

使能技术与国际安全：简编

2023 年版

关于作者



何雯婷是联合国裁军研究所安全与技术项目副研究员。她拥有日内瓦国际和发展问题研究所国际事务硕士学位和位于中国北京的外交学院外交学学士学位。

关于联合国裁军研究所

联合国裁军研究所（裁研所）是联合国内部一个由自愿捐款供资的自主机构。裁研所是世界上为数不多专注于裁军的政策研究所之一，提供裁军与安全方面的知识，并促进对话和行动。裁研所总部设在日内瓦，协助国际社会提出切实可行的创新想法，从而找到解决重大安全问题的办法。

注

本出版物所使用的名称和材料的编排方式并不意味着联合国秘书处对任何国家、领土、城市或地区或其当局的法律地位，或对其边界或界线的划分表示任何意见。在出版物中表达的观点由个人作者负唯一责任。它们不一定反映联合国、裁研所或欧洲联盟及其工作人员或赞助者的观点或意见。

致谢

裁研所核心资助者的支持为裁研所的所有活动奠定了基础。本出版物由欧洲联盟资助，是裁研所安全与技术计划的一部分，该计划得到了捷克共和国、德国、意大利、荷兰、瑞士和挪威政府以及微软公司的支持。

作者衷心感谢贾科莫·佩尔西·保利（Giacomo Persi Paoli）博士在整个起草过程中给予的宝贵指导和提出的真知灼见。特别感谢伊利亚·杜兰-史密斯（Elia Duran-Smith）在背景研究方面提供的帮助。此外，作者还要感谢詹姆斯·布莱克（James Black）和萨拉·格兰德-克莱门特（Sarah Grand-Clément）的全面审阅和建设性反馈，这极大地丰富了最终作品。

引用

何雯婷“使能技术与国际安全：简编（2023 年版）”。瑞士日内瓦：联合国裁军研究所，2024 年。

缩写与缩略语

5G	第五代蜂窝网络
6G	第六代蜂窝网络
AI	人工智能
AlaaS	人工智能即服务
AR	增强现实
AWS	亚马逊云科技
CPU	中央处理器
CSP	云服务提供商
DOD	国防部（美国）
EUV	极紫外线
GNSS	全球导航卫星系统
GPU	图形处理器
HTS	高温超导体
IaaS	基础设施即服务
ICRC	红十字国际委员会
ICT	信息和通信技术
IoMT	军事物联网
IoT	物联网
ISR	情报、监视和侦察
JWCC	联合作战云能力
LEO	低地球轨道
MRI	磁共振成像
NEMS	纳米机电系统
nm	纳米
NPU	神经处理单元
PaaS	平台即服务
PQC	后量子密码学

QKD	量子密钥分发
SaaS	软件即服务
SoC	片上系统
TPU	张量处理单元
TSMC	台湾积体电路制造股份有限公司
UAV	无人驾驶飞行器
VR	虚拟现实

目录

关于作者.....	1
关于联合国裁军研究所.....	1
注.....	1
致谢.....	1
引用.....	2
缩写与缩略语.....	2
执行摘要.....	4
1. 导言	4
2. 第 I 类：先进材料	5
2.1 半导体.....	5
2.2 超导体.....	7
2.3 纳米技术.....	8
3. 第 II 类：零部件	10
3.1 微芯片.....	10
3.2 传感器.....	12
4. 第 III 类：处理和计算	14
4.1 云计算.....	14
4.2 边缘计算.....	15
4.3 量子计算.....	17

5.第 IV 类：基础设施	19
5.1 5G 和 6G	19
5.2 物联网	21
5.3 云基础设施	22
5.4 卫星通信	23
6.结论	25
参考文献.....	27

执行摘要

先进材料、微芯片、传感器和连通基础设施等领域的技术进步正在促进其他技术领域的创新，尤其是在信息和通信技术（ICT）、人工智能（AI）和自主系统方面。这些使能技术正在重塑数字景观，并有可能应用于军事领域。虽然各种政府间进程在解决 ICT 及 AI 对安全的影响方面取得了进展，但对促进或推动其进一步发展的基础技术的关注相对较少。这彰显了我们迫切需要对使能技术及其对国际安全的潜在影响进行更彻底、更全面的审查。

为了填补这一知识空白，本简编致力于查明和分析使能技术中最突出的进展，特别强调那些仍处于早期开发或应用阶段的进展。简编探讨了四类使能技术：先进材料（半导体、超导体和纳米技术）、零部件（微芯片和传感器）、处理和计算（云计算、边缘计算和量子计算）以及基础设施（第五代和第六代电信（5G 和 6G）、物联网、云基础设施和卫星通信）。

简编重点介绍了所研究技术领域的若干总体趋势和发展情况。硬件微型化的持续趋势正促使诞生了更加紧凑和高效的设备，从而推动了使能技术在军事系统中的广泛集成。这些技术显著增强了军事能力，并有可能加强国际安全努力。然而，各国之间技术竞争加剧的可能性，以及全球供应链中与使能技术相关的网络安全风险和脆弱性，也会带来挑战。虽然私营部门的作用至关重要，但在军民两用技术方面的合作可能会带来新的风险，如危及敏感的军事信息。

因此，持续监测和分析新出现的趋势对于建立有效的治理框架，从而平衡使能技术带来的机遇和风险至关重要。

1.导言

先进材料、微芯片和传感器、计算能力和连通基础设施等技术正在促进或推动其他技术领域的创新和能力发展，尤其是在信息和通信技术（ICTs）、人工智能（AI）和自主系统方面。使能技术

的发展正在彻底改变数字生态系统，增加了为军事目的开发和应用这些技术的可能性。¹随着这些技术的不断进步，解决它们对国际和平与安全的影响变得越发重要。要利用这些技术的优势，同时降低其潜在风险，持续的“前瞻扫描”至关重要。

在关于“当前科学和技术发展及其对国际安全和裁军努力的潜在影响”的 2023 年报告中，联合国秘书长强调，人们持续关切与安全和裁军有关的科学和技术发展正在超过规范和治理框架管理风险的能力。²虽然各种政府间进程在应对 ICT 和 AI 的安全影响方面取得了长足进步，但对促进或推动其进一步发展的基础技术的关注却相对较少。这彰显了我们迫切需要对使能技术及其对国际安全的潜在影响进行更彻底、更全面的审查。

为弥补知识差距，本简编致力于查明和分析使能技术中最突出的进展。其中包括那些仍处于早期开发或应用阶段，但预计将对国际和平与安全产生重要影响的最突出进展。本简编专门侧重于探讨使能技术对数字生态系统的一阶效应，特别是与国际和平与安全相关的一阶效应。不过，某些技术领域的影响可能会超出本报告所涵盖的范围。

在随后的章节中，简编深入探讨了四类使能技术。第一类包括半导体、超导体和纳米技术等先进材料。第二类是零部件，包括微芯片和传感器。第三类包括处理和计算，即云计算、边缘计算和量子计算。第四类是基础设施，从第五代和第六代电信（5G 和 6G）、物联网（IoT）和云基础设施以及卫星通信。每一章都对所审查的技术进行了全面分析，包括最新发展和相关军事应用，随后评估了对国际安全的潜在影响。简编最后对使能技术领域的总体趋势和发展进行了总体审查。

2.第 I 类：先进材料

2.1 半导体

半导体是一类导电性能介于导体（如金属）和绝缘体（如玻璃）之间的材料。半导体的导电性可以控制和改变，使其成为包括二极管、晶体管和集成电路在内的现代电子设备和元件的基石。

半导体独特的电气特性改变了技术格局，推动了结构越来越紧凑、功能越来越强大、能效越来越高的电子设备和系统的开发。在电子工业中，硅是最常用的半导体材料，但砷化镓和锗等其他材料也用于专门用途。硅晶片通常是微芯片制造的基础，在数字技术的运行中发挥着至关重要的作用。

现在通常以纳米（nm）为单位的半导体制程节点，³是半导体技术的一个关键因素。制程节点的缩小使更多的晶体管可以封装进一个芯片，从而提高了性能和能效。数十年来，半导体节点尺寸

¹ 为本简编之目的，使能技术被定义为在裁研所安全和技术方案工作范围内的其他技术领域，包括网络、人工智能和自主以及系统集成，促成或推动创新和能力发展的技术。

² 联合国大会（2023 年）。

³ 一纳米等于千分之一微米，或十亿分之一米。

已大幅缩小，从最初的以微米（ μm ）为单位⁴到目前最先进的 3 纳米技术。⁵最先进的半导体制造商之一台湾积体电路制造股份有限公司（TSMC）计划从 2025 年开始生产下一代 2 纳米半导体。预计处理速度将比 3 纳米芯片高出 10%-15%。⁶

这一制程节点演变背后的驱动力就是众所周知的摩尔定律。这是英特尔联合创始人之一戈登·摩尔（Gordon Moore）基于经验和观察提出的规律，即从历史上看，微晶片上的晶体管数量往往大约每两年翻一番。因此，该定律认为，在计算机成本降低的同时，计算性能将继续增长。尽管这一理论在 21 世纪初大体仍然成立，但根据对当前物理学定律的理解，工程师们已开始接触到传统半导体材料的极限。因此，一些观察家甚至宣称摩尔定律已经消亡。⁷业界目前正在寻求创新的解决方案，以追求未来半导体的改进。

为满足日益增长的计算能力需求，其他材料已被查明为硅的潜在替代品。例如，化合物半导体结合了多种元素，生产出能够在性能上超越硅的材料。这些材料有望在推进新型连接技术和自动驾驶汽车方面发挥关键作用。⁸砷化镓是仅次于硅的第二大常用半导体材料，这种化合物以其出色的电子迁移率而著称，因而比硅具有更高的效率。其对过热的耐受性也更强。然而，砷化镓的大规模生产需要克服重大挑战，包括对有毒化学品的依赖，继而引发有关其对公众健康和环境影响的担忧。⁹

目前开展的研究工作正在探索在开发日益紧凑和高效的设备方面显示出巨大潜力的新型材料。最近的研究突出了一种名为立方砷化硼的材料在解决传统硅基半导体所存在的某些局限性方面的有效性，并有可能成为“迄今发现的最佳半导体材料”。¹⁰尽管立方砷化硼具有前景很好的特性，但目前仍处于实验阶段，其在现实世界中的应用还有待充分确定。除此以外，其他新兴半导体材料也受到了越来越多的关注，包括高功率氮化镓、锑基和铋基材料，以及石墨烯等二维（2D）材料。¹¹这些材料具有独特的物理特性，已被证明在特定应用中具有优势。不过，成本问题及其生产的复杂性阻碍了它们的广泛应用。

