Insights 的数据，在过去十年中，大约有 20 家相关公司实现了 10 亿美元的 IPO 或并购。

15-19%的高管已经从新方法和思路中获益。

云安全是下一个重大转变。公司正在迅速将业务（75%）和安全性（76%）转移到云计算领域。

4、建立应对任何情况的能力

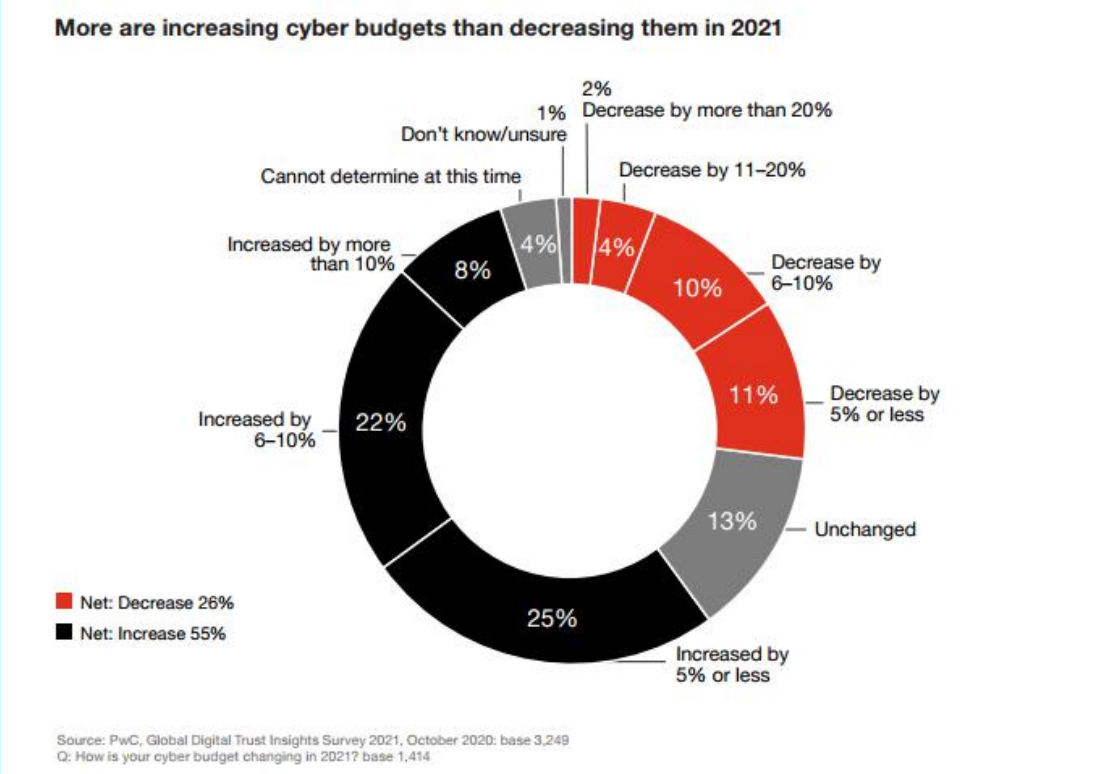
40%的高管计划增加弹性测试，以确保在发生破坏性网络事件时，关键业务职能能够保持正常运行。

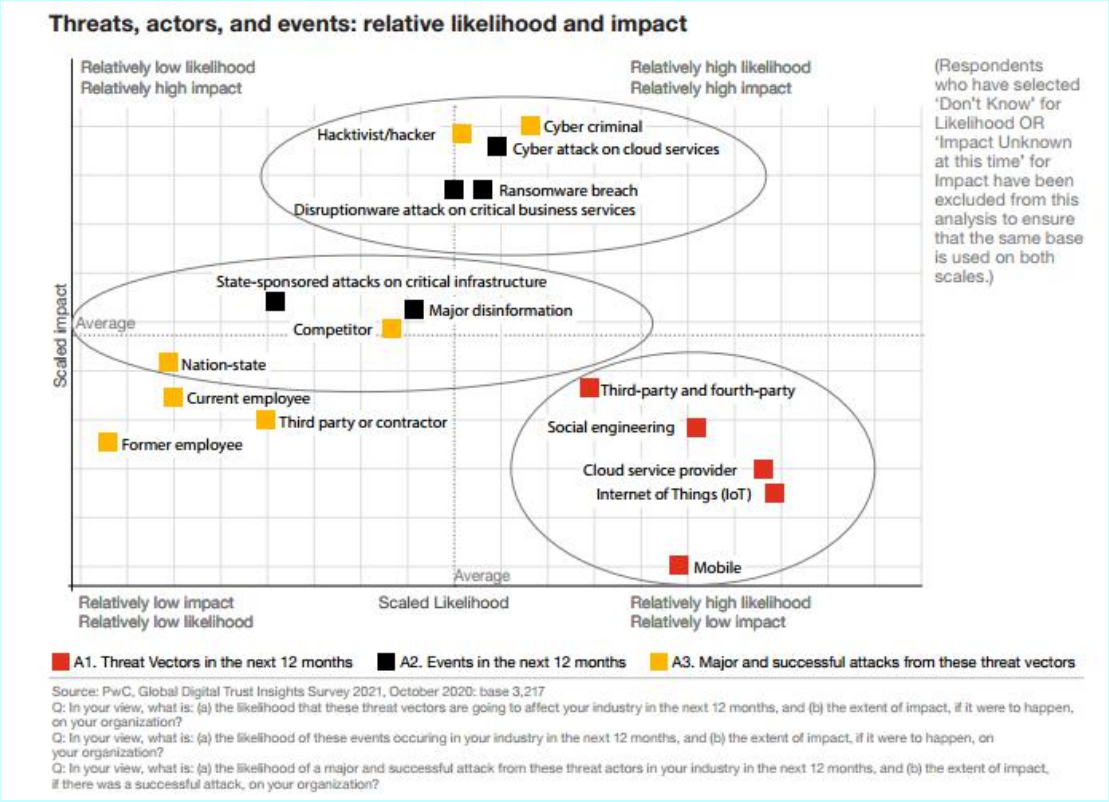
可能性相对较高但影响较小的威胁一直存在，例如通过物联网（65%的可能性，44%的负面影响）。

