



中国社会科学院大学

数字中国研究院

Institute of Digital China

University of Chinese Academy of Social Sciences

数字时代安全 科技价值报告

中国社会科学院大学数字中国研究院

2024年1月

摘要

DIGEST



本报告基于2023年全球数字社会的安全风险新形势和科技创新内在逻辑，对安全科技提出“伴生技术”的新定义，总结其具有的“压舱石”与“助燃剂”双重价值，并提出将安全科技视作新型公共产品的新思路。

安全科技正处在时代的转折点。首先，数字化安全风险已经进入快迭代、高智能、全覆盖的新格局。根据意大利信息安全协会2022年发布的研究报告显示，2021 年全球网络犯罪导致的损失估计约为 6 万亿美元，对工业4.0、车联网、交通、医疗等领域均造成重大影响，且在上网人数上升和数字化加速的背景下仍呈持续上升趋势。与此同时，2023年，AI大模型安全风险凸显，全球各界一致关切，业界开始推出“大模型质检”类安全产品，成为推进大模型安全健康发展的路径之一。安全科技已从传统的网络安全技术发展成当前更为通用、包含多个领域、多种前沿技术的复杂系统性技术，维持着数字社会的稳定运转，帮助各行各业加快数字化转型。

本报告提出，人工智能和安全科技将会是未来的两项通用技术，应该以公共品的定位来判断安全科技的价值，推动其发展。政企合作是安全科技成为公共品的核心驱动力，通过更多的公共力量投入，构建更好的安全科技实力和制度，采用数字化转型的“慢起飞模型”，新的安全技术将得到更好的发展，个人与社会为数字化转型所付出的代价也将更小。

目录

一、前言 1

AI大模型重构数字世界，安全问题质变时刻 1

二、数字社会进入新阶段，面临全新风险挑战 3

（一）数字化安全风险新形势：快迭代、高智能、全覆盖 3

（二）AI安全风险的紧迫性陡增 5

（三）有新技术的地方，就有新的安全风险 7

三、安全科技的关键技术能力及双重价值 10

（一）安全科技是一种伴生技术 10

（二）安全科技的五大趋势：零化、弹性化、匿名化、量子化和智能化 17

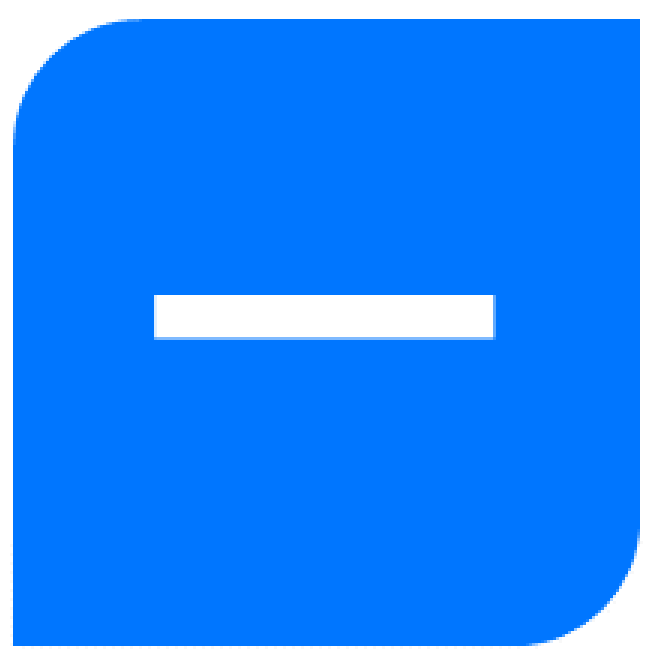
（三）安全科技的双重价值在放大 19

四、未来：安全科技必将成为新型公共品 33

（一）“慢起飞模型”：安全科技是技术向善的集中体现 33

（二）政企合作是安全科技成为公共品的核心驱动力 35

（三）结语 38



前言

AI大模型重构数字世界，安全问题质变时刻

2022年，全球发生数据泄露事件4,518件，数据量达到226.2亿条（Flashpoint）。

2021年，全球45%的数据泄露事件涉及个人数据（Verizon）。

平均而言，只有5%的公司文件夹受到适当保护（Varonis Systems）。

到2025年，全球网络犯罪每年造成的损失将达到 10.5 万亿美元。（Cyber security Ventures）

全球约40%的人口目前处于离线状态，一旦联网，他们将很容易成为网络攻击的目标。（Data Reportal）

未来将会是深度数字化的。在过去二三十年的时间里，数字化已成为越来越清晰的现实。不仅仅互联网，几乎所有的行业都在数字化转型，这是由现代科技内在的逻辑所决定的。只要我们仍希望凭借科技的进步，解决生活与工作中的各种问题，我们就必须做好迎接深度数字化未来的准备。这当中至关重要的一个部分，就是面对全面数字化可能带来的安全风险。

当下，我们正站在安全风险的质量变时刻。随着数字化的推进，新的深度智能开启。何谓深度智能？深度智能的核心是人工智能技术，在大数据的基础上，人工智能将数据建模，产生新的结论和应用，从而推开了“万物皆可智能”的大门。随着数据爆炸式增长、数字化基础架构错综复杂，网络攻击面的不断扩大，对应地安全风险也出现了新情况：此前，风险造成的影响是单点的。举个例子，如今，一辆汽车的网络安全问题都不再只影响这辆车本身，而可能影响整个城市交通；此前，数字化的地图上有一些区域是“不通行”的，如今，即使发电、供水等基础设施也深度数字化运行，风险在地图上更四通八达。

2023年AI大模型横空出世，大大推进了深度智能时代的到来，然而它对安全局面的影响同样可能是颠覆性的。最近引起全球关注的OpenAI公司因对AI安全不同观点而导致的人员变动风波，很好地说明了业界对当前AI安全高风险的态度，以及它在整个深度智能的社会中投下的令人不安的阴影。因此，站在深度数字化的转折时刻，对安全科技的关注与投入已刻不容缓。

安全科技的价值，既体现为“压舱石”，更重要是作为“助燃剂”：压舱石指的是守住技术的安全底线，防御可能存在的风险隐患，支撑和保障数字社会的稳步运行；助燃剂是提高技术的安全上限，降低技术运行的成本，让新技术得以规模化落地，推动产业焕发新机，让更多人从中受益。

数字化为何有安全风险？其实，风险自古至今都存在，只是因为产业运营、个人生活、国家组织的行为模式向数字化转型，风险也就相应地并轨转移。隐私数据泄露、商业勒索、基础设施瘫痪……放眼未来，有新科技的地方，就会有新的数字化安全风险，两者是本体和阴影一样不可分割的伴生关系。

我们判断，未来通用的技术有两个，一是人工智能技术，二是安全科技。人工智能作为最具颠覆性和战略性的核心关键技术，将在各行各业数字化的基础上进一步实现智能化，成为未来生产力的发动机；安全科技将作为方向盘，始终将各种新兴科技控制在向善的道路上。安全与人工智能并举，双方的融合创新与发展，将是我国强国战略中不可忽视的重要助推因素。因此，这两个领域，应该成为我们最关注、投入最大的领域。

过去，当人们提到安全科技时，想到的往往是防病毒软件和防火墙软件。但全球安全科技的版图和技术工具已远远超过这些。在网络安全、系统安全之外，还有数据安全、终端安全、人工智能安全、云安全等等，涉及众多技术门类，也包括了区块链、隐私计算、量子计算等前沿技术。在安全风险质变时刻的当下，提高社会对于安全科技的认知、重视与参与，非常有必要，这是本报告的核心议题。

另一方面，尽管安全科技行业已有了相当的发展，但仍存在多种迫切问题。尤其是缺乏明确的生态标准来加快前沿技术的规模化落地、缺乏合理的市场化机制，政企合作及生态联动方法来助推安全科技的发展等等。这也是本报告关注的关键问题。

我们必须明确，未来，安全科技将成为社会的公共品，它不只是一套技术，也不是企业的运营成本，而是数字社会的优先事项之一，因为最终它保护的并不是若干行业、某个业务、几段数据，而是这个社会里的每一个人，是技术真正造福于人类的可能性。

我们也特别感谢中国社会科学院大学哲学院教授、中国社会科学院科学技术和社会研究中心主任段伟文，科技部“云计算+大数据”国家重点专项课题负责人、数秦科技执行总裁兼首席科学家崔伟，北京大学客座教授、蚂蚁集团首席技术安全官韦韬，浙江工业大学网络空间安全研究院院长宣琦等多位专家学者在本次调研中，提出了宝贵意见和建议。



数字社会进入新阶段 面临全新风险挑战



（一）数字化安全风险新形势：快迭代、高智能、全覆盖



数字化安全风险来自哪里？操作者的人为失误是其中一部分，更大的来源则是第三方攻击，也就是网络犯罪。

网络犯罪，指滥用计算机或电信技术，对系统或信息进行攻击，破坏或利用网络进行其他犯罪的行为，包括常见的盗取和交易敏感信息、针对组织机构网络设施的攻击、网络霸凌、也包括利用暗网等技术手段销售毒品与人口贩运等。

网络犯罪的规模目前有多大？根据联合国发展署《2022年特别报告》，2021年，网络犯罪造成的损失估计约为 6 万亿美元，如果以国家来衡量，那么网络犯罪是继美国和中国之后的世界第三大经济体。同时，网络犯罪的规模自 2020 年以来迅速上升，亚洲成为全球受攻击最严重的地区，根据 IBM X-Force 《威胁情报指数（2022）》，亚洲在2021年遭受的攻击占全球攻击总数的 26%。在北京冬奥会期间，仅两个月时间受到的相关网络攻击共计3.8亿起。

多数人可能会对此数据感到惊讶，我们的日常生活中似乎并无相匹配的感知。一方面，这是出于不同的统计口径，并非完全从用户体验到的纬度。另一方面，日常的感知依赖于可靠的记录和曝光。举一个例子，当2013年底发生了有记录以来最大规模的数据泄露事件时，直到 2016年9月此事件才被报告（Lee 2016）。

数字化安全风险的历史与信息技术的进步保持同步，并非最新的产物。它长久以来处于公众雷达之下，本质原因是在20世纪至21世纪初期，我国上网民众基数不高。

事实上，在前互联网时代，就已经有了网络攻击，因为保护位于计算机内部的数据也属于网络安全的范畴。到了1987年，第一个防病毒软件产品出现。随着互联网的民用化程度提高，越来越多的人开始上网，网络犯罪便开始有利可图，于是20世纪90年代，网络安全风险爆发，早期那些炫技的个人黑客逐渐消失，黑客活动转向牟利驱动，形成了如今仍在不断壮大的网络犯罪产业。

