大数据时代的来临，面对海量的数据信息，传统计算机网络技术能够为企业管理提供的支持较为有限。而在计算机网络中有效应用 AI，则能够彻底打破传统计算机网络的局限性，有效优化其功能，助力企业大幅度提高管理效率，为企业经营决策，提供更充足、更完善的数据支撑。在企业管理中有效应用 AI，能够使计算机网络的计算能力和计算速度都得到有效改善。例如，目前很多企业都已在管理中应用 AI 软件，使前台工作与智能管理实现有机融合，进而大幅度提高管理效率与质量，降低人工成本和人工管理带来的风险，节省人力和物力。而且，在企业管理中应用 AI，还能够构建完善的 AI 信息处理平台，这对提高数据处理水平，进一步优化企业管理质量，起到了重要的基础和保障作用[4]。

4　结束语

综上所述，在大数据背景下，AI 在计算机网络中的有效应用是非常有必要的，这既是对传统计算机网络的一种有效创新，同时也是解决大数据时代互联网信息问题的一种有效方法。AI 在计算机网络中的有效应用，能够显著提高过计算机网络的运行效率，保护计算机网络安全，是为用户提供安全、可靠、高效的计算机网络信息服务的有效途径，对推动计算机网络的可持续发展，起到了重要基础性作用。

参考文献：

[1]董新颐. 大数据背景下 AI 技术在计算机网络技术中的应用现状及隐患研究[J]. 软件，2022，43（4）：145-148.

[2]杨晔，张恩国. 大数据下 AI 在计算机网络技术中应用研究[J]. 电脑采购，2022（30）：28-30.

[3]李佳. 分析计算机网络中大数据与人工智能技术的应用[J]. 百科论坛电子杂志，2021（17）：671.

[4]安宁，李文雯，武懿冰. 人工智能在计算机网络技术中的应用分析[J]. 信息技术时代，2022（5）：34-36.

总体国家安全观视域下“星链”的挑战及应对

◆汪培豪

（西安交通大学法学院　陕西　710049）

摘要：“星链”作为低轨卫星星座的代表自问世以来就备受关注，它具有全域覆盖、高速低时延、应用场景广阔等显著特点，技术也遥遥领先。近些年“星链”的发展逐渐显出对网络安全和外层空间和平使用的影响，“俄乌冲突”中的应用又让全球看到了它对军事作战带来的改变，这些背后潜在的安全挑战是我们需要迫切关注的问题。文章将“星链”的概况和应用实际相结合，在总体国家安全观视域下分析其对网络、太空、军事带来的安全挑战，并提出应对建议。

关键词：星链；低轨卫星；总体国家安全观

党的二十大报告中指出：“必须坚定不移贯彻总体国家安全观，把维护国家安全贯穿党和国家工作各方面全过程，确保国家安全和社会稳定”。总体国家安全观是一个内容丰富的宏观概念，其涵盖了政治、国土、太空等十六项具体方面的内容。

近年来卫星互联网产业高速发展，大多数国家开始着力打造属于自己的卫星星座，比如英国的 OneWeb、美国的 Starlink、中国的鸿雁、虹云等。其中尤以美国“星链”最具代表性，它的发展让我们在感叹其技术先进的同时也开始思考了其背后会带来的安全性挑战，而“俄乌冲突”中的应用大大提高了对该问题的关注。

当前研究“星链”安全问题的文章数量有限，大部分文章梳理的安全问题比较分散。因此需要基于总体国家安全观的视角，系统性梳理出美国“星链”对国家安全观涵盖的网络安全、太空安全、军事安全等方面可能带来的挑战，并提出对策性思考。