5、安全团队经得起未来考验

超过半数的高管（51%）计划在明年增加全职网络安全人员。最需要的是云解决方案（43%）、安全智能（40%）和数据分析（37%）方面的人才。

在新员工中，超过 40%的高管希望获得分析能力（47%）、沟通能力（43%）、批判性思维（42%）和创造力（42%）。





附件：3.《2021 年全球网络信任调查报告》.pdf

链接地址：

https://www.pwc.ch/en/publications/2020/ch-Digital-Trust-Insights-Survey-2021-report.pdf

【国家社科基金项目统计分析】

本模块通过统计及分析“国家社科基金项目数据库”中，“网络安全”相关项目的数据信息，以便学者了解网络安全领域课题研究动态。

“网络安全”国家社科基金项目统计

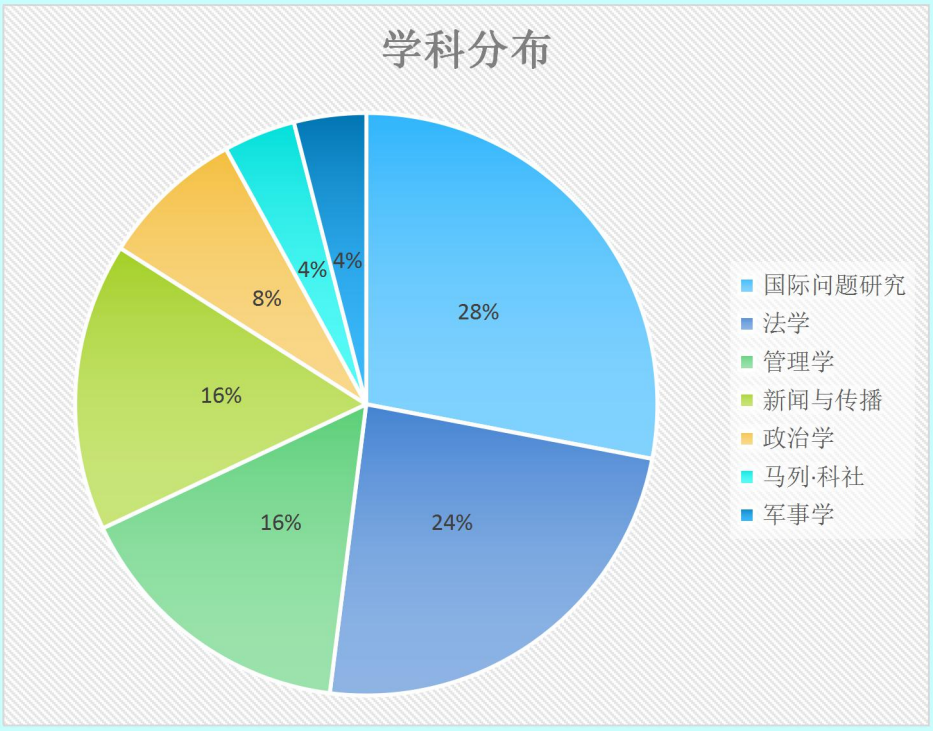
项目类别	学科分类	项目名称	立项时间	项目负责人	工作单位
青年项目	法学	网络安全信息共享的法律保障研究	2021 年	方婷	西北大学
青年项目	马列·科社	基于社会认知理论的大学生国家网络安全意识教育及对策研究	2021 年	罗青	南昌大学
一般项目	新闻学与传播学	5G 时代短视频生产与传播的网络安全引导体系研究	2020 年	路鹃	北京体育大学
重点项目	管理学	网络安全新业态视角下的关键技术风险分析及防控对策研究	2020 年	王斌君	中国人民公安大学
青年项目	管理学	网络安全危机管理研究	2019 年	程相然	战略支援部队信息工程大学
一般项目	管理学	多元主体网络安全漏洞披露风险生成机理与管控研究	2019 年	熊强	江苏大学
青年项目	国际问题研究	全球网络安全法律规则制定的推进策略研究	2018 年	左文君	中共武汉市委党校
一般项目	新闻学与传播学	《网络安全法》后移动应用程序 APP 个人信息保护研究	2018 年	付涛	对外经济贸易大学
一般项目	管理学	“科技冷战”背景下中国网络安全技术赶超的关键问题研究	2018 年	谢安世	浙江工业大学
一般项目	国际问题研究	网络安全国际规范与我国战略选择研究	2018 年	赵瑞琦	中国传媒大学
一般项目	国际问题研究	全球关键信息基础设施网络安全保护体系比较与启示建议	2018 年	陈红松	北京科技大学

