美国如何保证国防电子元器件供应链安全

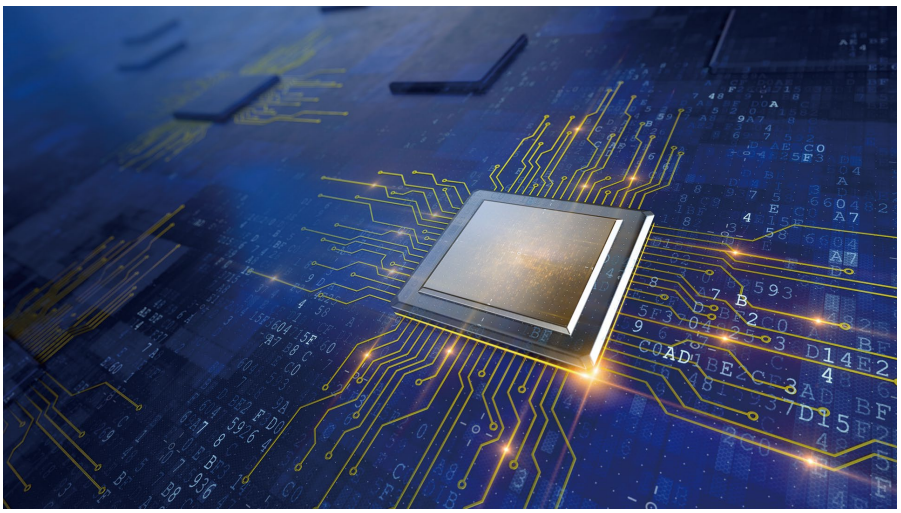
文／张倩 刘智成

2017 年 2 月底，美国国防科学委员会（DSB）网络空间供应链特别工作小组发布报告，指出美国国防电子元器件供应链安全所面临的严峻形势，包括假劣伪冒元器件的大举泛滥和软硬件漏洞的恐被植入。在分析了美国国防部采购话语权有限、元器件日益复杂、武器系统服役后长时间保持不变、国防元器件供应体系复杂等外部原因基础上，工作组对国防部现有供应链安全管理举措进行了审视，发现了项目保护计划不到位、数据库发展落后、信息管理机构缺少执行力、“可信代工”面临挑战等一系列问题，并针对性地提出了应对建议。

2017 年 2 月底，美国国防科学委员会（DSB）网络空间供应链工作组发布了名为《国防科学委员会网络空间供应链工作组》的报告。工作组对国防部现有电子元器件供应链相关安全措施展开全面调查，指出国防供应链中的薄弱环节，并提出相关建议。国防科学委员会是美国联邦咨询委员会，宗旨是为国防部部长提供独立的建议。

面临严峻安全形势

美国国防部自 2007 年起开展的一系列调查和举证显示出伪冒元器件已大量进入美军武器装备。2010 年美国商务部发布的《国防工业基础评估：伪冒元器件》报告中称，美国国防采办中伪冒元器件案件数由 2005 年的 3369 件增长到 2008 年的 8644 件，增幅达 2 倍多。2011 年美国政府问责署（GAO）在对国防后勤局、导弹防御局等国防部门和若干装备的调查中均发现了伪冒元器件。2012 年美国参议院军事委员会发布的《国防供应链伪冒元器件调查》报告中称，其调查的 1800 件伪冒元器件案件中，发现总数超过 100 万片的伪冒元器件已进入美军现役装备，包括空军 C-17、C-130J、C-27J 运输机和 P-8A 反潜机，海军陆战队 AH-64、SH-60B、CH-46 直升机，以及陆



根据目前硬件攻击手段，只需几百甚至几十个门电路就可植入比软件漏洞更难以去除的硬件漏洞

军“萨德”系统等。

美军表示伪冒元器件可导致武器系统可靠性每年下降 5% ~ 15%，甚至可使装备失效。美政府问责署例证，导航系统中的伪冒振荡器将造成无人机无法返回。参议院军事委员会也例证，已部署到阿富汗的 2 架 C-27J 运输机中发现伪冒存储器，会使飞机发动机状态、燃料情况、诊断数据等重要信息极易丢失。而更重要的是，伪冒元器件的大举入侵暴露出美国防电子元器件供应链安全措施的薄弱，美军担心恶意软硬件漏洞的植入会借由供应链的薄弱环节在美武器装备中长驱直入，实现从性能退化到功能故障，再到系统崩溃的各种攻击。美国国防科学委员会在此次调查中也发现了已被恶意植入武器系统但尚未实施攻击的漏洞。

