安全加社区

公益译文项目

2019

战略性网络空间作战指南

2018年11月30日

中部各州认证

美国陆军战争学院获中部各州院校协会高等教育委员会认证（宾夕法尼亚州费城市场街3624 号；邮编：19104；联系电话：（215）662-5606）。高等教育委员会是美国教育部长和高等教育认证委员会认可的公共认证机构。

免责声明：本指南中描述的系统、流程和观点均为编者的判断和理解，不一定代表司令部、陆军部、国防部或美国政府的官方政策或立场。

本文介绍并解释了现有的国家、国防、联合和军队等的系统、流程和程序，并将根据政策和原则的变化进行更新。

前言

1. 本文囊括了**美国政府的非机密**及**公开文档**，为美国陆军战争学院学生提供指导，帮助他们了解作战司令部（CCMD）、联合特遣部队（JTF）和联合职能司令部的网络空间作战的筹划、规划和执行。
2. 本战略性指南遵循联合条例5-0《联合规划》中详述的作战筹划方法和联合规划程序（JPP），并将这些原则应用于联合条例3-12《网络空间作战》中的网络空间领域。但是，在引用、复制或使用本文时不得将其视为原则或其他官方文件的替代品。

《美国陆军战争学院战略性网络空间作战指南》包括六章：

第一章概述了网络空间作战、作战筹划方法、联合规划和执行。

第二章介绍了作战筹划原则，并将这些原则应用于网络空间领域。

第三章介绍了联合规划过程并指出了网络空间作战规划时须考虑的问题。

第四章阐述了执行联合行动时的网络空间作战。

第五章概述了美国本土的网络空间作战情况。

第六章围绕网络空间作战，介绍了2008年俄罗斯与格鲁吉亚之间的冲突。

附录A概述了网络空间政策、战略和指导。

附录B介绍了美国政府、国防部、联合和军队网络空间组织。

3. 本文由本杰明·莱彻儿（Benjamin Leitzel）和格里高利·希尔布兰德（Gregory Hillebrand）共同撰写并编辑。
4. 修订后的第三卷（2018年7月31日修订）新增了《2018年国家网络战略》和《国防部网络战略》以及《国土安全部—网络安全与基础设施安全局（CISA）》。
5. 本文件以美国的政策和原则为基础，并将根据指导原则的变化定期更新。为不断优化本指南，欢迎各方将修改建议发送至：

宾夕法尼亚州卡莱尔市（Carlisle）莱特大道650号
战略领导中心战略概念与原则部
邮编：17013

目录

目录

第一章 概述

“我们……需要建立一个框架来阻止网络威胁。显然，威胁溯源、升级管理以及加固网络攻击防范措施等都需要加强。”

参谋长联席会议主席约瑟夫·邓福德（Joseph Dunford）将军[1]

1. 本指南遵循作战筹划方法和联合规划程序（JPP），并将这些原则应用于网络空间领域。网络空间指全球信息环境，由相互依赖的信息技术基础设施和驻留数据网络构成，包括互联网、电信网络、计算机系统、嵌入式处理器和控制器。网络空间作战（CO）指利用网络空间能力，在网络空间内部或通过网络空间实现目标。[2]由于战略任务的成功越来越依赖于网络空间的机动性，指挥官必须培养指导网络领域行动的能力。[3]

2. 总统、国防部长（SecDef）和参谋长联席会议主席（CJCS）根据战略方向，向国防部（DOD）传达其总体目标和针对具体问题的指导意见。这提供了统一思想，使联合参谋部、作战司令部（CCMD）、军队、联合部队、作战支援机构（CSA）等国防部机构的规划和行动协调一致地进行。[4]在作战层面，战略纲要发出后会根据规划转化为具体活动，以实现战略和作战目标，达成最终军事目标。[5]

3. 作战指挥官（CCDR）基于战略纲要和方向来制定指挥战略，重点关注本司令部的具体能力和任务，将国家战略纲要与战区或职能战略和联合作战联系起来。与国家战略一样，指挥战略确立了司令部为国家安全需要实现的总体长期目标。计划将战略转化为行动，目的是通过成功的行动来实现预期战略目标。[6]

4. 在国防部长的领导下，国防部借助于网络空间能力来塑造网络空间，并为国家防御提供综合的攻防方案。[7]通过精心控制的级联效应，网络空间行动能够让物理领域的活动更具机动性。[8]通过网络空间作战，CCDR和军队在网络空间内并通过网络空间制造效果，以支持军事目标。[9]CO在启动后要进行大量的战前协作和持续监控，以便在整个作战环境中进行有效协调，消除冲突。[10]

第二章 筹划

I. 作战筹划

1. 联合条例5-0《联合规划》中介绍了作战筹划和联合规划过程（JPP）。作战筹划是指挥官和规划人员用来构建和了解作战环境的方法。框架以迭代形式开发，统一了对作战环境的理解，识别并描述了该环境中的问题，并通过应用作战艺术（Operational Art）来规划方法，根据战略纲要和/或政策来解决这些问题。作战筹划和作战艺术旨在输出作战方法，让指挥官能够进一步规划，将概括性的战略和作战概念转化为具体的任务和工作，并输出可执行的计划。[11]

a. 作战筹划有四个主要组成部分（见图2-1）。各部分不分先后，各有特点。但是，在制定作战方法之前，必须先了解作战环境和问题。此过程具有连续性和周期性，需要在联合行动之前、期间和之后进行。

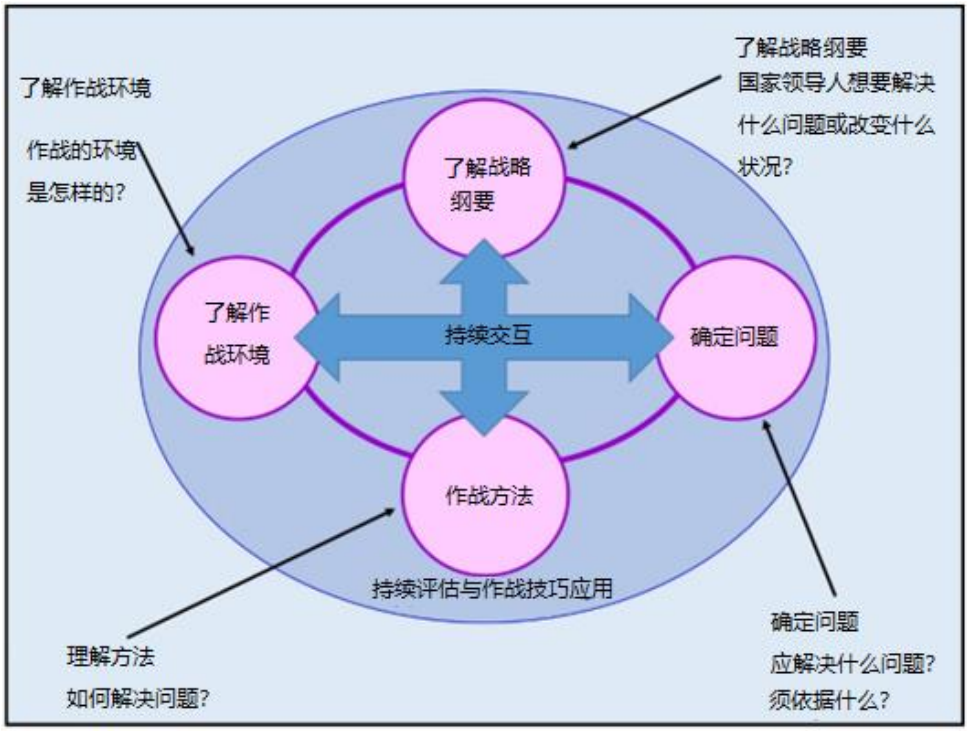


图 2-1 作战筹划框架[12]

b. 作战筹划的一般方法如下：

(1) 了解战略方向及纲要

(2) 了解战略环境（政策、外交与政治）

(3) 了解作战环境

(4) 确定问题

(5) 确定进行下一步规划所需的假设（战略与作战假设）

(6) 开发方案（作战方法）

(7) 进行决策，识别决策点（组织外进行）

(8) 改进作战方法

(9) 开发规划指南[13]

II. 战略方向与网络空间

1. 总统、国防部长和参谋长联席会议主席（CJCS）都会发布战略纲要。该纲要总体上提供了长期目标及中期或补充目标，应定义胜利或成功（**结束**）的要素，确定实现战略目标的可用力量、资源和机构（**手段**）。用军事能力实现目标的作战方法（**方式**）由受援指挥官制定和提出，但政策或国家立场可能会限制指挥官对方案的选用。将资源和战术行动与战略目标联系起来是作战指挥官的责任。[14]

2. **国家安全战略：**2017年12月，特朗普总统发布了《美国国家安全战略》（NSS）。该文件提出了保护美国人民及其生活方式、促进繁荣、通过国力维护和平以及提升美国在世界上的影响力的战略愿景。[15]

a. 为了保护美国人民、国土和美国生活方式，NSS列出了“在网络时代维护美国安全”的五项重点行动：

(1) 识别风险并确定其优先级：为了提高关键基础设施的安全性和韧性，将评估六大关键领域的风险：国家安全、能源电力、银行金融、卫生安全、通信及交通。

(2) 构建可防御的政府网络：我们将使用最新的商业能力、共享服务和最佳实践来实现联邦信息技术的现代化。

(3) 震慑并打击恶意网络攻击者：联邦政府将确保负责保护关键基础设施的人员拥有必要的权限、信息和能力，可提前阻止攻击，避免影响或威胁美国的关键基础设施。

(4) 促进信息共享和感知：美国政府将与关键基础设施合作伙伴合作，评估其信息需求，减少信息共享在速度和保密级别等方面的障碍。

(5) 由于威胁可在全球范围内毫无障碍地通过通信骨干网传播，美国政府将与私营部门合作，纠正网络层的已知恶意活动，提高所有客户的安全性。[16]

b. NSS的第二大愿景是促进美国繁荣，具体包括如下网络空间举措：

(1) 改善带宽，提供更好的宽带连接，防止持续的网络攻击，以支持美国未来的增长并振兴国内经济。

(2) 必须加强网络安全，保护美国国家安全创新基地（NSIB）。

(3) 为确保能源安全，美国将与盟国及合作伙伴合作，保护全球能源基础设施免受网络和物理威胁。[17]

c. 为通过国力维持和平，NSS重点提出了如下活动：

(1) 优化溯源、问责与响应：进行能力投资，以支持和提高网络攻击溯源能力，快速响应。

(2) 改进网络工具，提高专业性：改进应对各种冲突的网络工具，以保护美国政府资产和美国关键基础设施，并保护数据和信息的完整性。美国各部门和机构将招募、培训和维持能够执行这一系列活动的员工队伍。