半导体材料的持续创新将在未来的军事系统中发挥关键作用。从传感器、致动器和存储芯片到电子光学系统和微控制器，半导体在电子设备的一系列关键部件中都有具体应用。¹²这些半导体成为尖端电子设备提供支撑，在高速通信设备、雷达系统和精确制导武器等精密军事系统中占有重要

⁴ 例如，英特尔于 1971 年推出的 4004 处理器：

<https://www.intel.com/content/www/us/en/history/museum-story-of-intel-4004.html>

⁵ 截至 2023 年 9 月，全球只有两家公司能够生产 3 纳米半导体：TSMC

（https://www.tsmc.com/english/dedicatedFoundry/technology/logic/l_3nm）和三星

（<https://news.samsung.com/global/samsung-begins-chip-production-using-3nm-process-technology-with-gaa-architecture>）。

⁶ Ryugen, Hideaki (2023 年)。

⁷ Arcuri 和 Shivakumar (2022 年)。

⁸ <https://irds.ieee.org/topics/future-of-semiconductor-performance> IEEE（未注明日期）。

⁹ IEEE（未注明日期）。

¹⁰ Chandler (2022 年)。

¹¹ IEEE（未注明日期）。

¹² Gargeyas (2022 年)。

地位。此外，半导体技术还是人工智能和物联网（IoT）等变革性创新的催化剂。因此，新型半导体材料的出现具有加强国防能力的潜力，尽管它也可能开创一个国家间技术竞争的新时代。

此外，供应链的脆弱性目前也是一个主要挑战。半导体供应链是一个非常复杂且相互关联的全球网络，涉及不同的生产阶段和来自不同地区的公司。它还具有高度专业化的特点，例如，先进的半导体生产设施集中在东亚。无论是地缘政治紧张局势还是自然灾害，对该地区制造能力的任何破坏都可能对半导体的可供性产生负面影响，并对国家安全造成严重后果。不过，替代性半导体材料的开发有可能重塑现有模式，并提升全球供应链的多样化。

半导体：2023 年亮点

- 在制造更紧凑、更高效的半导体方面，我们正在不断取得进步。TSMC 和 三星 等领先的半导体制造商正在推进开发下一代 2 纳米半导体技术，预计处理速度将比目前最先进的 3 纳米半导体提高 10%-15%。
- 硅仍然是最常用的半导体材料，但它正在接近自身物理极限。目前开展的研究工作正在探索有可能提高性能的新型半导体材料，包括立方砷化硼和二维材料。
- 由于半导体供应链的复杂性和相互关联性，它很容易受到干扰，从而对国家安全构成重大挑战。不过，对替代半导体材料的探索有可能加强全球供应链的多样化。

2.2 超导体

超导体是一种能够导电而不产生任何阻力或能量损失的材料，并且在冷却到特定临界温度以下时能够排斥磁场。这种独特的性质使得电流可以在超导体内无限流动。

超导体卓越的电磁学特性有潜力提升多个领域，包括电子学、量子计算、能量传输和存储以及磁共振成像（MRI）技术。不过，由于要求极低的温度，昂贵的低温工程和冷却过程中的高能耗成为了必需，其实际应用目前受到了限制。大多数超导体材料的临界温度介于绝对零度和 10 开尔文（约-273 至-263 摄氏度）之间。¹³因此，大规模应用超导体目前还不现实。

超导体研究的主要重点聚焦于探索临界温度显著更高的材料。高温超导体（HTS）已被发现能在比传统材料更高的温度下表现出超导性。尽管被称为“高温”，但 HTS 指的是能够在液氮沸点 77 开

¹³ NCCR（2021 年）。临界温度是指超导体的电阻降至零的温度。

尔文（-196.2 摄氏度）以上超导的材料。¹⁴近年来，科学界越来越重视进一步突破极限，努力开发室温超导技术。虽然这项研究仍在进行，但迄今为止尚未取得突破。

未来的研发工作可有效降低运营成本，使超导体技术更易于实际应用。先进超导体在军事领域的应用预计将带来变革。可扩展室温超导体材料的开发可彻底改变电子学领域，带来前景广阔的应用，如超高速和高能效计算机芯片、低延迟宽带无线通信和高效电网。¹⁵此外，超导体还可用于构建量子比特（量子处理器的基本单元），为量子计算提供了广阔机遇。¹⁶目前正在开发新的超导体材料，以生成能够抵御外部干扰的量子比特，这种特性可以提高量子计算机的。¹⁷不过，室温超导体的出现可能会引发国家间新的技术竞争，从而可能导致有关专利、技术转让和市场准入的国际争端。¹⁸

超导体：2023 年亮点

- 目前，超导体的实际应用由于需要极低的温度而受到阻碍，这就需要昂贵的低温工程和高能耗。科学界正在努力实现室温超导。
- 可扩展的室温超导体的开发有望彻底改变电子领域，但它的出现可能导致有关专利、技术转让和市场准入的国际争端。

2.3 纳米技术

纳米技术有助于设计、制造和应用纳米级材料，通常为 1-100 纳米（1 纳米等于十亿分之一米）。

在纳米尺度上，量子效应和表面行为会产生独特的、通常是新颖的特性。¹⁹这些特性可用于各种应用，包括纳米材料和纳米电子学。在现代电子领域，纳机电系统（NEMS）的进步大大推动了设备微型化这一持续趋势。这些系统可用于创建更小、更高效的传感器、致动器和其他设备，在先进传感、计算和通信领域得到了关键应用。

¹⁴ Clynes（2023 年）。

¹⁵ Pedram（2023 年）。

¹⁶ 有关量子计算和最新发展的详细分析，请参见下文第 4.3 节。

¹⁷ Feldman（2023 年）。

¹⁸ Roa（2023 年）。

¹⁹ 美国国家纳米技术协调办公室（未注明日期）。

在传感应用方面，纳米技术可用于空气和水质的环境监测以及污染物检测。纳米技术的融入可以为军事行动制造出更小、更灵敏的传感器，例如可以探测生物和化学危害物剂。与传统的生物威胁检测方法相比，基于纳米材料的生物传感器可以实现更高的灵敏度和准确性，甚至可以减少样品量、制备时间和检测成本。²⁰纳米传感器可用于为军事行动提供有关潜在威胁的实时信息，从而改善对战场态势的感知。它们同样有利于生物武器和化学武器领域的裁军核查工作。

在计算领域，纳米技术通过促进碳纳米管、石墨烯和量子点等纳米材料的发展，为下一代计算铺平了道路。随着传统硅技术逐渐接近其物理极限，人们对替代材料和实现新计算模式的方案的兴趣与日俱增。近年来，研究人员查明碳纳米管是一种具有吸引力的在晶体管制造中替代硅的替代材料。²¹使用这种高导电性纳米材料可以促进创建更紧凑、更高效的晶体管，从而能够超越硅晶体管。²²不过，它们在实际应用中的优势还有待最终证实。²³此外，量子点（即通过纳米制造工艺合成的纳米级晶体）有可能彻底改变量子计算领域。量子点具有量子特性，可用作量子比特，构成量子计算机的根基，从而构建出一个可扩展、具有成本效益和容错性的工作机器。²⁴不过，该技术仍处于起步阶段，要实现量子计算机的实际大规模生产，还必须克服若干技术和商业障碍。

²⁵

此外，纳米技术还能促进军事行动中的先进通信，带来多种益处，包括降低能耗、通信设备微型化和增强连接性。在无线通信系统中，纳米技术的发展带来了更小、更便宜、更省电和更高效的无线传感器设备，并使 5G 网络成为可能。²⁶纳米材料还可用于制造高效天线，从而得以提高信号效率和可靠性。例如，研究人员已开发出纳米级天线，可在不同核心处理器之间以光速传输数据，且几乎没有损耗。²⁷

虽然纳米技术在增强军事信息和通信系统方面大有可为，但其开发和部署也存在一定风险。研究表明，纳米粒子可能具有各种各样的毒性和环境危害，继而对人类健康和生态福祉构成重大威胁。²⁸纳米粒子的尺寸和成分使其能够突破生物体的生理屏障，在人体内引起有害的生物反应（如肺部炎症和心脏问题）。²⁹生产过程中产生的纳米材料可能通过有意或无意的排放进入环境。一旦沉积到土壤中，它们就有可能污染地面，随后迁移到水系统中。³⁰

²⁰ Rowland 等人（2016 年）。

²¹ Fadelli（2023 年）。

²² Basheer 等人(2022)。

²³ Fadelli（2023 年）。

²⁴ Hecht（2022 年）。

²⁵ 有关量子计算和最新发展的详细分析，请参见下文第 4.3 节。

²⁶ Hamza 和 Jaafar（2022 年）。

²⁷ Kullock 等人(2020)。

²⁸ Kumah 等人（2023 年）。

²⁹ 同上。

³⁰ Ray, Paresh 等人。（2009 年）。

纳米技术：2023 年亮点

- 纳米技术的持续进步正在不断提升先进传感、计算和通信技术。碳纳米管和量子点等纳米材料有可能推动下一代计算，包括新兴的量子计算领域。不过，在实现切实可行的大规模生产方面仍然存在挑战。
- 纳米技术为军事信息和通信系统提供了潜在的益处，但也带来了风险。研究表明，纳米粒子可能具有毒性和环境危害性，对人类健康和生态福祉构成重大威胁。

3.第 II 类：零部件

3.1 微芯片

微芯片或芯片，又称集成电路，是在通常是硅片的一小块平整半导体材料上集成了晶体管、二极管和电阻器等微型电子元件（包括）的紧凑组件。

微芯片技术的意义举足轻重。它是现代电子和计算系统的基石，与分立元件构建的设备相比，它所打造设备不仅体积更小，而且性能更强大、更具成本效益且更加节能。微芯片可以执行各种关键功能，包括信息处理、数据存储和指令执行，可用作存储芯片、中央处理器（CPU）和图形处理器（GPU）。

随着半导体材料的不断进步，微芯片也在不断发展，从而以更低的成本实现了新的功能和更高的性能。³¹如上所述，半导体行业不断突破微型化的极限，开发出制程节点更小的晶体管。尺寸缩小后，单个微芯片上可容纳更多晶体管，从而提高了处理能力和能效。不过，由于目前以硅为基础的半导体技术正逐渐接近其物理极限，人们正在寻求替代材料和方法，以确保微芯片技术的持续发展和变革。

芯片设计的改进也推动了该领域的创新。人们提出了替代性芯片设计方法，如“多晶粒系统”和“基于芯片单元的设计”。³²与传统的单片芯片不同，多晶粒架构由一系列专用芯片组成，如内存和 CPU，这些芯片可以连接在一起，形成一个复杂的集成系统单芯片（SoC）封装。据信，这种创新的芯片设计能够支持大规模的 AI 机器学习，提高硅良率，最大限度地减少芯片制造过程中的浪