为此，2014 年 11 月美国负责采办、技术与后勤的副部长责成国防科学委员会成立网络空间供应链工作组，审查国防部电子元器件供应链安全管理举措，并研究如何减少缺陷和防范恶意软硬件漏洞在国防电子元器件中的植入。

外部原因分析

美国国防部用电子元器件强烈依赖全球半导体商业供应链。通过该供应链，敌方拥有多种机会来损害器件或利用 / 植入软硬件漏洞来发起攻击。确保国防电子元器件不受攻击是一项艰巨的任务，其中外部原因主要体现在以下几个方面。

元器件复杂度不断提升，传统测试难以发现漏洞

随着技术发展，担负系统信息处理功能的中央处理器、存储器等电子系统中最常用的数字集成电路动辄包含数十亿门电路，特别是使用日益广泛、具备更高灵活性、可在武器系统部署前后重新写入功能的现场可编程门阵列等器件。根据目前硬件攻击手段，只需几百甚至几十个门电路就可植入比软件漏洞更难以去除的硬件漏洞。而费时费力的传统性能测试仅能保证器件具备所需功能，由于无法穷尽对所有功能的测试，故无法保障元器件不包含非预设功能。

武器系统长时间保持不变，给予敌方充足攻击时间

武器装备长达数十年的服役期大幅增加敌方发现系统内可被攻击弱点的可能性。而且如能利用现有漏洞而无需植入，则是最具成本效益和最低风险的攻击实施方式，这将极大简化攻击的难度和缩短攻击实施时间。工作组估计，到 2025 年前，现已部署的武器装备所提供的军事实力占美国总军事实力的 80% 还多。这些系统就像多年来一直等待攻击的“静态目标”，如“爱国者”导弹、地面环境集成系统（AEGIS）和中距空 - 空导弹（AMRAAM）等前线作战系统就是最好的例子。因为维护或更换的招标公告是公开的，敌方可充分研究其所需的重要组件和供应链，定位关键部分的关键器件，进而找到可实施攻击的潜在漏洞。

国防电子元器件供应体系复杂，难以有效跟踪和防范

根据实施主体和目标的不同，国防部电子元器件供应链细分为全球商业供应链、国防部采购供应链和国防部维护供应链，每个供应链都在攻击范围内，为攻击者提供不同的成本和收益，具体如表 1 所示。每个供应链都包含多个主体，如生产商、分销商、子系统集成商和国防装备商等，每个主体又包含多个层级和多家企业，并呈现复杂的交织供应关系。在全球庞大、非线性商业供应基础上，进入国防部的电子元器件难以跟踪其流转过程。一旦敌方渗透进供应链并过滤出有关武器系统的功能和技术信息，就可通过寻找特定电子元器件和系统漏洞实施攻击。与此同时，装备系统日益复杂，国防部和国防装备商几乎难以了解最底层电子元器件使用情况。因此，即使确认了电子元器件中含有漏洞，由于没有全面的材料清单，也很难快速找出使用了这些电子元器件的武器装备。

特别是在国防部维护供应链中，由于武器装备系统经过数年的研制在投入使用时，所用电子元器件，特别是微电子器件极有可能已经停产，无法从原始生产商或授权分销商处获取。例如，根据国防部的长期采购经验，在武器装备部署前，大约 70％的电子元器件已经淘汰或不再生产。停产断档问题迫使国防部或国防装备商从未经授权或认证的分销商处采购，显著增加了买入已受篡改电子元器件的机会，在美国国防部此前的多项调查中也充分证实了这点。

国防部现有举措存在问题

工作组对国防部现有管理国防电子元器件供应链的机构和措施展开全面调查，发现尽管国防部一直在着力解决目前面临的严峻安全形势，但仍力有未逮。

项目保护计划实施不到位

2011 年，美国国防部意识到其严重依赖美国以外地区生产的微电子器件来实现尖端技术，要求项目管理人员在项目保护计划中解决供应链威胁。项目保护计划旨在制定出完备方法来保护包括网络安全在内的全面系统安全，以及采取行动来保护未保密的项目信息安全。