1　“星链”概述

“星链”并非一个无商业规划的纯科研项目，其从开始就有着构建新一代太空互联网产业的宏伟愿景。下文将介绍“星链”的发展、主要技术及特点。

1.1“星链”的发展及主要技术

“星链”由 SpaceX 创始人马斯克在 2015 年提出，目的是构建天地一体化通信网络为全球各区域提供互联网通信服务。该项目计划于 2024 年之前在近地轨道部署 1.2 万颗卫星，有关文件显示还准备再增加 3 万颗，使部署数量达到 4.2 万颗。目前正在进行的 1.2 万颗卫星部署分为三个阶段，各阶段部署计划如图 1。

轨道类型		数量 / 个	轨道高度 /km
LEO	阶段一	1 584	550
	阶段二	2 825	1 110、1 130、1 275、1 325
VLEO	阶段三	7 518	345.6、340.8、335.9

图 1　轨道部署情况

近两年全球新冠疫情肆虐，但“星链”的部署步伐仍井然有序。北京时间 2022 年 10 月 28 日，搭载 53 颗星链卫星的猎鹰九号运载火箭在美国加利福尼亚州发射升空，成功完成了本年度第 31 次星链卫星的发射。至今，星链共完成 66 次发射，卫星升空总数达到 3558 颗。关于历次发射时间和内容信息，参见图 2。

年份	发射次数	发射卫星数量	卫星总数
2019	2	120	120
2020	14	833	953
2021	19	989	1942
2022	31	1616	3558

图 2　卫星发射信息图

“星链”遥遥领先当前其他低轨卫星计划不仅因其具有科学规划、高密数量的特点，更突出体现在技术优势方面。

首先，“星链”可以实现星间链路通信。一般的卫星不支持该技术，卫星间通信必须通过地球网关中转。2021 年 SpaceX 发射了首批配置激光星间链路载荷的试验卫星，将激光星间链路投入使用，2022 年开始发射的卫星均配置了星间激光链路。“星链”将实现星间路由转换的方式进行通信（依托卫星间链路进行远程中继，再经由远程地面站完成互联网接入），相比传统的直接入网可以大大减少对地面基站的依赖。

其次，“星链”中卫星与终端设备通信使用的是一种有别于传统 IPv4/IPv6 的 P2P 网络连接协议。P2P 是一种去中心化的网络连接技术，这种方式的特点是资源并不集中在某一固定设备上，而是分散地储存在多个设备中。卫星绕着地球飞行会不停地经过用户地区的上空，数据链也会不断切换，而 P2P 用在“星链”卫星上使得每颗卫星和每一个终端用户都具备了服务器和客户端的功能，数据在协议的基础上可在设备间自由流通，大大提高了通信速率，并且其配备了端对端的硬件加密技术，极大提高了安全性。

1.2“星链”的特点

作为当前全球最大的天基互联网星座，“星链”具有的特点包括：

（1）成本低

卫星的发射和建造成本很低。“星链”卫星的发射使用的 SpaceX 公司自行研发的“猎鹰 9 号”运载火箭，这一火箭拥有全球最先进的回收技术，大大降低了火箭发射成本。此外，星链卫星每颗质量为 227~260 千克，质量轻便建造成本也相对较低。

（2）高密覆盖

“星链”加上增补的 3 万颗预计共部署 4.2 万颗卫星，如此庞大的卫星数量可以对地球实现无死角覆盖。根据 GSMA（全球移动通信系统协会）发布的《2022 全球移动经济发展报告》显示，全球目前仍有 6%的人生活在没有网络覆盖的地区。而星链可不受地球自身客观条件的限制，通过“空间移动基站”居高临下，动态覆盖全球，弥补地面通信的缺点，让全球的各个区域都能接入到网络。

（3）通信容量大、速度快

“星链”低轨道和高数量的优势，使其拥有巨大的通信容量和更快的传输速率。SpaceX 卫星系统中的每一颗卫星能够为用户提供的下行容量总和在 17Gbps 到 23Gbps 之间，具体数值取决于用户终端配置。