³¹ 有关半导体技术和最新发展的详细分析，请参见上文第 2.1 节。

³² 《麻省理工学院技术评论》洞察（2023 年）。

费。³³苹果、谷歌/字母表和亚马逊云科技（AWS）等公司设计了定制 SoC，以针对特定应用和工作负载优化芯片性能，这就是所谓的“定制硅”方法。³⁴

目前正在设计专门微芯片，以促进 5G 和人工智能等其他技术应用。5G 连接需要开发先进的微芯片，以满足该技术对高速度和低延迟的要求。AI 能力在很大程度上还依赖于张量处理单元（TPU）和神经处理单元（NPU）等专用微芯片的处理能力。与 CPU 等通用芯片相比，尖端人工智能芯片的速度和效率可以快数十倍到数千倍。³⁵

此外，极紫外（EUV）光刻技术目前在最先进微芯片的制造中发挥着重要作用。它有助于在硅晶片上制造超小型、高精度的元件，并推动微芯片不断微型化。为了进一步推进微型化进程，研究人员查明了一种更为复杂的方法，即高数值孔径 EUV 光刻技术，以实现下一代 2 纳米节点技术的大规模生产。³⁶预计到 2025 年，新的制造系统将全面投入使用。³⁷此外，先进的封装方法也在不断提高微芯片的性能和能效，特别是将多个芯片集成在一个三维结构中的三维（3D）堆叠封装技术。³⁸

未来几年，微芯片技术的新发展将继续塑造技术格局，对国际安全产生重要影响。电子系统在现代战争中的作用无处不在，这意味着微芯片性能的提升可以使军事行动的各个方面受益。其中包括提高先进武器的精确度和有效性，增强情报、监视与侦察（ISR）能力，加强通信系统，以及促进 AI 和自主性在军事系统中的整合。不过，这项技术也带来了新的安全挑战。从芯片设计和制造到封装、测试和分销，微芯片供应链是高度全球化和复杂的。最先进的技术和制造能力往往集中在某些地区，从而造成潜在的供应链脆弱性。例如，荷兰的 ASML 是目前唯一一家有能力制造用于大规模生产世界上最先进微芯片的 EUV 光刻机的公司。³⁹

另一个挑战与技术的双重用途性质和潜在扩散有关。智能手机和笔记本电脑等民用应用中使用的微芯片可以不受出口管制条例的限制，因此可以被用于军事目的或集成到军事系统中。⁴⁰使用微型芯片还涉及网络安全问题。鉴于集成电路架构的复杂性，硬件漏洞很难检测到。物理修改可能会被有效地隐藏在大量的有效组件和功能中，并在很长一段时间内不被发现。⁴¹与软件问题相比，硬件缺陷往往更难修复，修复成本也更高，这就打开了一个漏洞窗口，使更广泛的数字系统面临风险。⁴²

³³ 同上。

³⁴ Shilov（2023 年）。

³⁵ Khan 和 Mann（2020 年）。

³⁶ IBM（2023 年）。

³⁷ ASML（未注明日期）。

³⁸ Moore（2022 年）。

³⁹ ASML（未注明日期）。

⁴⁰ Gilchrist（2023 年）。

⁴¹ Levine 和 Pipikaite（2019 年）。

⁴² Giles（2019 年）。

微芯片：2023 年亮点

- 随着半导体技术的进步，通过微型化不断推动着以更低的成本实现微芯片性能和功能的提升。探索替代性半导体材料和方法，具有维持微芯片技术的发展和变革的潜力。
- 芯片设计和生产工艺的改进也推动了这一领域的进步。创新的芯片设计，如“多晶粒系统”，提供了复杂的集成芯片系统，可以支持大规模的 AI 机器学习。目前正在开发的高数值孔径 EUV 光刻技术旨在到 2025 年实现下一代 2 纳米节点技术的大规模生产。
- 尽管提高微芯片性能对军事行动有潜在好处，但面临的挑战包括供应链脆弱性、技术的双重用途性质和网络安全问题。

3.2 传感器

传感器是旨在检测物理特性和环境条件继而将该信息转换成输出信号的设备。

传感器，包括运动传感器、接近传感器、生物识别传感器和图像传感器等，具有广泛的应用和功能。从地面车辆、舰船和无人驾驶飞行器（UAV）到导弹和卫星，它们几乎在军事系统的方方面面都已变得不可或缺。因此，传感器技术的进步在国防能力现代化方面发挥着至关重要的作用，能够提高军事行动的整体效率。先进传感器应用可为军队提供更准确、更及时的数据收集，增强战场态势感知和防护能力，提高目标定位精度和威胁探测能力，并且有助于在动态作战环境中进行决策。

用于军事目的的传感器技术领域出现了许多进步。传感器融合是创新的一个关键领域。武装部队越来越多地寻求结合多种传感源，以获取更准确、更全面的战场信息。多传感器系统集成并分析来自不同传感器类型（如声学、雷达、光电和红外传感器）的数据，从而将态势感知能力提高到通常单独分析这些数据源所无法达到的水平。在地基军用交通工具中，传感器融合技术可为乘员或指挥官提供 360 度全方位环境视图，并促进与其他系统的信息共享。⁴³

量子传感利用量子态对干扰的固有敏感性，不仅能进行更精确、更灵敏的测量，还能释放测量过往无法测量的现象的潜力。⁴⁴量子传感有可能改变军事能力。例如，研究人员开发的量子传感器可以探测到隐藏在墙壁和其他障碍物后面的物体，这有助于侦察等军事应用。⁴⁵此外，量子传感

⁴³ Eshel（2022 年）。

⁴⁴ van Amerongen（2021 年）。

⁴⁵ 英国国家量子技术计划（未注明日期）。

技术还能提高船舶、潜艇和飞机所用惯性导航系统的精度。这将显著地增强在全球导航卫星系统缺失环境中的定位和导航能力。⁴⁶

传感器越来越多地与人工智能技术相结合，提供智能数据收集和分析，从而提高军事决策的效率。认知雷达系统利用机器学习能力来适应环境或对手行为的变化。⁴⁷此外，还开发了可穿戴生物识别传感器，用于实时监测士兵的生命体征（如心率、体温和水分）以及包括疲劳和压力水平在内的精神状态。将人工智能集成到未来系统中，对于加快过滤和解释从士兵可穿戴设备收集到的数据将是至关重要的。⁴⁸这一新发展有可能帮助指挥官做出军事决策，并推动提升军事人员的表现。

除了增强军事能力，传感器技术的进步还为国际和平与安全带来了新的机遇。遥感技术有助于监测正在发生的武装冲突以及对和平协议的遵守情况。⁴⁹利用先进的传感器还能提高检测环境中化学和生物制剂等有害物质的效率。这些应用有助于及早发现威胁，从而能够迅速采取应对和缓解措施，并有可能加强裁军核查制度。

不过，传感器的使用也带来了一系列独特的挑战，必须加以解决。传感器，尤其是涉及不同系统间数据共享的传感器，在很大程度上依赖于网络，因此很容易受到网络攻击的影响。恶意行为者可能试图破坏或操纵传感器系统，从而破坏数据完整性，导致决策失误。随着技术的进步，传感器获得了在系统中生成更大量数据的能力，这可能会导致严重的滞后时间，并影响数据质量。⁵⁰这可能会妨碍军事决策，除非同时改进网络架构。最后，通过收集和存储与军事人员和平民相关的信息，传感器应用可能会引发对个人隐私和监控行为的合理关切。

⁴⁶ Coggins 等人（未注明日期）。

⁴⁷ 英国国防科学技术实验室（2022 年）。

⁴⁸ Hamblen（2023 年）。

⁴⁹ Avtar 等人（2021 年）。

⁵⁰ Macri（2022 年）。

传感器：2023 年亮点

- 传感器融合可整合来自不同来源（如声学、雷达和红外传感器）的数据，提供全面的战场感知。
- 量子传感利用量子态对干扰的敏感性，实现了更精确的测量、障碍物后的物体探测，并改进了 GNSS 失效环境下的惯性导航系统，为军事应用带来了希望。将传感器与人工智能技术相结合可加强数据收集和分析，从而推动改进军事决策。
- 先进的传感器技术可以为国际安全努力做出贡献，帮助监测正在发生的武装冲突以及对和平协议的遵守情况，并及早发现危险物质。不过，必须解决网络安全问题和其他挑战，包括数据量增加可能导致的滞后时间。

4.第 III 类：处理和计算

4.1 云计算

云计算便于用户访问计算资源，而无需维护内部部署基础设施。它根据需求的变化灵活扩展资源。

云计算在云基础设施的集成硬件和软件组件的支持下运行。⁵¹近年来，云计算的能力已成为各种应用创新的催化剂，包括大数据分析、机器学习、无服务器计算、增强现实（AR）、虚拟现实（VR）和其他各种尖端技术。现在，基于云的平台推动了 AI 即服务（AIaaS）的外包，这有助于广泛获取 AI 的变革能力。⁵²此外，云原生技术已成为在云计算环境中构建、测试、部署和管理应用程序的一种新方法，具有提高效率、降低成本和可扩展性的优势。⁵³

云计算具有推动军事领域创新的潜力。具体来说，利用云技术可以加快军事系统软件的设计、开发和测试过程。⁵⁴这可以增强从人工智能和机器学习到软件现代化和网络安全等各种军事应用的能力。⁵⁵在军事训练中，基于云的平台可为人员提供逼真和沉浸式的训练环境，并通过 VR 或 AR

⁵¹ 有关云基础设施和最新发展的详细分析，请参见下文第 5.3 节。

⁵² Marr（2023 年）。

⁵³ 谷歌（未注明日期）和 AWS（未注明日期）

⁵⁴ 微软（2023 年）。

⁵⁵ 美国国防部（2023 年）。

等新兴技术实现。自 2022 年 9 月以来，英国陆军与一家私营公司合作，开发并推广了一种云分布式沉浸式陆战模拟，旨在为不同地点的实体和虚拟用户提供大规模的集体培训。⁵⁶此外，云计算还提供了在军事行动中进行大规模数据处理所必需的高速计算能力。鉴于军事数据的复杂性和庞大数量，云技术得以部署各种工具，帮助武装部队更有效地分析数据。这使他们能够在保持安全的同时，领先于快速发展的威胁。⁵⁷

不过，云技术也带来了潜在的威胁和挑战。将云计算融入军事行动引发了对数据安全的关切，尤其是在涉及第三方云服务提供商（CSP）的情况下。⁵⁸此外，连接问题（如偏远或具有挑战性环境中的高延迟）影响基于云的服务的可靠性，从而对运营效率和实时决策产生影响。最后，全球云技术竞争的加剧可能会成为国际紧张局势加剧的潜在催化剂，各国可能会寻求加强对先进云技术的出口管制，以符合其国家安全利益。⁵⁹

