如何分析来自无人机的网络威胁
——背景、分析框架和分析工具

凯瑟琳·莱贝斯特，乔恩·施密德，肖恩·蒂尔尼

执行摘要

在一个技术日新月异的世界里，最大限度地减少脆弱性是一场与对手的永无止境的竞赛，是一场与对手的技术及其开发、设备、思想、操作模式和战术的竞赛。在本报告中，研究了一个关键技术趋势的网络安全影响：公用无人机系统的发展和扩散。公用无人机系统（UAS）通常称为无人机，已经变得越来越普遍，更容易获得和更加复杂，它支持新的功能，如增加的数据收集和自主行为。因此，无人机正以两种关键方式重塑网络安全世界。首先，无人机系统提出了一种新的网络安全关键目标。对这些平台的网络攻击可能会破坏使用无人机的关键执法或数据收集任务。其次，对手手中的无人机可以为网络攻击提供新的途径，无人机本身就是“网络武器”，旨在传递恶意内容或产生动态影响。在本报告中，将无人机构成的威胁视为网络攻击的目标和载体。我们还研究了这些威胁与国土安全部（DHS）和受其保护的设施及资产的相关性。

无人机安全

这项工作探讨了快速增长的无人机技术的安全影响，特别是当前的漏洞和未来的趋势。随着无人机变得越来越普遍和复杂，安全威胁的可能性和潜在后果都会增加。据估计，到2021年，无人驾驶或无人驾驶飞机的销售额将超过120亿美元。

我们提出了概念性的方法，旨在对与无人机相关的网络威胁进行枚举和分类。这些方法使用“蓝色”（盟友）和“红色”（对手）的思维模式，帮助决策者阐明和理解其组织现在和将来可能面临的威胁种类。基于蓝色思维的方法专注于发现与无人机相关的系统中的漏洞，而基于红色思维的方法则围绕如何成功攻击系统而构建。

这些方法被应用到现实世界的威胁场景中，以测试它们的有效性，并说明当前可行的攻击类型。这些攻击示例以及与无人机网络漏洞有关的学术论文和其他文献的结构化综述，有助于描绘当今和不久的将来可能存在的威胁空间。

为了预测未来与无人机和网络安全相关的威胁空间，本报告还强调了行业趋势以及这些趋势可能产生的影响。无人机有望与安全和执法职能更加融合。无人机新技术的发展，包括引入更复杂、更自主的控制软件，以及通过移动网络创建无人机群的能力，扩大了潜在攻击

的范围和复杂性。无人机控制器和控制信号构成恶意参与者的漏洞和访问点。我们还探索了使用基于代理的建模技术来描述威胁，并帮助确定可靠的选项来防御恶意行为者。基于代理的建模与仿真是理解无人机攻击的一种有潜在价值的方法，可以为分析人员研究如何减轻潜在攻击提供有意义的见解。在今后的工作中进一步探讨这些趋势，可以发现新的威胁和防御方法，并估计其预期的可能性和后果。

无人机安全和国土安全部

本文的研究结果对国土安全部（DHS）有一定的指导意义。我们发现，国土安全部容易受到针对其运营的无人机（即无人机作为网络目标）和无人机启用的网络攻击（即无人机作为网络武器）的袭击。

国土安全部以无人机为目标

国土安全部的四个部门记录了在日常活动中使用无人机的历史情况：美国海岸警卫队（USCG）、海关和边境保护局（CBP）、联邦应急管理局（FEMA）以及网络安全和基础设施安全局（CISA）。国土安全部正在使用并将继续使用国防部开发的（捕食者和扫描鹰）和商业部门开发的无人机。然而，除了USCG外，所有部门都计划在未来投资商用无人机。然而，它们的引入也意味着CBP、FEMA、CISA以及ICE（移民海关执法）的资产将容易受到本研究中描述的新型攻击的威胁。也就是说，鉴于本研究发现商用无人机对网络攻击的高度脆弱性，各部门使用无人机在提供急需的新能力的同时，可能也威胁着执行以下操作的能力：

· CBP可能失去情报、监视和侦察能力，在侦查边境和港口的走私或其他邪恶活动时形成视觉盲点。CBP还可能选择在未来的其他活动中使用无人机平台。例如，在港口进行化学、生物、放射性、核和爆炸物扫描，在这些港口，受损的无人机系统可能会妨碍美国海关与边境保护局特工完成其职责，在系统固定的情况下，延迟货物移动会造成重大的经济损失，甚至发送错误的危险货物“安全”信息。如果CBP运营商不知道违规行为，受损的无人机也可能产生不可预知的风险。

· 受损的FEMA无人机系统可能会降低机构识别、接触或供应灾区处于危险或医疗困境中的个人的能力。这可能是因为受损的无人机不再能够按预期执行任务，或者是因为无人机可能导致其他空中操作的能力降低，如影响直升机飞行活动。如果在灾区使用无人机进行ISR(情报、监控和侦查），受损的FEMA无人机也可能导致态势感知能力下降。

· CISA无人机受损在某些情况下会降低其进行关键基础设施检查的能力，并可能导致网络物理攻击，以损坏其打算调查的关键基础设施。如果CISA运营商不知道违规行为，受损的无人机也可能产生不可预知的风险。

最后，ICE打算使用无人机来降低突袭期间的风险。受损的洲际无人机将降低总体作战能力，并增加战地特工的风险。如果ICE运营商不知道该漏洞，受损的无人机甚至可能产生不可预知的风险。

以无人机作为网络武器攻击国土安全部

我们发现，几乎所有的DHS部门和办公室都可能成为无人机主导的僵尸网络或数据泄露

攻击的受害者。这些部门和办公室都有物理位置，敏感数据和无线网络普遍存在，使它们成为此类攻击的目标。具有游荡能力的无人机，例如，在一段时间后能够再次着陆和起飞的无人机，允许这种隐蔽攻击，从而增加了未加固系统的风险。

随着连接设备的普及，无人机注射蠕虫或类似攻击的危险也会增加。此攻击载体不必限于 DHS 网络和连接的设备，因为 DHS 员工的个人设备或家庭网络也可能是恶意代码的接入点，以便通过无线方式或由员工将受感染的设备连接到 DHS 笔记本电脑来进入 DHS 系统。

1 导 论

1.1 背景和目的

在一个技术日新月异的世界里，最大限度地减少脆弱性是一场永无止境的竞赛，对手是其技术、设备、思想、运作模式、战术以及利用技术趋势来实现其政治目标。在本报告中，我们研究了一个关键技术趋势的网络安全影响：公用无人机系统（无人机）的发展和扩散。无人机已经变得更加常见、更加容易获得和更加复杂，它支持新的功能，比如增加数据收集和自主行为。因此，无人机正以两种关键方式重塑网络安全世界。首先，无人机系统提出了一种新的网络安全关键目标。对这些平台的网络攻击可能会破坏使用无人机的关键执法或数据收集任务。其次，对手手中的无人机可以为网络攻击提供新的途径，无人机本身就是“网络武器”，旨在传递恶意内容或动态影响。例如，大量携带爆炸物的无人机群可以攻击美国的政治权力象征，并通过级联效应摧毁相互依存的系统，如美国电网的关键要素。

很难预测新兴技术如何转化为新的网络安全威胁。为了帮助决策者更好地了解无人机是如何潜在地改变网络安全威胁空间的，本报告介绍了几种将无人机相关威胁列为网络目标或网络武器的方法。这些方法使用户能够识别和分类与无人机技术相关的威胁，将威胁分类应用于特定场景，并可视化威胁空间，以便有效地了解和交流威胁的性质以及改进无人机相关网络安全的机会。

在评估与无人机网络安全相关的风险和回报时，决策者必须从多个角度着手。如上所述，无人机既可以作为网络安全的目标，也可以作为网络安全的威胁。此外，盟国和敌国都可以在这两种条件的影响下操作无人机。图 1.1 提供了这四类威胁的一些可能例子，紫色方框突出显示国土安全部（DHS）的进攻机会，蓝色标记表示防御情况。要捕获图 1.1 中描述的所有场景类型，威胁枚举和分类必须同时包含“蓝色团队”和“红色团队”。蓝色团队的思维方式考虑了无人机可能如何脆弱，或者系统如何容易受到基于无人机的网络攻击。红色团队的思维方式包括设计攻击无人机或攻击系统的方式。

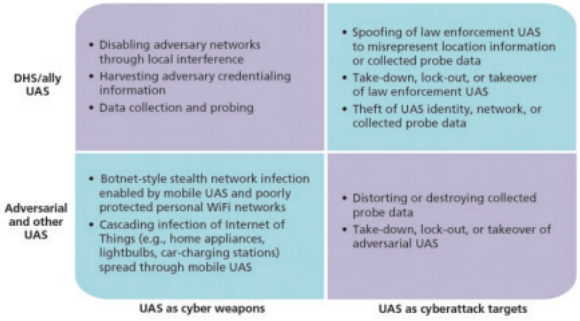

图 1.1 无人机相关网络威胁的分类

1.2 本报告的组织方式

在本报告中，概述了一组方法，从蓝队和红队的角度，允许列举和分类由无人机构成的网络安全威胁。第二部分概述了这些方法。在第三部分中，使用这些方法作为无人机网络安全文献样本审查的基础，并且将这些方法应用于特定的威胁场景。将所提出的方法应用到具体的案例中，证明了框架在解构攻击方面的实用性，并说明了当前可行的威胁范围。第四部分继续讨论未来的无人机系统和网络安全，研究无人机发展中出现的技术趋势与网络安全的关系。所考虑的趋势包括：越来越多地使用自主式（而不是遥控式）无人机、发展无人机交通管理系统、“成群结队”或基于群体的自主行为、使用机器学习（ML）和人工智能（AI）检测攻击，不断增加的硬件复杂性和攻击这些硬件系统的潜在技术，以及区块链技术的潜在用途。我们还探索了使用基于代理的建模（ABM）技术来描述威胁。反弹道导弹和仿真是了解无人机攻击的潜在有价值的方法，可以为分析人员提供有意义的见解，研究如何最好地减轻和挫败潜在的攻击。在今后的工作中进一步探讨这些趋势，可以发现新类型的威胁和防御方法，以及它们的预期可能性和后果。最后，在第五部分中，从 DHS 的角度考虑了无人机网络安全威胁的影响。具体而言，描述了特定 DHS 部门对本报告中描述的威胁的脆弱性，并建议了潜在的威胁缓解方法。第六部分是结论和建议。

2 了解无人机的威胁空间

技术进步有时会产生不可预测的后果。对新技术的不受欢迎的应用、巨大的成本以及与安全或可持续性相关的问题可能会弱化技术进步所承诺的新颖性和利益。例如，在电子产品中广泛使用多氯联苯作为绝缘体和冷却剂，未能预料到这种化合物的有毒和致癌特性。手机有助于通讯，但也可以用来触发简易爆炸装置的爆炸。未来主义者可能乐于把技术发展的乌托邦和反乌托邦的情景作为思维实验，但要想适应不断变化的世界，找到揭示新技术的风险和好处的方法也是一个实际的必要条件。例如，为了防止对执行关键执法功能的无人机的攻击，官员必须预见到黑客可以通过各种方式访问设备、其子组件或相关软件。同样，为了发起有效的无人机网络攻击，政府人员必须预见到他们可能会遇到的网络防御措施。在这一部分中，将介绍三种方法，帮助规划者从与无人机相关的网络攻击的防御者和实施者的角度来列举和理解无人机可能带来的网络安全威胁。