后期资助项目	军事学	可控网络安全控制理论	2018 年	卢昱	陆军工程大学
一般项目	新闻学与传播学	网络安全发展视角下“平台型”网络运营者的法律责任研究	2017 年	雷丽莉	大连理工大学
西部项目	新闻学与传播学	网络安全文化传播动力学模型与传播策略研究	2017 年	刘小洋	重庆理工大学
青年项目	法学	网络安全国际合作法律制度研究	2017 年	林婧	福州大学
青年项目	政治学	完善国家网络安全保障体系综合研究	2017 年	安静	北京科技大学
一般项目	国际问题研究	全球治理视角下的网络安全研究	2016 年	王孔祥	国际关系学院
重点项目	政治学	大国竞争背景下的中国网络安全战略研究	2016 年	王桂芳	军事科学院
一般项目	国际问题研究	中美网络安全审查制度比较研究	2015 年	李青	国际关系学院
一般项目	国际问题研究	国家空天网络安全研究	2015 年	王刚	空军工程大学
一般项目	法学	我国网络安全立法研究	2015 年	马民虎	西安交通大学
一般项目	国际问题研究	网络武器化与我国网络安全战略构建研究	2014 年	程群	华东理工大学
青年项目	法学	网络安全与网络个人信息保护的公法学研究	2012 年	江登琴	中南财经政法大学
西部项目	法学	网络安全监控的法律对策研究--以通讯协助执法法律制度的构建为视角	2010 年	马民虎	西安交通大学
一般项目	法学	信息网络安全法律问题研究	2003 年	张楚	中国政法大学

