免责声明：凡在本杂志发表的文章只代表作者观点，而非美国国防部、空军部、空军教育和训练司令部、空军大学或美国其他任何政府机构的官方立场。

虚空布兵：正确理解网空战争中的兵力集结和战斗力

Virtually Massive: Understanding Mass and Combat Power in Cyber War

约翰·科布，美国空军上尉（Captain John "Strider" Cobb, USAF）

数量之中自有其质重。

——据称为斯大林语，述及苏联在二战期间的武器生产。

美国空军对“兵力集结”（mass）所给的定义是，“集兵力于最有利的地点和时间，夺取决定性胜利。”[1] 空军作战准则 AFDD 3-12《网空作战》在呼应这一定义时提出，网空部队“必须整合并协同其他部队”。[2] 此定义从网空战略角度来看意味着什么？一些人建议，兵力集结的概念不再适用于网络空间，因为攻击者可能只是一些散兵游勇，却能从世界任何地方发动毁灭性的攻击。[3] 美国空军退役上校格雷戈里·拉特雷（Gregory Rattray）在《网空中的战略战》一书中探讨了诸如网空情报作战、目标判定、工具开发等能提高网空攻击效能的支援功能，其中涉及到和兵力集结相关的另一个层面——打击敌方目标，不仅需要发动攻击的“牙齿”，还需要组建在后面支援的整个团队即“尾巴”，才能确保持续攻击成功（因为他在书中建议，己方的分析员和程序员可能需要在数量上大幅度超过实际发动攻击的人员）。[4] 此观点显然有其独特之处，也是一个需要解决的重要问题。但我们在理解网空战争中的兵力集结时，不能只局限思考人员的数量。

兵力集结也能从攻击流量来思考，最直白地说，就是有多少字节或数据包攻入目标。有时候，也可从同时被释放的病毒的数量来判断，即依据防火墙和防病毒工具对来袭的恶意软件实施封锁所得到的结果来判断，从而获得对数量的更有意义的界定。也有时候，某种计算机病毒被攻击者或研究人员认定为是同一种类，却可能自我修改代码，表现为数百种不同的病毒，设法通过对方的过滤器。再一种情况是，可以从多少节点受到攻击来理解数量——在最低层次，可以计测多少装置受到攻击；在更高层次，可以计测多少网域或实体地点（如基地）受到攻击。虽然这样的分析过于简单化，但从这些不同角度来理解“数量”，可以更全面地解析网空“火力”。对网空战争中兵力集结的理解还应考虑另一个面向，这就是关注被保护的网络的坚固性或生存能力。一个网络，如果配备很多备用设备、宽带和冗余路径，就更能在各种攻击中生存下来（或至少能更迅速恢复）。还有一个常被忽视因而也需关注的情况是，我们配置了多少技术人员和技能来承当被攻击网络的维护和保护。最后一点，大多数国家在和平时期的网空行动要比在战争时期的网络攻击更有节制，因此和平时期中的隐蔽行动所表现的兵力集结，可能不似在公开网空战争中那样的多面性。

网空防御中的签名扫描和探试扫描

很多读者或许不熟悉防火墙和消毒软件如何保护网络，在此简单解释一下。典型的

防火墙扫描从局域网出入的访问流量，而消毒软件扫描计算机的硬盘。当然也有例外，如基于网络的入侵检测系统，或路由器的访问控制列表过滤器，但是保护网络的主要工具是防火墙或传统的消毒软件，其他常用的工具也不外乎使用类似的规则来扫描和过滤。[5] 扫描病毒有两种主要方法:签名（特征）扫描和探试扫描。网络防御最常用的方法是通过核实签名搜索出恶意软件，通常是将被扫描文件（或网络包）的一部分或全部与已知病毒完整清单进行对照和匹配。对于防御已知病毒的攻击，此举相当有效，但很显然它无法检测出大多数新型病毒攻击，而且通常难以捕捉住那些稍加修改的已知病毒的攻击。[6]