首先，将 STRIDE 威胁模型分类描述为对威胁进行分类的方法的一部分，并将其作为网络目标和网络武器应用于无人机。STRIDE 分类法有助于建立一个“蓝色团队”，即防御性思维，帮助用户列举未来可能面临的威胁。STRIDE 提供了对常见网络相关威胁类型进行分类的有效方法，并鼓励实践者将此作为对潜在攻击表面漏洞进行头脑风暴的框架。

其次，提出网络安全杀戮链作为一种手段，有助于建立一个“红色团队”，将攻击性思维纳入威胁头脑风暴的一种手段。网络安全杀戮链提供了一个框架，用户可以在此框架内计划

可能的网络攻击。此类计划有助于用户从对手的角度发现网络通信系统、操作软件或应用程序以及数据存储组件中可能存在的攻击载体和弱点。攻击载体是可以引入或利用以发起网络攻击的工具、平台、连接或安全功能。

最后，引入了一个新的模板，用于捕获特定场景中的网络安全状况，集成了攻击面和攻击载体方法，以便能够连贯地描述该场景中的网络漏洞和机会。该模板还允许对攻击载体和攻击面进行可视化描述。该描述提供了一种有效的方法，将许多技术细节汇总起来，它支持高层分析以识别常见的攻击面和攻击载体。

2.1 列举和分类威胁：STRIDE 分类法

防范网络安全攻击的第一步是了解可能存在的威胁空间。对于那些想要防范网络安全攻击的“蓝队”参与者来说，他们必须具有创造性、主动性，并且充分了解对手的能力。列举未来可能的攻击类型需要仔细审查现有和新兴技术所带来的威胁空间。将此类审查植根于可能的威胁类型的既定框架中可能会有所帮助，使用形式化的头脑风暴填充此框架以发现可能的威胁也可能会有所帮助。其中一个框架是 AdamShostack 的 STRIDE 威胁建模分类法，它概述了可以对安全威胁进行分类的六个领域（如图 2.1 所示）。STRIDE 的替代方案，如 Gunnar Peterson 的 DESIST 框架，为威胁枚举提供了其他分类法。虽然 STRIDE 分类法最初是为软件开发而设计的，但它所涵盖的六个领域对于列举与网络安全和无人机相关的威胁也很有用。

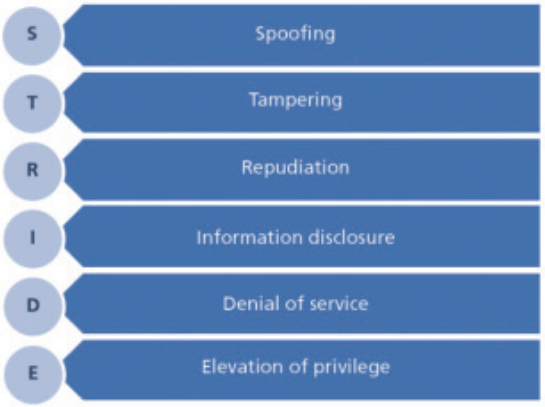

图 2.1 STRIDE 威胁分类法

STRIDE 框架中的 S 代表欺骗，包含一组违反身份验证协议的威胁，使攻击者能够假装自己不是某个东西或某个人。在以无人机为目标的与无人机相关的网络安全情况下，欺骗可能包括声称是无人机数据的授权接收机器。

STRIDE 框架中的 T 代表篡改，它涉及通过对受攻击系统进行某种修改来侵犯其完整性。在与无人机相关的网络安全中，无人机被用作网络武器，如果无人机被用于通过接近访问不安全的无线网络向目标计算机发送恶意软件，则可能会发生篡改。此类恶意软件可能会感染工厂或发电厂设备等高价值机械，或攻击供水系统和电网等高影响目标。

R 代表拒绝，攻击者拒绝对一个行为负责。这种威胁与无人机相关的网络安全领域最不相关。否认的一个可能例子是内部人滥用系统控制。例如，无人机操作员可以声称，他没有故意将失去控制归咎于通信网络的设计缺陷，从而导致设备崩溃。另一个例子是，在无人机是网络武器的情况下，可以通过干扰与损害或破坏点松散关联的通信节点，使攻击者的身份与

结果保持距离。这可能包括使用基于邻近性的网络攻击，来更改正在管理作为攻击目标的另一个系统的日志文件。

I 指信息披露，涉及违反保密原则的行为。在信息泄漏攻击中，代理将信息发布给没有接收信息的适当凭据的人。信息泄露威胁可能包括渗透无人机传感器数据系统以访问视频、音频或其他数据。代理人也可以披露信息，然后否认对此行为负责。

D 代表拒绝服务，是指拒绝被攻击系统正常运行所需的资源的可用性。拒绝服务的一个例子是当无人机成为目标时，可能涉及感染无人机控制软件，使设备对用户输入无反应。

STRIDE 分类法的最后一个字母 E 表示特权的提升，这涉及违反授权原则来执行不允许执行的操作。授权权限的一个例子是当无人机是目标时，它可能通过伪装成合法的控制器来劫持无人机。当无人机被用作网络武器时，它们可以用来传送数据、代码或其他信号，以削弱或改变受攻击系统的行为。

威胁场景或渐晕图开发可以与 STRIDE 框架结合起来以支持威胁头脑风暴、模型开发、测试和缓解计划。在本报告中，重点关注 STRIDE 支持威胁头脑风暴的能力。对威胁的高级分类在因果分析中的价值有限，但有助于根据不良行为者寻找漏洞的策略聚合关注点。当然，可以通过头脑风暴来创建可能的威胁场景。更正式的方法包括文献回顾、场景分析、流程图分析和创建攻击树。对历史攻击的回顾也可以突出潜在的弱点，补充非正式的头脑风暴。在场景开发和分析中，使用可能的对手行动的示例来了解可能的威胁。

通过研究未来可能的攻击场景，可以发现系统漏洞。流程图或数据图描述了信息和数据在系统中的流动，允许分析人员识别攻击者可能使用的潜在访问路径。在无人机可能是攻击目标的情况下，这样的图示可以描绘无人机与协助控制或数据收集的任何计算设备之间流动的所有数据连接。例如，这种方法将突出无人机内部的数据处理，以及外部设备上的任何有线或无线连接、信息传输和处理或数据存储基础设施，见图 2.2。这些图表不仅描述了无人机，而且还描述了控制器、其他计算设备和环境中的关键对象，例如巡逻时遇到的数据发射源、天气数据、计算设备或用于位置感知的信标。

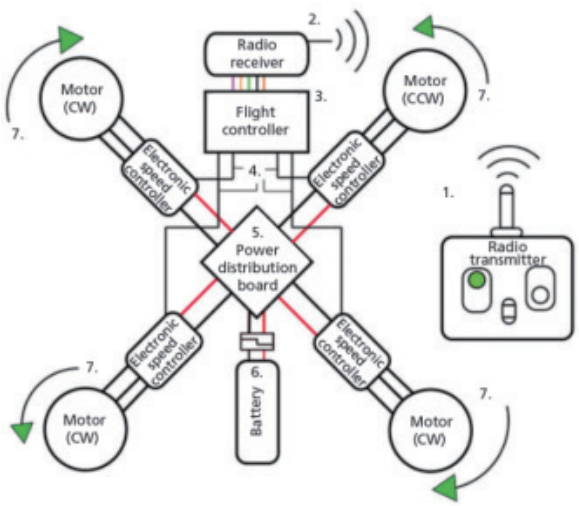

图 2.2 单无线电控制器的简易四旋翼机数据流程图

攻击树类似于场景分析。攻击树获取一个潜在的敌方目标，并详细说明为实现此目标必须执行的可能步骤，从而创建一个可能的攻击场景或渐晕图的描述。对于这种假设的方法，这些步骤可以包括获得对接收数据下载的计算

机的物理访问、在空中拦截数据传输或破解包含所需数据的在线门户的密码。

在应用了上述部分或全部方法后，分析师可以在 STRIDE 框架中填充一组威胁场景，以便在作出网络安全决策时加以考虑。这种防御的蓝队方法识别了对手可能利用的攻击面，并开始识别可能需要关闭或缓解的潜在漏洞，以加强与无人机相关系统的网络安全。

2.2 在场景中发现威胁：网络安全杀戮链

在给定的攻击场景中，如何发现无人机的脆弱性存在很大的差异。迫使决策者站在对手的角度（即扮演红队）可能有助于识别上一节中描述的“蓝队视角”STRIDE 框架方法没有发现的威胁。支持这种红队方法的网络安全杀戮链使用户能够识别特定系统在某个场景中何时以及如何易受攻击。这可以帮助设计针对特定威胁的知情防御。这种方法可以识别长链通信中的一个薄弱环节。

网络安全杀戮链确定了网络攻击的七个阶段：侦察、武器化、交付、利用、安装、指挥和控制以及行动。如图 2.3 所示，链代表一个有序的序列，其中每个阶段代表一个对手采取的行动。至关重要的是，每个阶段都提供了检测攻击的机会。由于阶段是连续的，因此早期检测与较少的破坏性后果和较低的修复成本相关。适当的防御行动取决于给定行动在链中的位置，指定无人机位于网络安全杀戮链上的位置有助于采取有效的安全措施。

图 2.3 网络安全杀戮链

在许多涉及无人机的攻击场景中，启动网络安全杀戮链的目的是对无人机本身采取行动。此类攻击旨在获得对无人机或其子系统的控制，以捕获或更改其数据、改变其航向或摧毁设备。在这种攻击中，无人机在网络安全杀戮链中的每一个环节都扮演着角色。我们把这种支持无人机的网络攻击的变体称为“无人机作为目标”。

在其他启用无人机的攻击中，攻击者利用无人机的独特性来攻击不同的（非无人机）目标。在这种情况下，无人机被用于网络安全杀戮链的至少一个中间环节，以对其他一些目标采取行动，或在最后一个环节促进行动。虽然此类攻击可能利用直接针对无人机的相同安全漏洞，但无人机被用作结束后一类攻击的手段。我们把这种攻击称为“无人机作为载体”，“无人机作为目标”与“无人机作为载体”的区别在于不同的攻击类型与不同的防御姿态相关联。在本报告的结论中，简要阐述了针对每种攻击变体的适当防御方法。

2.3 可视化威胁：无人机网络安全图模板

同时使用蓝色和红色透视法来列举可能存在的漏洞，可以揭示一个复杂而可怕的威胁空间。在这一部分中，介绍了一个新颖的无人机网络安全图模板，旨在以一种易于理解的方式描绘威胁空间。图表模板的应用程序通过提供一种直观的方式来捕获系统可能易受攻击的位置（攻击面）以及攻击如何访问系统（攻击载体），有助于阐明黑客可能在何处以及如何构成威胁。视觉描述还可以帮助有效地向广泛的受众传达可能的威胁类型。该模板分别捕获攻击面和攻击载体，形成两个互补图。

2.3.1 攻击面图解

攻击面模板包括定义通信边界的三个核心节点，如图 2.4 所示。这些节点是人类操作者、无人机本身和无人机环境，这意味着人类操作者和无人机之间以及无人机和环境之间存在通信信道。当无人机应用程序涉及视线之外的操作时，可以通过为人类环境创建一个节点来捕获其他细节。