数据来源：国家社科基金项目数据库

“网络安全”国家社科基金项目分析

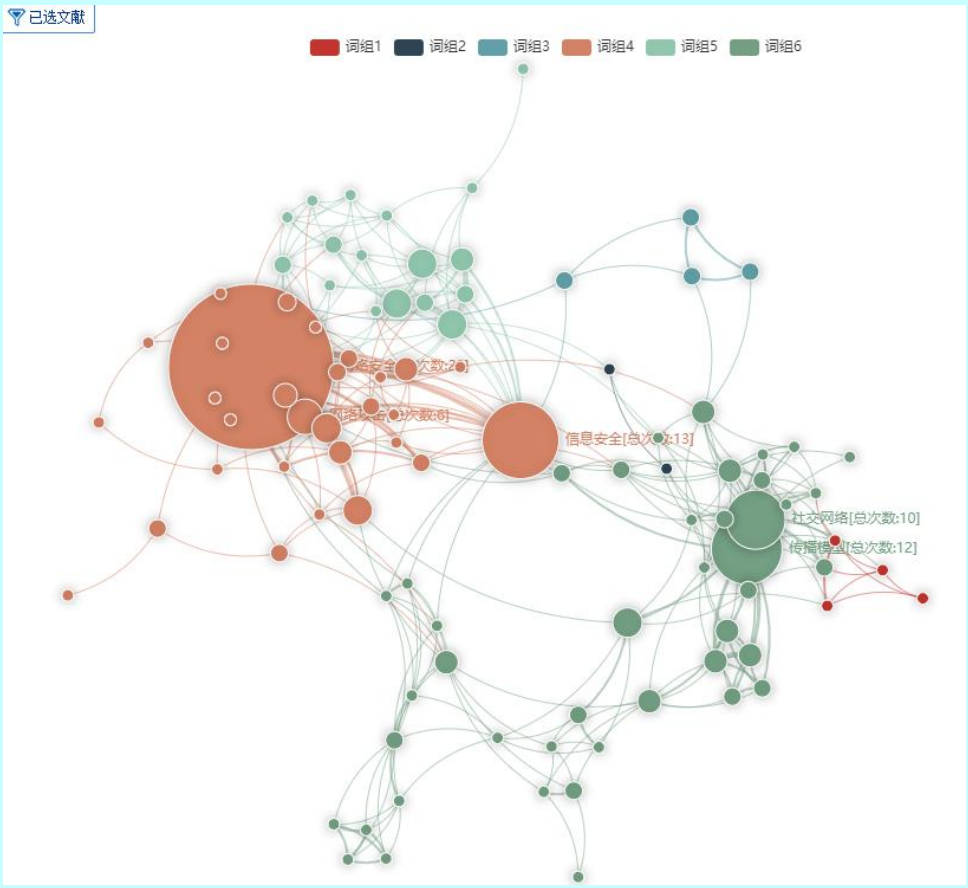
（一）学科分布



国家社科基金“网络安全”相关项目中，学科分布主要集中在“国际问题研究”（28%）、“法学”（24%）、“管理学”（16%）、“新闻与传播”（16%）等学科类别。

（二）关键词共现

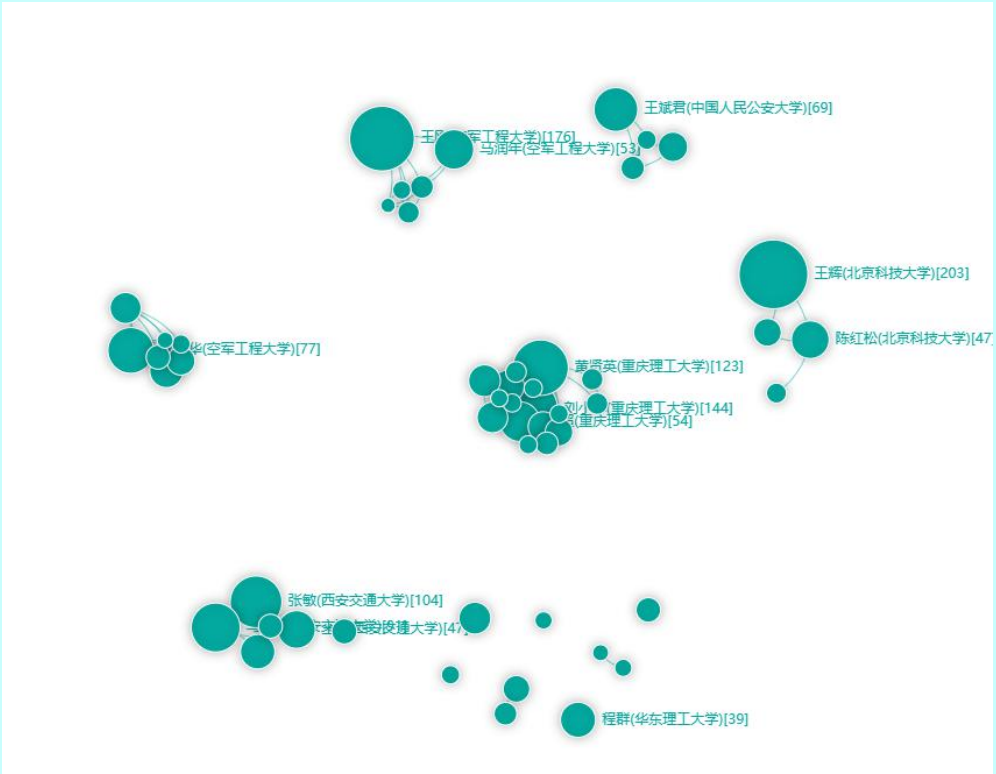
根据“网络安全”国家社科基金项目统计表中的项目名称，分别在知网中进行基金搜索，共检出相关基金项目成果文献 120 篇，对这些文献进行关键词共现网络分析，得出下图。



从上图的关键词共现网络可以看出，出现频率较高的关键词主要有：网络安全（28 次）、信息安全（13 次）、传播模型（12 次）、社交网络（10 次）。这些主题都是“网络安全”相关国家社科基金项目研究的热点话题。

（三）作者合作分析

对检出的 120 篇基金项目成果文献进行作者合作网络分析，得出下图。

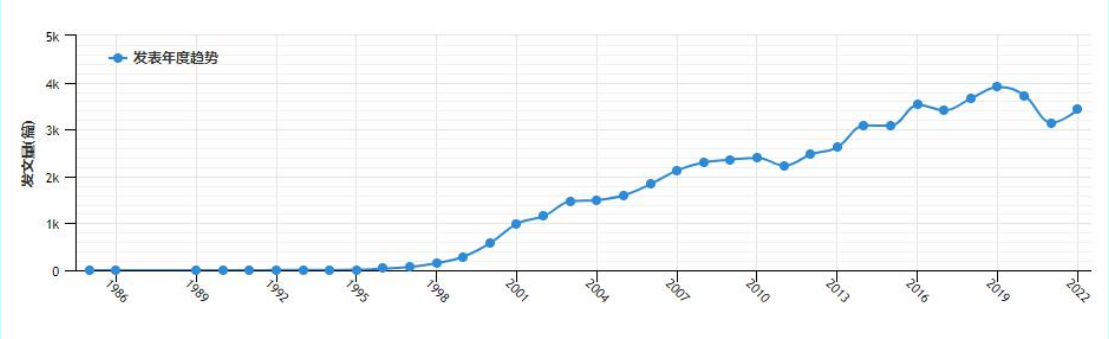


如上图所知可知，“网络安全”相关国家社科基金项目研究中，作者合作形成以项目负责人为中心，同机构研究人员为主的研究团队模式，如王刚（空军工程大学）、刘小洋（重庆理工大学）等都与同机构研究人员形成研究团队进行相关国家社科基金项目的研究。

