2022 2 24

46

RAND Corporation 2035

GLONASS
GPS Himars “
” Excalibur House of
Commons Library, UK Parliament

Contents

SecurityInfoWatch https://www.securityinfowatch.com/perimeter-security/robotics/anti-drone-technologies/article/21277392/weaponization-of-commercial-drones-is-a-global-threat)

无人机不仅用于侦察，也成为反恐行动的首选武器

不精准的特征空袭 (signature strike)

使用无人机的战略弊端在所谓的 "特征空袭 " (signature strike) 中表现得最为突出。由于无人机在巡逻过程中收集的信息, 以及由地面的军队和设备收集的信息往往不完善, 无人机攻击往往依赖已知恐怖主义分子和暴力极端主义分子的行为模式信息进行分析预测, 进而确定需要攻击的区域, 即通过"特征"定位。这种分析定位的手段被称为特征空袭, 最常在索马里、也门和巴基斯坦等地应用, 美国在这些地方既没有正式的军队部署也没有公开参与战争, 但有反恐的需求。与定点清除目标不同, 特征空袭不需要总统批准, 决策者往往不知道他们所针对的所谓恐怖分子或暴力极端分子的身份甚至人数。随之而来的不确定性和预测偏见, 无疑使民众的生命面临更大的威胁。需要注意的是, 只有更先进的无人机技术才可以让特征空袭变得精准有效。因此, 这是一个如何制定合理利用新技术的政策和战略问题, 而不是技术本身的问题。

在2021年8月, 美国武装力量从阿富汗的撤离期间非常混乱, 在呼罗珊 (Khorasan Province) 的一次袭击中, 13名美国军人和多达170名平民在喀布尔国际机场 (Kabul International Airport) 惨遭杀害。美军根据旧时的情报和目标的行动轨迹进行分析, 怀疑一辆白色丰田卡罗拉的司机携带爆炸物后, 军方官员对它当天的每一次停车都有预判, 最终决定实施一次致命的无人机特征空袭。五角大楼后来承认, 这次袭击误杀了10名平民, 包括7名儿童和司机, 而这名司机原来是在一个总部设在美国的人道主义组织工作的一名阿富汗雇员。

授权进行无人机袭击的人需要考虑造成民众伤亡的可能性。每当这些风险被认为是可以接受时, 还需要表明决策者的决定是符合国防政策、美军的联合条约以及涵盖军事必要性和人道主义等概念的国际法条约的。

如何决定是否使用武装无人机

1.**制定一个评估在空中反恐任务中**使用无人机的政策框架, 考虑长期影响, 提高决策水平。

如何正确使用无人机

Paul Scharre
Megan Lambert

Center for a New American Security CANS

desirability feasi-
bility

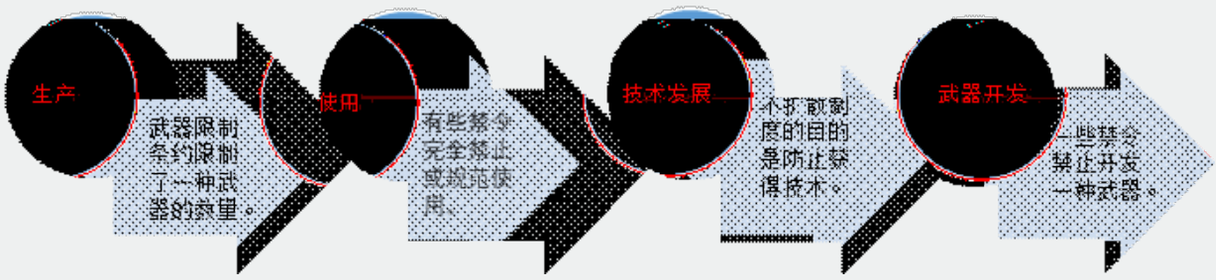
2022 8 17
https://www.armyrecognition.com/weapons_defence_industry_military_technology_uk/soldier_insights_drive_us_army_development_of_mixed-reality_training_system.html