(3) 促进美国政府各机构和程序之间的整合，根据需要对抗网络攻击者。与国会合作，共同应对当前及未来挑战，以便及时进行情报和信息共享、规划和作

战、开发必要的网络工具等。[18]

d. 最后，NSS要求提升美国的影响力。这一目标可通过多边论坛实现，以：

(1) 确保公共领域始终自由：美国将在国际法框架内提供领导和技术，塑造和管理公共领域，包括太空、网络空间、空中与海洋领域。

(2) 保护自由开放的互联网：美国将倡导开放的互操作通信，最大程度地减少全球信息和服务交换的障碍。[19]

3. **国防战略：**2018年1月，国防部就机密的《2018年国防战略》（NDS）发布了非机密概要，阐明了我们在这种环境中竞争、阻止攻击和取胜的战略。[20]

a. 战略环境既复杂，又充满了竞争：

(1) 当今，各个领域都存在竞争—空中、陆地、海洋、太空和网络空间。

(2) 国家已不再固若金汤。针对个人、商业或政府基础设施的恶意网络活动常以美国为目标。在生活、商业、政府和军队中，网络连接越来越普遍，带来了严重漏洞。在冲突期间，必须做好准备，应对针对美国的重要防御措施、政府和经济基础设施可能发起的攻击。[21]

b. 国防部的战略性方法包括在如下领域进行投资以提升杀伤力：

(1) 网络防御、恢复能力以及网络能力在各种军事行动中的持续融入。

(2) 从战术层面到战略规划的有弹性、可长存的联合网络和信息生态系统。投资会重点考虑获取和利用信息、阻止竞争对手获取相同优势、在防御国家/非国家攻击并追究相关攻击者责任的同时进行溯源的能力。[22]

4. **国防网络战略：**2018年9月，国防部更新了《国防部网络战略》（见附录A的网络空间政策、战略和指导）。

a. 战略确定了下述5个网络空间目标：

(1) 确保联合部队能够在竞争网络空间环境中完成任务；

(2) 开展网络空间行动，增强美国军事优势，最终提升联合部队的能力；

(3) 保护美国关键基础设施免受恶意网络活动的攻击，这些活动本身或作为攻击的一个环节会导致严重的网络事件；

(4) 保护国防部信息和系统免受恶意网络活动的影响，包括非国防部网络上的国防部信息；

(5) 扩大国防部与跨部门、行业和国际合作伙伴的网络合作。

b. 战略确定了下述5个战略方法：

(1) 建立更具杀伤力的联合部队

(2) 在网络空间中进行竞争，形成威慑

(3) 加强联盟并吸引新的合作伙伴

(4) 进行部门改革

(5) 培养人才[23]

III. 网络空间战略环境

1. 在分析战略纲要后，指挥官和规划人员统一对战略环境的认识，确认作战方法所适

用的领域。须考虑的因素包括：

a. 鉴于目前的美国政策以及外交和政治环境，可接受哪些行动或规划假设？

b. 美国的活动会对第三方产生什么影响（关注军事影响，但要认清可能出现的政治后果）？

c. 美国政府目前的国家战略目标是什么？是长期持续目标还是仅为短期目标？这些目标是否会导致意想不到的后果（例如，若向他国提供武器，是否有足够时间来制定有效的控制措施，防止将这些武器用于非预期目的）？[24]

2. 在作战环境内部，因全球因素的存在，可能需要从全球角度进行战略层面的考虑，这些全球因素包括国际法、对手/敌方的信息活动影响世界舆论的能力、对立和友好组织机构、国家和商业空基系统和信息技术的功能及可用性等。[25]

3. 恶意网络活动威慑政策和策略。根据2017年5月11日第13800号总统行政命令《加强联邦网络和关键基础设施的网络安全》，国务院起草了一份报告，其中包括如下恶意网络活动威慑战略和政策：

a. 美国依然强大，可阻止构成武力使用的网络攻击，因为传统的威慑工具—包括以牙还牙使用军事力量—仍然卓有实效。然而，对于暴涨的由国家支持的未构成武力使用的恶意网络活动，却很难发挥威慑作用。

b. 拒止性威慑（Deterrence by Denial）须为美国的基本威慑方法，这种威慑是指防御和保护关键基础设施和其他敏感的计算机网络，确保有效缓解恶意网络活动并及时恢复。

c. 美国进行威慑的最终目的是：

(1) 让针对美国及其伙伴和盟国的构成武力使用的网络攻击长期消失；

(2) 长时间内显著减少损坏美国利益的不同程度的破坏性但尚未构成武力使用的恶意网络活动。

d. 这种方法包括如下要素：

(1) 制定政策，明确美国何时可施加影响；

(2) 定义这些影响；

(3) 规划政策，明确如何施加影响；

(4) 建立合作伙伴关系。[26]

IV. 网络空间作战环境

1. 作战环境是影响功能使用的条件、环境和影响力的综合，是指挥官决策的重要参考依据。它包括空中、陆地、海洋和太空领域的物理区域和因素以及信息环境（包括网络空间）。了解作战环境有助于指挥官更准确地识别问题，预测潜在后果，并预知各种友好、敌对和中立行动的结果以及这些行动对于实现军事目标的影响。[27]

2. 网络空间的作战能力已成为至关重要的国家安全要求。信息战对军事行动的影响越来越大，这进一步提升了网络空间的重要性。技术能力和信息访问即时性的不断提高促进了实时通信和信息共享的实现。这些能力对经济和国家发展至关重要。但是，要依赖这些能力，必须对网络和信息进行保护。网络空间的敌对活动可能会威胁到美国在空中、陆地、海洋和太空领域的主导地位，因为这些领域之间的联系越来越紧密，对网络空间技术的依赖也日益增强。[28]

3. 独特的网络空间能力和特征。快速、动态的信息交换影响着生活的方方面面，而网络空间是实现这一切的全球推动者。它允许在全球范围内即时传递金融交易信息以及运输和跟踪产品和货物。但是，它同时允许攻击者随时随地访问此等信息并中断重要操作。网络空间易于访问，因而难以管控。从军事角度来看，网络空间活动几乎不要求军事力量进行空间转移，可以在长期对峙状态进行交战。网络空间还能够影响到其他领域所无法触及的人群。

a. **允许逆向工程：**与通常一经使用就被“毁尸灭迹”的弹药不同，网络空间活动中的代码可以保存、分析和重新编码，可能会被重新用来攻击盟友或友国。规划人员必须虑及“网络反弹”[29]的可能性，即网络活动因逆向工程而为发起人或其他非预期目标带来不利影响。

b. **没有单一的国家/国际所有权：**虽然网络空间的物理组成部分各有归属，但网络空间本身并不受任何单一国家或实体的完全控制。基础设施是公共和私有网络的异类组合，没有标准化的安全性或访问控制措施。这种设置可以实现信息的自由流动，但缺乏控制会影响全球问责制、标准化和安全性的实现。由于网络空间的性质，传统的领土完整概念在网络空间难以定义。

c. **缺乏合作/协作：**因为缺乏用以管理环境的国际法律法规，对该领域行动的响应异常复杂。网络攻击—尤其是由个人黑客发起的攻击—难以溯源，因而难以响应。另外，还存在这样一个倾向，人们常否认有网络空间攻击发生，以避免对组织的网络安全措施失去信任，这进一步阻碍了合作。

d. **低成本：**网络空间是对美国发动攻击的最经济的领域。病毒、恶意代码和培训都可以方便地从网上免费获得。攻击者会开发、编辑网络攻击工具并复用现有工具。得益于廉价的工具和培训，攻击者无需昂贵的船只、飞机或导弹便可发动攻击。此外，由于这些攻击者的存在，严重依赖网络空间的国家不得不在网络空间防御方面进行投资，从而背负沉重的经济负担。目前，对于大多数恶意攻击者而言，“军用级”网络空间能力仍然过于昂贵，但他们可以购买相对廉价的专业黑客服务。

e. **易变性：**网络空间攻击是否成功取决于对手网络中的漏洞。识别这些漏洞并创建网络空间能力有时所费巨糜。若对方发现了自己网络中的漏洞并将其修复，那么即使斥巨资开发了网络空间攻击技术，这些技术也会立刻沦为无用之物，这显然背离了初衷。因此，必须非常小心，防止打草惊蛇，避免让对手发现其网络中的漏洞。

f. **速度：**网络空间行动都很迅速。但是，这些行动往往要做大量的准备工作，包括对对手的网络进行深入研究，以了解系统规范及生活模式。因此，在没有充足准备的情况下，针对某个对手网络的网络空间部队可能无法重新聚焦至另一个目标。

g. **意外级联效应：**网络空间的另一个独特特征是可能出现意想不到的级联效应。自然领域的能力和弹药因距离的增加其影响逐渐减弱。然而，物理距离在网络空间无足轻重。虽然网络空间能力是在计算机实验室和网络空间范围内开发和评估的，但在浩渺的网络空间引入某项能力时，该能力的实现方式或发展方向永远无法确知。[30]

h. **分层：**网络空间包含三个相互关联的层：物理网络层、逻辑网络层和网络角色层（见图2-2）。每一层焦点不同，可以围绕该焦点规划、实施和评估CO情况。

(1) **物理网络层**指物理域中用于在网络空间内对信息进行存储、传输和处理的信息技术（IT）设备和基础设施，包括数据存储库和网络组件之间的数据传输连接。物理网络组件包括硬件和基础设施（例如计算设备、存储设备、网络设备以及有线和无线链路）。网络空间的各物理组件由公共或私人实体拥有，他们可以控制或限制对其组件的访问。在规划的所有阶段都必须考虑作战环境的这些独特特征。