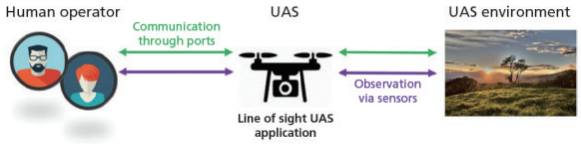

图 2.4 无人机攻击面图解模板

人类操作者和无人机之间的通信信道处理无人机的操作和控制。该系统中的第一个链路是一个人，他可以被视为无人机的主要操作员，但是向无人机发送人工命令可以通过各种计算设备（例如，使用飞行时间表指令的充电基地、用于飞行命令的云服务器、物理控制器、手机、笔记本电脑、平板电脑），所有这些都可以在图像模板中突出显示，以指出潜在的攻击面。图 2.5 的左侧提供了一些附加节点的示例，例如导航软件或控制器，这些节点可以添加到图像模板中以显示可能的攻击点。

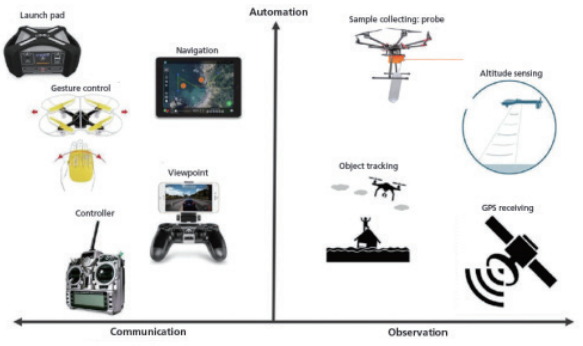

图 2.5 来自通信和观测的无人机信息

无人机与其作战环境之间的通信信道较少关注无人机控制所需的通信，更多关注从作战环境收集的信息。无人机对感官信息的采集可以涉及多种来源，如图 2.5 右侧所示，以获取各种环境因素，如 GPS 信号、高度信息以及视觉或其他传感器数据。模板可以用这些节点进行注释。

2.3.2 攻击载体图解

结合攻击面说明模板，提出了另一个模板，用于说明可用于网络攻击的载体（见图 2.6）。攻击载体图解回答了关于所示攻击的以下五个问题：

（1）漏洞是什么（网络武器）？

（2）它是怎么到达那里的（攻击载体）？

（3）它是从哪里进入的（系统接入点或攻击面）？

（4）什么失败了（安全漏洞或候选缓解措施）？

（5）发生了什么事（后果）？

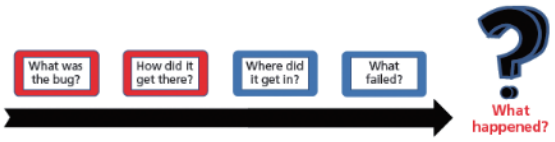

图 2.6 无人机攻击载体演示模板

为了能够直观地描述整个无人机和网络安全威胁空间的攻击载体，攻击载体模板隔离了网络安全杀戮链中与全面网络攻击的三个关键阶段相一致的三个连续段（见图 2.3）。在第一类序列中，通过详细描述与侦察和武器化相关的活动来展示计划或渗透的过程。该模板侧重于情报收集行为和网络攻击的制定。下一类序列涉及通过交付、开发和安装活动修改系统的

过程。在这个说明序列中，武器的交付和对特权标识的侵犯显示为更改网络或功能设置的结果。最后，一个关于劫持无人机行动的序列显示了与指挥控制和行动有关的活动。此部分说明了涉及无人机应用程序和操作的与损害、降级、破坏和拒绝有关的威胁条件。

结合上述针对攻击面和攻击载体开发的可视化模板，可以使用“分屏”方法来提供与无人机相关的网络攻击的完整可视化表示。图 2.7 显示了这样一个图像的示例，并使用此方法来说明第三部分中包含的渐晕图。

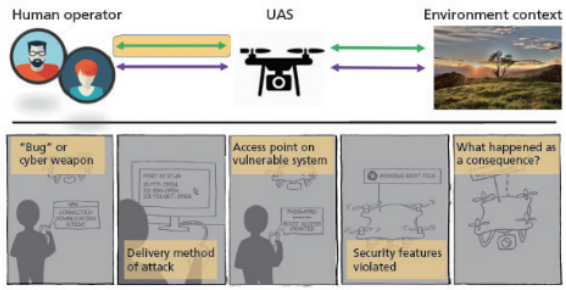

图 2.7 攻击面和攻击载体的“分屏”图示示例

3 无人机与当今网络安全威胁空间

学术文献、流行媒体和非传统媒体（如社交媒体和博客）中充分记录了商用无人机的漏洞以及使用无人机的网络安全攻击。在本节中，调查了这些来源，以描述当前的无人机和网络安全威胁空间。本节首先通过调查有关无人机攻击的文献，考虑了一系列看似合理的威胁。通过调查和编码现有的相关文献，能够创建一个攻击类型清单，并对其相对流行性做出初步判断。然而，尽管记录的漏洞种类繁多，数量庞大，为无人机的整体网络脆弱性提供了明确的证据，但从这些数据中获取与作战相关的信息需要应用概念框架。因此，在对威胁空间进行描述之后，将第二部分中描述的方法应用到四个与无人机相关的网络安全攻击案例中，以说明决策者如何从简单地清查威胁到制定网络防御计划。

3.1 无人机网络漏洞的程度

桑德·沃尔特斯（Sander Walters）编制了一份包含 26 个记录在案的无人机开发实例的列表。对攻击方法、目标无人机和攻击负责人的仔细审查表明，攻击面很大，针对被攻击的特定无人机具有广泛的复杂度，而对手所需的计算能力的阈值较低。对于整个攻击面而言，检查记录暴露了许多明显的漏洞，散布到所有主要的无人机子系统中。例如，成功利用漏洞的目标是较差的密码短语安全性、已知的默认设置和未受保护的 ad hoc 网络。在子系统方面，无人机本身及其接收器、光学传感器、控制器、导航应用程序以及连接这些子系统的所有通信链路都存在漏洞。

关于对手所需的技术能力，我们发现，大多数启用无人机的攻击不需要高度的复杂度。其中一个漏洞利用 Raspberry Pi 控制了一台无人机，这是一台只有基本功能且便宜（35 美元）的计算机，用于教授基本的计算能力。进行无人机攻击的手段是公开的，这一事实降低了对手能力的门槛。在许多情况下，负责攻击的个人在 YouTube 或个人博客等网站上记录他们的方法。实际上，在许多情况下，利用漏洞的代码被发布到 GitHub 这样的可搜索代码库中。

这些漏洞也不局限于早期或低端的无人机。记录在案的攻击目标包括价值 1500 美元的 DJI 幻影 4、价值 2000 美元至 3000 美元

的 DJI Inspire 和价值 3000 美元以上的 Yuneec Tornado。类似地，诸如 FrSky ACCST 和 DJI Naza-M 控制器等高级控制器也被成功攻破。一名 IT 安全顾问甚至劫持了一架价值 2.5 万至 3.5 万美元的专业级航空电子公司阿尔图拉天顶无人机，用于执法。

在大学研究人员进行的一系列复杂演示中，还发现了有关无人机脆弱性的其他证据。例如，得克萨斯大学达拉斯分校的博士候选人朱妮娅·瓦伦特（Junia Valente）的研究于 2017 年带领美国计算机应急准备小组（US-CERT）发布了可能被匿名劫持的四轴飞行器系列的漏洞说明。瓦伦特证明，这些飞机可能通过其本地 FTP 网络被匿名劫持。事实上，大学的研究人员已经证明了商用无人机在各种攻击下的脆弱性，包括面向互联网的僵尸网络攻击、ad hoc 网络攻击、数据收集和探测、无人机位置检测和跟踪、无人机劫持或攻击、媒体捕获和软件修改以允许无人机进入禁止飞行的空域。

为了了解文献中普遍存在的威胁类型，我们汇总了各种来源的历史或可能的未来攻击的引用，并根据攻击类型、无人机角色（作为目标或网络武器）和访问点（攻击面、攻击载体和使用的漏洞或武器类型）对其进行分类。总的来说，通过 STRIDE 分类法发现，在不同类型的源中记录的大多数网络攻击使用拒绝服务或欺骗攻击劫持活动的无人机。这些攻击的目标是无人机开放网络，如 WiFi 或 RC 连接，并使用无线电频率来压制原始所有者的信号。然后，攻击者试图用自己的信号替换移位的信号，向无人机发送新指令。在文献中的大多数例子中，无人机是网络攻击的目标，而很少用作网络武器。在无人机被用作网络武器的情况下，它们通常被修改为网络或射频扫描器，这是攻击中使用的真正的网络武器。图 3.1 提供了不同攻击类型、角色和攻击面的频率细分。

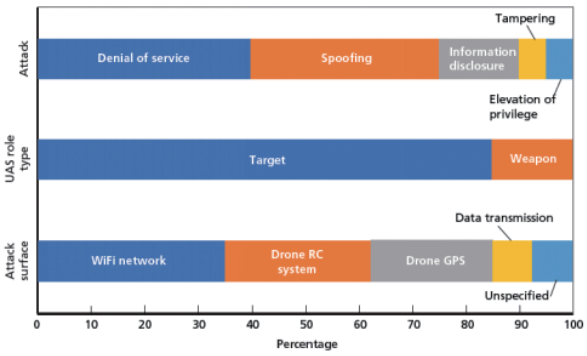

图 3.1 文献中某些网络攻击特征的普遍性分类

公用无人机中的漏洞无处不在。在下一节中，将回顾记录的跨源无人机攻击的文献。由于仅仅记录这一事实并不能说明适当的网络防御策略，因此遵循这篇文献综述，对四个特定的案例进行了更详细的调查。在这些案例中，应用了第二部分中描述的方法，以便深入了解如何防御网络无人机威胁。

3.2 选定的无人机网络攻击的案例

接下来的案例更详细地描述了对商用无人机的四种最复杂的攻击演示。前两个描述了直接针对无人机的实例。后两个案例描述了研究人员使用无人机接近目标，收集数据，然后通过无人机的自组织网络传播恶意软件的情况。对于每一个案例，都指出了 STRIDE 分类法和网络安全杀戮链是如何为理解漏洞提供分析手段的。特别是，STRIDE 框架有助于对攻击方法进行分类，网络安全杀戮链允许将攻击分割为离散的防御阶段。

3.2.1 无人机作为目标一：远程劫持无人机

事件摘要

“我们能够在无人驾驶飞机飞行途中访问和删除根目录下的文件。如果攻击者删除整个文件系统，无人机很可能会崩溃。”

攻击描述

麻省理工学院（MIT）的四名研究人员花了一个月的时间来识别和利用一种流行的无人机（DJI 幻影 3 标准）上的安全漏洞。研究人员使用网络映射工具从无人机的三个主要子系统（无人机、摄像机和控制器）捕获传出的数据包。一旦识别出每个子系统，研究人员就可以利用设备密码安全性差的特点获得根用户访问权限。对无人机文件系统的根访问允许修改系统文件，进而允许攻击者修改飞行路径或使设备崩溃。对摄像机的根访问将允许攻击者访问、删除或添加图像或视频。最后，研究人员发现了无人机 Android 应用程序中的一个漏洞，该漏洞允许攻击者绕过软件对进入联邦通信委员会（FCC）禁止空域的限制。