军备控制是什么

" "

nuclear nonproliferation
treaty NPT nonproliferation regime
cluster munition
arms-limitation treaties

贯穿武器开发和使用生命周期的军备控制措施



Micheal E. O'Hanlon
Brookings Institution

2022 2040

B-52
Military Aerospace https://www.militaryaerospace.com/trusted-computing/article/14073852/military-cyber-security-tactical-network

2040 ?
?
20 20
20

通讯

" "

计算机

在计算机方面，技术可能会持续快速地发展。利用现存的计算能力，无数的应用将继续被发明出来，在许多领域有巨大的开发潜力。未来计算机领域的发展将加速转向多核处理器和专业芯片的研发。

例如，计算能力的提高可以让众多卫星和其他传感器通过各种算法和人工智能自动整合数据。这些类型的多平台网络可以帮助降低反卫星武器攻击大型高价值军事资产的风险。如果美国国防部（Department of Defense，DOD）通过像国防创新单位（Defense Innovation Unit，DIU）这样的单位成功建立与硅谷等计算机产业发达地区的联系，这类科技将更快取得突破。

FORCECON 2022

https://www.af.mil/News/Article-Display/Article/3046295/forcecon-2022-spurs-collaboration-innovation-for-air-force-industry-academia

机

网络的脆弱

随着计算机技术的进步，网络变得越来越脆弱。美国无疑拥有世界上最好的、最顶尖的网络进攻能力。这些能力可以用来对付军队的计算机和网络，以及其他国家更广泛的经济和基础设施。然而，令人不安的是，考虑到美国高度数字化的现状，军队和国家的基础设施和关键系统都搭建在互联网上，美国也可能成为最容易受到攻击的国家之一。一个国家如果能将削弱网络能力的攻击整合到一个综合的作战计划中，就可能在战争的初期就取得巨大的胜利。

在网络领域，不确定性比比皆是。美国防火墙通常是可以被攻破的，系统密码是可以轻易破解的，缺乏双因子认证（two-factor authentication system）的系统也带来许多复杂的漏洞。其次，网络漏洞不是静态的，它们总是在博弈中不断发展。任何网络攻击的连锁反应往往不容易预见，即使发现了具体的漏洞，仅仅通过检查个别漏洞来评估这些可能性是困难的。总的来说，美国包括私营部门的网络系统、国家民用基础设施和武装部队的系统的安全都是令人担忧的。国防科学委员会（Defense Science Board）最近的一项研究指出，几乎没有一个美国武器装备的网络系统可以被自信地视为在面对敌人的攻击时具有韧性。

造成信号中断的攻击将更具威胁性。信号干扰（jamming）、对海底光缆以及卫星的攻击、对无线电和其他通信系统软件的网络攻击，都令人非常担忧，更不用说高空核感应电磁脉冲了（high-altitude nuclear-induced electromagnetic pulse）。正是出于这种担忧，位于佐治亚州本宁堡的美国陆军优秀机动中心（Army's Maneuver Center of Excellence）正在研究未来军事行动，探索如果一个旅在很长一段时间内与师部或军团总部隔绝，并且在这段时间内必须完全依靠自己的力量运作时，应该怎么应对。

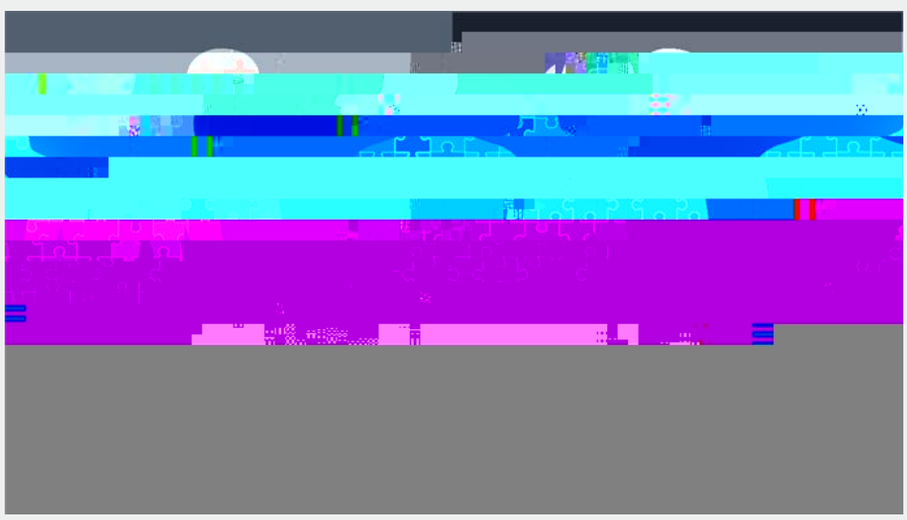
Erol Yayboke 是美国国际战略研究中心（CSCI）弱点与流动性项目（Project on Fragility and Mobility