(2) **逻辑网络层**由网络元素组成，这些元素从物理网络中抽象出来，相互关联，基于驱动网络组件的逻辑编程（代码）构建，也就是说，这些关系不一定与特定的物理链路或节点相关，而是与逻辑上被处理的能力和交换或处理数据的能力相关联）。单个链接和节点在逻辑层中表示，各种分布式网络空间元素也位于逻辑层，这些元素不囿于单个节点，包括数据、应用程序和网络进程。例如联合知识在线网站，它存在于物理域中不同位置的多个服务器上，但在万维网上用单一URL表示。

(3) **网络角色层**是网络空间视图，该视图通过利用适用于逻辑网络层的规则从逻辑网络层中提取数据来创建，以便以数字化方式来描述网络空间中的参与者或实体身份（网络角色）。网络角色层由网络或IT用户账号（人工或自动化）以及它们之间的关系组成。网络角色可与实际的人或实体直接相关。个人可以在网络空间使用多个标识符，以创建和维护多个网络角色（例如工作和私人电子邮件地址不同，或在不同的网络论坛、聊天室和社交网站上使用不同身份），虽然真实程度或有不同。相反，单个网络角色也可以对应多个用户，例如多个黑客可能使用相同的恶意软件控制别名，多个极端分子可能使用同一银行账户，或同一组织的所有成员使用相同的电子邮件地址。使用网络角色让网络空间行动很难溯源。[31]

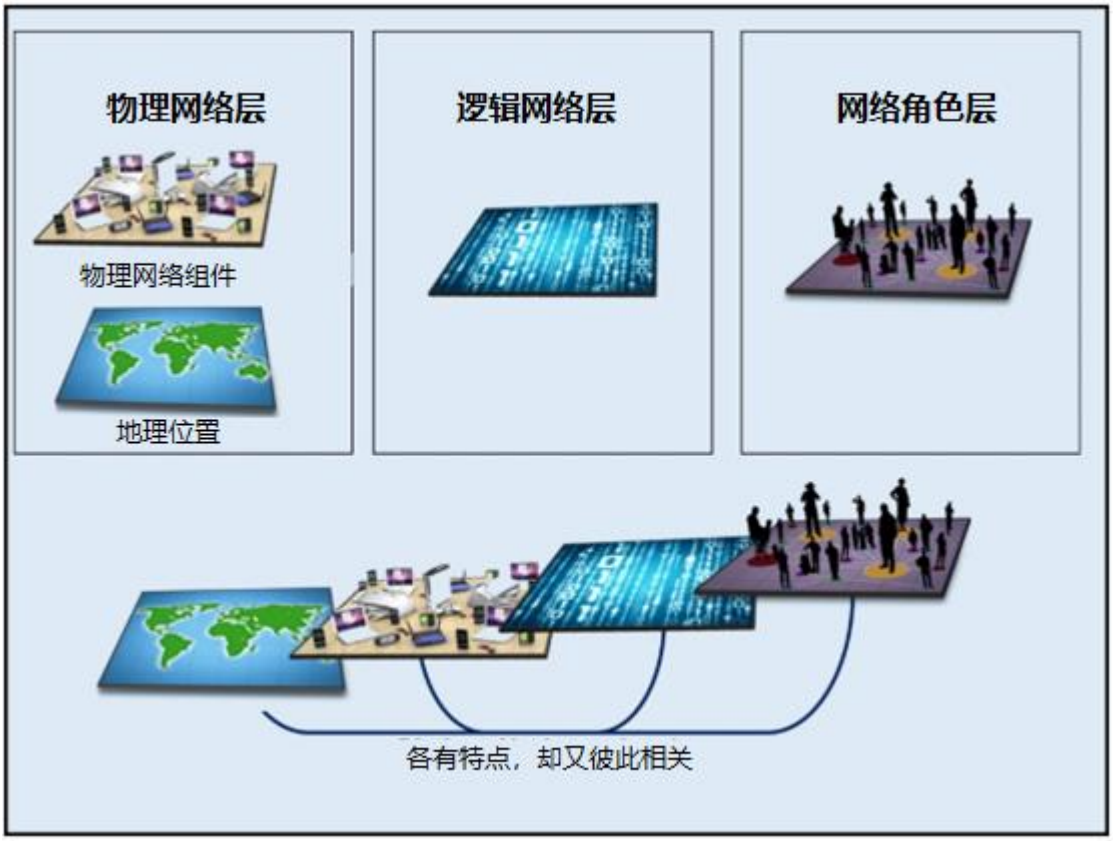


图 2-2 三层网络空间[32]

4. **网络空间位置和所有权。**在网络空间中的用兵很复杂，通常无法觉察。所以，规划、执行和评估作战环境的人员有必要基于位置或所有权来描述网络空间，以便快速了解事先规划的行动。

a. **蓝色网络空间**表示受美国及其任务合作伙伴保护的网络空间以及国防部受命保护的其他区域。虽然国防部常规仅保护国防部信息网络（DODIN），但网络空间部队时刻准备，会根据命令或应其他机构要求防御或保护美国政府其他部门或其他网络空间，以及与美国及其伙伴国关键基础设施和关键资源（CI/KR）相关的网络

空间。

b. **红色网络空间**指由对手或敌人拥有或受其控制的网络空间部分。在这种情况下，“控制”不仅仅意味着“存在”，因为威胁可能会不为人知地秘密访问全球网络空间中的网元，同时对系统的运行没有明显影响。这里，“控制”意味着指挥网络空间中某个特定链接或节点的行动的能力。

c. **灰色网络空间。**所有不符合“蓝色”或“红色”描述的网络空间都被称为“灰色”网络空间。[33]

5. **国防部网络空间。**DODIN由一系列信息功能和相关流程组成，根据需要为作战人员、决策者和支持人员搜集、处理、储存、传播和管理信息，包括互联和独立系统，以及自有和租用的通信和计算系统和服务、软件（包括应用程序）、数据、安全服务、其他相关服务和国家安全系统。DODIN涵盖所有国防部网络空间，包括机密和非机密全球网络（例如NIPRNET、SIPRNET、联合全球情报通信系统等）和许多其他组件，例如归属于国防部的智能手机、射频识别标签、工业控制系统、隔离实验室网络和平台信息技术（PIT）。PIT为专用系统（包括武器系统）中的软件和硬件，专门用于执行任务，对后者来说必不可少。国防部的几乎所有军事和文职雇员均使用DODIN来完成某些任务或职责。[34]

V. 确定问题：网络空间中的威胁与挑战

1. 确定问题对于解决问题至关重要，包括了解和隔离当前问题的根本原因—确定复杂、含糊的问题的本质。确定问题的第一步是审核相关参与者的倾向和潜力，并明确这些参与者各自的期望条件和目标之间的关系和相互作用。问题描述要明确说明行动变量如何抵抗或促进转换，以及如何利用作战环境中的惯性来确保满足期望条件。[35]在复杂的全球安全环境中指挥网络空间行动时，指挥官面临着一系列独特的网络空间威胁和挑战。

2. **网络威胁。**网络空间中，指挥官要面临从民族国家到个人攻击者带来的威胁。

a. **国家威胁。**这种威胁可能是最危险的，因为国家可以获得其他攻击者可能无法获得的资源、人力和时间。有些国家可能利用网络空间能力去攻击美国或针对美国进行间谍活动。国家威胁涉及传统的对手、敌人，在间谍活动中，甚至可能是传统的盟友。国家可能直接进行攻击，也可能将其外包给第三方，包括掩护公司、爱国黑客或其他代理，以实现其目标。

b. **非国家威胁。**非国家威胁指不受国界约束的正式和非正式组织，包括合法的非政府组织以及诸如犯罪组织、暴力极端组织等的非法组织，或其他敌人和对手。非国家威胁利用网络空间筹集资金，与目标受众通信或彼此通信，进行招募、规划行动，破坏对政府的信任，进行间谍活动等，并在网络空间内进行直接的恐怖主义行动。犯罪组织可能只在本国活动，也可能具有跨国性质，它们为私利窃取信息，用以出售获利或针对金融机构进行欺诈和盗窃资金。这些组织也可能被国家或非国家威胁雇佣，通过网络空间进行攻击或间谍活动。

c. **个人攻击者或小团伙威胁。**因为廉价的现成技术和恶意软件，个人或小团伙同样会攻击或利用美国网络空间。他们数量众多，各有企图。这些威胁利用漏洞获取访问权限，发现其他漏洞、敏感数据，或通过各种花招实现其他目标。道德黑客可能会将漏洞信息共享给网络所有者，但更常见的是，这些访问权限被用于恶意目的。有些威胁具有政治动机，利用网络空间传播诉求。这些小规模威胁的活动会被更复杂的威胁（例如犯罪组织或国家）所利用，通常在不知情的情况下对目标发动攻击，这样，威胁/赞助人一方面能够隐藏其身份，另一方面可以毫无破绽地矢口否认。

d. **事故或自然灾害。**网络空间的物理基础设施经常因操作员错误、工业事故和自然灾害而中断。与敌人的行动相比，这些不可预测的事件对联合行动的影响更大。

事故和危险事件的恢复会因某些因素的存在而非常棘手，比如需要非国防部部门进行重要协调和/或临时启用操作员可能并不熟悉的备用系统。[36]