消除威胁

STRIDE 框架有助于对本例所示的威胁类型进行分类。研究人员能够相对容易地（提升特权）获得对无人机所有主要系统的根访问权限。根访问权限允许修改系统文件（篡改）。研究人员通过使用公开的默认密码（信息披露）进入了无人机的 WiFi 网络和文件系统。

将网络安全杀戮链应用于攻击表明，可以通过阻止网络安全杀戮链的侦查阶段来阻止攻击。大多数公用无人机都会创建 ad hoc 网络，将设备与其控制器连接起来。所述攻击表明，这些网络对于网络映射和发现工具的应用仍然存在脆弱性。图 3.2 提供了第二部分中描述的攻击面和攻击载体可视化。

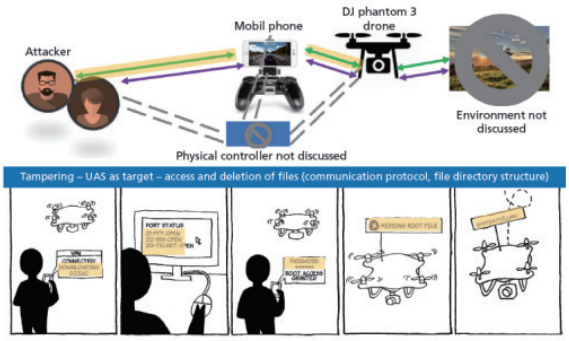

图 3.2 在飞行途中访问和删除文件的无人机攻击

3.2.2 无人机作为目标二：GPS 欺骗

事件摘要

“实地测试表明，对旋翼无人机实施破坏性的GPS欺骗攻击在技术和操作上都是可行的。”

攻击描述

德克萨斯大学奥斯汀分校的四名研究人员提出并实现了一种通过发送欺骗性的 GPS 信号来控制公用无人机的方法。在提议的攻击中，欺骗设备首先从 GPS 卫星接收合法信号。然后，欺骗器产生一系列伪造信号，迫使无人机接收器发送位置和速度信号。一旦实施人对设备施加了控制，他就可以操纵无人机的飞行路径或使飞行器完全坠毁。

消除威胁

在 STRIDE 框架中，此类攻击构成欺骗攻击。为了可靠导航，无人机通常将来自内部惯性测量单元（IMU）和 GPS 卫星的信息结合起来。民用 GPS 信号几乎没有安全措施。通过控制无人机接收的 GPS 信息，可以操纵无人机对位置

和速度的估计。对这些估计值的操纵使攻击者能够劫持或击毁目标无人机。GPS 欺骗可以在相当长的距离内秘密进行。

应用“网络安全杀戮链”框架可以深入了解如何防止攻击。在这种情况下，武器化（即配置和获取欺骗设备）对受害者几乎是不可察觉的。相比之下，交付阶段（当无人机接收到伪造信号时）可以通过防欺骗防御措施来防止，例如失真检测和到达方向感测。这些缓解特性的存在将支持持续的反馈回路，以应用其他控制策略或功能，直到可以放心地恢复主要控制策略为止。图 3.3 提供了第二部分中描述的攻击面和攻击载体可视化。

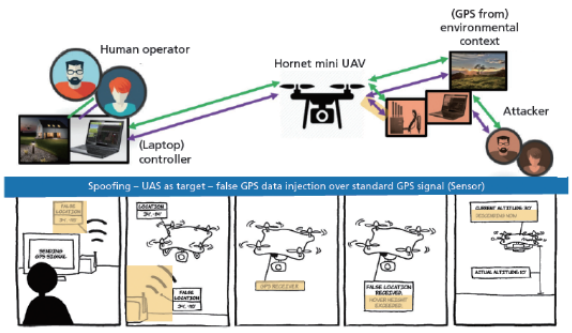

图 3.3 利用伪 GPS 信号欺骗悬停特性的无人机攻击

3.2.3 无人机作为载体一：无人机僵尸主机

事件摘要

“利用配置不当的无线网络安全性和在移动设备上的不良信任配置，使移动攻击无人机在本地加入网络和访问设备。”

攻击描述

史蒂文斯理工学院的三位研究人员提出了一种方法，首先使用一架无人机来建立并控制一个面向僵尸网络的隐藏互联网。在拟议的攻击中，一架增强型无人机在一个城市地区的上空飞行三次。在第一次飞行中，无人机调查并收集攻击区域内 WiFi 网络的信息。在第二次飞行中访问易受攻击的网络。在最后一次飞行中，无人机加入受损网络，并将本地主机加入僵尸网络。

消除威胁

在 STRIDE 框架内，该攻击构成 DOS 威胁。僵尸网络是指被恶意软件劫持的网络，可用于攻击与网络连接的设备。僵尸网络是一种主要的网络安全风险。它们可用于执行分布式拒绝服务（DDOS）攻击、窃取数据和劫持设备。僵尸网络由僵尸主机控制。在提议的攻击中，无人机的使用允许以隐藏僵尸主机的方式控制僵尸网络。因此，拟议的攻击方法中隐含的主要威胁是可能使用商用无人机通过僵尸网络匿名发起网络攻击。

将网络安全杀戮链框架应用于本案例，有助于确定无人机在更大规模攻击中的作用。图 3.4 描述了无人机在网络安全杀戮链上的位置。该图表明，无人机的作用是非常重要的，它用于接近和监视本地网络、传送恶意软件和匿名控制僵尸网络。如第二部分所述，图 3.5 提供了此渐晕图的攻击面和攻击载体可视化。

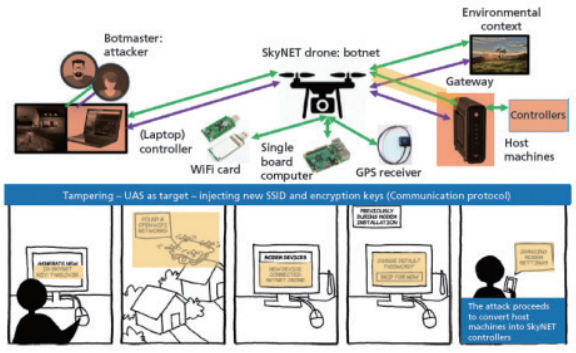

图 3.4 无人机和网络安全杀戮链——“无人机作为载体”利用（无人机僵尸主机）

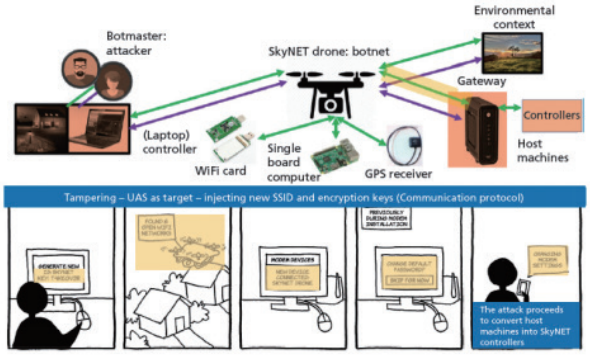

图 3.5 无人机攻击劫持开放网络并覆盖网络设备

3.2.4 无人机作为载体二：无人机注射蠕虫

事件摘要

“我们发现，在不考虑太多的情况下，可以在家庭、办公室和社区中建立一个由数十亿个具有自组织网络功能的微型发射器和接收器组成的密集网络。”

“通过使用这种新的通信媒介，将具有传染性的恶意软件从一个物联网设备传播到其所有物理上相邻的邻居，黑客可以迅速造成全市范围的干扰，而这些干扰很难阻止和调查。”

攻击描述

以色列和加拿大的四名大学研究人员使用 DJI 无人机在以色列贝尔舍瓦的一栋办公楼里注射蠕虫病毒并控制智能灯泡。攻击利用了用于连接灯泡的 Zigbee 通信协议中的安全漏洞。研究人员使用无人机到达离灯泡足够近的地方，发出工厂重置命令。无人机的软件随后更新了设备固件，控制了灯泡，并使它们在莫尔斯电码中闪烁“SOS”。

消除威胁

在 STRIDE 框架内，该攻击构成了一个篡改案例，因为该攻击注入了修改智能灯泡软件的恶意代码，使研究人员能够远程控制它们。

再次，将网络安全杀戮链框架应用到攻击中可以揭示无人机在攻击中的使用阶段。在这种情况下，无人机是在网络安全杀戮链的交付和指挥控制阶段使用的。特别值得注意的是，Zigbee 协议是物联网（IoT）设备的通用通信协议。虽然所讨论的攻击仅仅是为了表明存在安全缺陷，但攻击方法可用于永久禁用所连接的设备或发起 DDOS 攻击。此外，通过使用 Zigbee 无线通信来传播蠕虫，避免了与互联网通信相关的安全措施和流量监视。如第二部分所述，图 3.6 提供了此渐晕图的攻击面和攻击载体可视化。

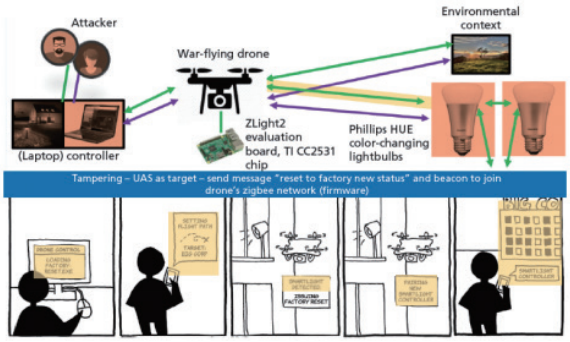

图 3.6 以无人机攻击实施智能灯泡的近距离控制

4 产业趋势与无人机网络安全的未来

无人机技术的变革步伐加剧了其带来的网络威胁。2017 年，无人机相关创新申请了 7356 项专利。其中，有 5696 项（77%）被分配给了中国组织。当技术变化如此之快时，网络安全专业人员经常被赶超。考虑到对中国制造的无人机安全性的担忧，以及中国企业在这一领域的明显优势，有可能会让美国网络安全专业人士停滞不前。尽管专利活动不完全代表技术创

新，但全球专利生产的重大变化有助于确定某一特定技术领域的国家科技优先事项和创新分布的长期趋势。

除了与无人机相关的技术创新的总体速度之外，新兴产业趋势可能会加剧本报告前几节所述的威胁。通过使用户和旁观者暴露于未经授权的特权提升或违反信息保证的风险中，提高无人机功能的趋势可以调节可感知的收益，这由 STRIDE 框架进一步详细说明。同时，这些趋势有可能减轻威胁。例如，由于无人机装备了额外的自主飞行能力，而人工操作人员变得不那么常见，异常系统行为被忽视的可能性会增加，特别是在没有部署自动检测系统的情况下。此外，自动化工具可用于识别和应对攻击。与无人机整体网络威胁相关的其他技术趋势包括：自主飞行能力的日益成熟和使用、无人机交通管理系统、使用 ML 和 AI 检测网络入侵，以及使用区块链技术记录数据和确保通信安全。接下来的部分首先考察了无人机技术的总体变革速度，然后考察了上述特定的新兴趋势。

4.1 技术创新与无人机系统

专利是技术创新的通用代表。专利权是一项创新的财产权，赋予其所有人对基础创新的专有使用权、转让权或合同权。为了获得专利，申请人必须向具有相关技术领域的主题专业知识的专利审查员证明潜在的创新是不明显的、新颖的和有用的。这一条件保证了专利的创新是指从现状出发的改进。然而，在很大程度上，专利是衡量技术变化率的一种有用手段，特别是当它被用于像现在这样大的集合中时。