Carol Kuntz

CSIS Center for Strategic and International Studies

genome manipulation

uniformed practitioner



2022 4 DNA
National Institute of Standards and Technology https://www.nist.gov/news-events/news/2022/03/first-complete-human-genome-poised-strengthen-genetic-analysis-nist-study

技术进步所带来的技术融合让DNA分子能够被刻意操纵，以创造出具有特定特征的新生命体。这种修改基因组的能力可以创造出 "有用的 "分子，从而产生新的材料，如自我修复的纺织物、由非石油原料制成的塑料、以及各种生物传感器。该技术还可以通过编辑基因组来生产蛋白质，从煤灰等废物中提炼出稀土元素。这类技术甚至还可以为新型的疾病制造量身定做的药物，配合使用精确的医疗算法来优化不同个体的治疗方案。这类编辑会带来越来越多的变革，伴随机器学习和生物信息学的发展，推进更多生物特征的遗传根源研究。

操纵基因组的能力来自三个技术进步的融合：DNA测序，CRISPR/Cas系统（原核生物的一种获得性免疫系统，用于抵抗存在于噬菌体或质粒的外源遗传元件的入侵），以及机器学习算法。DNA测序技术使特定生物体的DNA序列得以确定。CRISPR/Cas系统利用一种天然的防御机制来防止病毒的入侵，可以用来确定基因序列中需要修改的位置和具体的变化。机器学习算法凭借其在超大量数据量中识别微妙关联的能力，被用来预测获得特定的性状所需的基因编辑。

总的来说，编辑DNA的能力帮助建立一个规模达到每年数万亿美元的经济产业，可以生产新型材料、设计精准治疗的药物和定制化治疗方案、建设能够为战争带来变革的国家安全能力。然而，目前的美国未能从科学的进步中充分受益。尽管美国在科学发现和技术创新方面处于全球的领先地位，但它缺乏用来维持其领先地位，并将科学发现转化为前沿的技术应用的数据库、生物工厂以及技术劳动力。中国作为美国的一个战略竞争对手正在崛起，正伺机利用美国政策出台的延误或失误，超越美国。

第二，建立可遗传的人类基因组编辑相关的国际规范，让美国的研究合法化，抵御他国的非法研究。

2035

2050

Army Futures Command IT 5G
Washington Technology https://washingtontechnology.com/contracts/2022/02/how-bring-more-tech-soldiers-arm-futures-command-wants-know/361845/

最后，在步骤6中，我们从多个方面评估技术的可用性，包括技术的总体准备情况、与其
程度、技术发展的方向、美军现代化建设的优先事项（Amry modernization priorities）是否
及技术的发展能否满足当下的需求。研究中对润滑剂、量子技术、太空运输、飞行器、自
mous weapon systems，AWS）和生物科技等领域进行了详细分析，并在以下总结：

· **润滑剂**:润滑剂可以减少
的粘度变得非常令人担忧。因
加，生产了大量具有理想
滑剂的开发，例如单一
季节、省油的重型
能较低，但SCP

· **量**
军作战
（A
备
al S

人员的健康和
整个国防部的优
本研究计" (Tran
关注自组
r Re

Claire Mills

House of Commons Library, UK Parliament

NASA
https://www.kent.ac.uk/news/society/18567/donald-trumps-space-force-the-dangerous-militarisation-of-outer-space