【知识可视化分析】

模块一：年度发文趋势

以“篇名”或“关键词”包含“网络安全”，来源类别选择“全部期刊”，时间不限，在知网进行检索，得到 54032 篇文献，对检索结果进行知网自带的计量可视化分析，得到下图“网络安全”年度发文趋势。

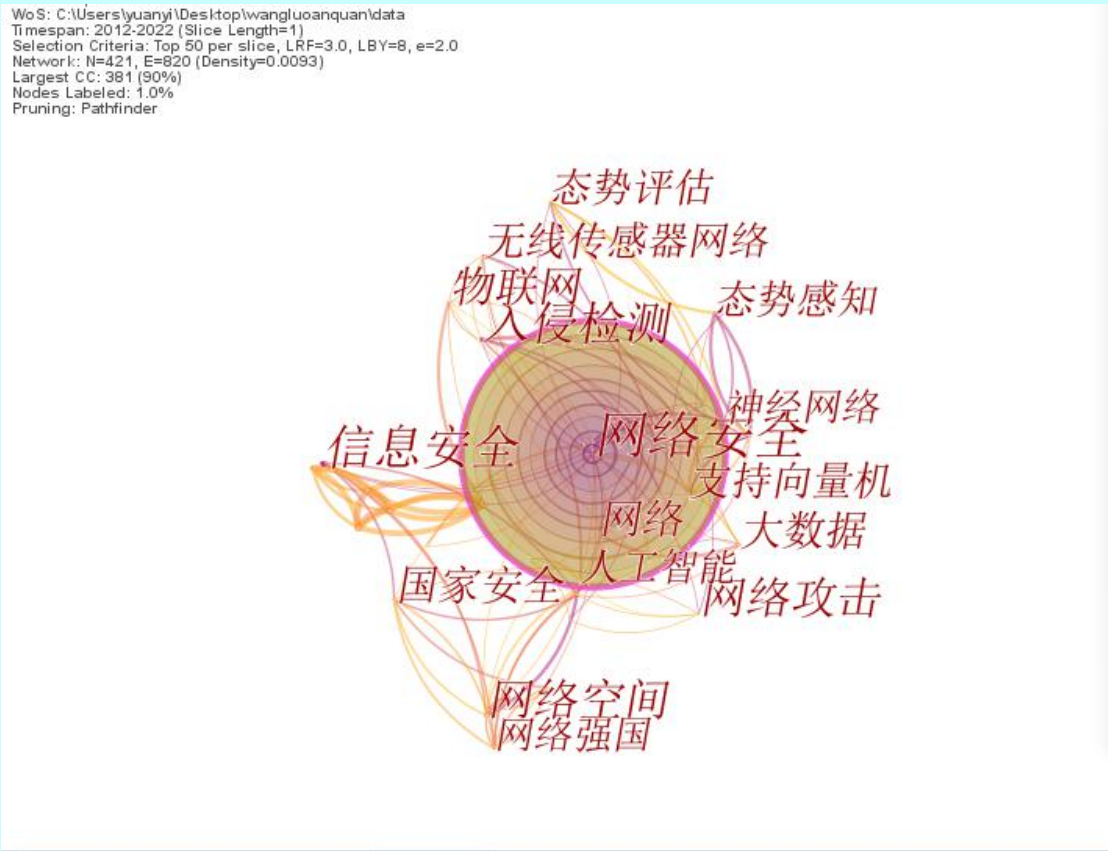


由上图可知，关于网络安全的研究始于 20 世纪 90 年代；2000 年之前网络安全相关文献数量较少；自 2000 年后，网络安全相关研究呈明显增长趋势，且研究数量较多，充分反映了网络安全近年来一直是热点研究领域。

模块二：研究热点分析

以“篇名”或“关键词”包含“网络安全”，来源类别选择“SCI 来源期刊”和“核心期刊”，时间限定为“2012 年—2022 年”，在知网进行检索，得到 2385 篇文献，运用文献计量工具 Citespace 对检索出的相关文献进行研究热点分析。

（一）关键词共现



运用 Citespace 软件绘制出网络安全研究领域的关键词共现知识图谱，如上图所示。图中的每一个节点均代表一个关键词，出现次数越多则节点越大。节点越大，则越说明其是该领域的研究热点。图中的线条纵横交错，表示各个关键词之间并不是独立存在，而是有着千丝万缕的联系。除关键词频次与节点大小以外，关键词中心度（大于 0.1，则说明为热点方向）在一定程度上也能反映研究热点，为了让最终呈现的结果更加严谨客观，在关注关键词频次的基础上，结合中心度对网络安全研究热点进行分析。