到21世纪初，在美国等互联网较早普及的国家，网络犯罪的规模、形式和恶性程度都达到了新的程度。例如在一次攻击事件中，黑客获得了超过 30 亿用户的雅虎账户访问权限。在2002年1月，美国记录了第一起网络犯罪谋杀案，一位罪犯通过雇佣黑客入侵医院的计算机系统，改变了他的竞争对手病人的处方（Krausz & Walker, 2013）。错误的处方最终导致一名病人死于一名无辜护士手中。

近20年来，网络犯罪的规模、范围、严重程度和复杂性均呈指数级增长，且日益超越地理边界，极大地挑战了传统司法系统应对挑战的效力。2021年2月初，一名黑客远程访问了美国佛罗里达州一家水处理厂的计算机系统，试图将供水中的氢氧化钠含量增加到潜在的危险水平；2022年1月，当国际油价已创近7年新高时，因遭到勒索软件的攻击，荷兰与比利时的几处港口无法完成石油装卸和转运，多艘油轮无法靠港；2022年4月，保加利亚的国家邮政系统遭到网络攻击，导致柜台养老金发放业务被迫中断。

能造成如此大的破坏，是因为网络犯罪如今是一个价值收入颇丰的“产业”，拥有机构化的管理结构和研发预算。攻击者能够使用人工智能等高级技术工具，并持续加快攻击生命周期，从侦察漏洞到发起攻击，仅需几天乃至几小时。这些例子清晰地表明，数字化安全风险已经进入到快迭代、高智能、全覆盖的新阶段。

在这个全新阶段，对抗安全风险已经远远不是商业机构内部的IT工作，而关乎每个人的幸福指数和全社会的安全稳定。2021年1月，美国国务院批准设立新的网络空间安全和新兴技术局（CSET），3月，美国政府发布《国家安全战略临时指导方针》，将提升网络安全作为美国政府首要任务，并鼓励私营部门与各级政府合作，同时加大基础设施投入，保卫美国免受恶意网络活动侵害。我国在2021年通过了历史上第一部“国家安全战略”《国家安全战略（2021–2025年）》，强调加快提升生物安全、网络安全、数据安全、人工智能安全等领域的治理能力，将安全提升到国家战略层面，实现国家安全战略与国民经济和社会发展规划同步。



（二）AI安全风险的紧迫性陡增

在2022年底AI大模型横空出世后，全球业界迅速形成共识：AI安全风险陡增，这是全世界需要迅捷反应、共同面对的巨大挑战。



AI安全风险目前来看主要可以分为三类：第一是内生安全。从人工智能内部视角看，人工智能系统和一般信息系统和应用一样，由软硬件系统组成，会存在技术本身的脆弱性、对数据的依赖性等自身缺陷原因而带来的安全问题。比如人工智能过分依赖于数据与算法，如果给数据库不断投喂带有特定价值观的数据，会对人工智能系统形成严重的干扰，很容易就产生“数据偏见”、“观点霸权”等问题。

这其中就涉及业界广泛关注的人工智能“价值对齐”与“决策黑盒化”问题。“价值对齐”就是应确保AI的价值观跟人类的价值观匹配，确保AI以对人类社会有益的方式行事，不对人类的价值和权利造成干扰和伤害。目前来看，仅靠大模型技术本身不太可能实现对齐这个目标，需要有更多其他技术的介入。“决策黑盒化”指的是难以彻底理解AI系统内部的结构和运转，只能通过其输出的内容来判断并得到一种外在的认知。未来，如果我们真的要大规模利用大模型的能力尤其是决策能力，必须解决黑盒问题，否则AI的安全永远是无根的。

第二是人工智能系统因其自身脆弱性被利用或不恰当使用，从而引发其他领域的安全问题，即衍生安全问题。比如人工智能系统失误可能引发一些重大安全事故。随着ChatGPT等大模型技术的成熟，某些别有用心的人将其作为违法活动的工具，例如生成虚假新闻、深度合成伪造进行诈骗与钓鱼攻击，侵犯他人肖像权、隐私权，大模型生成的内容本身也可能带有歧视、偏见。AI衍生安全影响AI的合规使用，还涉及人身安全、隐私保护、军事与国家安全、伦理道德和法律规范等一系列与社会治理有关的挑战性问题。

第三是外生安全问题，也就是面向人工智能系统的外部入侵攻击。当前，安全风险变得更加复杂、隐蔽、强对抗和更具破坏力。一方面，数字化、网络化程度越高，可被攻击的部位、结点就越多；对数字技术的依赖程度越高，网络破坏造成的后果就越严重。另一方面，黑灰产攻击模式也随着业务创新、新科技引入，逐渐呈现专业化、多样化、智能化、产业化的特点。因而，如何将人工智能驱动的业务风控系统建设的更强更智能，应对大规模网络攻击与入侵，已成为各个企业健康发展的必要保障。

出于对AI大模型风险的担忧，2023年3月，包括“深度学习”教父Yoshua Bengio、Stability AI CEO Emad Mostaque、特斯拉CEO伊隆·马斯克在内的多位科学家和业界顶级专家，参与签署了一封名为《Pause Giant AI Experiments: An Open Letter》的公开信，信中呼吁，因为人工智能实验室陷入了一场失控的竞赛，致力于开发和部署更强大

的数字思维，但是却没人能理解、预测或可靠地控制这些大模型，因此所有AI实验室应该立即暂停训练比GPT-4更强大的 AI 系统，为期至少6个月。

这些问题并不遥远，即使我们搁置AI是否有朝一日会脱离人类控制等由于“黑盒”而导致的更“哲学”的争论，在当前阶段，StableDiffusion、Midjourney等AIGC工具已展现出以假乱真的生图能力，ChatGPT等文本生成模型已具备高度接近人类的语言能力，一旦被别有用心地使用，当前并没有足够有效的办法对其进行辨别与控制。随着这些AI技术的推广和进一步的成熟，破坏能力将远超当下的网络欺诈等行为，对社会造成大量的混乱，对个人带去心理和财产的损失。考虑到AI进步的速度之快，影响范围之广，AI安全风险不可谓不紧迫。

此外，仅仅一年多时间，市面上已经有了各种各样的大模型。[这些大模型之间如何更好地协作，共同演进而不是各行其是造成资源的浪费与社会运行的混乱，或者在协作中触发隐私保护等问题，也是未来的关键挑战。](#)



 (三) 有新技术的地方，就有新的安全风险

除了上网人数快速增加这一诱因，近二十年，网络犯罪的急剧增长，也与科技进步有关。可以说，数字化安全风险是科技发展的内在组成，即使互联网行业消失，所有社交媒体全部下线，安全风险依然会存在，并成为社会的危机。因为数字化并非互联网及相关行业的特有属性，而是涉及到几乎所有行业、所有新兴技术。

工业 4.0，也被称为智能制造、第四次工业革命，即通过将信息技术集成到运营技术中，来提高工业生产的表现。这些信息技术就是我们耳熟能详的5G、云计算、人工智能、XR、数据科学等。全球来看，有两大因素驱动了制造业数字化转型，一是越来越多的制造型企业希望跳过中间商、服务商、代理商等，与用户直接交互；二是制造型企业希望从销售产品转为销售服务，譬如车企。

新技术工具改变了工业的运作方式，同时也导致了安全风险的蔓延，包括网络被入侵攻击，导致服务瘫痪、关键的信息和数据被窃取、大范围的人身伤害。

以供应链安全为例，科技部“云计算+大数据”国家重点专项课题负责人、数秦科技执行总裁兼首席科学家崔伟在接受本报告调研中介绍，供应链安全风险分为两种，一种是网络遭到破坏，数据中心停止工作，可能导致整个供应链中断或者瘫痪。如果是一些涉及到国计民生的重要物资，像是疫情中的药物运输，就会造成很大的社会影响。更危险的是，可能会发生数据篡改，导致供应链出错，譬如不正确的药品发给了某一人群，譬如疫苗试验数据被篡改，最终造成人身伤害。

另一种供应链安全在安全行业更常提到，是产品开发的供应链。如今，无论开发一个硬件还是软件，作为新一代的信息化产品，它必定用到了大量的第三方开源代码。而一旦这些开源产品存在安全漏洞，软件供应链就可能受到攻击，造成巨大的损失。2021年12月10日，Apache Java模块Log4j库第一个远程代码执行漏洞被公开披露，在全世界都导致了广泛的攻击。

根据2022年12月Make UK 的一份报告，42% 的英国制造商在过去 12 个月内成为网络犯罪的受害者，其中四分之一遭受了 5 万至 25 万英镑的损失。根据Security Intelligence的数据，制造公司也是新近流行的勒索软件最大攻击的攻击目标，占总攻击数量的四分之一，居于专业服务（17%）和政府组织（13%）之前。

当然，针对这些风险，制造业也有不少安全科技工具可以使用。比如，区块链技术可以提供分布式和不可篡改的数据存储，可用于确保供应链的透明性、防止数据篡改和验证设备的身份和可信性；人工智能技术可以基于历史数据和模式来预测和预防潜在的安全漏洞和攻击，从而快速发现异常和威胁；物联网安全解决方案可以提供设备身份验证、数据加密、访问控制和漏洞管理等功能，以保护连接的设备和传输的数据；边缘计算技术能将数据处理和分析推向接近数据源的设备，从而降低数据被攻击和泄露的风险。

工业 4.0也并不限于制造业，事实上，医疗、交通等与民生深度相关的行业，在迈向智能化的路上，面临着同样的问题。

比如医疗行业。作为数字化程度相对较高的行业，医疗已经采用了大量数字技术，比如人工智能被应用于医疗图像分析、诊断辅助、疾病预测和药物研发；大数据分析被用以处理大量的患者数据，发现潜在的病例模式和治疗趋势；传感器和物联网在监测患者的健康状况，实现远程健康监护和个性化医疗服务中日渐普及；云计算帮助医疗机构存储和管理大量的医疗数据，简化数据管理流程，并提供远程访问和协作功能。

与此同时，根据中国医院协会信息管理专业委员会（CHIMA）发布的《2018-2019年度中国医院信息化调查报告》，参与调查的 839 家医院中，仅有 43.95%通过了等级保护测评，其中三级以下医院中 75%未开展过等级保护测评。《2019 健康医疗行业观测报告》报告数据显示，在对15339家医疗行业相关单位的观测后，共计发现1029家存在僵尸、木马或蠕虫等恶意程序的单位，6446 家单位的应用服务端口暴露在公共互联网中，4546 家单位的网站存在被篡改安全隐患，其中261家单位已发生网站被篡改情况。