网络防御中发现恶意软件的另一种方法是使用“探试”扫描。这种方式不是去寻找已知是恶意的文字行或文件包，而是寻找可疑的模式或行为。这能更有效(虽然有欠完善)地逮住新的“零日漏洞”攻击，而且更能截获以往攻击病毒的新变种。缺点是，大多数探试式算法语言造成很高的假阳性率，在被截获的访问中，真正的恶意攻击并不多，许多合法的访问和通信却被错误挡住而造成虚警，因此操作过程会非常耗时，会令人沮丧。这些过滤器面临的统计问题，类似于对某些癌症的造影检视。[7] 毕竟，网络流量中的绝大部分并不含恶意，如果将其中的 95% 标以病毒警示而只承认 1% 为合法，结果只能是将真正的病毒文件淹没在大量假阳性警报中。[8] 很多商业产品结合使用这两种方法，安全研究人员也在研制探测攻击的一些替代办法。但是总体而言，目前除了最重要的和安全要求特别高的网络以外，大多数网络在很大程度上只依靠基于签名的扫描模式进行检测，因资源的缺乏而难以采纳其他方法。[9] 这样，对很多大型军事或工商业网络而言，新病毒攻击常常在得手之后才被检测到，此时网络已被攻陷。

网空中攻防双方兵力集结的诸种考虑因素和比较

由于网空防御中的这些限制，在目前的网空中，攻击的效果并非总是同其复杂程度成正比。攻击软件必须达到什么样的复杂程度才能成功，取决于被攻击目标的规模大小、复杂性、防御坚固程度和相互联系等因素。攻击者面对的政治限制，例如不得不隐身匿名、隐藏攻击源或伪造假攻击源等，常常提高网空攻击所需的复杂程度，以及攻击者的工作量。对重要军事目标和基础设施目标的攻击，因以上各种因素而效果各异。有些关键目标很难设防保安全，一经攻击就功能俱废；也有些目标，尤其是小型目标，即使不那么重要，却不怕攻击，只有那些非常复杂的攻击才能得手。拒绝服务攻击（DoS）简单易行，复杂性不及间谍企图性攻击。地理分布面广且节点多的网络在监控防御方面更加困难，难以堵住病毒攻击潜入。对于那些从商店直接购置的硬件和软件系统开展攻击，只要经过一般标准训练，使用一般工具，就可能得手。但若想攻击情报部门、核设施或某些基础设施的专门系统，可能需要经过周密的侦察和定制的攻击设计，才能得逞。[10]

托马斯·里德（Thomas Rid）曾著一文，其中某些假设虽需商榷，但正确地指出：凡隐形的、有高度针对性的“战略”攻击，如震网病毒，需要动用大量资源来编制复杂程序，而且不易重复使用。[11, 12] 这类攻击可能需要数十名情报分析员、程序员和操作员组成团队来设计、组装和发动。不同团队可能需要其成员接受其中部分或全部的训练，将

其技能加以组合。亦即，若想攻击那些高度戒备的目标，常常需要数十名训练有素的人付出数月努力才能完成。所以，要想迅速破坏或瘫痪大量的坚固和独立的目标，攻击方显然需要投入巨大的人力物力。如不得不匿名和隐藏攻击源，则投资更加高昂。那些参与对独立目标实施攻击的网络战士，就可能无法参与“日常”的网空情报工作，而日常情报工作也不可或缺。

也有很多网络目标的防护并非那么严密，其中一些可能是高价值的目标。震网病毒攻击的目标如核设施，可能网络入口防守严密，一应“闲人莫入”；但其他很多军事和工业系统必须允许大量和频繁通信出入，才能有效运作。例如，电网必须允许各发电站之间时刻保持联系,否则就运转不起来。这些“在线”通信虽然不至于像那些直接送上互联网的非加密通信，但是仍容易被攻击者所利用，可能一次攻击就能控制、削弱、甚至摧毁整个电网系统。当然，我们必须指出，像美国或俄罗斯这样的大国，“电网”系统是由一组区域电网松散连接而成。例如，美国有三个地区电网；[13] 俄罗斯虽比美国实施更加中央化的控制，实际上有七个地区电网，相互之间的联系很有限。[14] 很多军事网络与之相似，这些网络中必须容纳数量庞大的单位和基地，必须保持互相之间的联系，才能发挥现代军队所依赖的这种力量倍增器的效能。如果让外部的复杂攻击攻破其网络的一个节点，就很难防止其在网络中蔓延。