在 CiteSpace 中可以看到各个关键词出现的频次以及关键词中心度，表 1 为排名前 20 的网络安全研究热点关键词，中心度大于 0.1 的关键词见表 2。

表 1 2012—2022 年“网络安全”高频词 TOP20

序号	关键词	频次	序号	关键词	频次
1	网络安全	1496	11	攻击图	32
2	入侵检测	87	12	大数据	31
3	信息安全	77	13	网络安全态势	31
4	无线传感器网络	47	14	国家安全	30
5	网络空间	47	15	态势评估	30
6	软件定义网络	43	16	风险评估	28
7	网络攻击	41	17	物联网	28
8	僵尸网络	39	18	支持向量机	26
9	态势感知	38	19	神经网络	26
10	网络强国	33	20	网络	25

表 2 中心度大于 0.1 的“网络安全”关键词

序号	关键词	中心度
1	网络安全	0.56
2	信息安全	0.26
3	入侵检测	0.18
4	网络攻击	0.15
5	网络空间	0.14
6	物联网	0.14
7	无线传感器网络	0.13
8	网络	0.12
9	大数据	0.10

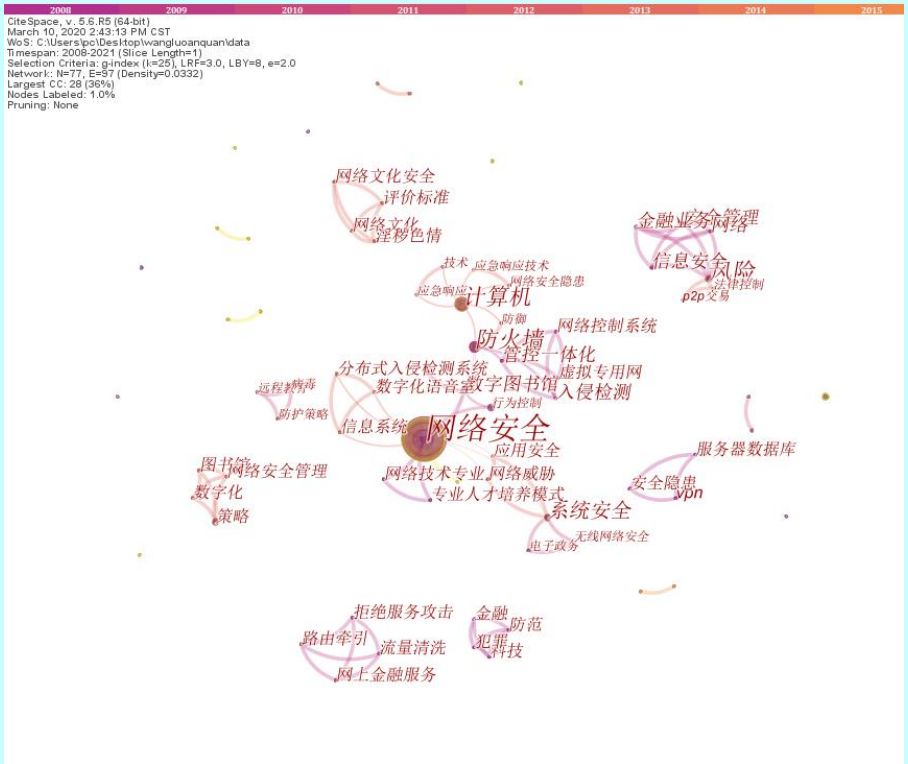
在综合关键词共现图谱、高频词表、中心度表后，我们可以直观看出，网络安全、信息安全、入侵检测、网络空间、网络攻击等关键词最为突出，反映了网络安全领域的研究热点。

（二）“网络安全”研究演进

运用 CiteSpace 软件生成 2012 年—2022 年网络安全研究的时区图谱，如下图。图谱上的每一个关键词所处的时区，即这个关键词首次出现的时间，彼此之间的相连线条体现了关键词间相互联系，由此反映出网络安全领域研究热点的演化过程。

十年间的网络安全相关研究演进图谱如上图所示，每年都会出现新的热点关键词，展现着网络安全研究领域的演进过程，例如从 2012 年的“网络空间”“网络攻击”“入侵检测”等热点关键词，到近两年的“深度学习”“层次分析法”等热点关键词，展现着网络安全领域不同阶段的研究热点。