3. **挑战。**除了上述威胁之外，指挥官在确定问题和制定作战方法时还必须应对重大的网络空间挑战。

a. **匿名及难以溯源。**在网络空间溯源时，最大的挑战是将特定的网络角色或行动与特定的个人、团体或民族国家以可验证的方式联系起来，信心十足地让后者负责。这项工作需要进行大量分析，通常还要与非网络空间机构或组织合作。因为在网络空间中可以隐藏特定恶意效果背后的赞助人和/或威胁，因而难以确定响应的方式、时间和地点。互联网的设计适合匿名，与旨在隐藏用户身份的应用程序相结合，溯源在可预见的未来将仍是一大挑战。

b. **地理挑战。**在网络空间，没有无国界的用兵空间。因此，当美国军队在外国网络空间活动时，具体的任务和政策可能要求他们秘密行事，不让**基础设施**所在国察觉。由于 CO 通常能够以有线或无线访问实现的虚拟状态远程执行，因此许多网络空间行动不需要在地理位置上接近目标，而是利用远程操作来实现目的，也就是说，虽然物理区域受限，作战范围却增大了。这里提及的全球作战范围不仅包含蓝色网络空间中的内部保护行动，还包括红色和灰色网络空间中的外部行动。

c. **技术挑战。**网络空间能力若依赖于对目标中技术漏洞的利用，可能会暴露其功能，影响未来执行任务时的有效性。没有硬件组件的网络空间功能可以免费或以很少的成本复制。这意味着一旦被发现，这些功能便会被大量的攻击者获取，在某些情况下，甚至在 DODIN 中的安全措施针对新威胁进行更新之前就被攻击者获取。此外，由于世界各地的类似技术有相似漏洞，因此单个攻击者可使用相同的恶意软件或漏洞利用策略同时针对多个目标。恶意软件可以修改（或设计为自动进行自我修正），因此很难检测和根除。[37]

4. **针对美国的网络行动（自 2010 年起）。**2018 年 2 月，国家情报总监（DNI）表示："随着数十亿台新增数字设备—其内置安全性相对较低—的入网，网络领域在未来一年及之后可能会出现更多的意外，国家和恶意行为者会变得更为大胆，由于网络工具包的广泛传播，装备也会更为精良。对手对美国近乎战争的网络攻击（例如数据删除或关键基础设施的局部和临时中断）的风险越来越大。"最后，情报总监总结道："俄罗斯、中国、伊朗和朝鲜将在明年对美国构成最大的网络威胁。这些国家将网络作战作为一种低成本的治国工具，我们认为，他们将利用网络行动来实现战略目标，除非他们的网络行动明显受挫。非国家威胁将继续利用网络行动进行金融犯罪，进行宣传并传递信息。在军事冲突外使用网络攻击作为外交政策工具仅零星见于低级别攻击事件，但俄罗斯、伊朗和朝鲜正在测试更具侵略性的网络攻击，对美国和美国的合作伙伴构成越来越大的威胁。"[38]美国政府确认的针对美国的网络空间行动列举如下：

a. **俄罗斯。**国家情报总监表示："我们预计俄罗斯将在明年进行更大胆、更具破坏性的网络行动，可能性最大的是，利用新能力攻击乌克兰。俄罗斯政府已经展开了各种行动，包括中断乌克兰能源分配网络、黑客入侵与泄露影响行动、分布式拒绝服务攻击和伪旗行动，但还不满足于此。明年，俄罗斯情报和安全部门将继续探查美国及其盟国的关键基础设施，并将对美国、北大西洋公约组织（NATO）和盟国发动攻击，以窥视美国政策。"[39]

2015 – DNI 指出，俄罗斯网络攻击者正在开发方法远程访问工业控制系统（ICS），管理关键基础设施。身份不明的俄罗斯攻击者已成功破坏了至少三家 ICS 厂商的产品供应链，导致客户下载了恶意软件，这些恶意软件使得攻击者可直接利用厂商网站以及合法软件更新发动攻击。[40]

2016 – 美国司法部宣布，某大陪审团对 12 名俄罗斯人提起诉讼，称这些俄罗斯人因企图干涉 2016 年美国总统大选而违反了联邦法律。所有这 12 名被告均为 GRU 的成员，而 GRU 是俄罗斯军方情报管理总局下属的俄罗斯联邦情报机构。[41]

2017 – 在参议院军事委员会的证词中，美国网战司令部（USCYBERCOM）指挥官、海军上将罗杰斯称，美国国土安全部（DHS）的国家网络安全和通信集成中心（NCCIC）于 2017 年 7 月就前一年冬季攻击乌克兰电网的新型恶意软件向公用事业公司发出了警告。他还补充说，造成史上最惨重损失的网络攻击 NotPetya 是由俄罗斯军方于 2017 年 6 月发起的，该病毒加密并彻底破坏了数千台乌克兰计算机上的硬盘。这场网络攻击迅速蔓延到乌克兰以外，给整个欧洲和远至美国的企业带来了数十亿美元的损失。[42]

b. **中国。**据 DNI 评估，中国将继续利用网络间谍活动并加强网络攻击能力，以支持国家安全优先事项。情报界和私营部门安全专家不断发现中国所进行的网络活动，尽管数量明显低于 2015 年 9 月美中双边网络承诺之前的数量。中国发起的针对美国私营企业的大多数网络行动都集中在特许国防承包商或为全球政府和私营部门网络提供产品和服务的 IT 和通信公司。自 2015 年建立战略支援部队以来，中国一直不断将其军事网络攻击和间谍资源整合到该部队中以提升网络攻击能力。[43]

2012 – 一中国公民承认其参与了长达数年的阴谋入侵美国主要国防承包商的计算机网络，窃取军事技术数据（C-17 战略运输机和某些战斗机），并将窃取到的数据发送回中国。[44]

2013 – 中华人民共和国人民解放军总参三部（3PLA）二局第三办公室（番号：61398）人员被控阴谋渗透六家美国公司的计算机网络，而这些公司当时正与中国的国有企业进行谈判、举办合资企业或采取法律行动。然后，他们利用非法访问，涉嫌窃取私有信息，包括公司员工之间发送的电子邮件以及与核电厂设计技术规范相关的商业秘密。[45]

2014 – 一家名为“社区卫生系统”（Community Health Systems）的美国公司告知美国证券交易委员会，诉称“来自中国”的黑客窃取了 450 万人的个人身份信息。[46]

2017 – 海军上将罗杰斯作证说，奥巴马总统和习近平主席在 2015 年承诺，两国不会为了商业利益借助网络窃取知识产权或在知情情况下对此种行为表示支持。然而，随后的证据表明，位于中国的黑客持续利用美国企业、大学和国防工业的商业机密和知识产权，进行网络间谍活动。2017 年秋季，司法部对三位中国公民提起诉讼，指控他们从美国的几家公司获得了超过 400G 的数据。此外，中国政府利用信息和技术产品的生产搜集外国的企业、政府甚至个人数据。[47]

c. **伊朗。**DNI 表示，伊朗会继续设法渗透美国和盟军的网络进行间谍活动，并为未来的潜在网络攻击做准备，尽管伊朗的情报部门主要关注中东对手—尤其是沙特阿拉伯和以色列。尽管伊朗最近未对美国或其西方盟友发动网络攻击，但德黑兰很可能将网络攻击视为应对所谓挑衅的有用工具。2016 年底和 2017 年初，伊朗对沙特阿拉伯发动网络攻击，删除了政府和私营部门数十个网络的数据。[48]

2011 – 2013 – 在伊朗伊斯兰革命卫队的支持下，一团伙针对 46 家大公司（主要是美国金融部门）进行了一次协同分布式拒绝服务（DDoS）攻击。在超过 176 天的时间里，攻击不断发生，造成目标银行网站瘫痪，客户无法访问在线账户，为此这些银行共花费了数千万美元进行修复，以对抗并减轻对其服务器的攻击。[49]

2013 – 一名伊朗黑客非法访问位于纽约州拉伊市的鲍曼大坝的数据采集与监控系统（SCADA）系统，反复获取有关大坝状况和运行的信息，包括水位和温度信息以及负责控制水位和流量的水闸状态。[50]

2014 – 计算机安全专家称，某伊朗组织的成员负责通过计算机操作对美国军方、运输、公用事业等关键基础设施网络发动攻击。[51]伊朗攻击者还对某美国赌场的网络进行了数据删除攻击。[52]

2017 – 伊朗于 2016 年底和 2017 年初对沙特阿拉伯（并非美国）发动了网络攻击，删除了政府和私营部门数十个网络的数据。[53]

d. **朝鲜。**DNI 表示，估计朝鲜会利用网络行动筹集资金、搜集情报或对韩国和美国发动攻击。平壤很可能有多种技术和工具能够发动突然袭击，包括 DDoS 攻击、数据删除和勒索软件部署。[54]海军上将罗杰斯补充说，我们认为，如果对私营部门目标、特别是关键基础设施发动网络攻击，朝鲜网络攻击者并不具备技术能力、也不认为自己有义务去控制损害。[55]

2014 – 联邦调查局（FBI）表示，朝鲜对索尼电影娱乐公司发动了一次网络攻击，窃取企业信息并将硬盘驱动器擦除恶意软件植入到该公司的网络基础设施中。[56]

2016 – 朝鲜攻击者从孟加拉银行窃取了 8100 万美元，对美国金融市场产生了间接影响。[57]

2017 – 从 WannaCry 与先前确认的朝鲜网络工具、谍报技术和作战基础设施的技术联系来看，朝鲜攻击者于 2017 年 5 月开发并推出了该款勒索软件。[58]

e. **叙利亚。**

2011 和 2013 – 两名叙利亚黑客被指代表叙利亚电子军（SEA）攻击了美国境内外的互联网网站。SEA 是一个支持叙利亚总统巴沙尔·阿萨德政权的黑客团体。被攻击的站点包括 2011 年总统行政办公室的计算机系统和 2013 年美国海军陆战队的征兵网站。他们使用“鱼叉式网络钓鱼”来收集用户名和密码、篡改网站、重定向域名至由自己控制的网站、窃取电子邮件以及劫持社交媒体账号。[59]

2014 – SEA 的一名成员涉嫌对多家国内外公司进行了一系列的网络勒索活动。[60]

2017 – 某联邦大陪审团提交了含有 11 项指控的起诉书，指控两名叙利亚男子作为 SEA 成员参与了计算机黑客行动。根据起诉书中的指控，两人主要进行了鱼叉式钓鱼，目标为美国政府、军队、国际组织和私营部门实体，包括总统行政办公室、美国海军陆战队、国家航空航天局、国家公共广播电台、美联社、路透社、华盛顿邮报、纽约时报、美国有线电视新闻网（CNN）、洋葱、今日美国、纽约邮报、时代周刊、人权观察等几十个实体和个人。攻击者发动了鱼叉式钓鱼攻击，窃取用户名和密码以篡改网站，将域名重定向到由其控制或利用的网站，窃取电子邮件并劫持社交媒体账号。[61]

f. **恐怖分子。**DNI 证实，恐怖组织将继续利用互联网组织活动、招募人员、进行宣传、筹集资金、搜集情报、教唆信徒采取行动、协调攻击等。鉴于他们的当前能力，恐怖组织的网络行动很可能会导致个人身份信息（PII）泄露、网站篡改，对不够安全的网络还会发动拒绝服务攻击。跨国犯罪分子将继续进行营利性的网络犯罪，例如对美国境内的网络发动盗窃和勒索攻击。[62]