沿此思路，兵力集结的第二个定义或许能提供更好的理解。有些目标容易受到单一团队发动的攻击，攻击一点而波及整个网络，如果攻击成功，能严重妨碍整个地区。互相关联的公共设施，特别是电网，就是这样的例子，它们通常比其他公共设施网络的规模更大，也更加相互依赖。另一个例子可能是用于指挥控制、后勤和作战势态感知的军事网络，这些功能必须覆盖战术和作战层面，要求一个由数量众多的关键节点共享的网络。在网空攻击频谱的最简单端，是分布式拒绝服务攻击，其兵力集结体现为对带宽的占有，由此倾覆目标网络。顺此网空攻击频谱向复杂端移动，我们看到，如果某攻击使用有效的自我修改代码，防御方就可能需要在数十至数千个网络外围布防，以拦截不只一个而是数百甚至数千个新病毒签名。保护每一个局部网络的防火墙软件都必须定时更新，将新的病毒签名随时加入其拦截病毒清单。

在有些攻击中，病毒软件使用的“探哨”（exploits）的数量，比病毒如何通过变异渗透过滤器可能更加相关——所谓“探哨”就是某种恶意代码，它利用目标软件的缺陷来控制系统；一旦探获出目标网络的缺陷或漏洞并加以利用，此攻击病毒就可能成功。[15] 大多数军事网络都配备技术人员，他们知道防火墙和消毒软件不能阻止所有攻击，但努力做到在攻击发生之前设法修补已知的缺陷和漏洞，以防被攻击者利用。如果相应的缺陷已有针对性地彻底修补，那么仅使用一个探哨代码的攻击就会失败。迅速实施彻底修补是一项艰巨的挑战。[16] 目前已有工具能在几天时间内就能完成对大型现代网络中众多系统的修补。[17] 如果某一攻击使用多个探哨代码，将增加防御方所面对的挑战。但是，探哨代码（尤其是零日漏洞探哨代码）可能是有重大价值的情报资产，很多政府反对随意透露这些恶意代码。[18] 另一方面，这些探哨代码的数量比人们想象的要更多，例如，在2012 年 1 月到 5 月间，微软就宣布了视窗 7 操作系统和常用应用程序（如微软办公套件）

中存在的 31 个严重漏洞，并为此发布补丁程序。[19]

此外，有些攻击是以有多少网络作为单次攻击或系列攻击的目标来作为兵力集结的考量因素。笔者在其他文章中曾探讨有些网空攻击能将局部网络与中央控制或反应隔离。[20] 在防御这些类型的攻击方面，关注地理位置的分布或受到攻击的局部网络的数量，可能比关注有多少人参与发动攻击或使用了那些攻击类型更有意义。这主要适用于对抗拒绝服务攻击和分布拒绝服务攻击，或适用于高度集中化控制的网络防御。[21] 如果在每个地点都配备熟练的网空防御人员，他们应能相对轻快地清除简单的攻击（尤其是分布拒绝服务攻击）。但如果采用更加集中化的网空防御方式，可能出现集中于一地的防御人员与其所管理的网络联系被切断，或导致防御人员供不应求，无法同时对所有地点遭受的攻击做出反应。

从防御一方来看，在这些类型的攻击中，人力可以是兵力集结的关键因素。拒绝服务式攻击与有高度针对性的攻击不同，前者在兵力对比上可能高度的不对称。攻防双方固然在开展“军备竞赛”,防御方努力在过滤器、扫描和其他网络工具上赶上黑客的技术，但总体而言，这些拒绝服务攻击可以由一个相当小的团队发起，防御方却可能需要配置大量人员来修补和清除受到攻击的每个局部网络的故障。