这种状况意味着什么风险？2019年，德国一家专注漏洞分析和管理的公司发现，一些服务器含有大量医疗放射图像，但暴露在了公共互联网上，其中有14个服务器系统与中国有关联，总计包含近28万条医疗数据。这些数据详细记录了患者的个人信息和医疗状况，攻击者借此在暗网上进行交易，获得了巨额利润。

世界已经到达了数字社会的新阶段。许多人认为数字技术是一种特色，有的行业有，有的行业没有。这种想法在十年前甚至五年前都可能是事实，当时数字技术和其他所有技术之间的界限更明显。但今天，每个行业都在走向数字化，从而提高技术水平。交通、医疗、制造业、建筑、发电...在使用和依赖数字化技术方面，彼此联系在了一起。

为什么新兴技术要采用数字技术？或者说，为什么数字化是科技发展的内在逻辑？现代科学源于17世纪的科学革命，这场革命的核心特征，就是将自然和科学数学化。唯有如此，我们才能更精确地观测、计算、实验与控制。因此，数字化技术也就成为了各门科学的核心工具。

以合成生物学为例，它通常指对现有蛋白质或生物材料进行重新编程，以实现新功能的。云计算和人工智能技术的兴起大大推动了这一学科的进展，生物学家们可以处理更大的数据集，以更快的速度和规模进行基因测序，从而精密地操纵和重新设计这些细胞，来驱动特定的结果，研发新的生物能源等。

既然数字技术无所不在，那么数字安全风险自然无所不在。只要有网络、有数字信息的地方，就需要有安全科技。小到微信登录，大到物流供应链系统的防火墙，疫苗生产系统的设计，都离不开安全科技。只要不出事故，我们常常感知不到这些科技的存在，但它已经遍布生活与生产的方方面面。

因此我们提出，未来有两项通用技术，一是人工智能，二是安全科技。“技术是把双刃剑”，在它以更快的速度变得越发强大时，我们不可能扔掉利刃，放弃科技；惟有以另一种科技打造足够安全的刀鞘。



安全科技的关键 技术能力及双重价值

 (一) 安全科技是一种伴生技术

什么是安全科技？

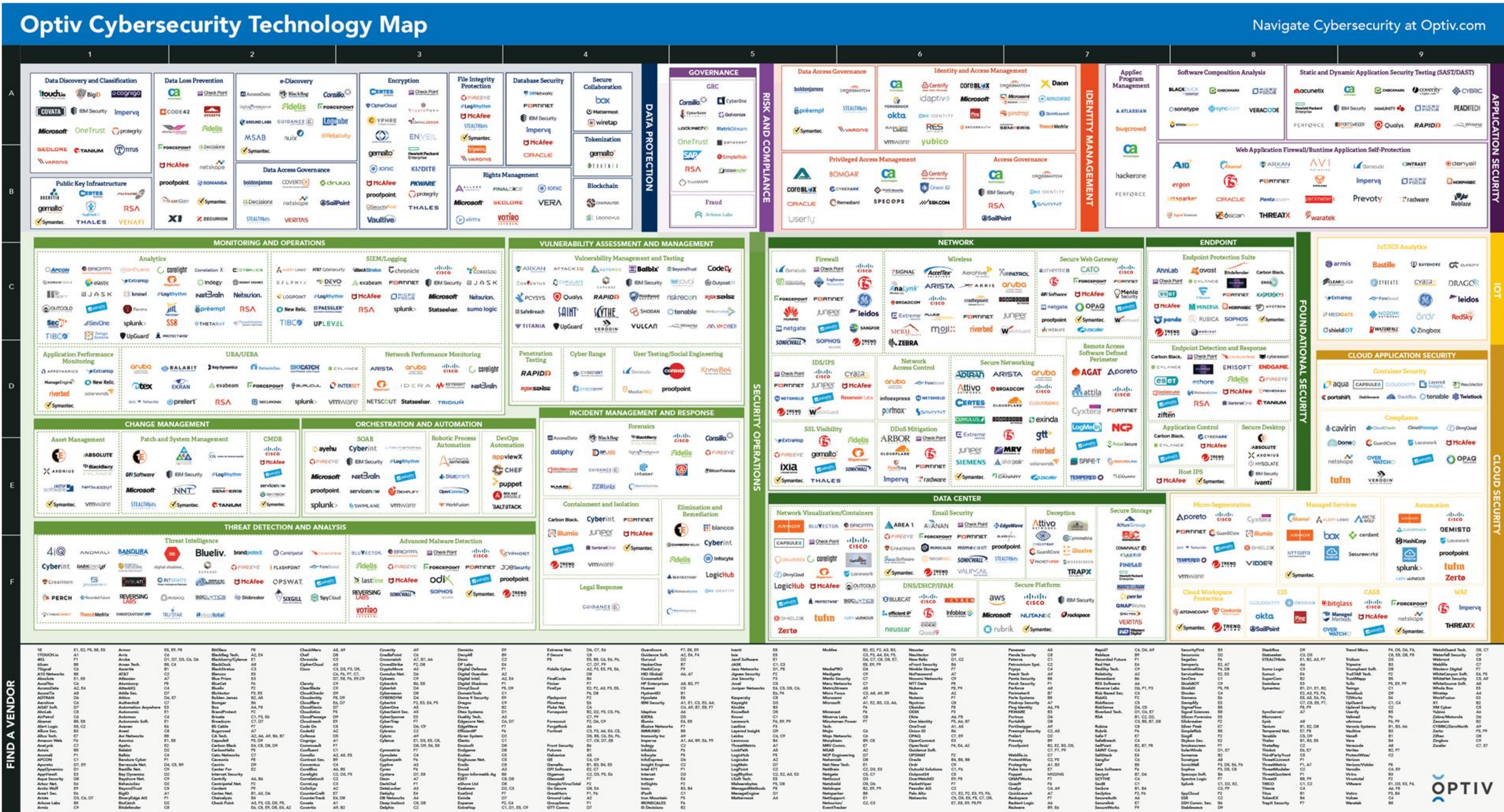
安全科技包括一系列旨在保护信息、网络和计算机系统免受未经授权的访问、攻击和威胁的工具、技术和系统，安全科技的市场包括了硬件、软件和服务，随着IT基础架构向云端的演进，软件市场的占比在不断提升。

在相当长一段时间里，网络安全（network security）即安全科技。过去二十年时间，网络安全得到了极大的发展，包括加密、防火墙、入侵检测等多种技术的进化。然而，随着数字化的深入，越来越多的细分领域涌现出来，使得传统的“网络安全”概念难以覆盖，而安全科技这个词在这样一个转型期中被提出，用以关涉多个领域的技术和理念。它的边界是不稳定的，因为新的安全风险层出不穷，安全技术一直在更新升级。

浙江工业大学网络空间安全研究院院长宣琦接受本报告调研时指出，**本质上，安全科技是一种伴生技术。它永远在面向新科技，面向新发展。**不管是哪个新技术在推进过程中形成了新的安全问题，比如人工智能，就会提出智能安全，比如生物科技，就会提出生物安全。新技术的发展有时候非常快速，所以安全技术的发展和创新也同样在高速变动。

从定义上讲，安全科技不仅超越network security的范畴，也超出了国外常用的cybersecurity范畴。因为security更多指向与对抗相关的安全内容，而安全科技还需要包含safety、reliability、transparency这几个相关但不同的概念，是一个极其复杂的学科。

安全科技包含系统安全、网络安全、数据安全、业务安全、AI安全等范畴。但在实际情况中，每一个技术域、每一个业务域都有自己的安全问题，都有自己的垂直分类，



（安全科技细分领域代表性企业， 图源：Optiv）

每一个垂直领域都很重要，区别主要在于行业侧重点不同。如用于保护各种应用（桌面、web、移动等）生命周期安全的应用安全；保护各类新型终端（IOT设备、OT系统）安全的终端安全；保护云基础设施以及用户基于云构建的应用与数据的云安全，还有芯片安全、身份管理、威胁检测和响应、统一威胁管理、风险与合规服务等等。

目前，全球行业共有数百家公司分布在各个垂直领域，是一个较分散的市场，且更新换代速度极快，整个安全科技产业的赛道细分远超过其他行业。美国拥有80-90%的网络安全公司，以色列、英国、法国、德国也正在创造新的明星企业。全球领先的公司有思科、微软、Palo Alto Networks、IBM、Check Point Software Technologies、Symantec、Accenture、Akamai Technologies、BAE Systems、BlackBerry等，我国也有深信服、奇安信、启明星辰、安恒信息、蚂蚁集团、华为、阿里巴巴、腾讯等企业在垂直领域拥有较突出的技术优势。根据全球权威知识产权机构IPRdaily发布的《安全科技专利分析报告》显示，截至2023年4月，中国是全球安全科技发明专利的最主要布局国家，共拥有专利申请数20445件，为第二名美国的2.23倍。科技型骨干企业成为安全科技专利的主力军，蚂蚁集团、华为、腾讯集团、国家电网、中兴、中国工商银行、中国移动位居全球安全科技专利申请前十名。

目前，安全科技的市场仍以传统企业占据主流，但基于云的新一代企业正在崛起，在全新的技术形式和安全需求下，新的参与者很有可能重塑这个分散的市场。

从时间上划分，安全科技的发展可以大致分成三个阶段：



1、本地保护阶段（20世纪70年代至2000年代初期）：这一时期的安全科技主要基于密码学和防火墙技术，其保护的對象是网络相关的基础设施。进入20世纪70年代后，随着个人计算机的普及，各行各业都迅速采用计算机处理各种业务。在计算机网络尚未大规模普及时，主要面临的威胁是来自非授权用户对计算资源的非法使用、对信息的修改和破坏。这时候计算机安全的主要目的，是采取措施以确保信息系统资产的保密、完整和可用。比较典型的是通过操作系统的访问控制手段来防止非授权用户的访问。

计算机网络尤其是互联网的出现是信息技术发展中的一个里程碑。从1994年，中科院高能物理研究所的IHEPNET与国际互联网络连通，这条带宽64K的国际专线完成了中国全功能IP连接，标志着中国迈进了互联网大门。从90年代到2000年代中期，我国信息化和网络迅速发展，这使得围绕计算机的安全正式进入网络时代，信息系统安全（也被称为网络安全）产业从0到1发展。

这时期的安全科技主要是保护信息在存储、处理和传输过程中免受非授权的访问，防止授权用户的拒绝服务，同时检测、记录和对抗此类威胁，主要威胁为病毒、木马、蠕虫。由此产生了防火墙、防病毒、PKI、VPN等安全工具的需求。20世纪90年代，NASA的研究员发明了世上第一个防火墙。