（4）“潜力”巨大

“星链”可以广泛用于商业通信、天文以及军事等方面。相比于之前“铱星计划”的失败，“星链”从设计到运营都进行了较好的成本控制，且有科学的建设规划。此外它的特性让其在特定的商业领域里具有极强的竞争力，比如在海事通信领域，可凭借其不受地理因素等限制的优势占据市场份额。伴随“星链”搭建的完成，未来也会衍生更多的应用场景，产生更多的价值。

2 “星链”带来的安全挑战

习近平总书记在 2014 年召开的中央国家安全委员会会议时提出“总体国家安全观”。党的二十大报告中“安全”一词出现了 89 次，首次将“确保国家安全和社会稳定”单列一个章节，足以看出党和国家对新时期“安全”层面的重视程度。“星链”带来的安全性挑战不容小觑，本章将基于“总体国家安全观”视角进行系统性梳理。

（1）网络安全挑战

国际电信联盟《无线电规则》中规定，除卫星广播业务外，本国不能向其他国家提出该国卫星网络不可覆盖国家领土的要求。这表示“星链”卫星能够覆盖我国领土且有在我国开展卫星通信的可能，但该业务不受我国监管。

“俄乌冲突”中，乌克兰境内能够快速开通星链服务就得益于 SpaceX 在乌克兰周边国家（土耳其、波兰等）地面基站供乌借用中转通信。当前我国周边的日本、印度尼西亚、菲律宾等国家准许了在其国内开展星链服务，并且部分国家已经建造了星链地面站。未来在我国境内的居民可以通过这些国家的基站进行星链通信，这将严重挑战我国网络主权。

此外，马斯克也在积极发展卫星手机产业，其计划使用第二代“星链”卫星为手机提供卫星互联网服务，一部手机即可直连星链实现全球通讯，这将对我国国内的网络监管带来巨大挑战，网络信号及卫星手机产业的安全监管都将会成为重大难题。

（2）太空安全挑战

首先，“星链”的出现使得本就有限的太空频谱轨道资源更加短缺。卫星轨道、频谱等资源属于全球性资源，由世界各国之间共享。根据国际电信联盟规则，对频谱及轨道资源按照先到先得的原则分配使用。“星链”的几万颗卫星将会大量占据轨道频谱，不利于他国开展卫星项目。

其次，“星链”会增加太空碰撞事故可能性。几万颗卫星会产生大量太空碎片，导致近地轨道被碎片覆盖，大大增加卫星间的碰撞概率。此前就发生过类似的安全问题，在 2019 年，欧洲航天局的“Aeolus”观测卫星为了避免与“星链”卫星发生碰撞采取了紧急制动；2021 年，中国常驻维也纳联合国和其他国际组织代表团向联合国秘书长发出照会，通报了美国“星链”在 21 年的 7 月和 10 月曾两次危险接近中国空间站的行为，这对中国空间站及站上航天人员的安全构成威胁。

（3）军事安全挑战

“俄乌冲突”中“星链”的应用让全球见识到它可以突破传统地面通信的局限性，在地面基站受损的情况下进行通信；它可以提供最强大的指挥通信网络，覆盖到其所连接的全球各处部队、无人机、轰炸机等；它安装简单，便于作战携带，能够很好适应机动作战环境下的应用要求。“星链”卫星还搭载模块化探测载荷，可以增加拍照、遥感系统，结合卫星数量众多，可以形成高性能的全天候卫星侦察体系，大大提高美军军事侦察能力。

同时，星链还在不断“进化”。美国“太空新闻”网站 2022 年 12 月 3 日称，SpaceX 公司近日宣布针对国家安全和军事部门推出新一代“星盾”业务并且在公司内部成了名为“星盾”的新业务部门，目标客户是美国国家安全机构和五角大楼，这显示“星链”向军事化迈出了关键一步。

此外，“星链”还助推了太空军事化进程。特朗普时期曾明确将太空认定为“作战领域”，并成立了太空司令部，设立了太空军，拜登政府仍保留了这一存在。据资料显示，“星链”卫星通过技术可以被改装为一种太空武器，用来攻击其他国家的航天器，这种潜在的性能势必影响空间和平。