2015 – 伊拉克和叙利亚伊斯兰国（ISIS）发布了有关美国军事人员的敏感信息，进行挑衅。[63]

g. **犯罪分子。**DNI 指出，犯罪分子在开发复杂的网络工具，将其用于各种目的，包括盗窃、勒索和辅助其他犯罪活动。使用欺骗和加密来阻止用户访问自己数据的“勒索软件”已成为极其流行的勒索工具。我们预测，因为各国将网络犯罪工具视为相对廉价和易于抵赖的攻击手段，犯罪和国家活动之间的界限会变得越来越模糊。[64]

2014 – 2016 – 四名个人，包括两名俄罗斯联邦安全局（FSB）官员，被指控涉嫌入侵了至少 5 亿雅虎账户。[65]

2016 – 犯罪分子使用勒索软件攻击医疗部门，影响了患者护理，破坏了公众对某些医疗机构的信心。[66]

2017 – 司法部指控 36 名个人隶属于 Infraud 组织，该组织是一家基于互联网的网络犯罪企业，从事大规模收购、销售和传播盗取的身份、被泄露的借记卡和信用卡、个人身份信息、金融和银行业务信息、计算机恶意软件等违法交易。[67]

h. **内部威胁。**

2010 – 经调查，陆军一等兵曼宁（Army PFC Manning）并没有犯下故意帮助敌人的严重罪行，但是因涉嫌将数十万份情报文件提供给维基解密而被认定 20 多项其他罪名。检察官称，曼宁从机密互联协议路由网（SIPRNET）上下载了大约 470,000 份重要活动（SIGACT）报告（来自伊拉克和阿富汗）。[68]

2013 – 爱德华·J·斯诺登（Edward J. Snowden）被控犯有以下罪行：未经授权披露国防信息、未经授权披露机密通讯、盗窃政府财产。[69]

2015 – 曾在美国核管理委员会工作的一名员工承认对能源部计算机试图发起鱼叉式钓鱼攻击，以入侵、利用和破坏包含敏感核武器信息的美国政府计算机系统，目的是帮助他国获取对该信息的访问权限或破坏重要系统。[70]

2017 – 瑞爱丽缇·李·温那（Reality Leigh Winner）是一位来自乔治亚州奥古斯塔的联邦承包商，被指控（后认罪）从政府机构带走机密材料并邮寄给新闻机构。[71]

5. **网络空间威胁技术。**对手使用各种网络空间技术来实现目标，其中包括：

a. **后门。**指获得对安全区域访问权限的非正常途径、隐蔽方法或绕过正常安全措施的其他方法，也被称为陷门。有时，后门被秘密地植入在网元中。但是，在某些情况下，会故意留有后门，以方便技术人员进行系统管理、维护和排障操作。

(1) 这些接口的安全性通常由用户 ID 和密码来保证。然而，密码通常是计算机安全方案中最薄弱的环节，因为密码破解工具不断改进，用于破解密码的计算机性能也在不断增强，曾经需要数周才能破解的网络密码现在几小时就能破解。

(2) 这种预留接口方便了服务提供商维护设备，但许多厂商建立了后门访问这些接口，以便远程排除设备故障。这意味着来自组织外部的技术人员能够访问系统，进行网络恐怖活动。

b. **拒绝服务攻击（DoS）。**这种攻击旨在中断网络服务，一般是通过每秒数百万次的请求拖垮系统，导致网络速度变慢或崩溃。

c. **分布式拒绝服务攻击（DDoS）。**DDoS 攻击作为更为有效的 DoS 攻击，使用大量的计算机集中攻击目标。这种攻击不仅通过更多的请求使目标过载，而且从多个路径发动 DoS 会使回溯异常困难，几无可能。很多时候，攻击者在计算机中植入蠕虫创建僵尸，这样便可在用户不知情的情况下用这些机器发动攻击。

d. **电子邮件欺骗（即网络钓鱼）。**电子邮件欺骗是指向用户发送电子邮件，将真实发件人伪装为其他来源。这种方法诱骗用户的花招通常包括诽谤性言辞或自称领导要求用户向其发送密码文件或其他敏感信息。

e. **IP 地址欺骗。**这种方法是使用其他人的 IP 地址构造 TCP/IP 数据包。路由器使用“目标 IP”地址通过互联网转发数据包，但忽略“源 IP”地址。此方法通常用于 DDoS 攻击，以隐藏攻击者的真实身份。

f. **键盘记录器。**这是一种软件程序或硬件设备，用于监视和记录用户的每次键入。安装了该程序或硬件设备后可查看目标用户的所有键入。因为这些程序和硬件设备监视的是实际键入，所以用户可轻易获取计算机操作人员可能不希望他人知晓的密码等信息。

g. **逻辑炸弹。**这是一种程序例程，通过重新格式化硬盘或在数据文件中随机插入无用数据来销毁数据。用户若下载了遭篡改的公共域程序，就可能将逻辑炸弹植入电脑。一旦执行，它会立即造成伤害，这与病毒不同，病毒是持续作乱。

h. **物理攻击。**指对计算机系统和/或网络（包括传输网络以及终端设备）造成的实际物理破坏。[72]

i. **勒索软件。**这是一种恶意软件，用于感染并限制对计算机的访问，直到支付赎金为止。勒索软件有多种传播方法，但大多利用网络钓鱼邮件或软件中未修补的漏洞。[73]

j. **嗅探器。**指监视网络传输数据的程序和/或设备。虽然嗅探器用于合法的网络管

理，但也可在网络攻击期间用于窃取网络上的信息，包括密码。嗅探器一旦安装，便很难察觉，并且可通过不同方式植入几乎任何位置。

k. **木马。**这是一种程序或实用程序，可伪装为正常程序，如屏幕保护程序。但是，一旦安装，它就会在后台执行某个功能，例如向其他用户开放目标计算机的访问权限或从目标计算机向其他计算机发送信息。

l. **病毒。**用于感染、破坏、修改计算机或软件程序或使计算机或软件出现其他问题的软件程序、脚本或宏。

m. **蠕虫。**这是一种破坏性软件程序，包含能够访问计算机或网络的代码，一旦进入计算机或网络内，便可通过删除、修改、分发等数据操控方法来破坏该计算机或网络。[74]

VI. 网络空间假设

1. 指挥官和参谋应审查战略纲要和方向，确定规划过程中是否加入了任何假设。若缺乏足够的信息或指引，指挥官和参谋会确定假设，协助制定解决方案。在此阶段，假设解决的是战略和行动差距，指挥官可以据此制定作战方法。[75]

2. 网络空间能力特征。网络空间复杂且不断变化，网络空间能力—无论是设备还是计算机程序—必须能够稳妥地实现预期效果。然而，网络空间能力要基于环境假设和对作战环境中预期出现的作战条件而开发。这些条件可能简单如对手使用的计算机操作系统类型，也可能复杂如所安装硬件的准确序列号或软件版本、可用的系统资源以及网络空间能力在如期激活时须运行（或不运行）的其他应用程序。这些预期条件应由能力开发人员妥善记录，有助于规划人员和目标定位人员理解能力的局限性。若通过情报、监视和侦察（ISR）来源无法确定目标的预期环境条件，则这种不确定性越大，使用该能力的相关风险水平就越高。在所有其他因素相同的情况下，优选具有最少环境依赖性和/或允许操作员重新配置能力的网络空间能力。[76]

VII.网络空间行动与作战方法

1. 作战方法是指挥官对部队为实现某个目标（以支持国家目标或实现最终军事目的）而采取的各种行动的描述。它反映了指挥官对如何通过行动将当前条件转变为预期条件的设想，也就是说，指挥官所期望的行动结束时应达到的可支持实现国家目标的作战环境。作战方法主要基于对作战环境的理解和指挥官所面临的问题。[77]

2. **网络空间的“内部”、“外部”行动以及“通过”网络空间进行的行动**在制定作战方法时，指挥官应将网络空间“内部”的行动和“通过”网络空间进行的行动与其他活动同步，以实现预期目标。网络空间的“内部”行动通常体现为攻防活动，目的是防止对手使用资源或操控对手的信息、信息系统或网络。另一方面，军方在执行如下职能时常“通过”网络空间展开行动：指挥与控制、情报、火力、行军与用兵、防护、保障和信息。这些联合职能包括相关能力和活动，这些能力和活动组合在一起，帮助指挥官统一、同步和指导作战行动（参见图 2-3）。[78]