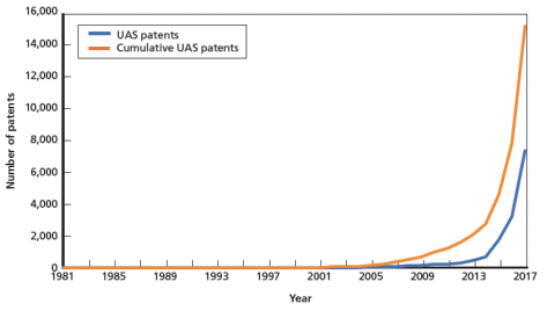

图 4.1 无人机专利数量

图 4.1 显示了无人机专利的年度数量以及累计产出。年度水平表明，随着时间的推移，无人机专利申请在快速增长。自 1981 年获得第一项无人机相关专利以来，已有 19333 项无人机相关技术获得专利。图 4.1 所示的时间趋势表明，无人机专利申请目前正以指数速度增长。2015 年至 2016 年，专利增长率为 76%。从 2016 年到 2017 年，无人机专利以 130% 的速度增长。

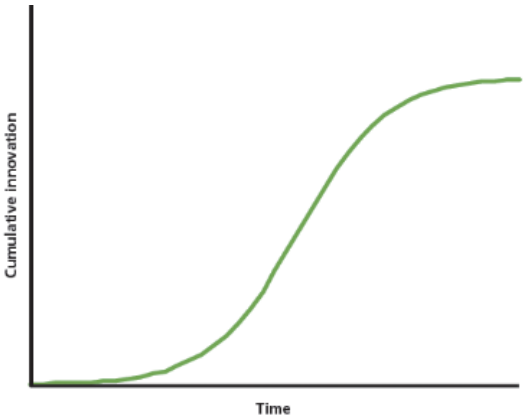

图 4.2 通用 S 曲线

累积曲线有助于评估无人机创新目前在技术创新 S 曲线上的位置。罗杰斯（2003）发现，技术采用通常遵循一种可预测的模式。具体来说，创新率通常遵循钟形曲线。绘制一段时间内的累积采用或累积创新会产生 S 形或逻辑曲线。图 4.2 提供了标准 S 曲线。虽然技术预测超出了

本研究的范围，但结合罗杰斯的洞察和对无人机专利权处于 S 曲线指数部分的观察，表明无人机专利权增长在短期内可能会继续保持较高水平。

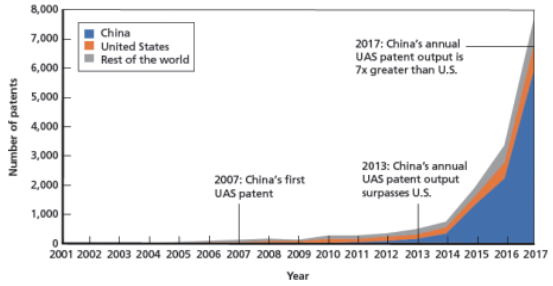

图 4.3 2001—2017 年美国、中国和世界其他地区的年度专利产量

仔细研究这一增长的来源可以发现，最近的增长主要是由中国机构申请专利推动的。图 4.3 描述了来自美国、中国和世界其他国家的组织的年度专利产出。2007 年至 2017 年，中国专利年平均增长率为 191%。美国和世界其他地区的平均增长率分别为 30% 和 40%。

表 4.1 无人机顶级专利组织

Organization	UAS Patents	Country of Origin	Organization Type
DJI	685	China	Firm
State Grid Corporation China	359	China	Firm (state-owned)
Boeing	345	U.S.	Firm
Ewatt Technology	193	China	Firm
Amazon	167	U.S.	Firm
Raytheon	140	U.S.	Firm
Honeywell	133	U.S.	Firm
University of Beihang	131	China	University
Guangdong Rongqi Intelligent Technology	121	China	Firm
Lockheed Martin Corporation	119	US	Firm
Avic Xian Aircraft Design and Research Institute	105	China	Firm
Haoxiang Electrical Energy	101	China	Firm
Southern Power Grid Company Limited	100	China	Firm (state-owned)
Shenzhen Autel Intelligent Aviation Tech.	98	China	Firm
IBM	96	US	Firm
University of Nanjing Aeronautics & Astronautics	91	China	University
Korea Aerospace Research Institute	85	South Korea	Government
Shenzhen AEE Aviation Technology Co. Ltd.	79	China	Firm
Northwestern Polytechnical University	79	China	University
Guangzhou Xaircraft Technology Co. Ltd.	77	China	Firm
Qualcomm	75	US	Firm
Wuhu Yuanyi Aviation Technology Co Ltd	73	China	Firm
United States Navy	70	US	Government
Zero UAV Beijing Intelligence Technology	62	China	Firm
BAE Systems	61	UK	Firm
Geer Technology Co. Ltd.	61	China	Firm
Prodrone Craft Technology Shenzhen Co.	61	China	Firm
Samsung Electro-Mechanics Co.	58	South Korea	Firm
Aerovironment, Inc.	56	Canada	Firm
China Academy of Aerospace Aerodynamics	54	China	Government

考虑到负责无人机专利的组织也是例证。表 4.1 列出了主要的无人机专利申请机构。该表显示，中国和美国的组织包揽了对无人驾驶飞机创新的最大份额。值得注意的是，美国在无人机领域的创新主要是由企业驱动的，而中国的无人机创新在私营部门、大学、政府实验室和国有企业之间的分配更为平均。

4.2 新兴无人机行业趋势

许多行业趋势对无人机的网络影响具有重要意义。这些趋势包括自主飞行能力、无人机交通管理、群集、使用人工智能检测无人机网络攻击、硬件复杂度和供应链增加以及无人机区块链。下面将描述这些趋势，并强调行业专家对无人机和网络安全未来的一些担忧。

4.2.1 自主飞行能力

典型的无人机需要远程飞行员来控制飞机的油门、航向、俯仰、偏航和横滚。飞行员还可以决定何时以及如何控制机载设备，如摄像机。然而，无人机制造商已经开发并正在继续开发能够自主操作的飞机。自主操作在这里被定义为无人机飞行的轨迹不是由人类飞行员连续控制的操作，人工智能系统具有实质性的规划权限，并适应飞行过程中遇到的情况。这种能力包括对意外情况的自适应响应，而不是根据预定义规则控制其子系统的自动无人机。作为展示自主飞行能力的产品的一个例子，Skydio 目前在市场上销售一种“自动飞行相机”无人机，能够跟踪和记录用户，同时感知和避开障碍物。Vantage 机器人公司还推出了一种能够感应和避开障碍物的无人驾驶飞机，它可以通过磁耦合

轻松分离，并采用笼形转子。这些功能使它成为联邦航空局（FAA）认证的唯一能在人群上方飞行的小型无人机。当前，几个知名新闻机构都在使用这种无人机。

其他公司也以其他方式增加了无人机的自主性。例如，“返回家园”功能已变得无处不在，通过该功能，无人机在激活该功能后会自动返回其操作员。类似的，支持 GPS 的航路点导航在流行的无人机平台上是标准配备，包括 DJI 幻影、Inspire 和 Mavic。Airobotics 出售“自动化工业无人机”，宣传“不需要飞行员”这一事实。

最近，研究人员在使无人驾驶飞机自主运行所需的技术小型化以及改进技术以实现高速自主飞行方面取得了进展。一家咨询公司估计，到 2022 年，一半的商用无人机航班将实现自主飞行。美国军方已经注意到自动无人机的实用性。美国空军的一份报告指出，与自动化系统不同，自主系统使无人机能够“在不可预测的环境和情况下以目标为导向”，因此这种系统在军事任务中提供了明显的好处。

如果无人驾驶飞机具有自主飞行能力，则很可能更难发现和应对网络攻击。更可能的是，在任何给定的时间都不会有操作人员监视单个无人机，这使得不太可能注意到异常或未经授权的系统行为。此外，自主系统所做的规划不一定能被人类理解或解释。例如，自主使能技术小型化的研究是基于一种称为无人机的“轻量剩余卷积神经网络结构”。这些技术从原始图像数据开始实时处理图像，然后迭代地应用多个卷积滤波器并降低结果的维数。在重复上述步骤几次之后，通常使用传统的神经网络来处理结果，并最终得到诸如物体检测等应用。对人类来说，追踪这样一个系统，并理解例如为什么一个系统在撞上障碍物之前没有看到障碍物是困难和耗时的。这使得很难将异常行为和可能的恶意行为与良性行为区分开来。这也增加了目标攻击的可能性，即“诱骗”自治系统以意想不到的方式运行。

4.2.2 无人机流量管理（UTM）

航空导航服务提供商（ANSPs）为常规载人飞机和航空母舰的飞行员提供空中交通管制和管理服务。这些组织确保利益相关者遵守既定的政策和程序，确保安全和高效的运作。它们在战术和战略层面上维持并向其他国家提供空中运输系统资源和相关信息（如天气预报数据）的态势感知。交通管制员可能会要求飞行员按照特定的航线飞行，并在出现问题时改变航线，以确保飞机之间的距离不会超过几海里或障碍物。交通管制员管理对共享资源的访问，如机场滑行道和跑道，避免不公平的结果。

美国联邦航空局（FAA）空中交通组织（ATO）在美国以及大西洋和太平洋附近地区充当 ANSP。特别是，FAA ATO 积极监测和管理“管制空域”的空中交通，包括相对繁忙的机场附近和较高高度的空域。对于在管制空域使用无人机的运营商来说，与无人机系统的协调是必不可少的。对于运营商在可能有另一架无人机、直升机或其他空中交通的无控制空域驾驶无人机，还需要某种形式的空中交通管制和管理。采用类似的方法来管理无人机的流量，可能不是最佳的，甚至是不可行的，因为目前的空中交通管制和管理是用来管理控制空域中的常规

飞机的。但是，很明显，某种形式的无人机流量管理是必要的。

相关系统通常标记为 UTM 系统，现在正在开发中。例如，泰雷兹生态系统 UTM 承诺“自动飞行授权以及紧急情况下的实时警报和干预”。AirMap UTM 平台包括“空域管理人员和无人机操作员之间的双向通信能力”。特别是，备受瞩目的政府机构正在努力“整合”无人机和常规飞机交通。这些努力通常会促使私人公司帮助建立并实现无人驾驶飞机交通管理的愿景。欧洲空中交通管理研究（SESAR）U-space 项目的目标是在近期内支持无人机的“电子注册、电子识别和地理围栏”，之后转向无人机的“飞行计划、飞行批准、跟踪和与常规空中交通管制的接口”。在美国，由国家航空航天局领导的一个项目简称 UTM，旨在开发支持空域设计、走廊、动态地理围栏、恶劣天气和风规避、拥挤管理、地形规避、路线规划和重新布线、分离管理、排序和间隔以及应急管理的技术。