云计算：2023 年亮点

- 云计算继续推动一系列尖端应用的创新，包括大数据分析、机器学习、无服务器计算、AR 和 VR。目前，基于云的平台允许将 AI 即服务 (AIaaS) 进行外包，从而使获取变革性 AI 能力的途径民主化。
- 在军事领域，云技术可以借助 VR 或 AR 等新兴技术，为逼真的身沉浸式培训环境提供便利。云计算同样提供了 在军事行动中进行大规模数据处理所需的高速计算能力。不过，远程环境中的高延迟等连接问题可能会影响基于云的服务的可靠性。

4.2 边缘计算

边缘计算采用分布式计算模式，将数据存储和计算迁移到更靠近数据源或网络“边缘”的地方，而不是依赖基于云的集中式系统。

在边缘计算中，数据处理是在位于网络“边缘”的设备或本地服务器上进行的。当数据需要在中央云数据中心处理时，只传输关键信息。⁶⁰因此，边缘计算通过在本地图存和处理数据以及缓解云网络和数据中心的潜在瓶颈，最大限度地减少了延迟并提高了计算能力。这些优势对于需要实时处理的边缘设备尤为重要，这一点在物联网、自动驾驶汽车和 AR 等应用中显而易见。

⁵⁶ Hadean (2022 年)。

⁵⁷ 微软 (2023 年)。

⁵⁸ 有关云技术相关数据安全问题的进一步分析，请参见下文第 5.3 节。

⁵⁹ Hayashi 和 McKinnon (2023 年)。

⁶⁰ 微软 Azure (未注明日期)。

边缘计算的发展有可能改变军事部门的运作方式，增强通信、数据处理和决策能力。⁶¹实地部署边缘计算可实现连接在同一边缘网络内的部队之间的即时数据共享，从而促进实时通信和协调。它还能将计算资源带到军事行动的战术边缘，减少对云数据中心的依赖。来自现场的大型数据集，如用于监视和侦察的传感器数据和视频馈送，可在边缘位置进行本地分析，加快响应时间并改善对态势的感知。因此，在战场上采用边缘架构可以增强军事物联网（IoMT）应用，并使军事人员能够对潜在的危险情况做出快速反应。⁶²

边缘计算确保为互联网连接时断时续的偏远地区提供数据资源和计算，甚至在极端环境下运行。先进的人工智能分析可以在恶劣环境中完全离线的情況下在边缘平台上有效运行，从而为搜救行动等关键任务提供支持。⁶³然而，部署在 UAV、卫星和地面交通工具等军事边缘设备上的 AI 应用往往面临各种限制，而且由于处理速度、工作内存和电力的限制，可能不如最先进的模型。⁶⁴此外，亚马逊云计算服务（Amazon Web Services）最近推出了 AWS Snowblade，这是一款新的边缘计算产品，专为与美国国防部（DOD）签订的联合作战云能力（JWCC）合同而设计。⁶⁵AWS Snowblade 使 JWCC 的军事用户能够在可能遭受极端温度、振动或冲击的边缘地点开展行动。

然而，边缘计算给军事应用带来了一定的安全挑战。分布式计算框架可能会增加攻击面，为网络攻击提供更多端点。边缘计算容易受到一系列网络安全威胁，包括拒绝服务（DoS）攻击、侧信道攻击、恶意软件注入攻击以及身份验证和授权攻击。⁶⁶边缘计算设施还容易受到物理损坏的影响，可能导致边缘网络中断和数据泄露。⁶⁷为了解决这些漏洞，目前正在努力加强边缘计算系统的安全措施。例如，AWS Snowblade 边缘设备采用了先进的加密技术，以确保数据安全并防止潜在对手进行未经授权的访问。⁶⁸

⁶¹ Lee 等人（未注明日期）。

⁶² Cameron（2018 年）。

⁶³ Thomas（2021 年）。

⁶⁴ Miller 和 Lohn（2023 年）。

⁶⁵ AWS（2023 年）。

⁶⁶ Xiao 等人（2019 年）。

⁶⁷ 北约合作网络防御卓越中心（2022 年）。

⁶⁸ Konkel（2023 年）。

边缘计算：2023 年亮点

- 边缘计算有可能改变军事行动，增强通信、数据处理和决策能力。此外，在偏远或极端环境中，边缘计算在确保数据安全和提供必要计算资源方面发挥着至关重要的作用。
- 边缘平台使 AI 分析能够在具有挑战性的环境中离线高效运行，为搜救行动等关键任务提供支持。处理速度、内存和电力的限制会影响军事边缘设备上的 AI 应用。
- 军事边缘计算所面临的持续安全挑战包括网络攻击面的扩大和易受物理损坏。目前正在不断努力加强安全措施，如 AWS Snowblade 中的高级加密。

4.3 量子计算⁶⁹

量子计算是一个新兴领域，它利用量子力学原理来解决复杂性超出传统计算机能力的问题。

量子计算机超越传统计算机的潜力归功于独特的量子现象，特别是叠加和纠缠。量子比特是量子计算中的基本信息单位，由于叠加原理，它可以同时存在于多个状态中（0 和 1）。当量子比特纠缠时，一个量子比特的状态会与另一个量子比特的状态直接相关，而不管它们之间的物理距离有多远。利用量子纠缠可显著提高计算速度，这使得量子计算机能够比经典计算机更高效地执行特定计算。

量子计算领域取得了显著的进步。包括 IBM、谷歌/字母表和微软在内的私营公司已在实用量子计算机的研发方面投入巨资。例如，IBM 稳步增加了单个芯片上的量子比特数量。2023 年 12 月，IBM 发布了 Condor（秃鹫）处理器，该处理器拥有 1,121 个量子比特，与之前 433 量子比特的 Osprey（鱼鹰）处理器相比有了显著进步。⁷⁰与此同时，该公司还推出了迄今为止性能最优的量子处理器 Heron（苍鹭），拥有 133 个高质量量子比特。⁷¹值得注意的是，Heron 处理器能够与其他 Heron 处理器直接连接，这有可能促进量子计算机的可扩展性。⁷²

⁶⁹ 裁研所即将发布一份题为“量子新世界中的国际安全：入门”的报告，该报告将进一步分析量子计算领域及其对国际安全的相关影响。

⁷⁰ Gambetta（2023 年）。

⁷¹ 同上。

⁷² Brooks（2023 年 a）。

然而，尽管取得了上述进步，该领域仍在努力应对有待解决的重大挑战。其中一个关键问题被称为退相干，这是一种量子现象，是由于物理量子比特与其环境的隔离度不够造成的，会在计算中引入噪声。因此，克服退相干和纠正量子错误变得至关重要。⁷³此外，尽管数学证明表明量子比经典模型更有优势，但由于没有量子比特数量足够的量子计算机，因此仍然缺乏经验证据。⁷⁴例如，据研究人员估计，要在 8 小时内破解最先进的加密技术，需要 2,000 万个量子比特。⁷⁵

虽然量子计算的实际应用仍有待实现，但潜在的未来发展对军事实践和国际安全具有深远影响。量子计算有可能给各种技术领域带来革命性的变化，特别是在提升人工智能和机器学习方面。经典机器学习算法的成功往往依赖广泛的参数和大量的训练数据。相比之下，量子机器学习通过利用量子粒子可用的各种状态，可能减少所需的参数和数据量。⁷⁶实证研究表明，混合网络结合了经典计算机和量子计算机的特点，可以改进机器学习模型的训练。⁷⁷这些进步可能会改变未来的军事 AI 应用，特别是在开发更精确的致命性自主武器系统方面。⁷⁸

此外，量子计算可以重塑网络安全格局，带来挑战和机遇。量子计算机能够实现解决某些数学问题的远远快于比经典计算机，这可能会危及一些常用加密算法（如 RSA 和 ECC 加密算法）的安全性。能够解密数字通信的量子算法，特别是肖尔算法，已经开发出来，一旦有了实用的量子计算机，就可以执行。⁷⁹这就带来了新的网络安全漏洞，并可能引发先窃后破（HNDL）攻击，即恶意行为者会先窃取敏感的加密数据，意图在解密技术未来可能取得突破后再进行解码。这种攻击会导致国家安全问题，使对手能够获取敏感的军事信息。⁸⁰为了应对潜在的量子威胁，正在努力发展后量子密码学（PQC）。这涉及到创建能够抵御量子计算机未来攻击的加密系统。新兴的量子技术，如量子密钥分发（QKD）⁸¹和量子随机数发生（QRNG）⁸²，也为加强加密机制和安全通信提供了机会。

⁷³ Lidar（2023 年）。

⁷⁴ Brooks（2023 年 b）。

⁷⁵ 同上。

⁷⁶ 同上。

⁷⁷ Xu（2023 年）。

⁷⁸ 美国国会研究服务处（2023 年）。

⁷⁹ van Amerongen（2021 年）。

⁸⁰ 美国国会研究服务处（2023 年）。

⁸¹ 北约（2022 年）。

⁸² Argillander 等人（2023 年）。

量子计算：2023 年亮点

- 量子计算已经取得了显著的进步。例如，IBM 不断增加单个芯片上的量子比特数量，并在 2023 年推出拥有 1,121 量子比特的 Condor 处理器时达到了一个里程碑。与此同时，该公司还推出了 Heron 处理器，可直接与其他 Heron 处理器连接，从而可能增强可扩展性。
- 实证研究表明，结合经典计算机和量子计算机的混合网络可以改进机器学习模型的训练。这一发展对军事人工智能的应用，特别是对开发更精确的致命自主武器系统具有深远影响。
- 然而，量子计算的发展也带来了重大的网络和信息安全挑战，特别是先窃后破攻击的风险，因为实用的量子计算机有可能危及广泛使用的加密算法。因此，一直在努力发展后量子密码学，以应对新出现的量子威胁。

5.第 IV 类：基础设施

5.1 5G 和 6G

5G 代表第五代蜂窝网络技术标准，可提供超越 4G LTE 等前几代的先进宽带连接。**6G** 指的是正在开发的第六代蜂窝技术，旨在超越 5G，提供更先进的网络功能。

当前这一代连通基础设施的特点是无线技术的长足进步，特别是第五代（5G）蜂窝网络的广泛应用。5G 技术与前代技术相比具有各种优势，因为它具有网络切片等新功能，并能在毫米波（mmWave）频段，指 30-300GHz 的高频无线电频谱。⁸³5G 通过提供更快的速度、减少延迟、提高网络可靠性以及支持更多设备的并发连接，大大提升了连接性。5G 的这些创新能力有助于满足日益增长的技术创新需求，特别是在基于 IoT 的应用中，使更多设备和对象能够连接到网络。