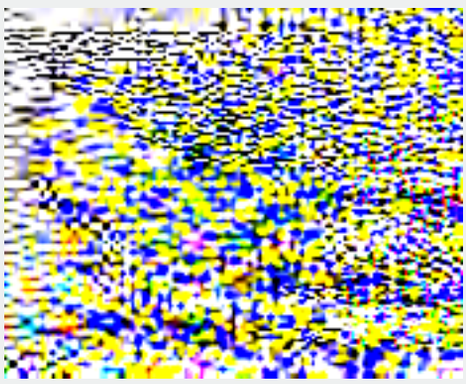
counterspace capabilities

太空中的军事资产在哪里? 2022 5 1
Union of Concerned Scientists 5,464
86% 4700 low earth orbit LEO 10.3% 565
geosynchronous earth orbit GEO geostationary orbit 2.6%
140 medium earth orbit MEO

在这些人造卫星中，10.6%（577颗）用于军事目的。其中一半以上（319颗）是在低地球轨道。低高度和短轨道周期的特点使低地球轨道军事卫星成为地球观测、成像、监视和侦察的理想选择。

大约四分之一的军用卫星（137颗）在地球同步轨道上。在这个轨道上的卫星和地球的旋转周期是同步的，这使它们成为天气监测、情报观察和构建通信系统的理想选择。许多机密的军事卫星都在地球同步轨道上。

还有94颗军用卫星在中地球轨道上。中地球轨道上的卫星比低地球轨道上的卫星有更大的地理覆盖范围，而比地球同步轨道上的卫星信号传输时间更短，普遍用于导航系统。美国的导航卫星全球定位系统（Navstar GPS）、俄罗斯的格洛纳斯系统（GLONASS）、中国的北斗系统和欧盟的伽利略系统（Galileo）都在这个轨道上运行。



US Army Acquisition Support Center

轨道类型	高度（千米）
低地球轨道（LEO）	高达约 2000
中地球轨道（MEO）	约 2000-35000
地球同步轨道(GEO)	约 35000

什么是反太空能力?

人们普遍认为，反太空能力或太空对抗能力（counterspace capabilities）是那些可以用来破坏、排斥、降级或摧毁太空系统的能力。这些能力在性质上可以是动能的（kinetic，涉及对太空资产进行直接的物理攻击或对一个物体进行物理干扰，使其脱离稳定的轨道）或非动能性的（non-kinetic，对一个目标产生影响而没有实际的物理接触）。反太空行动利用数据和软件瞄准想要攻击的太空系统，通过干扰（jamming）或电子欺骗（spoofing）或网络入侵等手段，破坏太空设备的传输和接收能力。这些能力可以是地面发射的（地球到太空），基于太空的（太空到太空）或攻击地球上的目标（太空到地球），包括：

- 直接升空的反卫星（ascent anti-satellite，ASAT）导弹（地球到太空）。它们能够瞄准低地球轨道上的卫星，如果射程足够大，也可能瞄准中地球轨道上的卫星。
- 共轨反卫星武器（太空到太空）。
- 地面或太空定向能武器（directed energy weapon），如激光、微波、电磁脉冲。
- 针对卫星和相关地面基础设施的网络攻击或电子战（electronic warfare），如上行卫星干扰。
- 太空导弹拦截器和全球攻击能力，旨在针对地球上的特定地点。

太空的管理

在发展太空武器方面，1979年《月球协定》（Moon Agreement）第三条禁止在月球上制造威胁或使用武力，同时禁止在绕月轨道上放置核武器。然而，《月球协议》只有18个缔约方，其中不包括英国、美国、俄罗斯和中国。当涉及到将武器或军事设备放入地球周围的轨道，现存规定对军事化的限制是有限的。《外层空间条约》（Outer Space Treaty）第四条规定，目前只有核武器或大规模杀伤性武器不得进入围绕地球的轨道，但它并不禁止将其他武器和军事装备放入地球周围的轨道。