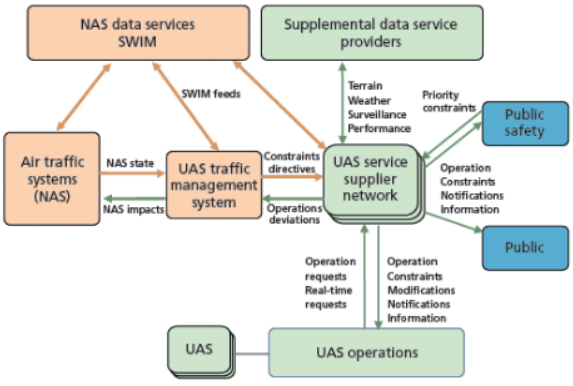

图 4.4 与 UTM 相关的通信

在美国航空航天局的 UTM 愿景中，无人机操作员向服务供应商发送数据和授权请求。这些服务供应商向无人机运营商发送通知和信息，使运营商能够提高其态势感知能力。服务供应商不是 UTM，服务供应商与 UTM 沟通，UTM 履行“调节器 /ANSP 功能”，服务供应商还与其他方沟通，例如获取航空气象数据。图 4.4 说明了支持 UTM 愿景所需的通信。

注意，使用 UTM 系统会创建新的通信通道，这些通道可能被利用。这些新通道提供了访问多个无人机、多个无人机运营商和 ANSP 的新方法。UTM 系统和服务供应商必须从多个无人机和多个无人机运营商收集数据。这个集合使得 UTM 系统和相关网络成为网络攻击的潜在目标。还要注意，联合技术管理系统和服务供应商可能成为安全和有效利用空域的关键。这个角色也强调了保护他们免受网络攻击的必要性。

UTM 系统开发人员目前正在使用移动电话运营商提供的相同的无线通信技术和基础设施。例如，在最近的一次演示中，高通公司使用 LTE 网络通信标准将无人机与 UTM 系统连接起来。虽然高通公司相信 LTE 可以支持一些无人机的使用，但它正在推广 5G 移动通信技术的广泛使用，认为这对于“大规模部署任务关键型无人机用例”是必要的。高通公司将“强大的安全性”列为 5G 的卖点之一。

4.2.3 无人机群集

无人机群集包括协调多个无人机的运行，以完成特别大规模或复杂的任务。群由多架飞机或（相对较少的）同类飞机组成，可以集中管理，也可以通过分散控制算法进行管理。一般来说，群集通常依赖于具有自主飞行能力的单个小型无人机系统，并使用成像和传感器来获取环境中的信息。群集可以利用这些信息进行机动，

并利用通信技术接收和传输信息。群集也会产生集体的功能能力，并可能表现出基于任何一架无人机的特性而不明显的计划外解决方案。

迄今为止最雄心勃勃的群集演习是 2017 年 4 月的美国服务学院挑战赛，由国防高级研究计划署（DARPA）的 OFFSet（进攻性群集使能战术）项目负责，该项目使美国军事学院、美国空军学院和美国海军学院在加利福尼亚州帕索罗伯斯北部的一个陆军国民警卫队哨所即罗伯茨军营上空相互对峙。每所学院都展示了他们在这一学年中发展起来的攻防战术。

两队一次在战斗方块内比赛，一方空域 500 米，高 78 米。每支队伍都有 20 架固定翼无人机和 20 架四旋翼无人机，根据游戏规则，每两轮 30 分钟的战斗中，每轮最多可部署 25 架无人机的混合舰队。每支参赛队都必须保护好自己的“旗帜”（一个巨大的充气地面目标），同时在时间耗尽前努力得分最多。如本次比赛中所示，群集的好处包括在可以并行运行的任务上提高性能，在不同位置同时执行多个操作的能力以及增强的容错能力。缺点包括群中的单个飞机相互干扰的可能性，其他飞机正在做什么的不确定性，以及部署和管理群的总体成本。无人机群通常也由自身能力有限的飞机组成，例如，识别或对抗恶意指令的能力。

DARPA 目前正在运行另一个名为 Gremlins 的项目，该项目正在调查从常规飞机上发射无人机群，其最终目标是为步兵部队装备更多的 S 型无人机。俄罗斯军方声称，它在叙利亚的基地遭到了无人机群的袭击。美国空军的一份技术报告指出，群集具有优势，例如“当从三个或更多的有利位置看到目标时，能够三角定位”。

现在有大量关于群集的学术文献，特别是群集所需的控制结构和算法。例如，一篇文章提出了“一种基于信息理论和分布式数据融合的分散方法，这种方法可以扩展到大量协作的小型无人驾驶飞机系统（S 型无人机）平台”。其他的研究工作则从成群的鸟和鱼群中获得灵感。作者注意到，考虑到来自多个 S 型无人机的传感器读数，定位目标的地理位置更加容易和快捷。

群集需要自主飞行能力，这引起了本节前面提到的与网络安全相关的担忧。群集还需要进行某种形式的管理。集中式管理权限是网络攻击的合理目标，因为对该权限的访问或控制将使攻击者能够同时获得数百架飞机上的数据或对其进行控制。即使是分散的管理方案也依赖于广泛的通信，这些通信可能会受到攻击，以帮助恶意参与者理解或更改操作。例如，注意图 4.5 中作者提出的“分散资产管理器”和其他资产之间的许多联系。正如 Higgins、Tomlinson 和 Martin（2009）所指出的，“群机器人可以显式或隐式交互”，但是，无论是以哪种方式，“任何开放的隐式或显式通信方法都可能被攻击者干扰、截获”。

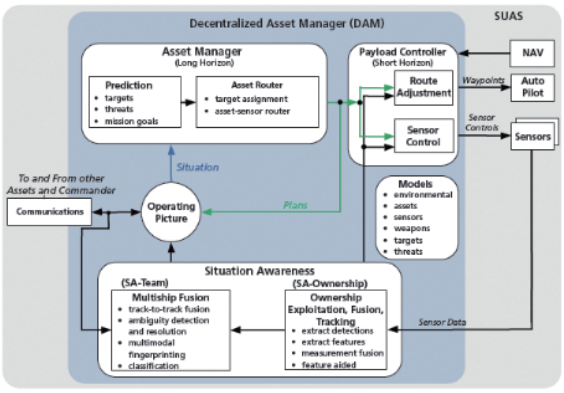

图 4.5 用于群集的分散式资产管理器

支持群集所需通信的技术包括射频（RF）和 LTE 技术。这些技术存在已知的网络问题。例如，LTE 使用具有已知漏洞的“商品硬件和软件”。干扰仍然是一种“未解决的威胁”，能够阻止射频和 LTE 信号的成功传输。软件定义的无线电将有助于通过促进对射频环境的动态感知和适应来减少漏洞。多孔径技术提供了进一步的选择，利用空间分集和相干性将传输转向预定的接收机，并使干扰源为零。为了改善射频传播，可以使用分布式相干和多天线技术来保持对射频环境的感知。

对大量无人机期刊文章的研究揭示了两个额外的见解。首先，近年来对无人机集群的科学研究已经加速，并且正处于指数增长轨道。其次，正如在整个无人机专利申请中所观察到的那样，无人机集群的科学文献越来越多地被中国的组织所主导。

图 4.6 描述了无人机集群领域的年度世界科研产出。自 2002 年发表第一篇关于这一主题的期刊文章以来，这一子领域呈指数增长。事实上，指数函数与数据的拟合显示了相对较好的拟合度。

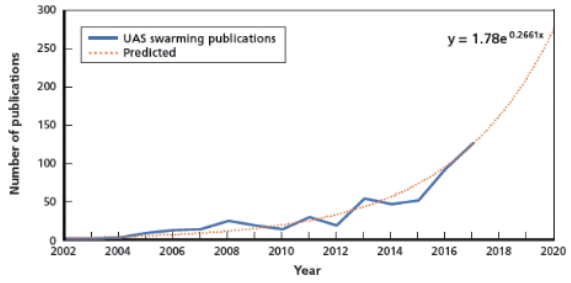

图 4.6 关于无人机群集的出版物数量

第二个观点是，中国的组织包揽了大部分的研究成果。表 4.2 显示了该子领域中最多产作者的隶属关系。图 4.7 描述了作者关系的协作（合著）网络。网络图显示，中国研究人员正在建立强大的科学实践社区。知识网络的存在表明某一特定部门有一个健康的国家科学界；它们表明存在组织间信息流动的渠道。在网络上观察到的 8 个合著群体中，有 4 个在作者职位贡献方面被中国组织所主导。北京航空航天大学与清华大学的合作关系在整个合作网络中是最强的。

表 4.2 大批出版物作者的隶属关系

Organization	UAS Swarming Publications	Country of Origin	Organization Type
Beihang University	51	China	University
Beijing Institute of Technology	19	China	University
Technical University of Dortmund	12	Germany	University
Cranfield University	11	UK	University
Tsinghua University	11	China	University
United States Air Force	10	U.S.	Government
De La Salle University	9	Philippines	University
Nanyang Technological University	8	China	University
Harbin Institute of Technology	7	China	University
PLA National University of Defense Technology	7	China	University

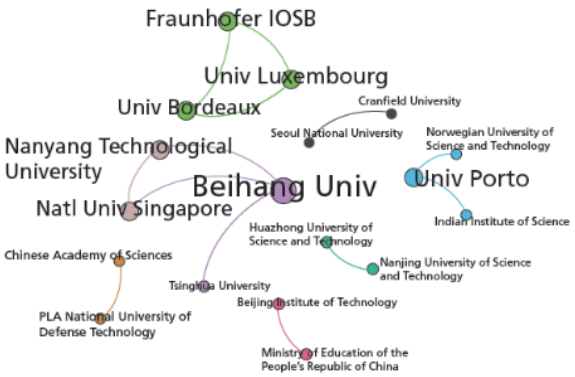

图 4.7 大量的出版物网络

4.2.4 利用人工智能检测无人机网络攻击

一些新出现的技术趋势可能有助于减轻本节前面概述的风险，以及报告中与入侵检测和篡改系统功能相关的其他部分。其中一个趋势

是使用 ML 和 AI 技术来实时检测网络攻击。

网络安全中的入侵检测问题涉及在使用网络系统的人员中识别恶意使用和违反政策的行为。许多研究者提出在网络和系统通信中使用 ML 和 AI 方法。Buczak 和 Guven 在 2016 年一篇关于这个话题的调查文章中指出，已经应用的技术包括神经网络、决策树、集成学习和支持向量机等。这些都是常用的 ML 方法。这些技术能够通过监视网络流量来识别各种类型的入侵和攻击。作者发现，无法最大程度地应用此类技术甚至无法进行公平比较的“最大差距”是缺乏训练数据，即包含已知入侵且可以用来训练算法以检测未来的威胁的数据集。Jones 和 Straub 注意到一些“机器学习技术已经被用来解决入侵检测问题”。作者接着介绍了一种专门针对“自主机器人”的入侵检测方法，其中包括一个识别“机器人决策中的特征”的组件，本质上是揭示机器人行为方式的重要活动，以及另一个基于“深度神经网络的活动，该网络被训练来检测偏离预期行为的命令”。

特征识别是基于先前识别信号的数据库。总体方法包括基于规则的系统和神经网络的组合。在这一领域中，类似的混合方法被相对频繁地提出。这种方法可能有希望检测网络无人机攻击，不过同样的，缺乏训练数据是一个挑战。