5G 技术可以为变革性军事应用释放巨大潜力，促进战场上的通信强化、快速数据传输以及实时决策能力。其高速、低延迟的连接能力可支持从通信和后勤到 ISR 以及指挥和控制等关键军事职能。最近的研究强调了实施 5G 后可能实现的三项具体军事应用：使用智能标签跟踪物品和设备，以改进行动；利用高频段 5G 网络进行数据传输，以获取大型传感器数据集；以及使用远程 5G 通信

⁸³ Gerwig 和 Goss. (2023 年)。

进行指挥和控制，以加强多国协调。⁸⁴通过 5G 网络在货运中使用智能标签跟踪，还可能降低常规武器和弹药转移的相关风险，从而有望推进军备控制工作。此外，5G 还能成为军事领域 AI 和 IoT 尖端应用的强大催化剂，为增强能力铺平道路。高速 5G 网络可促进 AI 的集成，从而高效处理战场上的大量传感器数据。例如，对手信号可以通过安全的 5G 网络实时传输，以便利用先进的信号处理算法进行进一步分析。⁸⁵

然而，5G 技术的集成也带来了新的风险，尤其是在网络安全领域。随着 5G 网络中数据量和互联设备的激增，潜在的安全漏洞可能会被放大，为恶意行为者提供更多利用和扰乱的机会。5G 技术的特点，包括开放接口和基于云的特性，也带来了更多的安全威胁，导致 5G 部署面临存在广泛威胁的环境。⁸⁶在多个 5G 子系统中，可能会出现各种各样的网络安全威胁，这些子系统包括从 5G 用户设备和无线接入网(RAN)到核心网络、云服务和多接入边缘计算(MEC)等关键组件。⁸⁷

6G 蜂窝网络的开发目前正在进行中，其前景甚至比目前的 5G 技术所见证的进步更大。预计它将在速度、延迟和连接性方面带来进一步改进，并有能力实现更广泛的新型技术应用。与前几代通信网络相比，6G 的研发更加注重通过将地面蜂窝移动网络与空中和卫星平台相结合，实现“陆、海、空、天”的全面网络覆盖。⁸⁸这种卫星-地面综合网络架构应该会在确保全球互联网覆盖和为物联网提供无处不在的通信支持方面带来巨大潜力。⁸⁹6G 技术预计将于 2030 年左右开始推广。⁹⁰

5G 和 6G : 2023 年亮点

- 5G 技术目前取得的进展释放了军事应用中的变革潜力，为战场上增强通信、快速数据传输和实时决策提供了支持。5G 还能促进尖端 AI 和 IoT 应用的整合，从而增强军事能力。
- 然而，由于数据量和互联设备的增加，5G 技术的引入扩大了潜在的网络安全漏洞。开放接口及其基于云的特性也为 5G 部署创造了广泛的威胁环境。
- 目前正在进行的 6G 蜂窝网络研究和开发的重点是通过卫星-地面综合网络实现陆地、海洋、空中和太空的全面覆盖，预计将于 2030 年推出。

⁸⁴ Lee 等人 (2023 年)。

⁸⁵ Tucker (2022 年)。

⁸⁶ Śliwa 和 Suchański (2022 年)。

⁸⁷ 北约合作网络防御卓越中心 (2022 年)。

⁸⁸ Chen 等人。(2023 年)。

⁸⁹ Tirmizi 等人。(2022)。

⁹⁰ Kharpal (2023 年) 和 Chen 等人 (2023 年)。

5.2 物联网

物联网 (IoT) 将集成了传感器、软件和网络连接的物理设备、电器、交通工具和其他物体的广泛网络连接起来，促进了设备和系统之间的数据收集和交换。通过使这些设备能够通过互联网或其他通信网络相互通信和协作，IoT 创建了一个可远程监测和控制的互联生态系统。

物联网 (IoT) 领域的最新发展与其他领域的技术创新交织在一起，特别是边缘计算、5G 网络和集成人工智能。⁹¹边缘计算的兴起促进了一种更加本地化的数据处理和存储方法，有效地减少了延迟并提高了 IoT 设备的实时处理能力。⁹²与此同时，5G 网络的推出也通过提供更快的数据传输速度、更低的延迟和更大的网络容量，加快了 IoT 的发展。⁹³此外，AI 技术的集成，特别是机器学习的集成，可以支持对 IoT 应用生成的大量数据进行实时分析和解读，从而实现更高效的决策和自动化。

IoT 技术正越来越多地应用于军事系统，以优化操作并提高效率，这促进了军事领域向更加互联和数据驱动的方向转变。军事物联网 (IoMT) 可以利用部署在各个领域的各种传感器，旨在复杂多样的冲突环境中实现全面的态势感知和有效控制。⁹⁴将传感器网络和无人系统纳入 IoMT 框架，可以显著提高监视和侦察能力，使军队能够跟踪战场环境，管理装备和交通工具，并监测士兵的健康状况。⁹⁵在军事行动中，利用 IoT/IoMT 技术有可能提高目标定位的精确度，并最大限度地降低平民伤亡的风险，因为集成在 IoT/IoMT 网络中的传感器可以引导武器更准确地瞄准预定目标。⁹⁶

此外，IoT/IoMT 技术的进步也显著地改善了军事通信系统。IoT 促进了无缝数据共享和连接，从而加强了联合部队和联军之间以及不同领域之间的协作。⁹⁷此外，在支持 IoT 的系统中集成安全通信协议并使用加密和数字签名，可以有效保护通信渠道，确保敏感军事信息的保密性、完整性和可用性。⁹⁸然而，如果没有强大的通信协议，IoT 技术的广泛应用会给相互连接的军事系统带来巨大的网络安全威胁。IoMT 网络的攻击面很大，包括 IoMT 设备、连接这些设备的通信通道、IoMT 专用后端应用以及后端数据存储。⁹⁹涉及 IoT 设备的网络行动的影响可能超出军事系统的范围，有可能对其他互连系统造成无差别的破坏，包括医疗设施、教育机构和其他敏感网络。¹⁰⁰

⁹¹ Coughlin (2023 年)。

⁹² 有关边缘计算和最新发展的详细分析，请参见上文第 4.2 节。

⁹³ 有关 5G 蜂窝网络和最新发展的详细分析，请参见上文第 5.1 节。

⁹⁴ Withrington (2023 年)。

⁹⁵ Khawaja (2023 年)。

⁹⁶ Douglass (2022 年)。

⁹⁷ 突破防御 (2023 年)。

⁹⁸ Kannan 等人 (2023 年)。

⁹⁹ Withrington (2023 年)。

¹⁰⁰ Renals (2021 年)。

物联网：2023 年亮点

- IoT 技术正越来越多地应用于军事系统，以优化行动（被称为军事物联网）。IoMT 采用多种跨领域传感器，以实现全面的态势感知和控制。集成在 IoT/IoMT 网络中的传感器还可以提高军事行动的目标定位精确度，从而最大限度地降低平民伤亡风险。
- 然而，由于缺乏强大的通信协议，在军事系统中广泛采用 IoT 可能会带来网络安全风险。IoMT 网络创建了一个重大攻击面，其潜在影响超出了军事系统的范围，会影响到其他关键部门，包括医疗设施、教育机构和其他敏感网络。

5.3 云基础设施

云基础设施包括通过互联网提供云服务所必需的硬件和软件组件。这包括服务器、存储、网络组件和数据中心等硬件，以及虚拟化软件等软件。

云基础设施是构建和交付云计算服务的基础。¹⁰¹近年来，云服务不断扩展，私营公司作为云服务提供商（CSP）发挥着至关重要的作用。主要的 CSP 包括亚马逊云科技（AWS）、微软 Azure、谷歌云、甲骨文云和阿里云。它们提供多种多样的云服务，主要分为三类：基础设施即服务（IaaS）、平台即服务（PaaS）和软件即服务（SaaS）。CSP 继续在全球范围内迅速扩大其云基础设施的覆盖范围，在各大洲都建立了存在。¹⁰²

云技术越来越多地用于提高军事环境中的行动效率和数据管理。军队不仅开发了其内部云基础设施，还引入了私营 CSP 的商业云功能和服务。例如，2022 年 12 月，美国国防部向四家领先的 CSP（AWS、谷歌、微软和甲骨文）授予了合同，以支持 DOD 的联合作战云能力。¹⁰³云基础设施使军队能够存储和管理大量军事数据，从 ISR 数据到后勤信息和其他关键任务数据。这可以促进来自不同地点的军事人员和部队之间的沟通和协调。

在军事领域部署云技术时，确保数据安全一直是一个重要的考虑因素。云基础设施通常通过强大的加密、身份和访问管理以及其他先进的安全功能，为敏感信息提供更高的安全性。值得注意的是，乌克兰政府积极主动地将其重要数据的很大一部分迁移到云端，从而改进了该国为抵御前所

¹⁰¹ 有关云计算和最新发展的详细分析，请参见上文第 4.1 节。

¹⁰² 八大云服务提供商的全球云基础设施地图：<https://www.cloudinfrastructuremap.com/>

¹⁰³ 美国国防部（2022 年）。

未有的网络攻击所做的准备。¹⁰⁴政府和 CSP 都在继续加强其云基础设施的安全措施，包括在云计算环境中采用零信任方法。¹⁰⁵

不过，云环境与其他数字平台一样，仍然容易受到潜在网络风险和脆弱性的影响。将敏感数据转移到云系统会加剧安全问题，以前的云安全事件就是证明。2023 年 2 月，由于微软 Azure 政府云平台上的电子邮件服务器配置错误，大量敏感的军事电子邮件被曝光。¹⁰⁶虽然利用主要 CSP 的商业云服务具有强大的安全协议和高度集中的专业知识的优势，但它也带来了一种可能性，即影响这些提供商的云基础设施的事件产生广泛的影响。¹⁰⁷此外，红十字国际委员会（ICRC）强调，在武装冲突期间，平民越来越多地参与数字行动，这可能导致越来越多地将包括云基础设施在内的民用基础设施用于军事目的。¹⁰⁸这种趋势增加了平民和民用基础设施成为攻击目标的风险，破坏了普遍支持的区分原则。¹⁰⁹

云基础设施：2023 年亮点

- 军队越来越多地采用云基础设施来提升运作效率和数据管理。虽然目前正在落实先进的安全措施，如强大的加密技术，但是，正如过往事件所证明的，在军事环境中集成云环境仍然容易受到网络风险的影响。
- 此外，ICRC 强调，在武装冲突期间，平民越来越多地参与数字行动，这可能会增加为军事目的使用包括云基础设施在内的民用基础设施。这增加了平民和民用基础设施成为袭击目标的风险，破坏了区分原则。