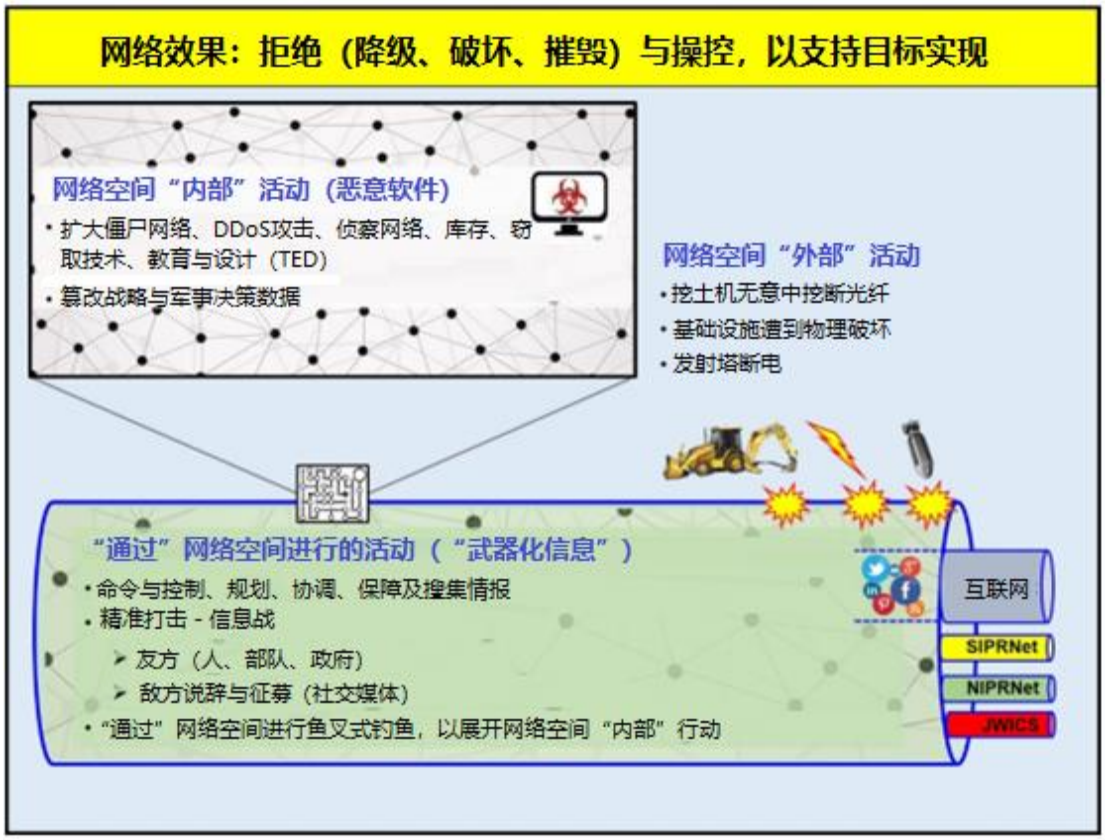


图 2-3 网络空间的“内部”、“外部”行动以及“通过”网络空间进行的行动

3. **美国军事对网络空间的依赖。**指挥官必须意识到，美国军队作战时严重依赖网络和信息系统。国防部内几乎所有部门都与网络相连，这些联网系统和部门与国防部规划军事力量和相关任务保障的能力密不可分。在过去的几十年中，国防部形成了“全谱优势”作战思想，认为信息优势大有可为，可将武力值成倍扩大。这种思想几乎完全依赖信息优势，在其强大影响下，国防部内几乎所有可以想见的部门均已联网，同时因为需要与其他政府部门、商业和私有实体以及联盟伙伴联系，彼此之间构成了复杂、相互交织的网络。这些无处不在的 IT 能力确有裨益，但也使美国对受保护的安全访问和网络中所包含数据的完整性有了越来越高的依赖性。这种思想的缺陷是相对于安全性来说，它更关注功能、连接性和信息优势，这和互联网的发展类似。

4. **网络空间漏洞。**美国军队的表现证明了联网系统的优越性以及强大的军事能力和训练有素的武装力量。敌方已然发现，连接和自动化虽为美国提供了巨大优势，但同时也是一个薄弱环节，使其可以用非常不对称的方式破坏美国能力。商业市场上的网络攻击工具唾手可得，敌方可以轻易获取。此外，经济实力雄厚的敌人会投资改进这些工具并建造更强大的武器来攻击美国的军事系统和国家基础设施。[79]

5. **网络空间任务。**网络空间中的行动若不只是依靠网络空间实现，则被视为如下网络空间任务：国防部信息网络（DODIN）作战、防御性网络空间作战（DCO）或进攻性网络空间作战（OCO）（见图 2-4）。CO 对于指挥官来说有直接的好处，有助于设计作战方法以及实现预期效果、条件和终极目标。要成功实施 CO，需要整合并同步这些任务。

   a. **国防部信息网络（DODIN）作战。**DODIN 作战任务指为保护、配置、操作、扩展、维护和保障 DOD 网络空间以及建立和保持 DODIN 的机密性、可用性和完整性而采取的行动，包括为解决 DODIN 或 DODIN 特定网段的漏洞所采取的主动的网络空间安全行动。DODIN 行动聚焦于网络，针对各种威胁：执行此任务的网络空间部队和人员尽其所能，将所有威胁拒之于所保护的特定网络或系统之外。尽管许多 DODIN 作战行动定期执行，但不应将其视为日常活动，而应作为长期任务，其总体目标是建立框架，为国防部大多数任务提供基础。

b. **防御性网络空间作战（DCO）。**国防部网络空间部队执行 DCO 任务是为了保护 DODIN 或其他受命保护的网络空间免受网络空间的主动威胁。具体而言，这些任务旨在通过挫败正在进行或即将发生的恶意网络空间活动，维持利用蓝色网络空间能力以及保护数据、网络、网络设备和其他指定系统的能力。这是 DCO 任务和 DODIN 作战的不同，DCO 是挫败绕过、破坏或即将破坏安全措施的特定威胁，而 DODIN 作战是在特定威胁活动发生之前设法保护国防部网络空间免受所有威胁。DCO 与特定威胁相关，一般为任务保障目标提供支持。DCO 任务是针对特定攻击威胁、利用活动或恶意网络空间活动的其他影响而展开的，根据需要，会利用从用兵、情报搜集、反情报、执法部门等来源所获取的信息。DCO 包括挫败或阻止对手对被保护网络空间元素所进行或将要进行的攻击行动，或以其他方式应对迫在眉睫的内外部网络空间威胁。DCO 的目标是消除特定对手的威胁和/或将被入侵网络恢复到安全状态并正常运行。DCO 包括如下要素：

(1) **DCO 内部防御措施（DCO-IDM）。**DCO-IDM 作为一种 DCO 任务，在被保护网络或局部网络空间内根据授权进行防御行动。DODIN 的 DCO-IDM 通过委托书授权，涵盖网络空间防御行动，对遭遇性能降低、入侵等威胁的国防部网络空间动态地反复确认或重建其安全性，以确保具有充分的访问权限，可完成军事任务。对于遭入侵的 DODIN 元素，可采取重路由、重构、恢复或隔离等具体策略。大多数 DCO 任务都为 DCO-IDM，包括针对高级和/或持续威胁的主动积极的内部威胁搜索以及用于消除这些威胁并减轻其影响的主动内部对策和响应。

(2) **DCO 响应行动（DCO-RA）。**DCO-RA 作为一种 DCO 任务，在被保护网络或局部网络空间之外采取行动而无需受影响系统所有者的许可。DCO-RA 行动通常发生在外国网络空间。有些 DCO-RA 任务中的行动可能需要升级到使用武力，根据作战大环境（例如公开敌对行动的存在或迫近、威胁溯源的确定性、威胁造成或预期造成的破坏以及国家政策考虑因素等），对敌方系统造成物理破坏或损毁。DCO-RA 任务要求有协调一致的军事命令，并周密考虑范围、交战规则（ROE）及可量度的目标。

c. **进攻性网络空间作战（OCO）。**OCO 作为 CO 任务，是指为支援作战指挥官（CCDR）或国家目标而采取的行动，目的是在外国网络空间内或通过外国网络空间营造影响力。OCO 可专门攻击敌方网络空间功能或在网络空间中创建一阶效应，以精准控制对物理域的级联效应，从而影响武器系统、C2 过程、后勤节点、高价值目标等等。若 CO 任务在蓝色网络空间之外且按指挥官意图进行，而不是保护蓝色网络空间不受正在发生或即将发生的网络空间威胁影响，则为 OCO 任务。与 DCO-RA 任务一样，有些 OCO 任务中涉及的行动可能会升级到使用武力，对敌方系统造成物理破坏或损毁。具体造成什么影响取决于作战大背景（例如公开敌对行动的存在或迫近以及国家政策考虑因素）。OCO 任务要求有协调一致的军事命令，并周密考虑范围、交战规则（ROE）及可量度的目标。[80]

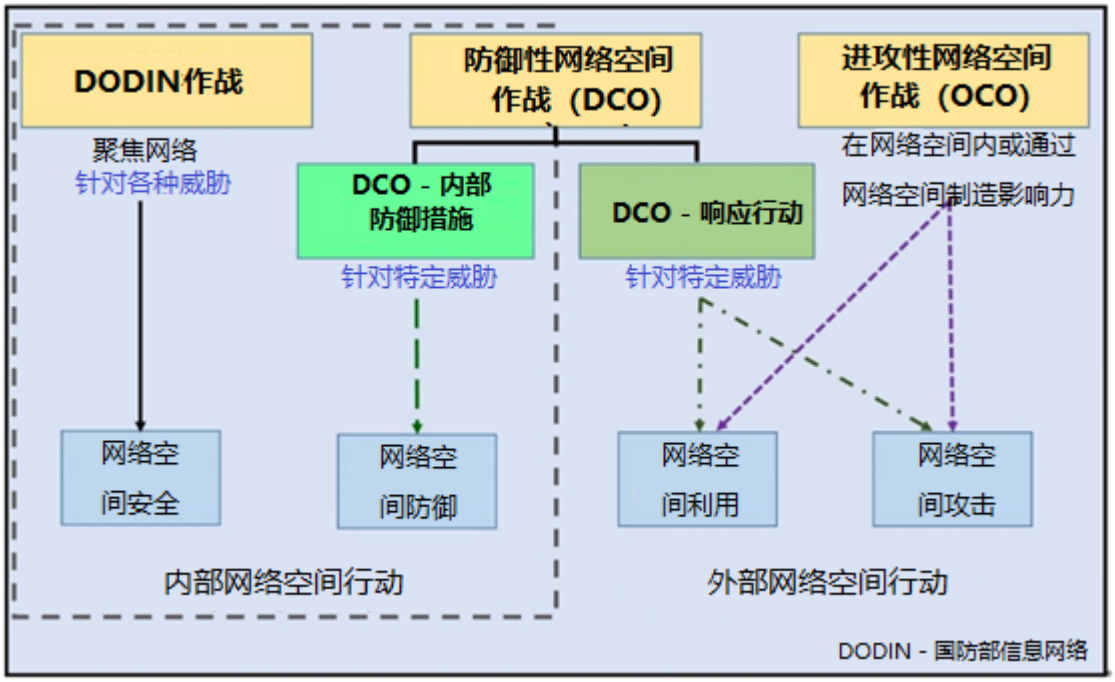


图 2-4 网络空间任务与活动[81]