对网空作战中战斗力的相对衡量和计算，依据攻击种类和需要保护的网络类型而不同。知识和经验丰富的技术和操作人员始终发挥着重要作用，[22] 但军队对人力配置的质量和数量需要做适当平衡，按照预见的攻击类别和工具相应做好搭配。当前军队都面临着预算限制，而可能发生的网络攻击种类很广泛，因此必须统筹兼顾做好人力搭配和取舍。如果主要威胁来自类似震网病毒的隐身攻击，目的是秘密破坏数据或损坏物理设施，那么网络防御团队必须训练有素，特别在病毒取证分析技术方面，而其人员数量则不需要远远超过攻击方的数量。并且防御方经常能在对方攻击成功（至少是部分成功）侵入后阻止攻击，因为攻击方为避免被察觉，其病毒传播通常较慢，造成的破坏也慢。如果攻击方的主要目的是迅速瘫痪或孤立关键的系统，则防御方需要配备大量人员，所需技能应着重于反击公开的攻击（并且复原被攻击瘫痪的系统）。为了获得对潜在敌人的足够了解从而预测其主要攻击方式，就需要大量培养网空情报人才队伍，有了充分的这类人才，就能成功应对和反击攻击。[23] 偶尔，可能出现对同一个目标同时开展两种不同类型的攻击，但在大多数情况下，对同一个网络和系统的这两种攻击会互相干扰，攻击方可能因此而失去对更高针对性目标精确攻击的控制。可能性更大的，是以公开拒绝服务（DoS）或分布拒绝服务（DDoS）攻击一个地区，而对远离此攻击的另一个系统或网络，则可能采用更精心策划的秘密攻击。当然，在当今任何冲突中，协调和化解网空冲突——无论是来自网空还是来自动能打击——都要求做好重要的作战策划。[24]

网空兵力集结与传统战争的比较

在思考网空的兵力集结问题时，回顾空中力量作战的历史，可能有助于澄清不同的集结方式——在某些方面，网络攻击方面临着与美国陆军航空兵及英国皇家空军在第二次世界大战期间轰炸德国工业体系时类似的问题。高度针对性的攻击（如震网病毒）是

以量身定制的、不可复制的独特攻击手段瘫痪几个孤立的高价值目标，通常缓慢而秘密地进行，有点类似二战中美国开展战略轰炸的方式。用这种方式，攻击方确定几个关键的节点，然后集中大量人力、时间和战斗力去摧毁这些节点，[25] 确信一旦成功摧毁，敌人便无法继续运作。相较而言，各种形式的拒绝服务攻击，有些类似英国轰炸德国的目标选定方式：英国没有针对具体的（通常有严密防御的）关键系统实施直接攻击，而是试图瘫痪这些关键系统所依赖的当地或区域网络的某些方面。二战中英国皇家空军打击敌方目标的过程中，最初是针对重要工厂，但是未能奏效且蒙受重大损失，经历初期失利之后，皇家空军转而着重轰炸重要的工业城市，把目标锁定在整个工业生态系统，而不是一系列分离的关键节点。美国陆军航空兵部队则将打击目标锁定在那些关键的节点，特别是飞机制造、燃料生产、交通运输、球轴承制造等，虽然在初期也经历了类似英国空军的失利，但通过从 1943 至 1945 年的持续打击，摧毁或瘫痪了其中一些关键节点（例如在施韦因富特的球轴承厂和在普洛耶什蒂的炼油厂），实现了严重打击德国工业系统的意图。[26] 美国陆军航空兵和英国皇家空军采用的具体实施方法并非全然不同（美国陆军航空兵 B-17 和 B-24 因为天气原因和德军防御的干扰，常常不能将炸弹投中目标），[27] 但是两国部队选定打击目标的方式，同上述讨论的两种网络攻击各有相似之处。当然，军队网络中的个人电脑和交换机等硬件基本上是没有争议的目标，不像打击工业城市的人口一样容易引起争议，但很多拒绝服务攻击不那么精确并更可能蔓延，祸及民用网络并产生意想不到的后果。值得注意的是，无论是高度针对性的定点打击，还是大面积攻击，此两种网空攻击方式都可能非常有效——前者有震网病毒的成功为证；后者有 2007 年对爱沙尼亚的分布式拒绝服务攻击为证，且此攻击影响深远。[28] 另一个例子是据称由俄罗斯 2008 年策划的对格鲁吉亚的拒绝服务攻击，这场攻击破坏了格鲁吉亚对俄罗斯装甲部队进攻做出反应的能力。[29]