当下的国际法缺乏太空军事化相关的规定，然而就监管达成共识并不容易。世界上主要的太空大国对监管应该是什么样子以及它应该实现什么目标都有自己的解释。美国一贯投票反对任何旨在通过更正式的条约机制防止太空军备竞赛的联合国决议。俄罗斯和中国都因长期以来支持对太空军备控制的而受到批评，它们同时也在建立反太空能力，包括反卫星能力等被广泛认为是带有挑衅和破坏稳定的行为。

美国

在过去20年，美国一直对太空的所有要素进行研究和开发。关于进攻性反太空能力的研究集中在动能和非动能的反卫星（ASAT）能力、定向能武器和电子战。作为修订后的导弹防御计划的一部分，太空拦截器的潜在作用也被重新评估过几次。在21世纪初，美国还对在太空部署常规快速全球攻击（conventional prompt global strike）能力进行了研究。

美国在太空中拥有世界上最广泛的态势感知（situational awareness）能力。其核心是一个地理上分散的地面远程雷达（ground-based long-range radars）和望远镜网络，太空望远镜，以及地球静止轨道上的红外卫星（infrared satellite）网络。红外卫星中最新的一代是天基红外系统（Space-Based Infrared System，SBIRS）。

美国没有专门的直接升空反卫星（direct-ascent ASAT）能力。然而，它拥有可运行的中段导弹防御拦截器（midcourse missile defense interceptor），过去曾证明这些拦截器对低地球轨道上卫星能够发挥反卫星作用。因此，如果需要，这些拦截器可以提供这种能力。虽然美国目前没有一个公认的发展共轨（co-orbital）（太空到太空）能力的计划，但作为其反卫星试验和早期导弹防御计划的一部分而被开发的楔狙鬗（钬홍 其的谁酉葭）漆欲能力没쉇酚웇

美国有一个在全球部署的电子战反太空系统（Counter Communications System, 反通信系统），并有可能对地球静止通信卫星提供上行链路干扰能力。美国军方也有能力干扰全球导航卫星服务的民用信号, 如俄罗斯格洛纳斯系统（GLONASS）和中国北斗系统。

2020年6月, 美国国防部发布了最新的《国防太空战略》（Defence Space Strategy），提出了四个主要目标：1）在太空建立全面的军事优势；2）将太空军事力量纳入国家和国际联合行动；3）塑造太空的战略环境；4）与盟友、伙伴、各产业和其他美国政府部门机构在该领域合作。

2021年5月28日, 拜登政府提出了国防部2022财政年度的预算请求。该请求指出206亿美元将被分配用于加强美国在太空的能力。2000万美元还被分配用于建立国家太空情报中心（National Space Intelligence Center），并对外太空（deep space）先进雷达增加了投入资金, 以探测和跟踪外太空物体。美国空军预算副助理部长（US Air Force Deputy Assistant Secretary for Budget）詹姆斯-佩奇亚（James Peccia）少将指出, 今年有远远超过8亿美元的机密项目进入太空部队。美国导弹防御局（US Missile Defense Agency）22财年的资金申请还包括2.92亿美元用于提高太空态势感知能力。

俄罗斯

在过去的几年里, 俄罗斯因一系列反卫星试验而被登上新闻头条, 这表明俄罗斯在发展直接上升反卫星

英国

英国《2021年综合审查及相关国防指挥文件》提出了英国的雄心壮志，即到2030年成为 有影响力的太空参与者（a meaningful player in space）。在未来十年，英国国防部（Ministry of Defense，MOD）将投资约50亿英镑，2025年交付"天网6号"计划（Skynet 6 programme），对其卫星通信能力进行资本重组和增强，并进一步投资 14亿英镑用于打造与太空相关能力。具体而言，国防部将在低地球轨道上建立一个新的情报、监视和侦察（intelligence，surveillance and reconnaissance，ISR）卫星群，应用光电（electro-optical）、红外线、合成孔径雷达（synthetic aperture radar）和高光谱解决方案。

Claire Mills是英国下议院图书馆研究员。


TSINGCHIH