6. 网络空间活动。进行 OCO、DCO 或 DODIN 作战行动时需要完成特定的战术级别的活动或任务，利用网络空间能力在网络空间中达成目标。所有的网络空间任务目标都是通过一个或多个这样的活动来实现的，这些活动完全由它们实现的效果类型来定义。要规划、授权和评估这些活动，指挥官和参谋须了解哪些活动已经根据他们当前的委托书进行了授权。DODIN 作战和 DCO-IDM 任务在任何时候都需要委托书，因此相关委托书涵盖了大多数网络空间安全和网络空间初步防御活动。然而，OCO 和 DCO-RA 任务具有偶然性，可能要求进行秘密的用兵和情报搜集行动，或者进行公开活动，包括交火。因此，外国网络空间中的 CO 活动需要获得专门的 OCO 或 DCO-RA 任务机构批准。网络空间活动包括：

a. **网络空间安全。**在受保护的网络空间内采取网络空间安全活动，以防止对计算机、电子通信系统、其他 IT（包括 PIT）以及所包含信息的非法访问、利用或损坏，确保其可用性、完整性、机密性和不可抵赖性，并进行身份认证。虽然网络空间安全活动以威胁为中心，但是要在实际安全入侵之前进行，是 DODIN 作战任务的主要组成部分。网络空间安全活动通过减少或消除可能被攻击者利用的漏洞和/或检测恶意网络空间活动来防范网络空间内的威胁。

b. **网络空间防御。**在受保护网络空间内采取网络空间防御活动，挫败已破坏或将要破坏网络空间安全措施的特定威胁，包括检测、描述、抵制和减缓威胁（包括恶意软件或非法用户活动）以及将系统恢复到安全配置。拥有或运营网络的作战司令部（CCMD）、军队或国防部机构通常被授权采取这些防御活动，但这些活动不得损害本部门之外网络空间的网元运行。

c. **网络空间利用。**网络空间利用活动包括军事情报活动、操控、信息搜集以及为未来军事行动做准备的其他活动。网络空间利用活动作为 OCO 或 DCO-RA 任务的一部分，包括灰色或红色网络空间中不具网络空间攻击效果的所有行为。网络空间利用的目的是通过如下活动获取情报，为当前和未来的作战环境准备提供支撑：获取和维持对网络、系统和军事价值节点的访问权限、获取有利位置、部署网络空间能力方便后续行动。网络空间利用还通过搜集信息支持当前和未来行动，包括定义红色和灰色网络空间以支持态势感知、发现漏洞、促成目标制定、支持军事行动的规划、执行和评估。根据国家政策，网络空间利用活动与其他美国政府部门和机构并无冲突。

d. **网络空间攻击。**网络空间攻击活动会在网络空间中产生明显的拒绝效果（即性能降低、中断或破坏），抑或通过操控导致物理域中的拒绝效果。网络空间利用为保证有效性一般秘密进行，而网络空间攻击则显而易见，因为删除了某些用户功能，系统操作员或用户即使一时疏忽，最终也会发觉。网络空间攻击作为一种火力，属于 OCO 或 DCO-RA 任务，需要与其他美国政府部门和机构协调，并与物理域中规划的火力协同一致。网络空间攻击活动包括：

(1) **拒绝。**通过下述活动，在特定时间内按指定级别拒绝提供目标功能或阻止对该功能的访问和操作：

- **降低性能。**拒绝对目标的访问或操作，其严重程度以占用容量百分比表示。可指定性能降低程度，若需要，还可以指定时间。
- **中断。**在一段时间内暂时性地彻底拒绝对目标的访问或操作。通常会指定预期开始和停止时间。中断若导致性能降低了 100%，则视为性能降低的一种特殊情况。
- **破坏。**指彻底拒绝对目标的访问或操作，且该等破坏无法恢复。破坏最大程度地延长了拒绝的时间和数量。但是，因为许多目标在给定足够时间和资源的情况下可以重建，所以破坏是根据冲突的范围来衡量的。

(2) **操控。**操控作为网络空间攻击的一种形式，指通过圈套、引诱、设置条件、欺骗、伪造和其他类似技术来控制或改变灰色或红色网络空间中的信息、信息系统和/或网络，实现物理拒绝效果。这是对手的信息资源挪为己用，在网络空间中造成的拒绝效果不会立即显现。被攻击网络看似正常运行，直到出现了二阶或三阶效应（包括物理效果），证明了逻辑一阶效应的存在。[82]

VIII. 确定网络空间需决策事务及决策点

1. 在规划期间，指挥官告知领导哪些事务需要决策、何时决策，以及决策和延迟所带来的不确定性和风险。这样，军事或文职领导人就提前获得了决策模板和提醒，可及时联系跨部门合作伙伴和盟友，共同寻求替代方案和机会，避免问题升级。决策矩阵还确定了预期指标，以支持情报搜集计划。[83]

2. **跨部门考虑因素。**在规划和执行期间，指挥官会适时与跨部门合作伙伴协调并整合其网络空间行动。有效整合跨部门因素对于成功的军事行动至关重要，特别是当联合部队进行修整、维稳以及向非军事机构活动过渡时。

3. **跨国考虑因素。**为保护多国部队网络，指挥官须考虑使用美国网络空间部队的可能性。指挥官还应预见并合入任务合作伙伴规划因素，例如合作伙伴的国内法律法规以及对各种网络空间能力和战术使用的限制。[84]

IX. 完善网络空间作战方法

1. 在整个规划过程中，指挥官及其参谋在指挥系统的各个层面展开正式和非正式的讨论。这些讨论有助于完善可能影响作战方法的假设、限制和决策点，确保计划始终可行、合理及周全。指挥官根据对各级指挥正式和非正式讨论的反馈等信息调整作战方法。[85]

2. **情报增益/损失（IGL）。**红色和灰色网络空间的用兵和交火可能会影响情报搜集活动的来源和方法。但凡条件允许，就要在此类行动之前进行 IGL 评估。因为在网络空间中存在非国防部美国政府部门和跨国合作伙伴，IGL 评估操作起来会很复杂。指挥官基于 IGL 分析对 CO 和通过其他方法实现预期目标的风险进行权衡。[86]

3. **找准目标。**虽然与具备网络空间能力的目标交战通常不会造成永久性损害，但由于网络空间的互联性，CO 的影响或可跨越地理边界，若规划不善，还可能产生意想不到的后果。因此，在网络空间内和通过网络空间与目标交战时，需要在国防部内部并与跨部门和跨国合作伙伴进行密切协调。[87]

4. 风险考虑。指挥官应想方设法，最大限度地降低使用网络空间对联合部队以及友好和中立国家、社会和经济体造成的风险。联合部队在协同行动时会使用各种网络空间能力，包括用于与国防部内外部人员进行通信的非机密网站和 Web 应用程序。[88]

X. 制定网络空间规划手册

1. 指挥官通过指挥官规划手册向参谋和合作伙伴简要介绍作战环境和问题，传达作战方法。在时间允许的情况下，指挥官可以在参谋开始联合规划程序（JPP）之前应用作战筹划来策划战役或行动。在这种情况下，指挥官提供初步规划手册，使参谋可以集中精力进行任务分析。参谋进行任务分析后，指挥官应继续进行分析，进一步了解和构思作战环境。在完成作战环境分析后，指挥官将适时发布规划手册，以统一参谋工作。[89]

2. 指挥官将 CO 纳入各级行动中，应针对如何有效整合网络空间能力、打击对手使用网络空间、识别和保护关键网络空间、访问网络空间中的关键区域、在性能降级的环境中行动、有效使用有限的网络空间资产以及将作战要求与网络空间能力相匹配等问题做出规划。指挥官提供初步规划手册，确定时间范围，概述初步协调要求，在指挥官权力范围内授权行军，并在必要时指挥其他行动。补充 CO 计划和原则应说明 CO 在指挥官工作中的角色和范围，阐述 CO 如何支持相应计划的执行。应指挥官要求，CDRUSCYBERCOM 可协助将网络空间部队和能力纳入指挥官的计划和命令。[90]

第三章 规划

I. 联合规划程序（JPP）

1. **规划。**规划旨在将战略转化为行动，期望通过成功的行动来实现预期战略目标。同样，行动效果（成功或失败）会改变作战和战略环境，需要不断评估战略层面的目标，确保其始终具有相关性和可行性。联合部队通过评估，确定其行动对作战环境（OE）产生负面影响的开始时间，同时，调整其作战和活动以保持行动和目标之间的一致性。[91]

2. **作战筹划。**作战筹划和 JPP 是整体规划流程的补充工具。在参谋支持下，指挥官在 JPP 的启动步骤中应用作战筹划，以了解作战环境、界定问题并为战役或行动制定具体方法。[92]

3. **JPP。**JPP 由一系列分析性的逻辑步骤构成，用以解决问题、检查任务，以及开发、分析和比较替代行动方案（COA）、选择最佳 COA、形成计划或命令等。作战筹划的应用为构建战役和行动提供了概念基础。JPP 提供了经过验证的流程，指挥官、参谋、下级指挥官和其他合作伙伴可据此组织工作，制定解决问题的合理计划。它侧重于定义军事任务以及制定并同步旨在完成该任务的详细计划（见图 3-1）。[93]

图 3-1 联合规划程序[94]

II. CO 规划

1. **规划整合。**指挥官将 CO 纳入各级行动中，并针对如何有效整合网络空间能力、打击对手使用网络空间、识别和保护关键网络空间、访问网络空间中的关键区域、在性能降级的环境中行动、有效使用有限的网络空间资产以及将作战要求与网络空间能力相匹配等问题进行规划。指挥官提供初步规划手册，确定时间范围，概述初始协调要求，在指挥官权力范围内授权行军，并在必要时指挥其他行动。补充 CO 计划和概念应说明 CO 在指挥官工作中的角色和范围，阐述 CO 如何支持相应计划的执行。