结果是，瘫痪一个反应堆可能极为困难，需要周密制定一个全新的攻击程序；而破坏军方的一个指挥控制或后勤网络则相对可行，只要使用“现成货架”黑客工具，就能发动相对简易的攻击。网空领域与其它作战领域的一个不同点是，网空中范围更大的且分布更广的目标，常常也是更容易受到攻击和瘫痪的目标。最近对网空战争的讨论，常常把平时的间谍活动误认为战争，一些评论人士倾向于高估探哨代码在战争中的重要性，以及隐形性在战争中的必要性，并以为大型军事或基础设施网络的防御能力同较小的情报系统或核系统通常配设的保护一样坚固。[30] 这些误解歪曲了网空战争中兵力集结的性质，可能导致我军在组建网空战争单位或设立网空防御时犯下严重错误。虽然网空间谍活动——包括在和平时代的秘密网空攻击——往往表现为隐形及定点打击，而在公开战争中，网空攻击可能包括上述讨论的所有形式的兵力集结和战斗力；对网空攻击的外交和政治限制也可能不相同，有些冲突可能限制为“仅网空”攻击，也有的冲突可能允许包括网空攻击在内的传统（火力）作战。但是这两种冲突中，都可能包含更多的公开性网空攻击，不再注重隐形匿名，而注重更狠更快，以有限的资源实现广大范围的打击效果。

结语

兵力集结是网空战争中的一个要素，而其含义因攻击性质和打击目标的不同而各

异。其对战术层面的影响可能不太严重（尤其是对非美国军队和/或地面部队而言，因为他们对网络的使用相对较少）；但在战役层面，现代军队非常依赖网络开展后勤补给和保持势态感知。这些网络是“重心”所在，如果被破坏，可能对严重依赖这些网络的部队的的作战效能造成巨大影响。高度针对性定点攻击可能产生毁灭性的效果，而各种形式的拒绝服务攻击，只要所选目标正确且实施得当，也能产生瘫痪敌人的效果。对网空战兵力集结和战斗力需做出正确的理解和界定，而此定义又随形势而变化，恰如网空本身。军队若将自身限制于仅发展某一个方面而使其作战准则和组织结构不能全面覆盖敌人发动攻击的各种方式，一旦遭袭，将面临被打败的风险。♣

注释：

1. Air Force Doctrine Document (AFDD) 1, Basic Doctrine [空军作战准则 AFDD 1：基本作战准则], p. 32.
2. AFDD 3-12, Cyberspace Operations [AFDD 3-12：网空作战], p. 16.
3. Martin Libicki, Cyberdeterrence and Cyberwar [网空威慑和网空战争], (Santa Monica, CA:RAND Corp, 2009), p. 59, http://www.rand.org/pubs/monographs/MG877.html.
4. Gregory J. Rattray, Strategic Warfare in Cyberspace [网空中的战略战], (Boston: MIT Press, 2001), pp. 100, 464.
5. Edward Skoudis,“Information Security Issues in Cyberspace”[网空中的信息安全问题], 见 Cyberpower and National Security [网空力量和国家安全论文集], ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, (Dulles, VA: Potomac Books, 2009).
6. “Antivirus Software”[消毒软件], Wikipedia, http://en.wikipedia.org/wiki/Antivirus_software.
7. Maia Szalavitz,“Why People Stick with Cancer Screening, Even When it Causes Harm”[透视检癌有害身体，为何人们乐此不疲 ?], Healthland, Time.com, http://healthland.time.com/2012/05/25/why-people-cling-to-cancerscreening- and-other-questionable-medical-interventions-even-when-they-cause-harm/
8. 见注释 6。
9. 更多介绍，参看 Shon Harris, CISSP All in One Exam Guide [信息系统安全认证考试指导大全], 4th ed. (New York:McGraw Hill, 2008), pp. 250-257.
10. 然而，那些专门的系统可能比与之类似的标准现成商品系统更薄弱，一旦被攻击者了解，便更易受到攻击，尤其是那些在设计时通常不考虑安全因素的基础设施系统。
11. Thomas Rid,“Think Again: Cyberwar”[网空战争三思而行], Foreign Policy, 27 February 2012, http://www.foreignpolicy.com/articles/2012/02/27/cyberwar?page=0,2.
12. 17147818　震网病毒是一个极端复杂的特洛伊木马类病毒，通过 U 盘传播，2010 年侵袭并破坏了伊朗的核设施，几个月后才被发现。参看“The Stuxnet Outbreak”[震网病毒爆发], The Economist, Sept 30, 2010. http://www.economist.com/node/.
13. Richard A. Clarke and Robert K. Knake, Cyberwar: The Next Threat to National Security and What to Do about It [网空战争：国家安全面对的下一个威胁以及如何应对], (New York: HarperCollins, 2010), 167.
14. Rinat Abdurafikov,“Russian Electricity Market: Current State and Perspectives”[俄罗斯电力市场：现状和前景], VTT Technical Research Centre of Finland, 2009, http://www.vtt.fi/inf/pdf/workingpapers/2009/W121.pdf.
15. “Exploit”[探哨攻击代码], Wikipedia, http://en.wikipedia.org/wiki/Exploit_(computer_security); 另参看注释 9 中 Shon Harris 文，第 62 页。
16. Stephen Northcutt, et al, Inside Network Perimeter Security [揭示网络周边安全], 2nd ed. (Indianapolis: Sams Publishing, 2005), pp. 257-258, 其中讨论了修补大型网络的困难因素。