目前的项目保护计划主要存在以下几方面问题，减小了其对整体项目和供应链质量的保护作用：

（1）未有效延续至维修保障阶段，即几乎没有证据表明在武器装备部署后仍在持续有力地实施项目保护计划，或当武器装备通过维修不断升级时，相应记录也在持续更新。

部署到阿富汗的 2 架 C-27J 运输机中发现伪冒存储器，会导致飞机发动机状态、燃料情况、诊断数据等重要信息极易丢失

表 1 三个国防供应链易受攻击程度对比

	全球商业供应链	国防部采购供应链	国防部维护供应链
含义	以商用现货采购为主，是大多数电子元器件的来源，也是国防部采购和维护供应链的基础	由国防主承包商设计和主导，用于支持武器系统的研制和生产	由国防部武器装备维护部门或装备集成商设计和主导，主要采购装备维修用电子元器件
供应链介入难度	容易	供应商数量众多，介入难度中等	对供应商有一定的审查要求，介入相对困难
攻击精准度	因国防需求只占总市场的极小份额，攻击精准度最低	一旦介入，可知晓元器件的使用情况，提高攻击精准度	可明确知晓使用位置，攻击精准度最高

（2）不同项目保护计划的质量、重点和深度差异较大，如一些项目侧重于保护电子元器件的可用性，一些项目则强调保护人员或系统安全，还可能因要获得阶段性批准的压力而限制了保护的范围和深度。

（3）负责制定和执行项目保护计划的项目管理办公室缺乏足够的专业知识、专家指导和系统工程界的参与。

（4）此前研发的武器装备并没有采取项目保护计划，关键电子元器件的认定方式也未统一，供应商也未接受今天所要求的审查。

（5）任何已发现的漏洞仍然存在，没有正式的移除步骤，也没有对新发现的攻击做出反应的机制。

数据库发展滞后且上报不及时

美国用于报告元器件失效，以及收集和发布电子元器件、零部件和材料信息的数据库称为“政府－行业数据交换项目”（GIDEP），这是一个先于互联网存在的自愿参与计划。GIDEP 目前是国防部收集和发布关于伪冒电子产品或其他不符合要求零部件报告的主要手段。

然而 GIDEP 在传播伪冒元器件信息方面并非迅速且可靠的方法，主要存在以下问题：

（1）因为资金不足，GIDEP 无力更新其信息系统使其变得现代化，仍在采用已过时的方法来履行其重要责任，具体体现在主要依靠参与者（政府和承包商）的主动报告，不能自动捕获所有疑似或已确认的伪冒电子产品；没有引入大规模数据分析技术来处理和应用大型数据集，无法适应不断扩大的威胁和加速对这些威胁的反馈。

（2）无法实现“立即”和“所有”上报的预期效果，如在国防部相关条例中，规定“在承包商意识到的 60 天内”向 GIDEP 以书面方式报告伪冒电子产品事件，而且国防部并没有明确规定所有国防供应链参与者均有责任进行报告，部分承包商会担心因此蒙受声誉损失或其他不利商业后果而避免上报。

（3）信息无法立刻有效传达，GIDEP 并非立即将所获取的伪冒电子产品报告公之于众，也因未能将攻击信息与可能受影响的设备相关联，无法将该信息告知处于风险中的用户，阻碍了向操作者发出警告、阻止攻击扩散、及时采取应急和修复措施等进一步操作。

（4）对伪冒电子产品的报告既不解决电子元器件中软硬件漏洞的引入，也不代表建立隔离和识别恶意植入或潜在漏洞的现行行业标准或“最佳做法”。

联合联邦保障中心缺少执行力

2015 年 2 月，国防部根据《2014 财年国防授权法案》中的要求，创建了联合联邦保障中心（JFAC），目标是“建立联邦联合能力来支持可信防御系统的需求，确保国防部开发、采购、维护和使用的软件和硬件的安全”。JFAC 由指导委员会领导，成员包括国防部副部长和国防部首席信息官（CIO）、军事部门、导弹防御局（MDA）、国家安全局（NSA）、国家侦察局（NRO）、国防信息系统局（DISA）和国防微电子中心（DMEA）。JFAC 强调通过联邦内部及协作机构和团体来开发、维护和提供软硬件漏洞检测、分析和修复能力。JFAC 负责联系和协调工作，各成员进行不同数量的研究、工具开发和评估，