这阶段的另一标志是发布了《信息技术安全性评估通用准则》，此准则即通常所说的通用准则(Common Criteria, CC)，后转变为国际标准ISO/IEC 15408，我国等同采纳此国际标准为国家标准GB/T 18336。

2、网络保护阶段（2000年代中期至2010年代中期）：随着互联网发展，越来越多的设备接入并融合，技术的融合将传统的虚拟世界与物理世界相互连接，形成了一个空间。互联网成为个人生活、组织机构甚至国家运行不可或缺的一部分。此时以入侵检测、反病毒和漏洞扫描等技术为代表的网络安全是主流。

3、智能保护阶段（2010年代中期至今）：大数据、人工智能、云计算等新技术的出现和产业应用，改变了安全科技的面貌。另外，这个时期信息安全威胁来源从个人上升到犯罪组织甚至是国家力量，信息安全保障的概念形成并成熟。此外，智能互联设备成为新的攻击目标，系统安全风险加大。安全科技开始向智能化、自适应、自愈合等方向发展，并从技术扩展到管理，从静态扩展到动态，通过各种安全技术和安全管理措施的综合融合，构建深度的主动的防御体系。

主要标志是《信息保障技术框架》（IATF）。2009年5月29日，美国发布《网络空间政策评估:确保信息和通信系统的可靠性和韧性》报告。2016年12月，我国发布了《国家网络空间安全战略》，明确了网络空间是国家安全的新疆域。

可以看出，伴随着IT架构的演进，安全科技也同样逐渐走向了无边界。在初期和发展期，政府和企业数据基本存储在私有数据中心，员工也基本在公司内办公时，几乎所有的资产在防火墙技术的保护下；到了创新阶段，数据存储走向云端和本地的混合形式，移动化办公也开始普及，“办公网络”的边界变得模糊；未来，大部分的数据将会上云，终端多样化、办公分布式；安全科技也将从被物理硬件塑造转向被软件定义。

经过长期的发展，安全科技领域目前已经有了大量的技术储备。正如前文提到的，安全科技覆盖面极广，不同技术侧重于不同的垂直领域，且都具有各自应用场景下的重要性。**根据技术的成熟度与前沿性，我们从应用价值角度将安全科技系统分为四大板块，分别是：基础安全、业务安全、AI安全、未来安全。**

其中，基础安全包含了传统的物理安全、系统安全、网络安全、数据安全、身份与访问安全、密码学等，是数字世界网络中任何企业与机构都必须具备的安全防御技术能力。基础安全包括了大量已经成熟应用的技术：

7种主流成熟技术

01 密码学与加密技术

- 密码学是网络安全技术的基础，加密技术可用于保护数据的机密性和完整性，例如对数据进行加密和解密操作。随着时间的推移，密码学逐渐演变为更复杂、更强大的形式，以应对不断增长的安全威胁。

02 防火墙

- 20世纪80年代初，第一个商用防火墙问世。防火墙被设计用于监控并控制网络流量，防止未经授权的访问和攻击。

03 身份认证和访问控制

- 身份认证技术用于确认用户身份，访问控制技术用于限制和管理用户对系统资源的访问。

04 公钥基础设施（PKI）

- PKI是一种基于非对称加密算法的安全架构，用于确保通信和数据的机密性、完整性和身份认证。PKI的引入使得加密和数字签名技术成为网络安全的重要组成部分。

05 入侵检测系统（IDS）和入侵防御系统（IPS）

- IDS和IPS用于监测和防止未经授权的网络活动和攻击。IDS负责检测潜在威胁，而IPS能够主动阻止攻击并采取措施应对。

06 漏洞管理和漏洞扫描

- 为了及时发现和纠正系统中的漏洞，并防止黑客利用这些漏洞进行攻击，漏洞管理和漏洞扫描工具成为网络安全的重要组成部分。

07 威胁情报和情报共享

- 建立威胁情报平台，持续收集、分析和共享威胁情报，以提前了解并对抗新型威胁。

应用和业务安全是在基础安全技术保障了基础运行后，企业根据自身业务需求，针对可能遇到的业务风险而研发配置出的一系列技术。业务风险主要是指不法分子利用业务规则漏洞和技术手段，进行数据爬取、账户盗用、交易欺诈等，因此，风控技术是业务安全技术的核心，包括风险识别、风险预警、风险管控、风险处置。近几年，风控技

术加速智能化，风控模型从传统的基于规转变为基于大数据与人工智能，国内部分企业如交通银行、蚂蚁集团、腾讯集团开始将图技术、隐私计算等技术整合进入风控模型。

AI安全是一个新领域。过去几年，通过应用AI来提高安全技术的效率和成功率，已经成为技术领先企业的常态，譬如通过从已有数据中学习，人工智能可以更快地识别攻击的模式和趋势，从而预测未来攻击，并配置自动响应威胁，在更快的时间内对抗网络威胁。

而随着AI大模型的诞生，AI技术的影响力迅速增加，不再只是助力安全，自身也成为安全的对象，逐渐形成全新的“AI安全”研究领域。目前，AI安全还处于相对基础的探索阶段，主要是具备AI能力的企业为保障自身AI技术应用而进行安全研发，比如AI算法模型的安全、AI原始数据的去毒清洗等等。

在AI之外，面向未来的安全形势，另一些前沿技术也已经出现。尽管目前它们的使用规模很小，但有着相当大的潜力改变整个安全版图，比如量子信息安全技术。

整体来讲，安全科技生态系统存在许多尖端和前沿科技，包括：

- 1、人工智能和机器学习：通过从已有数据中学习，人工智能可以更快地识别攻击的模式和趋势，从而预测未来攻击，并配置自动响应威胁，在更快的时间内对抗网络威胁。

2、区块链技术：区块链提供了去中心化、安全性强的数据存储和传输机制，可用于数据完整性验证、身份认证和分布式防御。

3、零信任安全模型：零信任模型意味着“从不信任，总是验证”，它围绕着假设防火墙两侧的所有内容都可能有害——无论它是否源自外部组织内部，因此要求对所有用户和设备进行严格的身份验证和授权，并实时监测和评估其访问行为。

4、隐私计算：隐私计算是一个包含了安全多方计算、同态加密、差分隐私、零知识证明、联邦学习以及可信执行环境等主流技术子项的相关技术体系，可以让数据以“可用不可见”的方式进行安全流通。

5、物联网安全：随着物联网设备的快速增长，物联网安全成为关注的焦点，包括对设备的认证、数据加密、远程管理和漏洞修复等方面的技术。

6、云安全：随着云计算的普及，云安全技术变得至关重要，包括数据加密、访问控制、虚拟化安全和云供应链安全等方面的技术。

7、生物特征识别和多因素身份认证：生物特征识别技术，如指纹识别、虹膜扫描和声纹识别，以及多因素身份认证技术，如使用密码、指纹和面部识别等，可以提供更强大的身份验证和访问控制机制。

8、量子安全：量子安全是在未来的量子计算时代中，传统加密算法受量子计算攻击而失效后，保护信息安全的一种技术。常见的量子安全技术包括量子密钥分发、量子随机数生成、量子认证、量子安全通信协议等。量子计算技术极大地提升了算力上限，并动摇了密码学的基础，目前在全球范围内引起了创新热潮。



企业与机构根据不同业务需求，针对内容安全、交易欺诈等业务风险研发的安全技术

数字世界企业或机构必须具备的底层安全能力，
含传统的系统安全、网络安全、数据安全等

在AI之外，面向未来安全形势的一些前沿技术，如量子信息安全技术

找到安全科技的共性并不难，大多数情况下，安全科技趋势是由最新的漏洞驱动的。因此安全科技的最大特点，就是攻防。网络犯罪者无休止地挖掘和利用新漏洞来发起攻击，安全战线的一方尝试消极或积极的防御。

有过体育竞技经验的人都知道，一味的防守不仅效率低下，而且表现常常难以令人满意。为了提高防御的效果，需要预先对攻击者做出判断。未来主要的数字安全风险会出现在哪里？哪些技术有可能成为关键？

近几年，面对新的安全威胁和新的应用需求，涌现出一大批新的安全技术，信息安全专家、中国科学院院士冯登国将这些新技术呈现出的特征概括为智能化、零化、弹性化、匿名化、量子化。这五个特征，也可以概括为安全科技生态系统的整体发展趋势。



1、智能化特征：在大模型的潮流下，人工智能安全必将成为主流的安全关切，该领域主要包括人工智能模型自身安全、应用导致的安全风险，以及人工智能在安全领域中的应用等方面。

AI在安全领域中的应用包括防御和攻击两个方面。在防御方面，AI赋能防御技术提升防御的能力和水平。AI可有效提高威胁检测与响应能力；AI可提供较高的预防率和较低的误报率；AI可准确、快速地预防、检测和阻止网络威胁，识别分析未知文件；AI可

克服人性的弱点抵御以人为突破口的社会工程学攻击；在攻击方面，AI赋能攻击技术提升攻击的精准性、效率和成功率。深度学习赋能恶意代码生成可提升其免杀和生存能力，攻击者利用深度学习模型可提升识别和打击攻击目标的精准性；AI赋能僵尸网络攻击可提升其规模化和自主化能力；AI赋能漏洞挖掘过程可提升漏洞挖掘的自动化水平；AI可实现智能化和自动化的网络渗透能力。

2、零化特征：由于云计算和虚拟化等技术的发展，网络边界越来越模糊。零信任安全架构就是基于这样的现状提出。零信任（zero trust）不是一种技术，而是一个框架和思想，核心是“从来不信任，始终在验证”（never trust, always verify）。它的工作原理是假设每一个连接都是威胁，无论来自外部还是内部，针对这些威胁需要进行防护。零安全技术主要包括零信任架构、零知识证明（如交互零知识证明、非交互零知识证明）、零中心技术（也就是无中心技术，如无中心公开密钥基础设施、区块链）、零存在模型、零密钥协议等。

3、匿名化特征：匿名化针对的是未来将越发凸显的数据安全问题，核心是隐私保护技术体系。部分隐私保护技术可用于解决使用中的数据安全问题，这类技术也被称为数据使用安全技术，如机密计算（confidential computing）、联邦学习、同态加密、安全多方计算。其中，机密计算是当前最热门的数据使用安全技术，它可提供硬件级的系统隔离，保障数据安全，特别是多方参与下、正在使用中的数据安全，实现多方信息流通过程中数据的“可用不可见”提供安全解决方案。