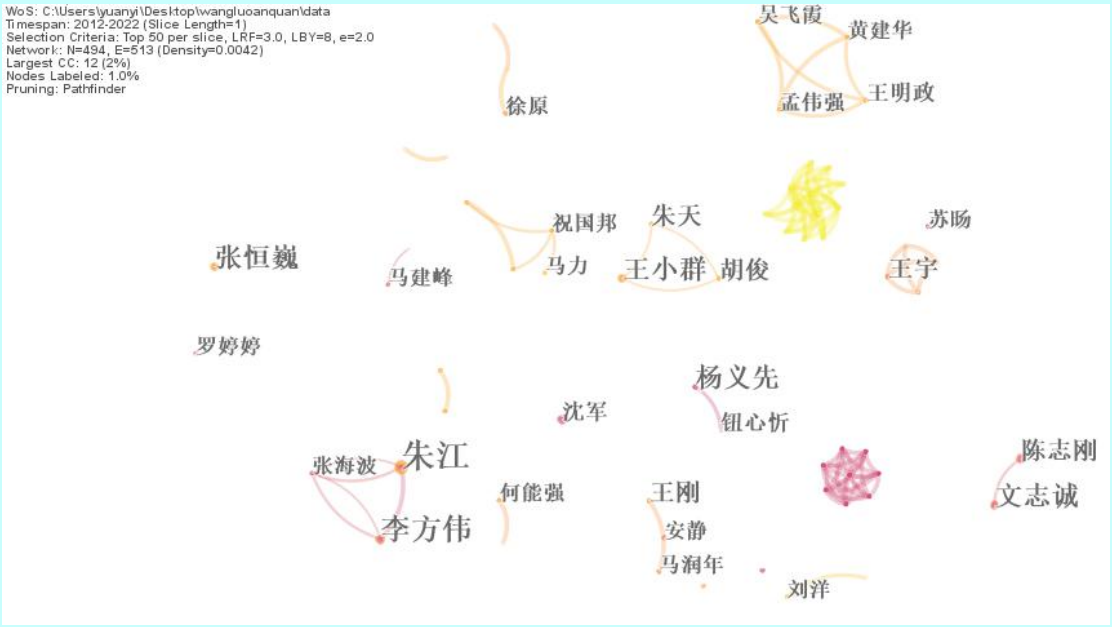
（三）“网络安全”我校研究热点



关注我校师生网络安全领域研究热点，在知网中限定作者单位为“河北金融学院”，并且主题为“网络安全”进行检索，得到我校师生共发文 25 篇。运用 Citespace 软件对文章进行关键词贡献分析，如上图所示。我校师生在网络安全

领域的研究关注计算机、防火墙、系统安全等等主题，张四大、何志强、许美玲等老师对这些领域有持续关注和研究。

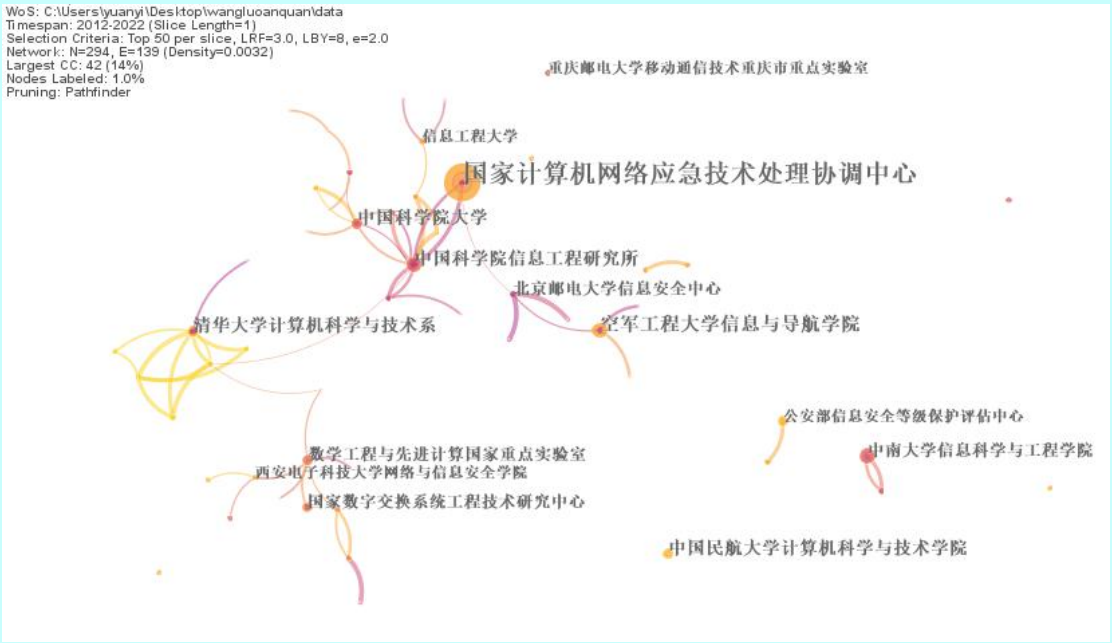
模块三：作者合作分析



通过作者共现可以识别研究领域内的核心作者群体，还可以明晰作者间的合作关系。从作者出现的频次来看，发文量最多的是朱江（19 篇）、李方伟（13 篇）等。在一定程度上说明当前网络安全的研究领域存在高产作者。