并对项目管理办公室提供支撑。

虽然 JFAC 向国防部提供有关软硬件保障的重要专业知识，但其设立方式意味着没有自己的权力、资源或能力。JFAC 支撑项目管理办公室并帮助改善国防部软硬件保障的能力完全取决于 JFAC 成员的自愿承诺。鉴于每个成员都有自己的管理方向、资金和独立于 JFAC 的优先事项，尽管个别 JFAC 成员可能通过向其对应的国防部机构报告来向项目管理办公室提供一定程度的支撑工作，但总体而言不太可能提供实际支持。JFAC 提供了建立机构间协同工作并分享方法和结果的媒介，但 JFAC 章程中没有任何内容可确保会实现此类工作或共享，或使项目管理办公室受益。

“可信代工厂”面临管理和资金挑战

为建设并维持武器装备和情报系统用微电子器件的供应基础，并能够持续享用不断进步的先进商用工艺带来的技术优势，美国国防部从 2004 年开始实施“可信代工”项目，扶持了 IBM 公司建设可信代工线，又从 2007 年起进一步对微电子器件设计、掩模、制造、封装、测试等全产业链的供应商进行认证，增加可信代工线数量，以满足军方更丰富的需求。

“可信代工”项目通过利用双重用途的商业设施提供了解决方案，但外资所有权和全球商业竞争将降低国防部对其的控制力。2015 年 7 月 IBM 公司微电子制造业务出售所有权给隶属阿联酋的格罗方德公司后，格罗方德经过资格审查取代 IBM 成为国防部最先进微电子制造工艺的唯一可信供应商。而在全球掌握最先进制造工艺的公司中，美国仅英特尔公司占有一个席位。但是，如果由国防部出资来建立和运营一个国防部所有的代工厂，以解决国防部可依赖的本土微电子制造商数量不断减少的困境，在资金成本上并不可行。并且在未来，随着智能或自动化系统的增长，国防部将持续需要获得可靠、先进、专用微电子器件，这部分不断上涨的需求将得不到满足。

其他问题

网络空间觉知演习缺少定期实施机制。网络空间觉知演习可发现关键武器系统中可被利用的网络供应链漏洞。如果定期对主要武器装备系统和子系统进行演习，其结果将很好地服务于目前处于购置和维护阶段的系统。目前还没有一种机制可以向项目管理办公室和项目管理人员常规性地提供网络空间觉知结果，或向后勤人员和实践维护人员提供适当分类和分级的网络空间觉知培训。在国防科学委员会此次发布的报告中，并未对网络空间觉知演习做出详细说明，须直接联系美军方以获取更多内容。

没有专门负责硬件漏洞事件收集的国防部机构。从 20 世纪 90 年代初开始，美国计算机应急准备队（CERT）协调中心（最近被称 US-CERT）运营着一个跟踪软件漏洞报告的数据库，以及一个与漏洞相关用户和需对漏洞做出反馈的供应商列表。国防部通过“信息保障漏洞警报”（IAVA）流程来应对漏洞警告。但是 US-CERT 并不跟踪硬件漏洞，国防部内部也没有一个与软件漏洞已建立过程相类似的稳定的硬件漏洞数据库或警告工作流程。

对元器件淘汰和漏洞跟踪缺乏国防部级别的统筹。国防部缺乏对武器装备所用电子元器件的全面掌控，导致出现问题时更换受损器件或子系统是一个缓慢的自下而上的过程。国防部机构也未能定期将系统安全工程要求施加给承包商，为控制供应链风险而采取的供应商审批方法差异较大。而现有批准电子元器件供应商的人工认证过程在确保真实性和防止伪冒或受损电子元器件进入国防供应链方面是一个低效的方法。

加强和改进建议

在全球半导体市场快速变化的背景下，国防部必须适应快速发展的外部环境，通过制定包括技术研发、设计、制造、部署、维护等在内的全生命周期策略，来保证国防电子元器件供应链的安全。