少量但不断增长的文献更具体地关注于无人机的入侵检测。该主题通常与故障检测联系在一起，这是一种在无人机的某个组件出现故障时进行实时识别的相关思想。例如，Abbaspour 等人（2017）提出了一种基于神经网络的方法，该方法可检测“无人四旋翼传感器”的故障和错误数据注入攻击。Gil Casals，Owezarski 和 Descards（2013）描述了一种基于支持向量机的“机载网络攻击自主检测”方法。这里的机载网络包括相互通信或与地面系统通信的飞行器。Sedjelmaci 和 Senouci（2018）描述了一个“安全框架”，用于减轻对机载网络的攻击。作者描述了不同的数据如何与不同的目的相关，例如，如何使用“数据注入率”来检测“虫洞和黑洞”攻击，而“信号强度”则可用于检测“干扰”和“GPS 欺骗”攻击。Aktaş、Gemci 和 Yağdereli（2015）同样对威胁进行分类，然后提出应对此类威胁的一般指导。作者指出，无人机“必须具备防御能力和措施，以便能够自动和动态地应对意外和故意的缺陷和攻击”。

4.2.5 硬件和制造复杂性

商用无人机正变得越来越复杂。硬件和软件复杂性增加的一个后果是，跟踪和验证在特定平台上运行的各种进程变得更加困难。此外，将自动化和计算机辅助设计引入无人机和组件的制造，意味着对系统组件的监督和责任可能越来越难以追踪。通信（例如蓝牙、GPS、WiFi、USB）、传感器（例如红外、雷达、激光雷达）和飞行控制（例如自动驾驶仪的人工智能、动态跟踪、群体行为）系统中的特定组件可能很容易受到攻击，暴露于此类漏洞可能越来越难以发现。

从本质上讲，无人机充当一个组件网络时，这些组件相互通信，并具有不同级别的相互依赖性。与软件病毒一样，硬件组件（主要是集成电路）也可能被注入恶意代码，从而基于定义的输入序列导致不必要的行为。这已经在无人

机中发生了。大多数公用无人机模型由第三方知识产权块组成，其中一个或多个可能在设计、制造、配置甚至使用阶段受到感染。新技术为感染这些硬件系统提供了新的攻击载体。例如，以色列本古里安大学（Ben Gurion University）的研究人员在2016年演示了对三维（3D）打印无人机螺旋桨的首次完全破坏攻击。如今，用于制造大多数电子电路的计算机辅助设计（CAD）工具提供了类似的攻击入口点，例如，通过恶意绘图文件导致内存损坏。

对于硬件威胁识别，这些组件故障的级联性质增加了复杂性，并且可能无法发现，除非使用专门的仿真软件。恶意逻辑可能导致不必要的情况，例如导致系统将数据输出到错误的端口或地址（信息泄漏）、监视和修改系统的输出数据（篡改）或通过更改系统的内部计时或控制禁用系统。所有这些都可以通过改变或添加内部逻辑来实现，这样传统的测试和验证工具就不太可能检测到这些逻辑。

4.2.6 无人机区块链

区块链技术也与无人机扩散对网络安全的影响有关。区块链是存储在分布式公共分类账本中的加密记录列表。第一个引人注目的区块链记录交易涉及比特币数字货币。比特币的每个用户都维护一个区块链副本，所有区块链副本都会定期更新。公司区块链开发管理比特币的工具。值得注意的是，比特币被贴上了为有组织犯罪和恐怖组织洗钱的标签，它可能被用来资助本报告所述类型的攻击。事实证明，区块链特别擅长支持自动化、安全的交易注册。

许多公司已经提议使用区块链来记录无人机交付的货物（如Dorado、Walmart）。其他人建议使用区块链来管理无人机运营商和“航空当局”之间的通信，包括那些可能管理或使用UTM系统的人（例如，应用区块链）。正如一个宣传网站所指出的，许多联合技术管理的研究和开发工作都在寻求“建立一个不需要持续的人类监测和监视，并且仍然能够确保真实性、安全性的系统，低空空域无人机的安全和控制……区块链可以促进所有这些功能”。学术研究人员已经开始研究区块链在UTM中的潜在用途。最近一篇文章提出了一种基于区块链的无人机“交通信息交换网络”。

区块链的分散性、重复性，特别是通过设计对区块链正常运行中使用的数据质量进行冗余检查，使得攻击者很难调整或删除记录。例如，此功能可能使攻击者难以修改UTM系统中的飞行计划。加密的使用支持安全通信。这种加密可能会使对手更难从无人机上收集信息。此外，数据存储的分布式特性引起了安全问题。区块链技术可用于记录、收集和轻松搜索无人机曾在何处或做过什么的信息。此方面可能会导致攻击或应用程序识别恶意无人机或无人机使用中的意外模式。

《哈佛商业评论》的一篇文章称，由于技术的相对新颖性和复杂性，区块链“距离充分发挥其潜力还有几十年”。2017年10月发表的一项研究，包括对供应链和物流专业人士的调查，发现只有20%的人实施过任意形式的“区块链解决方案”。据接受调查的专业人士称，阻碍区块链广泛使用的主要障碍包括：“监管不确定性”，不同方面的需求同意并使用一个

共同的系统，以及“缺乏技术成熟度”。数据安全也是一个主要问题。目前还无法判断区块链对商用无人机的网络安全会产生什么样的影响，但这绝对是一项技术和趋势，值得在未来几十年内进一步审查。

4.2.7 改进的黑客和恶意软件交付支持

除了上述可能有助于提高无人机性能、安全性或识别和应对攻击的能力的一些趋势外，新技术还支持攻击者。许多型号的无人机很容易被恶意行为人禁用甚至增选，而现成的技术有助于支持这种行为。

例如，SkyJack 是一个可以利用民用无人机弱加密 WiFi 接入端口的应用程序。它使无人机或计算机能够寻找并控制附近的其他无人机。SkyJack 通过网络安全软件瞄准了 Parrot AR. 2.0 无人机。Airpack–ng 是一种安全软件，用于通过 WiFi 接入点识别目标的无线网络和客户端。在获得对网络及其客户端的访问之后，应用程序通过断开所有连接的客户端并请求控制现在“不受控制”的无人机来控制目标。SkyJack 值得注意的是它是可伸缩的。一个 SkyJack 实例可以危害多个目标，而且它很可能适用于多种不同类型的无人机，因为它的源代码是公开的，并且利用了无人机上一个通用的未受保护的 WiFi 访问端口。

Maldrone 是一种可以远程或本地使用的恶意软件，它可以在所有者不知情的情况下访问无人机的操作系统。它被设计为“有史以来第一个无人机后门”，并且通过将自己作为中间人插入无人机的自动化软件和硬件之间的通信中而起作用。它监听来自真实端口的流量，并使用代理端口向命令程序发送伪造和合法命令的组合。Maldrone 的源代码是对公众开放的，可以很容易地适应感染许多类型的无人机。Maldrone 也可以远程上传到无人机中，有可能使恶意参与者一次捕获多个无人机。因此，恶意行为者可以使用 Maldrone 向受感染的无人机发送各种命令，从远程监视到获得对无人机飞行的控制。

4.2.8 基于代理的无人机防御建模与仿真

本报告不包括关于反无人机的大量文献。然而，在某些情况下，对无人机的物理防御实际上可能有助于防止无人机用于传递恶意软件或通过接近获得对系统的访问的网络攻击。因此，发展改进的仿真技术来辅助建立物理无人机防御系统是值得注意的。由新西兰国防技术局开发的地图感知非均匀自动机（MANA）等技术越来越多地被用于了解各种防御方法的威胁和效能。这种模拟允许用户研究无人机特性（例如，射击速度、飞行速度、有效载荷）和防御特性（例如，通信系统、识别精度、延迟）对攻击结果的影响，为决策者提供对其对抗无人机能力的洞察，无论是现在还是将来，无论是攻击方还是防御方都可能取得技术进步。

表 4.3 无人机的主要特点和趋势概述

Trend	Key UAS Feature	STRIDE Taxonomy Threat	Vulnerabilities and Attack Vectors
Simplified Control and Operation	Camera view-based flight; following target on camera	Repudiation and Information Disclosure	Third-party monitoring of user activities
	Gesture and speech-directed flight control	Elevation of Privilege and Tampering	Alteration of factory-installed configurations
Self-Operation and Vigilance	Location or sensor-based payload manipulation (e.g., crop spraying, medical supply delivery)	Elevation of Privilege	Intercept of payload usage or delivery
	Swarm drone maneuvers; multi-UAS operations	Elevation of Privilege and Tampering	Scaled-propagation of operational errors
	Preplanned hovering; patrol routines	Spoofing or Tampering	Override of authentic GPS signal or uploaded navigation files
Self-Maintenance and Protection	High-speed obstacle avoidance	Spoofing and Denial of Service	Sensor saturation or interference for obstruction of “view”
	Auto-docking; recharge; return to home	Repudiation and Information Disclosure or Spoofing and denial of service	Third-party monitoring of user activities and sensor interference for failure to register “home” state

表 4.3 总结了本节讨论的一些与无人机相关的主要趋势。此表还确定了由于这些技术发展而可能面临更大风险的跨距维度。该表还指定了由于这些技术趋势而可能打开的攻击载体。

4.3 行业趋势：结论

网络安全和无人机领域的专家对上述趋势有许多共同的担忧。在致力于市场引进的同时，许多生产公用无人机的公司忽略了有意义地解决强化其平台以抵御网络攻击的问题。然而，随着这些无人机开始被用于 DHS 任务，它们将不得不遵守围绕网络安全和数据保护的新兴标准。许多业内人士将等待标准发布，以便在市场上脱颖而出，在美国政府和地方执法市场上抢占市场份额。

下一步有助于解决行业领袖和政策制定者的一些担忧，可能是建立更加标准化的无人机测试方法。很明显，其他由联邦政府资助的研发中心和无人机专家将支持这一战略。为此，建议政府采取统一和合作的方法，建立一个无人机测试范围，可以测试和验证供应商声称的实际公用无人机性能。

5 无人机、网络安全和 DHS

本节着眼于无人机网络漏洞和功能影响国土安全部（DHS）的方式，以及潜在的和当前的 DHS 为解决无人机网络问题而做出的努力。首先研究了以无人机为目标或载体的 DHS 攻击。然后研究了相反的情况：DHS 可能在进攻性地使用无人机。最后，通过研究 DHS 部门和办公室如何减轻这些担忧，DHS 内目前正在进行的与无人机网络安全相关的项目，以及当前和未来的政策可能有助于或阻碍 DHS 决策者，来了解 DHS 如何解决无人机网络担忧。

5.1 对 DHS 资产的攻击

5.1.1 DHS 以无人机为目标

如第三部分所述，将无人机网络漏洞分为两大类——针对无人机自身的漏洞和将无人机作为网络攻击载体的漏洞，可以提供分析优势。尽管一小部分 DHS 办公室和部门目前易受一种或两种类型的攻击，但公用无人机的普遍使用以及与之相关的这些系统的易用性将进一步提高 DHS 在多个方面的风险水平。

有四个 DHS 部门记录了无人机在日常活动中的历史使用情况：美国海岸警卫队（USCG）、美国海关与边境保护局（CBP）、联邦应急管理局（FEMA）及网络安全和基础设施安全局（CISA）。这些部门中的大多数还计划扩大其对无人机的使用：USCG 计划为其全部国家安全部门配备小型无人机，CBP 正在探索使用小型无人机来补充其资产，FEMA 也表示有兴趣扩大其对无人机的使用。此外，ICE 还处于了解无人机如何增强其战地代理能力的初始阶段。

DHS 组件正在使用并将继续使用国防部开发的（捕食者和扫描鹰）和商业开发的无人机。然而，除了 USCG，所有组件都计划在未来投资商用无人机。这意味着 CBP、FEMA、CISA 和 ICE 的资产都将以下列方式易受第三部分所述类型的攻击。