上图所示，网络安全研究领域呈现几个小规模的“研究团体”。例如，以朱江（重庆邮电大学）为中心形成的合作团体，其成员李方伟、张海波均属重庆邮电大学，研究主题主要为网络安全态势。再如，吴飞霞、黄建华、孟伟强等作者形成的合作团体也多为同一机构成员组成，但是成员合作发文数量较少，尚未形成稳定的研究团体。总体来说，网络安全研究领域存在一些小的研究团体，且多为同一机构成员组成。

模块四：机构分析



由上图发文机构共现图谱可知，节点较大的机构，发文数量也较多。由于 Citespace 未能识别规范同一机构不同简称，如将“清华大学”和“清华大学计算机科学与技术系”按两个机构分析，为规避这一情况，将单位进行手动规范后，发现发文量最多的几个机构是国家计算机网络应急技术处理协调中心（59 篇）、清华大学（31 篇）、空军工程大学（24 篇）等。有关网络安全方面的研究，中国科学院信息工程研究所与外部机构合作次数最多，与它合作的机构包括国家计算机网络应急技术处理协调中心、中国科学院大学、武汉理工大学、清华大学等 7 个机构。总体来说，目前网络安全领域发文机构非常广泛，且存在对网络安全持续关注的科研机构。

【资源获取门户】

1. 中国网络安全产业联盟网站

http://www.china-cia.org.cn/

中国网络安全产业联盟于 2015 年在北京成立。联盟的宗旨是搭建产业创新平台，聚合产业势能，营造良好产业发展环境，促进产业创新发展，加强行业自律，提升网络安全技术产业和服务水平，推动网络安全产业做大做强，提升中国网络安全产业竞争力和国际话语权，维护用户网络安全和利益，为实现网络强国战略提供坚实保障。中国网络安全产业联盟网站包括联盟动态、行业资讯、公益翻译等板块。

2. 中共中央网络安全和信息化委员会办公室网站

http://www.cac.gov.cn/

中央网络安全和信息化委员会办公室是中央网络安全和信息化委员会下设的办事机构。网站中包括网络安全、信息化、网络传播、教育培训、政策法规、国际交流、业界动态、网络研究等板块。其中网络安全专题板块中包括治理监管、预警通报、网络安全审查、安全动态、云计算服务安全评估等内容。

3. 工业和信息化部网络安全产业发展中心网站

http://www.miitxxzx.org.cn/

工业和信息化部网络安全产业发展中心是工业和信息化部直属事业单位，承担与国家网络安全产业相关的发展战略、规划、政策、标准研究，数据监测、发布与分析，安全测试、成果转化以及部机关网络信息技术保障等工作。网站中包括新闻动态、研究报告、重大专项、网络安全产业合作与研究等板块。

公众号：

数说安全：专注于网络安全垂直领域的自媒体。以数据为基础，结合科学的

方法论做行业研究。从企业经营、产品技术、市场营销、资本等多个维度进行深度商业分析，旨在升级认知，洞见趋势。

SecPulse 安全脉搏：关注最新安全事件，分享独家技术文章；安全资讯、安全报告实时共享。

MS08067 安全实验室：北京交通大学安全研究员徐焱的公众号，专注于普及网络安全知识。出版专业书籍《Web 安全攻防：渗透测试实战指南》《内网安全攻防：渗透测试实战指南》《Python 安全攻防：渗透测试实战指南》等。

【馆内图书】

序号	索书号	题名	出版者
1	TP393.08/D371/4	网络安全与攻防策略	机械工业出版社
2	TP393.08/Q100	走进新安全:读懂网络安全威胁、技术与新思想	电子工业出版社
3	TP393.08/J254	网络安全态势感知	电子工业出版社
4	TP393.08/D827	网络安全态势感知:提取、理解和预测	机械工业出版社
5	TP393.08/H001	网络安全之机器学习	机械工业出版社
6	D922.175/Y930:2020	网络安全法律解析	华中科技大学出版社
7	D922.17/Z562	中华人民共和国网络安全法	中国法制出版社
8	TP316.85/L957	Linux 网络安全精要	机械工业出版社
9	TP393.08/L036/4	网络安全传输与管控技术	人民邮电出版社
10	D922.174/X174	网络安全法和网络安全等级保护 2.0	电子工业出版社
11	TP393.08/Z755	计算机网络安全理论及应用	中国水利水电出版社
12	TP393.08/S032	网络安全监控	机械工业出版社
13	TP393.08/Y074	网络安全实验教程	南京大学出版社
14	D922.174-53/X724	网络安全立法研究	法律出版社
15	TP393.08/B691	网络安全监控实战	机械工业出版社

主编： 刘雁 周莉

编辑： 苑艺 王凯艳 邸烨梅 张琪 谭朔金 张福学 刘程