实施武器系统全生命周期保护

项目保护计划应转化为全面管理包括新系统和现有系统在内的关键武器系统全生命周期安全性的文件，要确保广泛的保护和可恢复性。具体包括以下几个方面：①从系统设计之初，明确提出可恢复性设计要求，允许基于检测到的异常行为对子系统进行全部或部分的快速替换或更新，如采用能实现隔离和容错功能的模块化系统架构以提高响应和对抗攻击的能力，采用能快速升级的系统架构以改进通过消除受影响组成部分实现从攻击中恢复的能力；采用能提供内置主动监控的设计策略以提高检测开发和响应的能力。②在电子元器件设计、制造、装运过程

2015 年 7 月 IBM 公司微电子制造业务出售给所有权隶属阿联酋的格罗方德公司后，格罗方德经过资格审查取代 IBM 成为国防部最先进微电子制造工艺的唯一可信供应商

中，防止器件受到恶意植入漏洞等篡改，并做好对潜在停产元器件的预案。③在运行过程中，及时获取元器件和子系统上的最新漏洞信息；主动搜索和连续自动监控以全面检测系统故障和进行脆弱性评估；在子系统和系统级别采取有效的响应程序以便对预期或已检测到的故障进行补救。④加强对供应商的考核，采用更好的器件来源保证策略，加强对电子元器件采购、操作和维护人员的培训，提供从设计到退役的全生命周期的专家级安全设计和审查支持。

建立硬件漏洞数据库和加强数据共享

建立一个共享的漏洞数据库和器件应用情况数据库，如建立硬件 CERT 以跟踪商用现货软硬件漏洞，将极大促进漏洞信息和修复举措在整个武器系统内的传播。一旦发现一次攻击事件，国防部具备迅速找到类似设备的能力，并将事件信息及时有效反馈给有同样危险的系统的操作者。在数据库的建设中，国防部应更多地了解和学习商业公司在数据型供应链风险管理中运用的策略和方法论，并使用先进的自动化工具、信息收集和分析技术来识别供应链中薄弱环节暴露的弱点，对已暴露或受损的器件自动发出提示，甚至可根据攻击事件做出行动，减少由此招致的攻击及降低攻击发生时带来的危害。

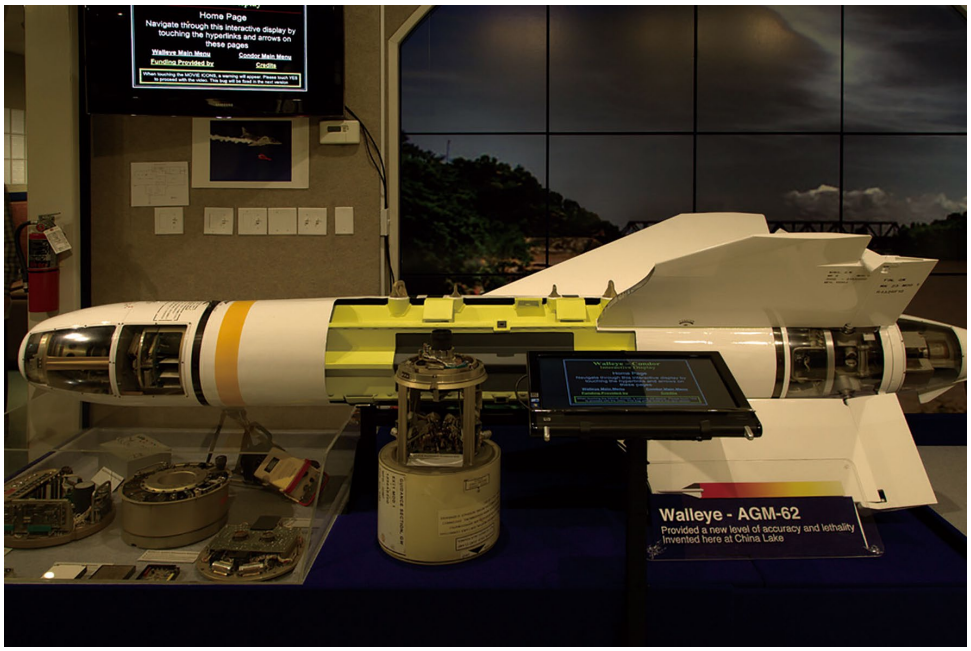
国防部应指示国防标准化计划办公室对 GIDEP 报告系统进行现代化升级，包括：①提高 GIDEP 的功能、资金和人员配置，要能将漏洞、事件和消除措施快速传达给遭受攻击或处于危险中的电子元器件用户；②扩大 GIDEP 章程范围以涵盖对软件、固件和硬件攻击的报告；③通过自动化手段向 JFAC 报告仿冒电子元器件信息。此外，国防部还应颁布新法规，消除企业自行上报伪冒元器件产品中的阻碍因素。在关键电子元器件的鉴定中，还需要一套成体系的方法和标准，并对《国防联邦采办补充条例》（DFARS）做出相应修订，不能再沿用现阶段只能通过可嵌入证明和可跟踪信息来证明电子元器件血统和来源的方法。