3 应对“星链”安全挑战的对策建议

卫星网络是未来网络的重要组成部分，“星链”带来的安全性挑战需要我们积极应对，具体来说可以从以下方面进行：

3.1 网络安全层面

（1）完善相关法律制度

当前我国在卫星通信领域没有统一的卫星系统信息安全标准，要实现卫星网络统一化管理、加强国内卫星网络监测，需要我们建立相应的卫星网络安全机制和卫星网络产业的监管规范。具体而言，要结合当下卫星网络发展现状完善我国《卫星通信业务管理规则》《卫星电视广播地面接收设施管理规定》及其他卫星网络法律规范。

（2）加强境内防范

国家相关部门应根据我国卫星网络的具体发展实践采取防范措施。具体而言可以采取：推动构建卫星网络“防火墙”、加强卫星运营业务的许可及通信终端设备的管控、发展卫星信号监测技术。确保“信号可防、信号可截、终端可控、信号可监”。

（3）规划卫星通信产业发展

伴随卫星通信技术的成熟，卫星手机一体化将成为未来发展的主流，这将给我们带来巨大的监管难题。虽然国家可以对境内卫星手机的生产、销售进行严格管控，但对境外流入的管理具有极大不确定性。因此需要我们对产业发展尽早部署规划。

3.2 太空安全层面

（1）完善外层空间的法律制度

当前，外层空间的法律架构主要由五大协定构成，协定制定时间较早且主要针对航天活动搭建了笼统的法制框架。五十多年前的条约框架已难以规范当下商业化航天发展。基于此，各方应探索形成新条约的可能性或对现有条约进行修补，完善外层空间的法律制度。

（2）促进联合国介入外空发展治理

“星链”卫星的发展必然会促进其他各国低轨卫星发展，这将导致频率和轨道资源的争夺将日益激烈；对此，我国应当积极推动联合国及相关国际机构（国际电信联盟）介入这一问题的治理，注重发展实际与公平原则的结合。

（3）加强太空活动管理

卫星使用过程中无法避免地产生碎片，而现有的技术无法做到有效处理。为了航天活动安全，我国应积极推动世界各国从法律层面对碎片管理明确其需承担的义务和责任，维护太空环境安全。同时，随着航天活动的日益增多，我们要加快与其他国家建立航天活动应急反应机制，减少航天器碰撞等危险的发生。

（4）合理布局我国低轨卫星发展进程

国家应大力支持类似今年新启动的“秦岭卫星星座”等项目的发展，通过建设我国自己的低轨卫星星座抢占轨道和频率资源，提前规避因他国抢占而造成的轨道资源耗竭。同时，对我国已经获得的频段资源，要统一管理，有效使用。

3.3 军事安全层面

“星链”在未来必定会让美军在作战中“如虎添翼”。对我国，若要在未来信息化战争中与先进技术缩小差距，掌握主动权、维护和平安全，要注重新型作战方法的研究，注重技术创新，也要加速布局属于我国自己的卫星网络系统--“五云一天工程”。同时积极跟踪“星链”及其他国家星座计划的发展，加强对其应用研究，针对可能出现的不同应用场景，生成相对应的解决方案。

我国还要积极推动“禁止太空军事化”进程。现阶段，我国应倡导更多国家共同提出大力推进太空和平使用的方案，保障太空安全。

4 结语

总体国家安全观要求我们既重视内部安全也重视外部安全，把维护国家安全贯彻到方方面面，以安全保障发展。“星链”自问世以来，就展现了其与众不同，它所具有的特点和技术将会改变全球网络通信的格局，极大促进互联互通。“俄乌冲突”中的应用让我们又看到其在军事方面的重大价值，并对它未来还会出现在何种应用场景、带来何

种价值充满好奇。但作为美国的一项星座计划，我们也需要对其时刻保持警惕，“星链”对网络主权、网络监管、太空以及军事带来的安全挑战值得我们研究，探索出可能存在的安全问题并早做应对打算，更好地保障我国的内外安全环境。

参考文献：

[1]何康.星链：全球卫星互联网时代的传播体系重构[J].湖南工业大学学报（社会科学版），2020，25（04）：23-31.