5.1.2 以无人机为载体的 DHS 攻击

几乎所有的 DHS 部门和办公室都可能成为无人驾驶僵尸网络或数据过滤攻击的受害者。

它们都有敏感数据和无线网络普遍存在的物理位置，使它们成为此类攻击的目标。例如，具有游荡能力的无人机（能够在一段时间后再次降落和起飞的无人机），允许进行这种隐蔽攻击，进一步增加了未加固系统的风险。

随着连接设备的普及，无人机注射蠕虫或类似攻击的危险也会增加。此攻击载体不必限于 DHS 网络和连接的设备，因为 DHS 员工的个人设备或家庭网络也可能是恶意代码的接入点，以便通过无线方式或由员工将受感染的设备连接到 DHS 笔记本电脑来进入 DHS 系统。

5.1.3 以无人机为载体的 DHS 攻击性网络行动

尽管如上文所述，DHS 可能是敌方无人机的攻击目标，但它当然可以使用无人机执行自己的攻击性网络行动。DHS 可以使用无人机秘密观察目标或可疑对手。例如，无人机可以进入涉嫌协调走私行动的本地网络。这种类型的访问也可以用于公开的攻击性方式，例如禁用或向联网的安全摄像头提供虚假信息，并在 ICE 的突袭之前立即发出警报。

无人机对无人机的攻击性网络行动也可能是有用的。当地面或载人平台缺乏追击这些快速目标所需的机动性或快速反应能力时，CBP 可以利用无人侦察机来捕获或摧毁参与走私的无人侦察机。联邦应急管理局可以选择使用无人驾驶飞机在灾区拦截或禁用无人机，以便直升机能够安全通行。一个更具选择性的版本可能涉及一个联邦应急管理局的无人机，只攻击那些没有发出敌友识别码的无人机。最后，DHS 可以使用自己的无人机部队巡逻敏感的物理位置，并使在该地区靠近任何 DHS 组成部分的敌方无人机失效。这一特性可能会对 CBP、FEMA、CISA 和 ICE 产生特别的吸引力。然而，如前一节所述，出于对无线网络和未来物联网的考虑，几乎所有 DHS 办公室和部门都是潜在的目标。

5.1.4 DHS 部门和办公室作为缓解措施

DHS 的某些部门和办公室在降低这些风险方面处于领先地位。特别是，CISA 和科学技术董事会可以制订技术解决方案，而管理董事会、业务协调厅和战略、政策及计划厅可以从政策角度解决问题。

缓解战略可能来自三种途径。以无人机为目标，根据当前和未来的趋势，有三项建议可能有助于 DHS 更好地定位自身：（1）DHS 应与无人机制造业接洽；（2）DHS 采购部门和政策制定者可以创造一个环境，使 DHS 在尽可能小的风险下运营安全的无人机。（3）对于作为载体的无人机，所有的部门和办公室都可以通过保护和强化其网络，开发防御作战行动，以随机化无人机的部署配置，利用二级数据源进行网络篡改检测，并在实地任务时间表内实施功能完整性检查，从而降低风险。

如第三部分所述，无人机作为目标具有多个漏洞，并且这些漏洞在潜在的攻击载体中大量存在：糟糕的密码安全性、已知的默认设置和未受保护的 ad hoc 网络都是攻击者的入口路径。各个子系统及其通信链路中也存在漏洞。DHS 应通过合作与行业领袖接触，制定安全公共用途无人机的标准。虽然此类标准不会在整个行业内采用，特别是外国制造商，但这一过程可以鼓励制造商创建对安全问题更为敏感的无人机。不过，需要注意的是，敌方将有同样

的能力购买这些网络化的无人机。这种典型的攻防竞争的措施和对策周期应鼓励 DHS 科技部门在允许的情况下投资于无人机网络脆弱性威胁和缓解研究，以确保 DHS 始终处于这些主题知识的前沿。

DHS 的决策者和采购部门必须确保其购买满足安全考虑的无人机，从而跟进研究和行业参与。战略、政策和计划办公室以及管理局都对整个政策部门有影响。将要使用无人机的所有部门和办公室（如前所述，CBP、FEMA、CISA、ICE 和潜在的 USCG）也必须支持无人机安全政策，并为购买安全无人机的收购创造激励。

为减少无人机作为载体，所有 DHS 办公室和部门应确保其网络安全可靠，抵御无人机发起的网络攻击。与以无人机为目标一样，战略、政策和计划办公室和管理董事会可以制定激励措施和政策，以确保实现这一目标。DHS 还应就物联网和不安全设备带来的危险对员工进行教育，以降低恶意行为人从受损信息技术平台进入的风险。在评估无人机反措施（包括反无人机的潜在使用）时，无人机部门应与总法律顾问办公室和隐私办公室联系，以确保这些反措施及其使用是合法的。

5.1.5　相关 DHS 项目

虽然已经提出了 DHS 在未来如何选择行动来保护自己免受无人机网络攻击的问题，但需要注意的是，DHS 已经在解决这个问题。DHS 最近运行了（并且正在运行）几个与此报表相关的项目。DHS 在其科学和技术理事会中设有无人驾驶飞机系统（PEO UAS）项目执行办公室。该办公室的一项职能是“启用”无人值守飞机，以便在 DHS 的活动中进行整合和就业。PEO–UAS 最近发布的一份关于这一主题的情况说明书指出，最近完成的一项研究和对在 GPS 技术受到威胁的环境中使用的 sUAS 的模拟揭示了其弱点。

作为 2016 年和 2017 年第一响应者电子干扰演习的一部分，DHS 试图“演示和分析电子威胁对 sUAS 技术的影响”。DHS 担心，能够破坏电子通信系统的廉价设备的可用性日益增加，而 sUAS 技术是潜在的有吸引力的目标。这些演习为 DHS 提供了一个机会，在存在威胁的现实环境中研究脆弱性。

5.1.6　与 DHS 和无人机网络安全有关的当前和未来政策

正如时任 DHS 部长 Kirstjen Nielsen 最近强调的那样，当前的政策限制了 DHS 为维护国土安全和自身利益免受包括网络攻击在内的无人机攻击所做的努力。然而，最近提出的立法表明，在不久的将来，这些限制可能会放松，使 DHS 能够更自由地应对与无人机有关的网络威胁，并从无人机平台上发起攻击性的网络选择，尽管某些关切领域仍可能限制 DHS 的权威和行动。

然后，尼尔森部长在《华盛顿邮报》的一篇社论中指出，“除非采取行动改变政策，否则美国政府将无法识别、跟踪和减轻空中的武器化或危险无人机”。具体而言，DHS 缺乏处理其资产所在地的无人机威胁的权力和设备。它无法拦截和覆盖无人机控制信号或采取防御行动，因为现行政策将无人机视为等同于有人驾驶飞机。征用无人机的控制信号也违反了《窃

听法》《计算机欺诈和滥用法》等法规。拟议立法将给予政府机构豁免，特别是在处理无人机时。此外，现行法律禁止在城市地区和属于DHS管辖的大型公共活动等相关操作环境中测试新的防御技术。

无论未来立法采取何种形式，在打击无人机威胁时，它仍将限制DHS的行动和能力，但须考虑维护公民隐私和新闻自由，以表达可能反对DHS权威的公众意见。事实上，最近的参议院法案很快从最初的草案中修正，包括将国土安全监测和反措施的范围和持续时间限制在“合理”水平的措辞。这项拟议的立法表明，能够快速检测、跟踪、识别和应对威胁的技术将对DHS具有很高的价值。然而，反无人机工具和概念必须限制附带损害（例如，劫持特定控制信号，而不是对宽带的全面干扰），并保护隐私。

6 结论与建议

在本报告中，着重于了解和记录与无人机和网络安全相关的漏洞和攻击机会的框架和方法。本节介绍了一个工具包，它可以帮助决策者了解相关的网络安全威胁空间，并对当今各种来源的威胁进行调查。我们还总结了未来可能随时间改变威胁空间的趋势。最后，我们关注这些话题与DHS的相关性。

本报告主要针对网络安全对无人机威胁进行分类，并提出一种有助于分析这些威胁的方法，目的是指导缓解和防御策略的工作。然而，重点强调的威胁的优先次序和后果的可能性没有得到解决。在识别和理解这些威胁类型后，决策者仍然需要了解每一种威胁发生攻击的可能性、这种攻击的后果以及防止或利用这种攻击的机会。作为保护自身免受无人机相关网络攻击或成功使用无人机作为网络资产的第一步，DHS可以使用本报告中概述的方法来了解攻击载体集和攻击面。这是一个必要的步骤，但不足以为网络防御或攻击性网络行动建立一个连贯的无人机和网络安全计划。

在更好地了解威胁空间后，DHS必须继续与高级决策者、网络安全专家以及其他政府和执法机构合作，朝着统一的无人机网络战略迈进。这项工作将涉及对无人机平台进行清查和分类，了解无人机相关网络攻击的可能后果和缓解方案，并跟上可能改变威胁空间的新技术发展。DHS应与私营部门、国家实验室和其他政府利益相关者合作，投资运营一个或多个无人机测试靶场。这一步骤将有助于确保行业遵守安全和安保协议，并有助于机构间协调。捕获和控制一架更大、更重的固定翼无人机，能够飞得更远并携带沉重的载荷，将比当地公园的一名爱好者驾驶的小型四翼无人机面临更大的风险。当运营商从事更为敏感的操作时，涉及无人机运营商数据被盗的攻击将更加严重。

DHS还应优先考虑最关键的漏洞，并找到关闭攻击载体和保护攻击表面的方法。为了了解缓解方案，DHS将需要监测反无人驾驶飞机系统的技术发展，并试验新的攻击技术。可能需要一个协调和可更新的监测和干预系统，因为网络攻击和对策的创新周期表明，即使是加固系统也无法保证免受攻击。

最后，DHS将需要监测无人机的采用情况，

并预测无人机广泛扩散的影响。自主飞行和群集等能力将拓宽无人机的应用空间。随着无人机在更广泛的活动中的使用，在任何给定时间合法使用无人机的数量都将增加。从减少威胁的角度来看，在无人机密集的新环境中，最重要的任务之一将是区分合法与非法活动。

关于作者

凯瑟琳·莱贝斯特，兰德智库工程和应用科学部的副研究部主任和运营研究员。她的研究兴趣集中于运筹学和金融工程方法在国家安全、战略规划、风险管理和教育领域的应用。莱贝斯特的国家安全工作包括军队发展和战备、部队规划和资源配置、军事人力和劳动力发展问题。她还对高等教育财务、财务决策、教育技术、数据管理和隐私感兴趣。她曾在 Oliver Wyman Financial Services 担任公司风险顾问。莱贝斯特在密歇根大学获得工业工程博士和硕士学位，在弗吉尼亚大学获得系统工程学士学位。

乔恩·施密德，兰德智库专职研究员。近期发表《推进自主系统：2019 年海上无人驾驶技术现状与未来分析》等文章。

肖恩·蒂尔尼，兰德公司技术分析师。他曾与兰德阿罗约中心、国防研究所、国土安全行动分析中心等合作，在部队现代化、部队结构分析、工业基础分析和数据管理等领域开展一系列政府和国防相关项目。蒂尔尼获得了宾夕法尼亚州立大学航空航天工程学士和硕士学位。他在那里的研究集中在自主旋翼机控制系统上。

（此报告内容由编辑部翻译整理）