4、弹性化特征：弹性的目的是使系统具有预防、抵御网络攻击的能力，以及在遭受网络攻击等不利事件时，仍能继续运行的能力，因此是贯穿基础安全、业务安全等领域的概念。弹性安全技术主要包括弹性公钥基础设施（PKI）、定制可信空间（TTS）、移动目标防御（MTD）、棘轮安全机制、沙箱隔离、拟态防御（MD）、可信计算等。其中，弹性PKI被认为是新一代数字认证基础设施。

网络环境下实体（人员、设备）的身份认证是一个普遍而重要的问题，需要像电力基础设施这样的通用基础设施来支撑。PKI就是这样一个数字认证基础设施，可用于解决网络环境下实体身份认证和行为不可抵赖性等问题。在PKI环境中，其自身安全保障的重要性是举足轻重的。根据重要程度不同，可将PKI分成不同等级。弹性PKI主要用于国家级认证根或电子政务内网等重要部位，必须考虑众多安全威胁，包括内部人员犯罪、系统木马攻击等。

5、量子化特征：安全技术通常与算力有关，量子计算技术可使计算能力大幅度提升，解决现实世界中的复杂计算问题，同时，量子计算技术将直接动摇现有安全技术的基础。因此，抵抗量子计算攻击的安全设计理论、安全分析评估方法、安全解决方案及新型困难问题的寻找和优化实现等都成为当前的研究热点。

如果产学研各界能够把握这些新特征，尽快进行面向未来的安全科技研发，将有效提高数字社会的安全水位。另一方面我们需要时刻记住，数字安全风险是和数字化转型紧紧相联的，掌握了最先进安全科技的组织和国家，也将在产业发展上获得先机，从而提高经济的动力。



(三) 安全科技的双重价值在放大



总结起来，安全科技有着“压舱石”与“助燃剂”的两重价值：



总结起来，安全科技有着“压舱石”与“助燃剂”的两重价值：

第一，守住技术的安全底线，防御外部风险隐患，让技术“难作恶”。如利用安全科技打击在线洗钱、防御DDos攻击、拦截非法访问等。这是数字社会稳步运行的压舱石，也是大部分人对安全科技的既有理解和定位。

第二，提高技术的安全上限，降低技术运行成本，让产业“跑起来”，让更多人受益。这一作用被许多人所忽视，是导致安全科技长期被视作是“成本”而非“动力”的根源。在新技术的前期发展中，常常出现因为安全隐患而无法投入实践的问题，就好像在刹车被发明出来前，汽车行业不可能出现。可以说，安全技术是新兴技术真正获得产业起飞的必要助推器。

当前人工智能技术蓬勃发展，适逢其时地为人类有效求解复杂问题带来了强有力的新手段。但随之而来的数据隐私、技术滥用、失控等安全问题引发全球担忧。加强人工智能这一新兴技术的潜在风险研判和防范，确保人工智能安全、可靠、可控，已成为人工智能产业发展的核心要素。

两重价值具体如何发挥，下面以终端安全保障、隐私计算保护技术，以及备受瞩目的 AI 大模型安全等为例。

◆◆ 案例一：终端设备升级，保护普通人安全的第一道防线

得益于移动互联网和物联网的普及，智能手机、平板电脑、智能手表、天猫精灵、自助零食柜等各类智能终端越来越高频地出现在人们的日常生活中。这些不断衍生发展的智能设备兼具着计算、存储、通信、链接和交互等功能，同时支持安装和运行各种应用程序，是绝大多数人与数字世界的连接口。



智能终端市场规模高歌猛进的这些年，也是各种隐私数据窃取、欺诈、诱骗等安全事件爆炸式增长的时期。根据中国互联网络信息中心 (CNNIC) 发布的第 50 次《中国互联网络发展状况统计报告》显示，我国网民遭遇各类网络安全问题的比例中，遭遇个人信息泄露的网民比例最高，达到了 21.8%。

而终端安全的定义，就是从每台智能硬件设备的底层入手，从源头保护用户免受黑产活动的侵害。从行业案例来看，终端安全技术架构主要分为端、边、云三个层面：

第一，让芯片更可信，从底层构筑安全基础设施，防范注入攻击和数据篡改，这部分主要覆盖 IoT 领域。

第二，打造终端可信中间件，软件层面将风控模型注入终端，让数据在本地可计算。

第三，强调端云协作，进行多层精准防控，提高效率。

通常来说，互联网业务的底层逻辑是流量从移动终端开始，经过 APP 发出业务请求、进入网关，最后进入到业务服务器。端边云融合的终端安全技术架构，刚好可贯穿全流程。整个过程一言以蔽之，风险发生在哪，就在哪阻断。

此前，在终端隐私保护的技术和制度上，苹果手机一直表现比较突出。近几年，国内多家手机终端厂商也纷纷投入终端安全技术，采用创新的方式提升产品的安全等级，从而加强对用户的隐私安全和财产安全保护。2021 年底，vivo 推出了安全风险检测引擎“千镜可信引擎”，通过在端侧对手机芯片、内核、框架和应用各层级进行综合可信度量，为用户提供安全防护。2022 年 4 月，荣耀发布了全新操作系统 Magic UI 6.0，其中部署了和蚂蚁集团联合推出的“可信隐私沙盒”，该技术合作可以在降低用户数据端云流动的情况下，在手机系统层面增强感知风险的能力，使 Magic 4 系列旗舰手机具备本地反诈风控能力，保护用户的信息和资金安全。2023 年 12 月，OPPO 推出了国密二级安全芯片的安全解决方案，相比传统的软件安全方案，芯片级的加密方式可以将敏感权限的管理、授权开关，与操作系统分离，锁进安全芯片的硬件层，由芯片级安全子系统进行管理。



◆◆ 案例二：与黑客赛跑，安全技术为冬奥会拧紧“安全阀”

“科技冬奥”是2022北京冬奥会的特色之一，跨度百余公里的三个赛区、26个场馆、数千名运动员的沟通和场馆协作需要依赖大量技术；共有61个项目、228项技术先后在赛事相关活动中应用。大量数字技术的应用导致网络系统空前复杂，被攻击与利用的风险急剧增加。因此，北京冬奥会在赞助商体系里首次添加了网络安全类别，奇安信成为网络安全服务和杀毒软件官方赞助商。

据奇安信网络安全保障中心统计，在北京冬奥会期间，累计监测到各类网络攻击超过2.4亿次，跟踪、研判、处置涉奥舆情和威胁事件105件，累计发现、修复安全漏洞5782个。其中0 day漏洞是网络安全领域最高难度的问题之一，奇安信基于指令执行序列检测技术构建了安全引擎，并利用指令流反溯技术，定位攻击者所利用漏洞的具体位置，能够第一时间发现0 Day漏洞并进行封堵。

人工智能技术也在冬奥会网络安全保障中起到了重要作用。冬奥会期间，奇安信的安全团队日均监测各类系统日志超40亿条，监测日志数量累积达1189亿条。要从这样数量级的多源异构数据中，发现潜在的威胁和安全风险，降低误报率和漏报率，就需要借助人工智能的分析和预测能力。

奇安信搭建的人工智能安全分析引擎针对网络攻击进行了智能化的提取特征，构建攻击行为模型；并通过采集冬奥组委会信息网络中的流量及相关设备和系统的日志，开展多源数据关联分析，从中挖掘攻击行为的关联性；通过数据与攻击行为的对齐，实现了威胁的智能发现及威胁检测方法的优化，达到了减少告警的误报和冗余的目标，从而能够更精准、更有效地应对未来所面临的未知威胁。

国际性活动的影响力大，攻击行为不仅造成相当的经济损失，社会负面作用更难以估量，2018年平昌冬季奥运会受到APT攻击，互联网、广播系统和奥运会网站都出现了问题，导致许多观众无法打印他们的入场券，直接影响了开幕式的进行。随着数字化的加深，国际大型活动将越来越依赖大量技术，如果没有先进的安全技术，不少地区可能将失去承办大规模活动的能力。