5.4 卫星通信

卫星通信涉及利用人造卫星在地球上不同地点之间建立通信联系。

卫星通信系统在确保全球互联网覆盖、弥合数字鸿沟和提高连接基础设施的复原力方面发挥着至关重要的作用，特别是在传统地面通信网络受到限制或无法使用的地区。卫星技术是军事行动不可或缺的一部分，该领域的不断进步持续推动着国防部门的创新。目前，低地球轨道（LEO）卫星星座部署的增加预计将大大提高绕地球轨道运行的卫星数量。与传统的地球同步卫星相比，

¹⁰⁴ Lewis（2023 年）。

¹⁰⁵ 美国国防部（2023 年）。

¹⁰⁶ Martin 等人（2023 年）。

¹⁰⁷ Maurer 和 Hinck（2020 年）。

¹⁰⁸ 红十字国际委员会（2023 年）。

¹⁰⁹ 同上。

LEO 上由较小卫星组成的大型星座可显著降低延迟，提高带宽容量，并提供稳定的全球覆盖。私营实体在 LEO 卫星的发展中处于主导地位，其中包括美国太空探索技术公司的星链、一网和亚马逊的柯伊伯计划。¹¹⁰

军队可利用 LEO 系统提供的更强连接性实现实时数据传输，从而提高军事行动的精确性和效率。正如在俄罗斯和乌克兰冲突中观察到的那样，美国太空探索技术公司的 LEO 卫星星座星链在促进乌克兰民用和军用关键通信方面发挥了至关重要的作用，包括部署在无人机上进行监视和侦察。¹¹¹除国防应用外，LEO 星座还有可能弥合全球数字鸿沟，在传统地面基础设施难以部署的偏远或农村地区提供高速互联网。¹¹²

卫星通信领域内另一项引人注目的创新是量子技术的整合。量子密钥分发（QKD）可通过应用量子力学原理来创建和交换双方之间的加密密钥，从而确保卫星通信的安全。2022 年 9 月，欧洲航天局宣布与欧盟委员会以及 20 多家欧洲航天公司合作，在该地区推出首个天基 QKD 系统，即 Eagle-1 卫星。¹¹³该卫星支持连接系统将为欧洲的超安全网络铺平道路。与此同时，包括中国¹¹⁴和新加坡¹¹⁵在内的国家也在努力开发 QKD 技术，以加强卫星通信的安全性。

卫星技术为全球连接和安全通信开启了巨大的可能性，也带来了一系列安全问题。其中一项挑战与卫星系统易受网络威胁和潜在数据泄露影响有关。卫星通信在传输对军事行动至关重要的敏感信息方面是不可或缺的，任何对系统的破坏都会导致重大的战略劣势。军用卫星通信系统已成为网络攻击的目标，可以导致关键服务停止和中断。¹¹⁶在轨卫星的部署，特别是大量 LEO 卫星的部署，也会带来安全问题，如与空间交通和日益增多的空间碎片有关的问题，这对空间安全和可持续性构成威胁。¹¹⁷此外，鉴于私营实体在卫星通信领域发挥着举足轻重的作用，军队将继续利用商业技术为自己谋利。不过，冲突期间关键通信基础设施对商业行为者的依赖，凸显了私营和公共实体之间在激励机制、运作原则和问责机制方面的差异所带来的潜在隐患。¹¹⁸

¹¹⁰ Borowitz (2022 年)。

¹¹¹ Jayanti (2023 年)。

¹¹² Marquina (2022 年)。

¹¹³ 欧空局 (2022 年)。

¹¹⁴ Laursen (2022 年)。

¹¹⁵ SpeQtral (2022 年)。

¹¹⁶ Menn (2023 年)。

¹¹⁷ Mukherjee (2021 年)。

¹¹⁸ Jayanti (2023 年)。

卫星通信：2023 年亮点

- 卫星通信领域的重大创新包括美国太空探索技术公司的星链等由私营实体主导的 LEO 卫星星座激增。这些不仅有助于改善全球连接，还能在冲突期间促进关键通信，从而在军事行动中发挥至关重要的作用。此外，将量子密钥分发技术融入卫星系统还为实现更安全的通信铺平了道路。
- 不过，卫星通信也可能带来安全挑战，包括面对网络威胁以及空间碎片问题的脆弱性。此外，随着军队继续利用商业卫星技术，关键是要强调与公共和私营实体之间的激励措施、运作原则和问责机制差异有关的潜在隐患。

6.结论

在本文审查的技术领域中，出现了若干总体趋势和发展。特别是，硬件技术的一个持续趋势是不断微型化，从而创造出越来越紧凑和高效的设备。最近在半导体材料、纳米技术、微芯片和传感器方面取得的突破都在推动这一变革性转变方面发挥了关键作用。这一趋势正在推动军事武器和系统广泛采用使能技术，从而促进军事装备的现代化。

利用使能技术将显著提升各种军事能力。其中包括更加了解局势、精简指挥和控制、加快数据传输和处理，以及提高先进武器的精确度。值得注意的是，某些使能技术，如微芯片、云计算和量子计算，成为军事应用创新的催化剂。它们促进了 AI 和机器学习能力等变革性技术的整合，进一步提升了军事行动的进步潜力。此外，使能技术有可能通过加强裁军核查和冲突监测机制来加强国际安全努力。例如，可以通过使用先进的传感器来检测环境中的化学和生物制剂，并监测对和平协议的遵守情况。

然而，近期使能技术的进步也带来了重大风险和挑战。虽然云技术和量子密钥分发方面的创新可以提高通信、信息存储和数据处理的安全性，但大规模部署使能技术会增加对网络安全风险的脆弱性。技术领域的扩展可能会扩大攻击面，给保护军事系统免受潜在网络威胁带来更多挑战。尤其是量子计算，由于其预期的密码破译能力，它有可能破坏广泛使用的加密协议和标准。

此外，追求使能技术的尖端创新有可能加剧国际紧张局势，助推国家间的技术竞争。各国可根据其国家安全利益，对先进技术实行严格的出口管制。此外，供应链的脆弱性也构成了使能技术领域的一个重大挑战。微芯片等硬件元件的供应链是一个高度全球化的复杂网络，全球某些地区具有高度集中的生产专业化。无论是地缘政治紧张局势还是自然灾害对这些地区制造能力的破坏，都会对技术的可用性产生负面影响，并影响国际安全。

最后，许多技术领域的发展凸显了私营部门所发挥的关键作用。私营公司一直在推动各种技术应用领域的进步和创新，包括云技术、卫星通信和量子计算。军队早已开始与私营实体合作，以利用最先进的技术，但这种参与并非没有风险。对私营公司基础设施造成影响的事件可能会产生广泛的影响，敏感的军事信息也面临被泄露的风险。由于私营实体和公共实体在激励机制、运作原则和问责机制方面存在差异，对私人行为者的依赖还可能导致潜在隐患。

使能技术的进步将继续对军事实践和国际安全产生重大影响。这就有必要持续对新的和正在出现的趋势进行前景扫描，并进一步审查潜在治理框架，以便在利用机遇的同时降低风险。在今后的研究项目中，裁研所将继续查明和审查新技术和新兴技术，以及更加成熟的技术的新型应用，并提供面向行动的政策建议，以有效地治理不同技术类别。

参考文献

亚马逊云科技 (AWS)。2023 年。“宣布 AWS Snowblade 在美国上市国防部 JWCC 客户”。6 月 6 日。截至 2023 年 12 月 6 日：<https://aws.amazon.com/about-aws/whats-new/2023/06/aws-snowblade-us-defense-jwcc-customers/>

作者不明。未注明日期。“云原生是什么？”。截至 2023 年 12 月 6 日：<https://aws.amazon.com/what-is/cloud-native/>

Arcuri, Gregory 和 Sujai Shivakumar。2022 年。“摩尔定律及其实际意义”。战略与国际问题研究中心。10 月 18 日。截至 2023 年 12 月 6 日：<https://www.csis.org/analysis/moores-law-and-its-practical-implications>

Argillander, Joakim 等人。2023 年。“基于钙钛矿发光二极管的量子随机数字生成”。《通讯物理学》6, 157。截至 2023 年 12 月 6 日：<https://doi.org/10.1038/s42005-023-01280-3>

ASML。未注明日期。“EUV 光刻系统”。截至 2023 年 12 月 6 日：<https://www.asml.com/en/products/euv-lithography-systems>

Avtar, Ram 等人。2021 年。“遥感促进国际和平与安全：其作用和影响”。《遥感》13, 3: 439。截至 2023 年 12 月 6 日：<https://doi.org/10.3390/rs13030439>

Basheer, Taha 等人。2022 年。“纳米技术与计算机科学：趋势与进展”。《存储器——材料、设备、电路和系统》2, 10 月。截至 2023 年 12 月 6 日：<https://doi.org/10.1016/j.memori.2022.100011>

Borowitz, Mariel。2022 年。“轨道上小型卫星的军事用途”。法国国际关系研究所。3 月 4 日。截至 2023 年 12 月 6 日：https://www.ifri.org/sites/default/files/atoms/files/m._borowitz_military_use_small_satellites_in_orbit_03.2022.pdf

突破防御。2023 年。“当我们谈论什么将使 JADC2 成为可能时，我们真正谈论的是作战物联网”。3 月 22 日。截至 2023 年 12 月 6 日：<https://breakingdefense.com/2023/03/when-we-talk-about-what-will-enable-jadc2-were-really-talking-about-the-internet-of-warfighting-things/>

Brooks, Michael。2023a。“量子计算的下一步”。《麻省理工学院科技评论》。1 月 6 日。截至 2023 年 12 月 6 日：<https://www.technologyreview.com/2023/01/06/1066317/whats-next-for-quantum-computing/>

Brooks, Michael。2023b。“量子计算机：它们有何裨益？”《自然》。5 月 24 日。截至 2023 年 12 月 6 日：<https://www.nature.com/articles/d41586-023-01692-9>

Cameron, Lori。2018 年。“物联网与军事和战场的结合：连接装备和生物识别可穿戴设备，实现 IoMT 和 IoBT”。IEEE 计算机协会。3 月 1 日。截至 2023 年 12 月 6 日：

<https://www.computer.org/publications/tech-news/research/internet-of-military-battlefield-things-iomt-iobt>

Chandler, David L。2022 年。“最好的半导体？”《麻省理工学院新闻》。7 月 21 日。截至 2023 年 12 月 6 日：<https://news.mit.edu/2022/best-semiconductor-them-all-0721>

Chen, Zhi 等人。2023 年。“专家对 6G 技术的看法”。《中国日报》。8 月 7 日。截至 2023 年 12 月 6 日：https://www.chinadaily.com.cn/a/202308/07/WS64d01ddca31035260b81a8d3_1.html