强化联合联邦保障中心的作用

JFAC 作为专业知识来源应扮演更重要的角色，以更好支持项目管理人员实施全生命周期项目保护计划和系统安全工程。JFAC 章程应更新为：（1）将 JFAC 建成为国防部范围内的软硬件保障机构；（2）为软硬件保障流程和工具制定规范性标准和要求；（3）在项目无法遵守标准或要求情况下，项目管理人员和 JFAC 指导委员能独立表达所含风险；（4）根据新的攻击和安全技术定期（如每年）更新标准和要求。

研发拆分制造和安全认证技术

面对半导体先进制造能力不断向亚洲集中的现实，应研究拆分制造技术和实施方案，以此作为利用不完全信任的最先进代工厂的一种解决方案。拆分制造指先在先进制造工艺代工厂中制造晶体管，然后移至可信但制造工艺相对落后的代工厂中进行布线。在这种方式中，第一个工厂并不会知晓芯片的功能，由第二个工厂的可信来保证器件的安全。由于制造布线层这一生产步骤的成本和技术水平都相对较低，使得这一方法的监管和维护较为实现。在可信代工厂的下一步发展上，国防部不应局限于现阶段所要求的可信，而应通过与商业最先进代工厂建立多层次的合作关系来满足发展需求。



伪冒元器件可导致武器系统可靠性每年下降 5% ~ 15%，甚至可使装备失效

与此同时，国防先期研究计划局等国防部研发管理机构应继续推进新识别和验证技术及配套工具的发展，多手段防范电子元器件被篡改。保护对象既包括芯片设计过程中的设计库、计算机辅助设计工具和模拟器、掩模版设计和制造，也包括器件在供应链流转过程中对裸芯片的独特识别等，使得国防部可以放心使用各种来源的电子元件器件，而非只能依赖“可信代工”这唯一来源。研究内容包括可连续监控关键系统和成本可接受的传感器，对各种电子元器件进行标识的标签、监控和认证方法等。

其他建议

加强合作。美国国防部应和其他联邦机构和国际通信组织开展充分合作，如 US-CERT、国土安全部工业控制系统网络急救反应小组（ICS-CERT）、信息共享和分析中心（ISAC）、信息共享和分析组织（ISAO）等，共同提高对已知或者疑似网络—物理攻击的信息采集，加快通知和评估，并建议应急和修正措施。

非最先进器件可选择替代方案。在不需要最先进性能的情况下，应优先使用来自可信供应源的现场可编程门阵列产品。DMEA 则继续提供无法在商业上买到的非最先进的元器件，同时保证不违背与现有硬件和软件的透明集成。

重视网络空间觉知演习。国防部应以一定组织实体为单位开展至少一次全面网络觉知演习来测试供应链攻击的脆弱性，并形成定期进行网络觉知演习的工作规范。

结语

在全球商业领域已出现大量伪冒元器件，并正不断向国防等传统相对封闭领域快速渗透。除了可使系统功能退化和失效的伪冒元器件外，各国更担心的是被植入软硬件漏洞的电子元器件，因为后者不仅可使系统功能退化和失效，还可进行信息窃取和监听，以及对武器装备的操控和使作战任务失败。要防范武器装备不被植入软硬件漏洞，需建立电子元器件和武器装备两个层级的全生命周期项目保护计划，以及研发必需的技术、标准和流程，严格保证两者在各自的设计、制造、使用、淘汰各个阶段的安全。同时，充分利用大数据采集、智能分析等现代化技术手段，促进硬件漏洞信息的收集和共享；加强对装备所用电子元器件的了解，收集装备各组成部分的材料清单，建立“电子元器件—装备—用户关联在一起”数据库，确保在发现漏洞或潜在威胁可以迅速通知到位，将损失降至最低。CONMILIT