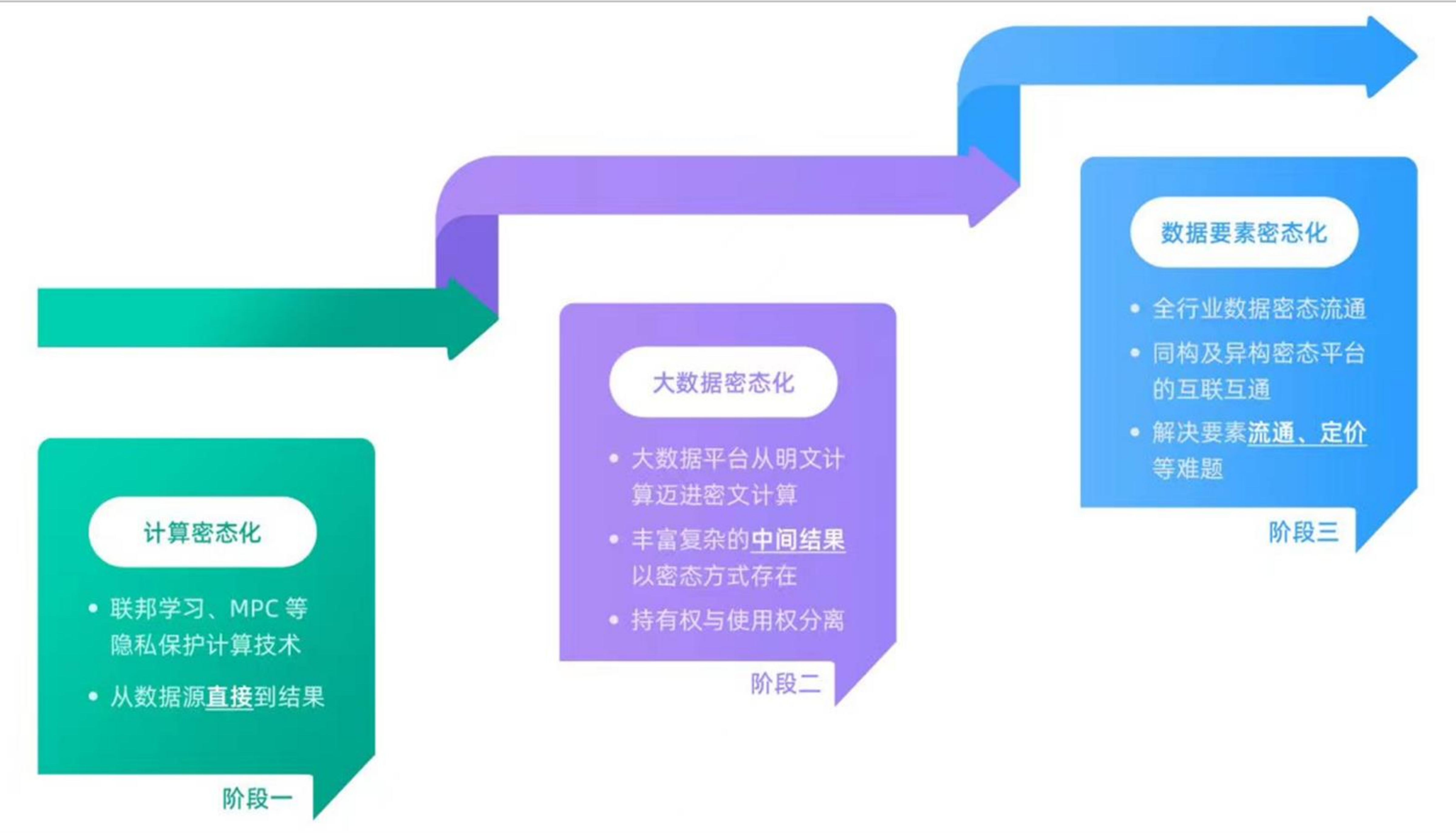
◆◆ 案例三：打破独立烟囱，加速数据要素价值释放

与冬奥会侧重“保障”已有的事物平稳落地不同，隐私计算技术更侧重推动产业解决未来的问题，从而让产业能够顺利进入下一阶段。

隐私计算技术是隐私保护领域的一整套技术体系，主要技术方案包括多方安全计算（MPC）、可信联邦学习、可信执行环境。安全多方计算可以保障多个参与方进行协同计算，同时各方除了计算结果之外，无法获取任何其他信息，从技术层面实现了数据的可用不可见。联邦学习（FL）通过建立一个基于分布数据集的联邦学习模型，能够在原始数据不流出的条件下，完成机器学习的任务。可信执行环境（TEE）则包含了硬件技术，通过构建一个抗篡改的软硬件安全环境，去执行计算等任务。

这是一个全球范围的前沿技术领域，尽管国外企业在技术布局上早于中国，如微软、谷歌、Intel SGX、AMD SEV等已经探索多年并累积了一定成果，但在商用实践上，中国企业通过技术和产业实践协同的模式，在金融、政务、商业营销等产业的应用需求推动下，跨平台隐私计算建设、国产芯片厂商的可信硬件等技术取得了快速的发展，在其中一些领域拥有了一定的优势。根据全球权威知识产权第三方机构IPRdaily发布的2022年《全球隐私计算技术发明专利排行榜(TOP100)》显示，截至2022年3月8日，全球隐私计算专利榜前10名企业分别为蚂蚁集团（1152）、中国平安(423)、Microsoft(374)、阿里巴巴(313)、IBM(252)、华为(206)、国家电网(206)、微众银行(204)、Intel(180)、Samsung(154)。

北京大学客座教授、蚂蚁集团首席技术安全官韦韬将隐私计算技术的发展分为三个阶段，第一阶段是计算密态化，第二阶段是大数据密态化，第三阶段是数据要素密态化。数据要素密态化，对应的状态正是《“十四五”数字经济发展规划》中提出的“强化高质量数据要素供给，加快数据要素市场化流通”。也就是说，成熟的隐私计算技术，可以打开数据要素市场化的大门，实现数据要素的安全流通和价值的充分释放。



（图：数据密态发展将经历三个阶段）

门外面是众多期待着进一步数字化的产业。大数据时代已经开启近10年，如今许多企业和机构都积累了大量数据，但这些数据如果仅限于自身内部使用，价值就会大打折扣，需要“横向”和“纵向”地流通起来。

横向流通上，譬如在疫苗研发场景下，如果更多的医疗机构能提供自身的相关数据，将会大大加速研发速度并让疫苗对于更多人群拥有更平等的效果，然而在没有隐私计算技术的情况下，机构间的数据流通让个人医疗隐私信息承受着巨大的被泄露风险，导致合作无法实行。再比如，政务机构拥有大量个人数据，在隐私计算技术的保护下，不同部门可以横向共享数据，降低组织间的数据协作审核成本，也提高政务机构服务质量，让公众更方便。

纵向流通上，对于中小型企业特别是小微企业的价值尤为明显。大数据的拥有者往往是行业龙头或头部机构，小规模的企业通常没有能力采集和保管大量数据，因而无法在同等程度上利用数据提升经营表现。而如果小微企业可以在合规的前提下，按需从大企业采购数据，使得数据在产业内部安全地纵向流通，将大大提高小微企业的经营效率，降低经营成本。

具体来说，隐私计算技术可以让数据“可用不可见”、“可控可计量”：在数据提供方不泄露原始数据的前提下，对数据进行分析计算，让数据安全流通；使用多方安全计算技术，控制数据的用途以及用量，进而实现数据用途的可控制与可计量，且在融合区块链技术的条件下，进一步帮助数据的确权、定价与交易的体系建设。

中国信通院云计算与大数据研究所副主任闫树在由中国信息通信研究院、中国通信学会、隐私计算联盟主办的“2023隐私计算大会”上介绍，在今年如火如荼的大模型浪潮中，鉴于AI大模型的云部署方式，以及使用方的自身数据可能包含隐私信息，加上用户担心输入数据被用于后续推理或训练，隐私问题已经成为业界的核心关切之一。隐私计算技术同样能在这一问题上起到作用。隐私计算可以在模型微调训练阶段，通过联邦学习，实现数据不出域的多方联合训练，以及通过TEE结合硬件加速方式，汇聚多方数据进行安全高效的大模型训练；而服务方通过TEE部署的方式，可以解决大家普遍关心的大模型泄露隐私的问题。

隐私计算的价值是面向未来的，它在大数据时代的积累上，给予数据流通使用的可能。对于产业数字化而言，这就好比从自给自足的经济模式迈入了货币交易模式。



据韦韬介绍，目前隐私计算行业正从第一个阶段迈向第二个阶段。在数字化比较领先的行业，像金融、运营商业、医疗等，对隐私计算的认知越来越强，逐渐有落地应用，但仍缺乏规模化，需要跨行业和技术域共同推进。

技术演进上，韦韬提出“密态天空计算”或许是行业未来。“密态天空计算”是指基于技术信任的数据跨云互联，提供数据的跨云密态流转和计算服务，其目标是允许基于数据密态的应用能跨多个云厂商运行。天空计算（Sky Computing）作为伯克利大学RISE Lab提出的一种新的云计算架构，其目标是实现云之间的互操作性，让用户可以跨越不同的云厂商和服务，按需获取最优的计算资源和服务。“密态天空计算”是对跨云的“天空计算”更进一步的发展。

◆◆ 案例四：一枚安全芯片，让车联网产业链“跑起来”

车联网是另一个备受关注的领域。根据德勤汽车安全团队的分析，全球联网车辆的数量预计将从现在的2.5亿辆增长到2040年的10亿辆以上。2023年11月，我国工信部等4部门决定开展智能网联汽车准入和上路通行试点工作，将我国的车联网发展推向一个新阶段。

车联网正在从1.0时代的车身状况监测，迈向2.0时代的数据应用、交互。车联网的发展历史可以分成两个阶段。最早期的车联网功能主要是车身状况监测，比如近10年前，一些车厂在出厂时会对车辆配置锁发动机的能力，可以远程监测这辆车并锁上发动机。当时用的是4G联网的通道。现在的新能源车热潮正在做的是车联网2.0，或者叫智联网，它要做的是完全把车身数据和车的内容做高度融合，具体来说是将基于车载驾驶辅助系统与通信技术相结合，实现每个车辆的行为能通过网络被传播、共享、分析。

智联网时代可以做哪些事？譬如可以生成一张实时交通网，将车、路、行人全部于云端连接在一起。当我们在驾驶汽车时，每个人只能看到视线范围内的信息，用上激光雷达的车可以看得比较远，大致在200米左右。可如果在前方一个十字路口，有一辆被挡住的大货车正在高速驶向路口，直行车辆不减速的话就会有冲撞风险，这种情况下人类司机和雷达都是无法预判的。但通过实时的车联网，就能够提前给车主发出警告，这些功能通过现在技术上都可以做到。

但这里存在非常多的安全风险：一旦这个联网系统被破坏，所有的车、路，路边的摄像头、温度传感器，它们的信息都可能被篡改，发出错误提示，如此一来，车主反而可能受到更大的威胁，甚至整个城市交通直接瘫痪。根据Upstream Security发布的《2020年汽车信息安全报告》，2016年至2020年1月，汽车信息安全事件的数量增长了605%。

因此可以说，[车联网的安全科技，主要解决的不是守住安全底线的问题，而是提高安全上限，让产业“跑起来”的问题](#)。无论是二轮车还是四轮车，在不做数字化新功能的情况下，目前的安全性能基本足够。车联网对于安全科技的需求，主要是为了提升数字化服务的体验。车联网的运营能力、服务能力，跟安全能力是不能分开的。只有拥有安全的网络，才可能采用远程控制；只有确保数据可信，才能考虑数据如何使用。

目前，车联网行业的安全风险相对于互联网行业来说不算非常严重，但车辆被劫持、数据泄露等案例已经开始蔓延。此外，一个新出现的风险，是如今很多新能源汽车公司会尝试开发自己的车联网服务，包括导航、影音、在线升级等，并通过企业的数据中心来提供服务。然而在产业的转型期，这也造成了新的不确定性。以前一个车企业出现经营问题，导致业务停止，造成的问题主要是车主的车难以维修，但现在可能是服务的瘫痪。譬如国内有一家新能源车企最近出现了破产问题，这家公司此前已售卖出近十万辆车，在企业停止服务后，一些车主开始自己架设服务器，用开源的产品来更新车联网的信息，但这可能导致出现各种被攻击的风险。

2022年，美国达特茅斯大学的两个学生发现，部分本田和讴歌车型存在漏洞（CVE-2022-27254），黑客可以通过该漏洞获得锁定、解锁、控制车窗、打开后备箱和启动目标车辆发动机的访问权限，防止攻击的唯一方法是永远不要使用遥控钥匙，或在攻击发生后从经销商处重新设置钥匙。这只是无数同类新闻中的一例。和手机应用不同，人们在乘坐高速行驶的汽车时，能够承受的安全风险微乎其微，因此，车联网的安全风险正在成为中心议题，在相当大的程度上制约自动驾驶、智慧交通的发展速度。

目前，车联网产业链包括基础网络连接、内容应用和服务能力等部分，相应的安全技术主要包括：身份认证，实现远程控制身份的管理；内容安全，将产生的数据存储加密；数据可信任，比如通过区块链、硬加密技术等等，保证数据的可信。根据业界专家介绍，短期内车联网行业应该不会出现革命性的新技术，重点在针对各个应用场景，把已有的技术加快落地，通过规模化的应用降低技术成本，从而进一步在行业普及。因为这同样涉及多个领域，如系统安全、芯片安全、数据安全、信息交互安全和内容安全等，能够综合贯穿整个产业链的企业并不多，国内仅阿里、华为、蚂蚁等大型互联网公司可以提供包含整个链路的完整解决方案。