[2]余南平，严佳杰.国际和国家安全视角下的美国“星链”计划及其影响[J].国际安全研究，2021，39（05）：67-91+158-159.

[3]李陆，郭莉丽，王克克.“星链”星座的军事应用分析[J].中国航天，2021（05）：37-40.

[4]张深，陈春岐，田维珍.星链组网手机终端加入军事应用赛道带来的新启示[J].国防科技工业，2022（04）：56-58.

[5]俞润泽，江天骄.“星链”对太空军控的影响[J].现代国际关系，2022（06）：35-41+61-62.

[6]李小历.警惕“星链”的野蛮扩张和军事化应用[J].国防科技工业，2022（05）：54-55.

[7]任园园，张小艳，王青.浅谈“星链”计划及其影响[J].网络安全技术与应用，2022（05）：34-35.

[8]陈妹元.太空物联网——星链计划的建构与哲思[J].数字通信世界，2022（08）：158-160.

[9]王太军，唐鲫慕，周超.“星链”在俄乌军事冲突中的应用探研[J].通信技术，2022，55（08）：1006-1013.

美国《国家网络安全战略》解读

◆方毅飞

（战略支援部队信息工程大学（洛阳校区）　河南　471003）

摘要：2023 年 3 月 2 日，美国白宫发布了《国家网络安全战略》，该战略以网络安全形势研判为基础，围绕建立数字生态体系的战略目标，通过明确 5 大支柱、27 个战略目标和 31 项具体举措，指明了美国在网络安全领域的防护重点和优先事项。《网络安全战略》是美国政府指导网络安全工作的纲领性文件，既继承了特朗普政府时期的部分网络战略理念，又在总体目标、安全形势研判、手段选择和塑造互联秩序方面有着鲜明特征，反映了拜登政府对网络空间安全态势和未来发展的主要预判，值得我国密切关注。

关键词：美国；网络空间；网络安全；网络安全战略

“网络安全对美国经济的基本运作、关键基础设施的运行、美国民主体制和机构力量、数据和通信的隐私性以及美国的国防都至关重要”[1]。基于对网络时代安全形势的判断和对网络安全重要性的新认识，美国白宫于 2023 年 3 月 2 日正式发布了《国家网络安全战略》（National Cybersecurity Strategy，以下简称《战略》）。该战略以 2018 年美国《国家网络战略》和 2022 年美国《国家安全战略》为基础和指导，围绕“建立一种可防御且富有弹性的数字生态体系”的战略目标，以保护关键基础设施、破坏和消除恶意网络行为者的威胁、塑造安全且弹性的市场力量、用投资来打造有韧性的未来以及建立国际伙伴关系为 5 大支柱，明确了美国在网络空间的作用、责任和资源上必须发生的两个根本性转变，概述了美国在网络安全领域面临的挑战和应对方式。该战略是美国政府指导网络安全工作的纲领性文件，反映出拜登政府对网络空间安全态势和未来发展的主要预判，值得我国密切关注。

1　《国家网络安全战略》的出台背景

此次国家网络安全战略的出台并非一蹴而就，而是建立在拜登政府执政以来在网络空间领域的持续努力基础之上，与美国政府当前亟待依托网络空间领域重点推动的一系列重大问题均密切相关。