Clynes, Tom。2023 年。“高温超导体的五大理念”。IEEE Spectrum。9 月 18 日。截至 2023 年 12 月 6 日：<https://spectrum.ieee.org/high-temperature-superconductors>

Coggins, Kevin 等人。未注明日期。“量子传感：在全球定位系统缺失的环境中维持 PNT 的新方法”。《美国海军学会》。截至 2023 年 12 月 6 日：

<https://www.usni.org/magazines/proceedings/sponsored/quantum-sensing-new-approach-maintaining-pnt-gps-denied>

Coughlin, Tom。2023 年。“2023 年及以后值得关注的 9 大 IoT 趋势”。TechTarget。7 月 12 日。截至 2023 年 12 月 6 日：<https://www.techtarget.com/iotagenda/opinion/IoT-trends-to-keep-an-eye-on>

Douglass, Robert。2022 年。“导言：IoT 促进国防和国家安全”。载于《IoT 促进国防和国家安全》（R. Douglass、K. Gremban、A. Swami 和 S. Gerali 编辑）。截至 2023 年 12 月 6 日：

<https://doi.org/10.1002/9781119892199.fmatter>

Eshel, Tamir。2022 年。“陆地战车的传感器融合”。《欧洲安全与防务》。4 月 26 日。截至 2023 年 12 月 6 日：<https://euro-sd.com/2022/04/articles/exclusive/25763/sensor-fusion-for-land-combat-vehicles/>

欧洲航天局（欧空局）。2022 年。“量子加密促进欧洲的自主”。9 月 22 日。截至 2023 年 12 月 6 日：

https://www.esa.int/Applications/Connectivity_and_Secure_Communications/Quantum_encryption_to_boost_European_autonomy

Fadelli, Ingrid。2023 年。“研究人员展示了将对齐碳纳米晶体管扩展至低于 10 纳米节点的技术”。Phys.org。7 月 27 日。截至 2024 年 1 月 3 日：<https://phys.org/news/2023-07-scaling-aligned-carbon-nanotube-transistors.html>

Feldman, Andrey。2023 年。“新型超导体可能带来量子计算突破”。《先进科学新闻》。7 月 18 日。截至 2023 年 12 月 6 日：<https://www.advancedsciencenews.com/new-superconductor-could-lead-to-quantum-computing-breakthrough/>

Gambetta, Jay。2023 年。“量子公用事业时代的硬件和软件已然就绪”。IBM。12 月 4 日。截至 1 月 11 日：<https://www.ibm.com/quantum/blog/quantum-roadmap-2033>

Gargeyas, Arjun。2022 年。“半导体在军事和国防技术中的作用”。《国防与外交》杂志 11, 2 (1-3 月)。截至 2023 年 12 月 6 日：<https://capsindia.org/wp-content/uploads/2022/07/DD-Journal-January-March-2022-Arjun-Gargeyas.pdf>

Gerwig, Kate 和 Michaela Goss。2023 年。“5G 关键术语和短语必备词汇表”。TechTarget。10 月 19 日。截至 2023 年 12 月 6 日：<https://www.techtarget.com/searchnetworking/feature/The-essential-5G-glossary-of-key-terms-and-phrases>

Gilchrist, Karen。2023 年。“在存在制裁的情况下，美国微芯片如何在助力俄罗斯军队”。CNBC。8 月 7 日。截至 2023 年 12 月 6 日：<https://www.cnbc.com/2023/08/07/how-us-microchips-are-fueling-russias-military-despite-sanctions.html>

Giles, Martin。2019 年。“修复芯片中的网络安全漏洞仍需太长时间”。《麻省理工学院科技评论》。6 月 3 日。截至 2023 年 12 月 6 日：
<https://www.technologyreview.com/2019/06/03/135108/cybersecurity-flaws-in-chips-are-taking-too-long-to-fix/>

谷歌。未注明日期。“云原生是什么？”。截至 2023 年 12 月 6 日：
<https://cloud.google.com/learn/what-is-cloud-native>

Hadean。2022 年。“Hadean 获得英国陆军建造模拟探路者的合同”。7 月 14 日。截至 2023 年 12 月 6 日：<https://hadean.com/news/hadean-awarded-british-army-contract-to-build-simulation-pathfinder/>

Hamblen, Matt。2023 年。“Stephanie Brown 谈士兵佩戴传感器以获取重要数据”。Fierce Electronics。6 月 6 日。截至 2023 年 12 月 6 日：
<https://www.fierceelectronics.com/sensors/tesla-recalls-2-million-cars-software-update-provide-visual-and-audible-alerts>

Hamza, Ekhlas Kadum 和 Shahad Nafea Jaafar。2022 年。“无线通信系统中的纳米技术应用”。载于《电子应用中的纳米技术——材料地平线：从自然到纳米材料》。施普林格，新加坡。截至 2023 年 12 月 6 日：https://doi.org/10.1007/978-981-16-6022-1_6

Hayashi, Yuka 和 John D. McKinnon。2023 年。“美国期望限制中国使用云计算以保护先进技术”。7 月 4 日。截至 2023 年 12 月 6 日：<https://www.wsj.com/articles/u-s-looks-to-restrict-chinas-access-to-cloud-computing-to-protect-advanced-technology-f771613>

Hecht, Jeff。2022 年。“纳米材料为下一代计算铺平道路”。《自然》。8 月 10 日。截至 2023 年 12 月 6 日：<https://www.nature.com/articles/d41586-022-02147-3>

IBM。2023 年。“为什么芯片的未来需要 EUV 光刻技术”。6 月 26 日。截至 2023 年 12 月 6 日：
<https://research.ibm.com/blog/what-is-euv-lithography>

电气和电子工程师协会（IEEE）。未注明日期。“半导体性能的未来”。截至 2023 年 12 月 6 日：
<https://irds.ieee.org/topics/future-of-semiconductor-performance>

未注明日期。“半导体材料”。截至 2023 年 12 月 6 日：
<https://irds.ieee.org/topics/semiconductor-materials>

英特尔公司，未注明日期。“英特尔®4004 的故事”。截至 2023 年 12 月 6 日：
<https://www.intel.com/content/www/us/en/history/museum-story-of-intel-4004.html>

Jayanti, Amritha。2023 年。“星链与俄乌战争：商业技术与公共目的案例？”《分析与观点》，哈佛大学肯尼迪学院贝尔福科学与国际事务中心。3 月 9 日。截至 2023 年 12 月 6 日：
<https://www.belfercenter.org/publication/starlink-and-russia-ukraine-war-case-commercial-technology-and-public-purpose>

Kannan, B. Maruthu 等人。2023 年。“利用加密技术确保军事应用中支持 IoT 的嵌入式系统中的安全通信”，2023 年第二届边缘计算与应用国际会议（ICECA），印度纳马卡尔，第 1385 至第 1389 页。截至 2023 年 12 月 6 日：
<https://doi.org/10.1109/ICECAA58104.2023.10212400>

Khan, Saif M.和 Alexander Mann。2020。“AI 芯片：它们是什么以及它们为什么重要”。安全与新兴技术中心。四月。截至 2023 年 12 月 6 日：
<https://cset.georgetown.edu/publication/ai-chips-what-they-are-and-why-they-matter/>

Kharpal, Arjun。2023 年。“电信业老板们称下一代移动互联网——6G——将于 2030 年推出，即使 5G 普及率仍处于低位”。CNBC。3 月 7 日。截至 2023 年 12 月 6 日：
<https://www.cnbc.com/2023/03/08/what-is-6g-and-when-will-it-launch-telco-execs-predict.html>

Khawaja, Saleem。2023 年。“IoT 在国防应用中的军事用途如何不断扩大”。《陆军技术》。3 月 28 日。截至 2023 年 12 月 6 日：
<https://www.army-technology.com/sponsored/how-military-uses-of-the-iot-for-defence-applications-are-expanding/>

Konkel, Frank。2023 年。“AWS 面向极端环境下国防客户推出边缘设备”。Nextgov/FCW。6 月 8 日。截至 2023 年 12 月 6 日：
<https://www.nextgov.com/digital-government/2023/06/aws-unveils-edge-device-defense-customers-most-extreme-environments/387302/>

Kullock, René 等人。2020。“用于光的电驱动八木乌达天线”。《自然通讯》11，115。截至 2023 年 12 月 6 日：
<https://doi.org/10.1038/s41467-019-14011-6>

Kumah, Elizabeth Adjoa 等人。2023 年。“纳米粒子对人类和环境的影响：当前文献范围综述”。《BMC 公共卫生》23，1059。截至 2023 年 12 月 6 日：
<https://doi.org/10.1186/s12889-023-15958-4>

Laursen, Lucas。2022 年。“随着中国量子密钥加密卫星的缩小，其联网能力却在增长”。IEEE Spectrum。8 月 25 日。截至 2023 年 12 月 6 日：<https://spectrum.ieee.org/satellite-qkd-china>

Lee, Ki 等人。未注明日期。“战术边缘的分散决策”。Booz Allen。截至 2024 年 1 月 6 日：<https://www.boozallen.com/s/insight/blog/decentralized-decision-making-at-the-tactical-edge.html>

Lee, Mary 等人。2023 年。“欧洲 5G 军事应用的机遇与风险”。加利福尼亚州圣莫尼卡：兰德公司。截至 2023 年 12 月 6 日：https://www.rand.org/pubs/research_reports/RRA1351-2.html

Lee, Sukbae 等人。2023a。“第一个室温常压超导体”。arXiv。7 月 22 日截至 2023 年 12 月 6 日：<https://arxiv.org/abs/2307.12008>

—2023b。“超导体 $\text{Pb}_{10-x}\text{Cu}_x(\text{PO}_4)_6\text{O}$ 在室温和大气压力下的悬浮现象及其机理”。arXiv。7 月 22 日截至 2023 年 12 月 6 日：<https://arxiv.org/abs/2307.12037>

Levine, Edlyn V.和 Alirde Pipikaite。2019 年。“硬件是一种网络安全风险。我们对此需要知道的事”。世界经济论坛。12 月 19 日。截至 2023 年 12 月 6 日：<https://www.weforum.org/agenda/2019/12/our-hardware-is-under-cyberattack-heres-how-to-make-it-safe/>

Lewis, James Andrew。2023 年。“加快联邦云的采用，以实现现代化和安全”。战略与国际研究中心（CSIS）。7 月 28 日。截至 2023 年 12 月 6 日：<https://www.csis.org/analysis/accelerating-federal-cloud-adoption-modernization-and-security>

Lidar, Daniel。2023 年。“一位科学家解释标志着量子计算机到来的一个临近里程碑”。Phys.org。11 月 20 日。截至 2023 年 12 月 6 日：<https://phys.org/news/2023-11-scientist-approaching-milestone-quantum.html>