对于车联网行业的安全水平而言，统一技术与应用标准，并加强与相关行业的技术合作，是加快发展的关键。这其中已有一些成功的案例。2015年，为了应对身份数据泄露、身份认证等问题，多家机构联合成立了互联网可信认证生态联盟IIFAA，以推动可信认证技术发展和行业技术规范的制定。原本IIFAA的服务对象主要是手机终端，但随着数字化在其他行业的发展，IIFAA也成为推动车联网场景下身份认证技术普及和发展的重要力量。2022年，有150多万台电动自行车使用了IIFAA数字车钥匙的方案，具体方式如下：

首先，由技术服务商结合IIFAA技术规范，设计了一套“芯片-手机-应用”软硬一体化方案；然后由芯片研发企业了提供硬件设计能力，打造“IIFAA芯片”，将存储根密钥做在芯片的“保险箱”里，保证芯片信号不可篡改伪造；接着，在设备软件里打造一个“保险箱”，并在两个“保险箱”中间搭建加密通信专线，从而让车辆的开锁、落锁、定位等动作能在全密态环境中完成，由此，实现防范盗车、隐私泄漏等风险。

电动自行车的数字车钥匙的完整解决方案很好地体现了跨行业的技术合作与生态标准建设的重要性。据公开数据显示，我国每年二轮电车以3000万-4000万台的规模增长，背后有超19.7万家二轮电车品牌商及软硬配件制造企业，不同芯片厂商、硬件制造商在数字化过程中缺少统一生产标准和安全标准，导致整个产业链中存在大量碎片化的对接工作，制造厂商如果自研数字车钥匙，还需要解决复杂的技术问题，整体研发周期至少

需要4个月。一旦有可信的第三方能提供统一的芯片标准或解决方案标准，就为产业链上下游提供了可行的行业标准，大大加速了研发和生产效率。

在车辆安全风险更受关注的网约车行业，该套方案也有很好的落地实践。2023年12月，结合IIFAA安全芯片研发的行业首个网约车专属“驾驶风控引擎”已经发布。该引擎通过集成车联网安全系统、司机安全驾驶模型及司机信用模型三大产品，构建了人、车、平台三位一体的安全管理体系，提升网约车运营效率，消除风险管理盲区。在车载终端，搭载了安全芯片的数字车钥匙，可防范恶意盗车风险；针对驾驶行为，基于车身感应、人脸识别等技术共建的司机安全驾驶模型，通过识别司机驾驶状态，对疲劳驾驶、接打电话等危险驾驶行为进行及时干预，确保司乘安全。在客观上对驾驶行为进行精准度量的同时，司机历史信用也是网约车风险管理的重要依据。司机信用模型则会根据司机的驾驶能力、从业经验、历史履约、经营能力等指标进行信用评定，形成科学的司机评价体系，引导司机提高服务质量，推动行业良性发展。



（图：IIFAA安全芯片）

◆◆ 案例五：大模型“质检员”，让AI更可信

AI大模型无疑是当下科技领域最受关注的技术。在普通用户惊叹于其表现之时，业内人士对于它的安全性早已展开了激烈的争论。从技术发展的规律而言，大模型的出现是必然的，一旦出现，摒弃它已不可能，合理的安全利用思路是为它打造一套可靠的“质检”标准，就像当初的杀病毒软件的发明一样，将大模型中有问题的部分精准定位并去除，安心使用它好的部分。



(图：大模型安全性关键环节)

具体到运营和应用层面，当前AI大模型的安全质检主要有三个需求：

一，训练阶段的数据质检。大模型的训练是基于公开的数据集，数据采集是否存在偏见、不当、数据被投毒等问题，关乎大模型产生是否公正、有效。另外行业领域微调的过程会涉及一些数据标注，这些标注是否涉及诱导错误的人类对齐、错误价值导向、谣言虚假信息等标注，也会给大模型生成的内容带来问题。

二，模型的可控质检。因为大模型的深度黑盒属性，模型本身是否可靠、稳定、鲁棒存在较大风险，必须进行彻底的检验，防止推理过程黑盒的不可控问题。

三，大模型的应用质检。在具体的应用场景中，根据不同用户的交互需求或可能存在的外部诱导攻击，谨慎评估大模型的安全风险。

蚂蚁集团对于智能化技术的投入比较早，在可信 AI方面做了很多积累。蚂蚁集团安全实验室首席科学家王维强公开分享了相关探索实践，他表示，大模型安全既要“快”也要“慢”，大模型安全防御方面要“快”，要能快速检测、查杀病毒，确保服务无毒害；在大模型安全可信方面要“慢”，要能长远地、体系化地保证整个系统环境的可控、可信。

2023年9月，蚂蚁集团发布了业界首个大模型安全一体化解决方案“蚁天鉴”，包含大模型安全检测平台“蚁鉴2.0”和大模型风险防御平台“天鉴”两大产品。其中“蚁鉴2.0”可以诊疗检测、定位问题，它相当于站在“黑产”角度，通过智能攻击对抗技术，自动生成数百万的诱导性问题，对生成式大模型进行诱导式问答，并对大模型的回答实时、自动化检测计算，24小时不眠不休“找茬”大模型存在的弱点和安全问题。而“天鉴”可以进行“防治”，防患于未然，帮助大模型挡住外界的恶意提问，同时对生成的回答内容进行风险过滤，保障大模型上线后从用户输入到生成输出的整体安全防御。



(图：大模型安全一体化方案“蚁天鉴”)

随着大模型浪潮的演进，安全将会成为AI领域的关键能力，无论是拥有自身大模型的大企业，还是第三方安全科技企业，都会推出更多聚焦AI安全的产品。最终，成熟的产品生态和完善的标准体系会成为平息业界争论，将更先进的AI能力带到更广人群面前的最佳途径。

案例六：防范大宗贸易上下游协作风险，客商准入提效 50%

安全科技在防范“新技术带来的新风险”的同时，也在应对存在上千年的老风险。大宗贸易是人类最古老的经济活动之一，历来会面临地缘政治动荡、市场波动、盗窃和信用欺诈等风险。

北京中铁建工物资有限公司隶属于中铁建设集团(以下简称：中铁建设物资公司)从事了 30 多年大宗贸易。业务安全一直是他们最关注的问题。比如，对哪些上游企业可以预付款?对哪些下游企业可以赊账? 授信额度多少? 会不会有相关风险?

由于大宗贸易往往体量很大，一旦出险，便带来千万级的资损。行业的通用做法是，先去客商现场考察生产、经营情况，再去市场上调研其上下游对该客商的评价，以及通过各个分散的网络平台查询该客商的涉诉情况、不良舆情等，最后形成调查报告和客商信用分，判断授信额度。这类传统的做法，经验成分较多，缺少精准度量，存在风险误判的情况。另一方面，尽职调查至少需要 1-2 周，人力成本高。而随着市场波动，风险也在不断变化，人工调查结果，无法动态更新。

中铁建设物资公司希望用数字化手段改变这一现状。首先，要解决客商数据线上化、

标准化的问题，其次要使用 AI 手段对数据进行风险量化评估，并将风控决策切入业务流程。中铁建设物资公司与蚂蚁数科安全技术品牌蚁盾共建了产业风控平台，依托蚁盾提供的合规、安全的数据管道，可以一站式查询企业资质、经营信息、司法诉讼、关联风险、新闻舆情等多维度数据，也可以了解细分行业的发展趋势。同时，中铁建设物资公司将大宗行业风控制度规范、专家经验注入 AI 模型，与蚁盾共建客商评级模型、客商授信模型。覆盖准入阶段的客商风险评估、授信额度评定，合作阶段的风险监测、预警以及事后风险处置和模型调优。

以往，中铁建设物资公司与每一家客商合作之前，都需要去现场调查。现在用上数字化手段，可以排除掉一批明确不符合要求的企业，减少了线下调查的时间成本;而明确要合作的客商，其授信额度也有了一个更科学、可量化的参考范围;针对已经合作的客商，中铁建设物资公司能在线上观察客商风险变化，及时调整合作策略.相关负责人表示，该项升级至少提升了 50%的工作效率，并且可以实时防范潜在资金风险。





未来：安全科技 必将成为新型公共品



（一）“慢起飞模型”：安全科技是技术向善的集中体现



尽管我们在论述安全科技的价值时，着重于它对新兴科技的护航、控制以及对产业发展的促进，但必须强调的是，安全科技并不是一个纯商业范围的议题。本报告希望从两个方面厘清安全科技的公共品特征：

第一，产品运作层面。防病毒软件、入侵防御系统等等商业安全系统是私有产品，但威胁情报、漏洞信息共享、隐私计算、基础设施保护等等技术和平台，都具有明显的公共品属性。

第二，长期以来，安全科技属于商业和技术界的话题，关于它的讨论一直与企业保护、IT基础设施建设等词汇相联，个人和社会在其中缺乏足够的表达。但我们认为，安全科技的完整内涵不只是对攻击者的防御体系，还包括保护平等发展、社会团结与个人尊严的技术与服务。

对安全科技背后价值观的厘清，有助于加强我们对安全科技乃至整个科技价值的理解和发展路径的思考。[普通人为何要关注安全科技？因为安全科技事关每个人的尊严、人际交往、健康及对社会的认知。](#)

举例而言，当前相当普遍的电信诈骗，其中的个人信息从何而来？一方面，可能是犯罪分子通过非法手段购买得来，但有很大比例的来源，是来自于受到网络攻击的企业内部数据。尽管企业或许没有从攻击中受到直接的损害，但每个个人都承担了相应的风险。电信诈骗的主要受害人群不仅遭遇了经济上的打击，往往也在心理上承受压力，部分人群如老年人会因此而被子女劝阻使用数字化工具，这对于人格尊严无疑是一种伤害。更进一步，即使一个人没有受到诈骗，他依然可能因为数据泄露而遭受网络暴力等问题，在心理上遭受严重损害。这种心理上、人格上的伤害目前是相当普遍，却未被统计，未被纳入安全科技的充分讨论中。

另外根据相关学术研究，不同人群在面临被网络欺诈或被在线欺凌后，选择退出使用数字化设备并导致健康状况恶化的比例不同，最容易受到影响的是儿童和青少年、残疾人、老年人等相对边缘的群体。这说明不安全的数字环境将扩大群体间的不平等。