1.1 “太阳风”网络攻击事件是引发思考“网络安全”的序曲

2020 年底，黑客利用太阳风（Solar Winds）公司的网络管理软件漏洞，攻陷了多个美国联邦机构和财富 500 强企业网络。2020 年 12 月 13 日，美国政府确认国务院、五角大楼、国土安全部、商务部、财政部、国家核安全委员会等多个政府部门遭入侵[2]。“太阳风”网络攻击事件涉及全球多个国家和地区，将“网络安全”这一现实问题摆在了世界各国的面前——“太阳风”网络攻击事件突显数字时代大国竞争的新形势和新趋势，即通过信息技术手段窃取机密，并进行旨在破坏和降级实体功能的有限行动[3]。“太阳风”事件引起美国社会各界的巨大震荡，使得刚入主白宫的拜登不得不面临来自网络空间的巨大安全挑战，美国国内迫切希望新政府出台行之有效的网络安全战略以维护美国在网络空间领域的优势与安全。

1.2《重塑美国优势——国家安全战略临时指南》是《战略》出台的前奏

为消除“太阳风”事件带来的动荡，2021 年 3 月，美国白宫国家安全委员会火速发布了《重塑美国优势——国家安全战略临时指南》（Interim National Security Strategic Guidance，以下简称《指南》），该文件列出美国当前国家安全的优先事项和战略方向。《指南》明确了美国当前面临的两大国家安全挑战，即来自地缘政治对手与日俱增的竞争压力和技术革命对美国的全方位、颠覆性影响。基于这一认知，不难看出“服务大国竞争”和“重塑美国优势”成为拜登政府一系列政策和战略的基本锚点。《指南》在“美国国家安全优先事项”一章中强调了网络攻击和虚假信息对美国安全可能构成的威胁，同时指出关键基础设施和新兴技术可能对美国网络安全造成的冲击。《指南》还指出在塑造新的全球秩序（规范）方面，尤其是在网络空间问题上，美国与盟国和合作伙伴之间加强合作的可行性和必要性。在此基础之上，《指南》初步描绘了拜登政府对于网络安全的愿景。

1.3 特朗普时期的网络政策“遗产”是推动《战略》形成的内动力

尽管特朗普执政期间，美国政府机构先后发布了《国家安全战略（2018 年版）》、《国防部网络安全战略》、《国家网络战略》和《国土安全部网络安全战略》等多项涉及网络安全的战略文件，但因为重要职位长期空缺、网络外交中断等种种原因导致美国国内对有关网络安全的成效不甚满意。然而，特朗普政府网络政策的一些“遗产”却给《战略》的形成带来不可磨灭的影响。

一是强调网络安全技术创新。特朗普政府认为维护网络安全的最核心手段是通过创新和保护网络安全技术来培养一个充满活力和弹性的数字经济市场[4]。二是发展网络实力，加强进攻性网络能力建设。特朗普政府采取更具进攻色彩的网络安全政策，在关键基础设施遭受攻击之前，国家予以主动的攻击[5]。三是突出合作对网络安全的重要性。特朗普政府认为美国应该与盟友加强合作，建立稳定且富有弹性的数字经济体系对确保网络空间的安全至关重要。

1.4 美国《国家安全战略》是《战略》制定的上层指导

2022 年 10 月，拜登政府公布了其任内的首份《国家安全战略》（National Security Strategy）报告，此份战略报告显示，未来“决定性十年”在政治、经济、军事、情报和网络领域呈现出全方位大国竞争态势，同时指出网络安全领域的规则塑造是美国全球优先事项之一。《国家安全战略》中有关网络安全的集中论述有三处：

一是第二部分“投资我们的实力”中的一项举措，即“实施现代产业和创新战略”。在关于网络时代的安全形势判断中，《国家安全战略》指出美国推行现代工业和创新战略的原因是投资可以增强美国抵御能力的关键领域，并强调关键基础设施安全和基础网络安全是其中的重中之重。

二是第三部分“我们的全球优先事项”中的一个事项，即“合作应对挑战——恐怖主义”。《国家安全战略》认为网络攻击成为现代化冲