Macri, Kate。2022 年。“陆军正在对传感器进行现代化改造，以实现数据驱动型决策”。GovCIO 媒体与研究。3 月 4 日。截至 2023 年 12 月 6 日：<https://governmentciomedia.com/army-modernizing-sensors-data-driven-decision-making>

Marquina, Claudia。2022 年。“低地球轨道卫星技术如何连接未连接者”。2 月 18 日截至 2023 年 12 月 6 日：<https://www.weforum.org/agenda/2022/02/explainer-how-low-earth-orbit-satellite-technology-can-connect-the-unconnected/>

Marr, Bernard。2023 年。“2024 年每个人都必须准备好迎接的 10 大云计算趋势”。《福布斯》。10 月 9 日。截至 2023 年 12 月 6 日：<https://www.forbes.com/sites/bernardmarr/2023/10/09/the-10-biggest-cloud-computing-trends-in-2024-everyone-must-be-ready-for-now/?sh=7ab779e66d67>

Martin, Peter 等人。2023 年。“五角大楼和微软正在调查军方电子邮件泄露事件”。彭博社。2 月 22 日截至 2023 年 12 月 6 日：<https://www.bloomberg.com/news/articles/2023-02-22/pentagon-and-microsoft-investigating-leak-of-military-emails>

Maurer, Tim 和 Garrett Hinck。2020。“云安全：决策者入门”。卡内基国际和平基金会。八月。截至 2023 年 12 月 6 日：https://carnegieendowment.org/files/Maurer_Hinck_Cloud_Security-V3.pdf

Menn, Joseph。2023 年。“网络攻击导致俄罗斯军方卫星通信中断”。《华盛顿邮报》6 月 30 日截至 2023 年 12 月 6 日：<https://www.washingtonpost.com/technology/2023/06/30/satellite-hacked-russian-military/>

微软 2023 年。“BAE 系统公司与微软联手为国防项目装备创新云技术”。4 月 14 日截至 2023 年 12 月 6 日：<https://news.microsoft.com/en-gb/2023/04/14/bae-systems-and-microsoft-join-forces-to-equip-defence-programmes-with-innovative-cloud-technology/>

微软 Azure。未注明日期。“边缘计算是什么？”截至 2023 年 12 月 6 日：<https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-edge-computing>

Miller, Kyle 和 Andrew Lohn。2023 年。“机载 AI：约束与限制”。安全与新兴技术中心（CSET）。八月。截至 2024 年 1 月 6 日：<https://cset.georgetown.edu/publication/onboard-ai-constraints-and-limitations/>

《麻省理工学院技术评论》洞察。2023 年。“多晶粒系统决定半导体的未来”。3 月 31 日。截至 2023 年 12 月 6 日：<https://wp.technologyreview.com/wp-content/uploads/2023/03/Synopsys-Report-v6.pdf>

Moore, Samuel K。2022 年。“3D 芯片技术颠覆计算的 3 种方式”。IEEE Spectrum。3 月 16 日。截至 2023 年 12 月 6 日：<https://spectrum.ieee.org/amd-3d-stacking-intel-graphcore>

Mukherjee, Supantha。2021。“我们应该担心空间碎片吗？科学家解释”。世界经济论坛。11 月 24 日截至 2023 年 12 月 6 日：<https://www.weforum.org/agenda/2021/11/space-debris-satellite-international-space-station/>

国家研究能力中心（NCCR）。2021。“在二维过渡金属氮化钨中发现超导性和高临界温度”。Phys.org。5 月 5 日。截至 2023 年 12 月 6 日：<https://phys.org/news/2021-05-superconductivity-high-critical-temperature-2d.html>

北约。2022 年。“利用量子技术确保通信安全”。9 月 27 日。截至 2023 年 12 月 6 日：https://www.nato.int/cps/en/natohq/news_207634.htm

北约合作网络防御卓越中心 (CCDCOE)。2022 年。“军事行动：5G 网络带来的风险”。研究报告。截至 2023 年 12 月 6 日：https://ccdcoe.org/uploads/2022/06/Report_Military-Movement-Risks-from-5G-Networks.pdf

Pedram, Massoud。2023 年。“室温超导体可彻底改变电子技术——一位电气工程师解释材料的潜力”。The Conversation。3 月 28 日。截至 2023 年 12 月 6 日：<https://theconversation.com/room-temperature-superconductors-could-revolutionize-electronics-an-electrical-engineer-explains-the-materials-potential-201849>

Ray, Paresh 等人。2009 年。“纳米材料的毒性与环境风险：挑战与未来需求”。《环境科学与健康杂志》，C 部分，27:1，1-35。截至 2023 年 12 月 6 日：<https://doi.org/10.1080/10590500802708267>

Renals, Pete。2021。“军事网络行动的未来发展及其对平民伤害风险的影响”。红十字国际委员会人道主义法律与政策。6 月 24 日。截至 2023 年 12 月 6 日：<https://blogs.icrc.org/law-and-policy/2021/06/24/future-military-cyber-operations/>

Roa, Carlos。2023 年。“我们创造了魔法石吗？决策者应关注室温超导体”。《国家利益》。8 月 2 日截至 2023 年 12 月 6 日：<https://nationalinterest.org/feature/have-we-created-philosopher%E2%80%99s-stone-policymakers-should-care-about-room-temperature>

Rowland, Clare E 等人。2016。“基于纳米材料的生物危害物剂探测传感器”。《今日材料》，19，8，10 月。截至 2023 年 12 月 6 日：<https://doi.org/10.1016/j.mattod.2016.02.018>

Ryugen, Hideaki。2023 年。“台积电将在台湾南部新厂生产最先进的 2 纳米芯片”。《日经亚洲》。8 月 10 日。截至 2023 年 12 月 6 日：<https://asia.nikkei.com/Business/Tech/Semiconductors/TSMC-to-make-cutting-edge-2-nm-chips-at-new-plant-in-southern-Taiwan>

三星。2022 年。“三星开始采用 3 纳米 GAA 架构制程技术生产芯片”。截至 2023 年 12 月 6 日：<https://news.samsung.com/global/samsung-begins-chip-production-using-3nm-process-technology-with-gaa-architecture>

SpeQtral。2022 年。“SpeQtral 宣布 SpeQtral-1 量子卫星用于超安全通信任务”。2 月 9 日。截至 2023 年 12 月 6 日：<https://speqtralquantum.com/newsroom/speqtral-announces-speqtral-1-quantum-satellite-mission-for-ultra-secure-communications>

Shilov, Anton。2023 年。“定制硅的黄金时代临近”。《电子工程专辑》。7 月 26 日。截至 2023 年 12 月 6 日：<https://www.eetimes.com/the-golden-age-of-custom-silicon-draws-near/>

Śliwa, Joanna 和 Marek Suchański。2022 年。“军事 5G 系统中的安全威胁与对策”，第 24 届国际微波与雷达会议 (MIKON)，波兰格但斯克，第 1 至第 6 页。截至 2023 年 12 月 6 日：<https://doi.org/10.23919/MIKON54314.2022.9924818>

台湾积体电路制造股份有限公司 (TSMC) 。未注明日期。“3 纳米技术”。截至 2023 年 12 月 6 日：https://www.tsmc.com/english/dedicatedFoundry/technology/logic/l_3nm

Thomas, Arthur。2021。“搜救行动战术边缘的 AI”。微软 6 月 22 日。截至 2023 年 12 月 6 日：<https://www.microsoft.com/en-us/industry/blog/government/2021/06/22/ai-at-the-tactical-edge-for-search-rescue-operations/>

Tirmizi, Syed Bilal Raza 等人。2022 年。“面向 6G 的卫星——地面混合网络：关键技术和未决问题”。传感器 22, no.21: 8544.<https://doi.org/10.3390/s22218544>

Tucker, Patrick。2022 年。“军方将如何使用 5G？一项新的无人机实验提供了线索”。防务一号。9 月 28 日。截至 2023 年 12 月 6 日：<https://www.defenseone.com/technology/2022/09/how-will-military-use-5g-new-drone-experiment-offers-clues/377745/>

英国国防科学技术实验室。2022 年。“传感：国防科学技术能力”。3 月 31 日。截至 2023 年 12 月 6 日：<https://www.gov.uk/guidance/sensing-defence-science-and-technology-capability>

英国国家量子技术计划。未注明日期。“用量子潜望镜观察周围角落”。截至 2023 年 12 月 6 日：<https://uknqt.ukri.org/wp-content/uploads/2021/10/Look-Around-Corners-With-The-Quantum-Periscope.pdf>

联合国大会 (UNGA) 。2023 年。“当前科学技术的发展及其对国际安全与裁军努力的潜在影响”。联合国 A/78/268 号文件，8 月 1 日。

美国国会研究服务处。2023 年。“国防入门：量子技术”。10 月 25 日截至 2023 年 12 月 6 日：<https://crsreports.congress.gov/product/pdf/IF/IF11836>

美国国防部。2022 年。“美国国防部宣布采购联合作战云能力”。12 月 7 日。截至 2023 年 12 月 6 日：<https://www.defense.gov/News/Releases/Release/Article/3239378/department-of-defense-announces-joint-warfighting-cloud-capability-procurement/>

—。2023 年。“美国国防部在云计算方面取得进展”。3 月 29 日。截至 2023 年 12 月 6 日：<https://www.defense.gov/News/News-Stories/Article/Article/3345260/dod-makes-headway-on-cloud-computing/>

美国国家纳米技术协调办公室。““纳米”有何特别之处？”截至 2023 年 12 月 6 日：<https://www.nano.gov/about-nanotechnology/what-is-so-special-about-nano>

van Amerongen, Michiel。2021。“量子技术在国防和安全领域的应用”。《北约评论》。6 月 3 日。截至 2023 年 12 月 6 日：<https://www.nato.int/docu/review/articles/2021/06/03/quantum-technologies-in-defence-security/index.html>

Withrington, Claire。2023 年。“军事物联网”。The Cove。8 月 24 日。截至 2023 年 12 月 6 日：<https://cove.army.gov.au/article/internet-military-things>

Xiao, Yinhao 等人。2019 年。“边缘计算安全：技术现状与挑战”，《电气与电子工程师协会会报》107, n8, 第 1608 至第 1631 页，8 月。截至 2023 年 12 月 6 日：
<https://doi.org/10.1109/JPROC.2019.2918437>

Xu, Tammy。2023 年。“利用量子计算机建立更好的机器学习模型”。IEEE Spectrum。11 月 15 日
截至 2023 年 12 月 6 日：<https://spectrum.ieee.org/quantum-machine-learning-terra-quanta>