平等发展角度的另一个例子是，大公司往往有更好的安全科技能力，当前中小型企业也常认为部署安全科技能力是顶级规模的企业需要关心的议题。但现实是，勒索软件等恶意软件对中小型企业 and 中型市场公司会构成生存威胁，而对大型企业通常不会，因为较小的组织在遭遇打击后，更可能面临重大的、公开的服务中断。例如，2019年5月美国德克萨斯州一家中型钢结构制造商遭受了勒索软件攻击，其工具和财务会计软件被永久加密，在赎金难以支付的情况下被迫破产。此外，一旦公司不得不公开处理安全问题，客户的信任可能很难恢复。根据麦肯锡关于数字信任重要性的研究，近10%的受访者表示在得知数据泄露后停止了与供应商的业务往来。

新技术会造成新的社会问题，比如假新闻问题。去年以来的AIGC热潮加大了该问题的严重性。为了保护信息的真实与完整性，各国政府正在制定新的法律法规以及标签系统和水印技术，帮助人们识别虚假内容。可以预料，在deepfake技术的蔓延下，假新闻将比算法导致的信息茧房更进一步造成社会面的撕裂，加大社会成员间的沟通成本。

技术不仅仅是工具的集合，它反映了我们的价值观，安全科技是其中的典型。当我们讨论与投资安全技术时，我们讨论的不仅仅是代码与数字，而是科技的伦理、社会的结构、人群的互动和个人的安全感。

中国社会科学院大学哲学院教授、中国社会科学院科学技术和社会研究中心主任段伟文表示，数字化转型应该采取“慢起飞模型”，在鼓励新技术发展、产业升级的同时，不单追求转型的速度，而是在社会需求方面投入更多力量，通过更好的安全科技和制度构建，尽量减少个人与社会为数字化转型所付出的代价，让起飞能惠及更多人。

“慢起飞模型”和技术的创新冲动与商业的盈利需求，一定程度上存在矛盾，要实现这一点，需要多方努力。一方面，要求企业真正以ESG的思维进行运作，不仅投入更多资金和人力在加强安全科技能力上，并且需要转变理念，不再将安全仅仅视作企业运行的成本，而是企业的社会责任和社会影响力的核心落脚点，是技术向善的重点领域。另一方面，这也要求安全科技真正成为公共品，由国家、社会和产业界共同推动新安全技术的低门槛、规模化应用，建立数字化安全风险公共治理空间等等。

那么，如何能让安全科技成为公共品？我们认为，**推动力可能有4种：合规激励、商业保险、标准建设、安全思维。**

01	02	03	04
			
合规激励	商业保险	标准建设	安全思维
目前国内缺乏更具体的安全追究制度规范。合规细化和惩罚制度的逐步实践将成为安全风险改善的重大推力	建立数字安全事件评估及赔偿标准，将风险从企业内部问题变成更公开事务，引导企业改善自身安全表现	没有清晰的标准，会导致责任认定模糊，增加参与方顾虑。充分利用安全标准可帮助中小企业建立高质量安全保障	以人为本的安全设计，有助于减少人为失误。运维与建设并重的安全构建思维，有利于提升企业安全保障系统

数据爆炸正催生越来越多技术、数据链路的复杂性难题，然而大多数企业往往更倾向于把资源投入到IT研发而不是安全保障上。目前国内大多数企业和机构在100名IT研发人员中，配备的安全工程师不到0.5名。在大部分企业自身没有直接动力来投入安全时，需要政府通过合规者的角度来推动相关的保障投入。在这方面，欧盟在2016 年通过的《通用数据保护条例》法案，对于产业界起到了重大的指导意义。根据CNBC的数据，2021 年，GDPR 罚款总额为 12 亿美元。2023年7月26日，美国证券交易委员会通过《网络安全风险管理、策略、治理及事件披露》，确立了美国上市企业的两项新披露义务：（1）重大网络安全事件的及时披露义务；（2）网络安全风险管理、战略和治理的年度披露义务。

我国近些年在数字化安全领域同样颁布了如《网络安全法》《密码法》《数据安全法》等，为企业建立起基本的安全框架和安全心态。但其中较多为定性规定，数字安全事件惩罚的定量及赔偿标准依然难以确定。下一阶段，**合规的细化和惩罚制度的逐步实践将成为安全风险改善的重大推力。**

商业领域的创新是落实合规的重要助手。商业网络安全保险也能有效帮助建立数字安全事件评估及赔偿标准。网络安全保险由私人保险公司向企业和其他实体提供，保护第一方（投保人）和第三方（投保人客户）免受网络事故（如网络中断、数据盗窃等）带来的损失，例如信息系统的机密性、完整性和可用性遭到破坏等。网络安全保险有两种形态，一是只覆盖网络风险的独立保单，二是作为一般保险（覆盖多种类型风险）的一揽子保险范围的一部分（如一般商业责任保险）。随着该险种的发展，市场接受比率

不断提升，2023年上半年，美国企业的网络保险索赔频率增长了12%，索赔严重程度增长了42%，平均损失金额超过11.5万美元。

能够为合规买单的企业基本只有大型企业，从商业运作上来说，能够为中小企业的安全风险买单的，是保险公司。而因为保险公司运作要求对风险有精确的评估、监控和响应，因此商业网络安全保险市场的发展将显著提高这一领域的透明度，将安全风险从企业内部问题变成更公开的事务。另外，不同企业的保费评估能有效补充法律的定性规范，在不作为和直接触犯刑法之间的设置精细的处罚梯度，来引导企业与机构改善自身的安全表现。因此，商业网络安全保险有利于政府与企业、市场合作，共同攻克业态尚未成熟时期的发展瓶颈。

根据网络安全公司Delinea的研究显示，美国企业和机构获得网络安全保险所需的时间和精力正在显著增加，需要花六个月或更长时间的企业数量逐年增加，企业正在加快购买全面保险，同时还有许多企业积极投资网络安全解决方案，以满足网络安全保险政策的要求。同时，大多数有相关市场的国家也在通过对商业网络安全保险保费的财政补贴，加强企业的参与度。



标准建设同样是一个生态合作的范畴，借助政府、头部机构与企业的带头作用，为全社会的安全技术建设提供标准。

标准建设分为两个部分，第一，是具体产业中的标准建设，比如上文中提到的IIFAA联盟对于车联网数字钥匙的技术规范，比如隐私计算在不同产业大规模落地时所需要的统一国家标准。没有清晰的标准，就会导致责任认定的模糊，特别在新技术落地方面，大大增加了参与方的顾虑。

第二，是更高层面的安全框架规范，如美国国家标准与技术研究所（National Institute of Standards and Technology）制定的网络安全框架（Cybersecurity Framework），将美国政府运行多年的《联邦信息安全管理法》经验集中输出为标准，旨在“确定现有的自愿共识标准和行业最佳实践，以将其构建成网络安全框架”，以最佳实践方式推动安全。因为参与制定安全框架标准的专家通常是中小公司无法雇用的顶级专家，因此充分利用好安全框架准则可以有效帮助中小型组织实施高质量的安全措施。

最后，在安全思维方面，我们也将重点讨论两种思维转变的需求：以人为本的安全设计、运维与建设并重的安全构建。

根据世界经济论坛的《2022年全球风险报告》，95%的网络安全漏洞是由人为错误造成的。显然，个人在对抗网络风险方面承担了不相匹配的责任。一个企业乃至一个社会基础设施的网络安全不应依赖每个个人的持续警惕，必须要求有更多专业资源的机构通过更有效的防护机制建设来减少人为失误的风险。以人为本的安全设计（Human-centric security design）就是其中一个必要的机制。它要求在整个安全风险的控制管理流程中，优先考虑参与者的体验，而不仅仅是技术考虑。通过借鉴行为科学、用户体验等学科，以人为本的安全设计有助于最大限度地减少人为失误。

运维与建设并重的安全构建，针对的是当前我国在安全方面的一个普遍倾向，即企业和政府部门构建信息化系统时，普遍存在“重建设轻运营”现象。这意味着企业在进行信息系统建设和开发时，往往只关注硬件设施的建设，而忽略了持续更新维护系统的重要性。某个企业要建设一套数字化的管理系统，运维费用一般来说只有建设费用的十分之一，甚至更少。

然而，数字化的特点之一就是从量变走向质变的速度很快。信息化系统运维必须有足够的运维量，这要求我们的安全构建思维，从传统的硬件模式，转向更偏重软件的服务模式。



（三）结语



正如数字化安全风险以及安全科技的内涵所体现出的生态融合特征，合规激励政策的细化、商业保险市场的发展、行业标准的建设、安全思维的更新，都要求政府、企业、学术界以及公众各个层面的合作。安全科技作为一种伴生技术，本身便具有浓厚的伦理取向，需要社会各界的积极关注与参与。这种关注与参与，是我们在数字化社会中安全、平等、团结与有尊严生活的必修课。而安全科技作为未来的通用技术之一，尽早对它进行投资，支持我国企业在相关领域上的研发和应用，将有助于掌握新兴技术发展产业迭代的主动权，使安全科技成为建设世界科技强国的基石之一。

（报告完）

参考文献：

- [1] 中国软件评测中心：《医疗行业网络安全白皮书（2020 年）》
- [2] 中国信通院：《中国网络安全产业白皮书（2022 年）》
- [3] 中国信通院：《量子信息技术发展与应用研究报告（2022年）》
- [4] 中关村网络安全与信息化产业联盟：《数据安全治理白皮书 5.0》
- [5] Deloitte: Industry 4.0 and cybersecurity
- [6] An Introduction to Cybersecurity Ethics, Shannon Vallor, Ph.D. William J. Rewak, S.J. Professor of Philosophy, Santa Clara University
- [7] 美国白宫：NATIONAL CYBERSECURITY STRATEGY
- [8] 联合国发展署：Digital technology’s threats to human security
- [9] 麦肯锡：Perspectives on transforming cybersecurity
- [10] OPTIV: NAVIGATING THE SECURITY LANDSCAPE
- [11] The Ethics of Cybersecurity , Markus Christen, Bert Gordijn, Michele Loi, ISBN: 978-3-030-29052-8
- [12] 冯登国. 准确把握网络空间安全技术发展的新特征 全力助推国家安全体系和能力现代化. 中国科学院院刊, 2022, 37(11): 1539-1542
- [13] 科技日报：《中国安全科技发明专利总量全球第一》
- [14] 21世纪经济报道：《蚂蚁集团赵闻飙：安全科技已成数字化发展新动力》
- [15] 浦东时报：《浦东新区物联网企业给芯片装上“安全双保险”》
- [16] 通信世界：《四个首创“黑科技” 揭秘冬奥网络安全保障“零事故”的背后》