17. Microsoft Security Update Guide [微软安全更新指南], 2nd ed. Microsoft, 2011 http://www.microsoft.com/en-us/download/details.aspx?id=559; 关于补丁系统的简介，还可参看“WSUS Overview”[自动更新服务概述], Microsoft Technet, http://technet.microsoft.com/en-us/library/cc539281.aspx.

18. 见注释 3，第 57 页。

19. “Patch Tuesday [周二补丁日], (January-May 2012)” Microsoft Technet, http://technet.microsoft.com/en-us/security/bulletin/ms12-jan , http://technet.microsoft.com/en-us/security/bulletin/ms12-feb , http://technet.microsoft.com/en-us/security/bulletin/ms12-mar, http://technet.microsoft.com/en-us/security/bulletin/ms12-apr, http://technet.microsoft.com/en-us/security/bulletin/ms12-may.

20. John Cobb, “Centralized Execution, Decentralized Chaos: How the Air Force is Poised to Lose a Cyber War”[集中执行，分散乱套：美国空军网空战败相已露], Air and Space Power Journal, Summer 2011, http://www.au.af.mil/au/cadre/aspj/airchronicles/apj/2011/2011-2/2011_2_16_cobb.pdf.

21. 拒绝服务攻击（DoS）是通过大流量攻击某系统或网络使其超载而瘫痪。分布式拒绝服务攻击 DDoS 是一种特殊类型的 DoS 攻击，来自世界各地的电脑发送出洪水般的网络流量，从而瘫痪目标服务器或网络，导致其死机或停止对合法的流量做出反应。参看注释 9 中 Shon Harris 文，第 1010-1013 页。

22. 更深入的讨论，参看 Kamal Jabbour, “Cyber Vision and Cyber Force Development”[网空远景和网空兵力发展], Strategic Studies Quarterly, Spring 2010, www.au.af.mil/au/ssq/2010/spring/jabbour.pdf.

23. 见注释 4，第 142 页。

24. 有关消除网络攻击的深入讨论，见空军作战准则 AFDD 3-12，第 25-26 页。

25. Elinor Mills, “Expert: Stuxnet was Built to Sabotage Nuclear Plant”[专家认为震网病毒意在破坏核工厂], Insecurity Complex, CNET.com, http://news.cnet.com/8301-27080_3-20017201-245.html?tag=mncol;1n.

26. Geoffery Perret, Winged Victory [胜利女神], (New York: Random House, 1993), pp. 240-244.

27. 见注释 11，第 280 页。

28. 这场分布式拒绝服务攻击据称由俄罗斯操纵(俄罗斯政府否认有官方参与),对爱沙尼亚银行和政府造成重大破坏。参看 注释 13 Clarke and Knake 文，第 11-16 页。

29. David Hollis, “Cyberwar Case Study: Georgia 2008”[网空战例研究：2008 格鲁吉亚之战], Small Wars Journal, January 6, 2011 http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008, p. 5.

30. 这些错误的假设出现在多篇文章中，包括上面的 Rid 文（例如其文中第 5 页）和 Libicki 文（见其文第 56-59 页），以及对比上述提到的补丁指南文件，特别是注释 16 中 Northcutt 文中的介绍。事实上，修补一个大型网络少则数天，多则数周，工作量巨大，而且如果修补过程太快，补丁本身可能瘫痪关键系统。

作者目前在美国空军大学司令部担任信息工程组负责人。在此之前，他外驻日本三泽空军基地，参加第 35 通信中队中的三泽蓝军队，负责网络作战方面的工作。