2. **规划考虑因素。**尽管 CO 规划人员与物理域行动规划人员一样具有相同的作战筹划

考虑因素和挑战，但在规划 CO 时存在一些独特的考虑因素，例如，由于网络空间中无法预见的关联性，某些 CO 的高阶效应可能更难预测。这可能需要更多的分支和后续规划。此外，网络空间中的许多元素与地理位置相对应，要充分了解对手在网络空间中的部署和能力，不仅要从基础物理网络层而且要从逻辑网络层和网络角色层了解目标，包括系统用户和管理员信息及其与对方关键因素的关系。要规划国防部网络空间的内部行动，国防部信息网络（DODIN）作战和防御性网络空间作战—内部防御措施（DCO-IDM）规划人员需要知悉对手可能攻击的友军或能力、最有可能被利用的 DODIN 漏洞以及对手行动的潜在影响、涉及的任务保障风险，还要了解适用的国内外和国际法律以及美国政府（USG）政策。网络空间的威胁可能来自于国家、非国家团体或个人，他们控制的网络空间不一定位于其所在国的地理边界内，也不一定与其地缘政治影响对应。在网络空间中，犯罪分子、政治团体甚或资源充足的个人其活动范围和能力可能优于多数国家。此外，许多对手在与美国地理位置相关或由美国实体控制的网络空间中运作其网络空间能力。因为上述各因素，CO 规划执行起来颇为复杂。

3. **规划时间表。**对于外部任务，重要的是进攻性网络空间作战（OCO）和 DCO 响应活动（DCO-RA）规划人员要知道由谁来执行所提议的特定 CO 活动。根据行动阶段不同，执行机构也会不同。制定外部任务时间表时要考虑下述活动所需的提前期：获得必要情报以确定目标、获取目标访问权限、确认负责机构、完成必要的协调（包括跨部门协调和/或同步）、基于技术保证评估结果验证网络空间能力是否达到预期目标。对于内部任务，规划人员在制定 DCO-IDM 和 DODIN 作战时间表时要考虑其他因素，包括网络状况管理的自动化水平、商业提供商可提供的安全解决方案及其许可要求、可能影响防御者机动性或让系统断网以便更有效保护系统的运营考虑因素等。然而，规划的基本原则不变，尽管整合 CO 有其他的考虑因素和挑战，规划人员基本上沿用传统流程，按照指挥官的意图和指导行事。[95]

4. **网络空间规划和 JPP。**与其他所有联合能力和功能一样，CO 能力考虑因素和选项也集成到 JPP 中。

a. **规划启动（步骤 1）。**有关领导确认为支持国家目标或应对潜在或实际危机可能需要动用军事能力时，联合规划开始启动。在战略层面，该领导—总统、国防部长（SecDef）或参谋长联席会议（CJCS）主席—一旦决定制定军事方案，就启动规划。指挥官发现其他（非上级领导指示）规划需求时，也会在其职权范围内启动规划。[96]

(1) 网络空间规划人员将与上级司令部的规划人员进行协调，获取当前和未来 CO、连续评估和其他 CO 规划产物等方面的信息。

(2) 关键输出：

- 网络空间效果连续评估（更新）[97]

b. **任务分析（步骤 2）。**指挥官和参谋分析战略方向，据此修改任务说明并由指挥官审批，下级和支援指挥官根据该任务说明开始自己的评估和规划工作，完成后交由上级司令部批准。联合部队的任务由单项或多项工作组成，目的明确，规定了要采取的行动以及行动原因。任务分析的目的是研究所分配的工作并明确完成任务需要做的其他工作。[98]

(1) 网络空间规划人员以网络空间和信息环境为重点，搜集、分析、合并作战环境的当前状况信息。规划人员与情报人员合作，了解敌人和对手的能力以及他们使用网络空间的情况，以便开发模型、情景模板及事件模板，识别高价值目标和特定关注领域，从情报过程获得其他输出，如敌人和对手的网络空间信息。

(2) 关键输出：

- 网络空间信息需求清单
- 支持 CO 的情报产品
- 最有可能实现以及最危险的敌人行动方案（COA）
- CO 明示及暗示需要完成的工作

- 网络空间局限性和约束条件
- 网络空间假设
- CO 连续评估（更新）[99]

c. **行动方案（COA）制定（步骤 3）。**COA 是完成指定任务的可能方式（解决方案、方法等）。参谋开发 COA，为指挥官提供不同方案供其选择，均以完成最终军事目标为导向。合理的 COA 可在指挥官的指导下完成任务，具有灵活性，可在执行期间满足不可预见事件的需求，并为未来行动部署联合部队。此外，它能让下属部门最大程度地发挥主动性。规划人员可修改 COA，在作战环境中调整所使用的联合部队能力，将这些能力灵活组合，以有效利用信息环境（包括网络空间）和电磁频谱。[100]

(1) 网络空间规划人员开发初步 CO 方案，明确网络空间支持工作，阐述指挥官应如何使用 CO 来支持作战方针，并重点描述用兵方案。

(2) 关键输出：

- CO 信息需求（更新）
- 高价值目标清单初稿
- CO 草案，包括目标和效果
- CO 连续评估（更新）[101]

d. **COA 分析、作战模拟（Wargaming）、比较和审批（步骤 4、5、6）。**COA 分析中要仔细检查待选 COA 以发现细节，指挥官和参谋可基于这些细节初步判断有效的 COA 并发现所提交的每份可用 COA 的优缺点。指挥官和参谋根据指挥官手册逐个分析 COA。作战模拟是进行此分析的主要手段。COA 分析完成后，参谋对 COA 进行主观评比，逐个审议 COA，并根据参谋和指挥官共同制定的一套标准进行评估/比较，目的是推选出最有可能完成任务的 COA。最后，参谋向指挥官简要介绍 COA 分析、作战模拟和比较结果，指挥官将个人分析与参谋建议相结合，进行 COA 审批。[102]

(1) 网络空间规划人员改进 CO 方案，确保它与用兵方案一致。规划人员会在 COA 评比过程中提供参考建议。最佳 COA 必须首先符合道德，其次应最有效且效率最高。指挥官将发布最终规划手册，对指挥官意图、指挥官的关键信息要求以及关于优先事项的任何其他指导进行修改。

(2) 关键输出：

- 针对指挥官的关键信息要求所提供的网络空间输入（优化后）
- 针对高价值目标清单所提供的 CO 输入（优化后）
- CO 方案（优化后）
- 网络空间效果与连续评估（更新）
- 建议行动方案
- 网络空间效果与连续评估（更新）
- 指挥官批准的 COA[103]

e. 计划或命令拟定（步骤 7）。在计划或命令拟定期间，指挥官和参谋与下级和支持部门/组织合作，完善与已批准 COA 相关的初始作战方针（CONOPS），形成详细的计划或作战命令（OPORD）。CONOPS 简明清晰地介绍了指挥官打算完成的任务以及如何利用现有资源完成任务，分析了联合部队成员和支持组织为完成任务应如何整合、同步和分阶段完成各项活动，包括或有分支和后续活动。[104]

(1) 所有规划输出最终定稿，包括 CO 连续评估和网络效果请求格式表（CERF）。若时间允许，参谋可对所选择的 COA 进行更详细的作战模拟。[105]

5. **为 CO 规划提供情报支持。**借助于专注于网络空间领域漏洞和威胁的情报产品，情报小组可帮助指挥官和参谋深入洞察和了解网络空间环境。通过对敌方网络空间能力的评估（包括对理论原则和战术、技术和程序（TTP）的审查）和在网络空间领域观察到的敌方行动模式，可以大概确定敌方的 COA。[106]

a. 了解作战环境是所有联合作战行动（包括 CO）的基础。情报可从网络空间军事行动信息中或其他来源获得。对 CO 的全源情报支持利用了其他军事行动所使用的相同情报过程，同时兼具支持 CO 规划所需的独特属性。该过程包括：

(1) 规划和指导，包括识别目标漏洞（以便持续规划和指导反情报活动，防止针对美国公民/设施的间谍、破坏和攻击）以及定期审核任务成功标准和相关指标以评估 CO 并传达指挥官的决定；

(2) 利用采集传感器获取网络空间信息；

(3) 处理和利用搜集到的数据，包括从实时或事后数据中筛选出有用信息；

(4) 对情报产品所产生的信息和输出进行分析；

(5) 传播、整合网络空间方面的情报并将其应用于作战；

(6) 对情报有效性和质量进行评估和反馈。[107]

b. 情报需求（IR）。进行任务分析时，联合部队参谋要确定关于对手和作战环境其他相关方面的重大信息差距。在进行差距分析之后，参谋制定一般或具体 IR，表示需要搜集信息或生成情报。情报需求识别后，参谋会提出更具体的问题，即信息需求（指用以生成指挥官所需情报而必须搜集和处理的信息项目）。与网络空间相关的信息需求包括网络基础设施和状态、对手设备和人员的到位情况以及独特的网络空间签名标识符（硬件/软件/固件版本和配置文件等）。要满足情报需求，需同时利用军事情报和国家情报源。[108]

6. **深度理解规划。**在上述专家帮助下，规划人员洞悉了可用的网络空间能力，能够将这些能力与其他领域结合起来。

a. **避免对称思考。**对手通过网络空间进行攻击，并不意味着我们只能在网络空间进行响应。指挥官和参谋在网络空间“内部”行动的同时应考虑攻击网络空间物理层。

b. **尽早发现潜在的网络空间需求。**网络空间能力的审批链很长，有时开发时间也很长。应在早期规划中确定需求并部署网络空间规划人员，确保获得必要权限。

c. **定制 CO 请求。**鉴于 CO 的全球属性和潜在的级联效应，有关部门一般会谨慎授权。规划人员应制定具体需求，如仅用于某些情况、限制时长、限定受影响网络的范围。规划人员可申请进行不连续行动，以提升批准几率，亦可能缩短审批时间；还应在规划中尽早就预期网络活动进行跨部门协调和沟通。

d. **网络空间损害通常很难评估。**友方网络空间作战人员可能会上报任务完成情况。但与实体弹药不同，网络空间不会有弹坑，无法验证结果。规划人员必须使用其他方法来衡量 CO 成功与否，比如分层评估。例如，如果网络空间作战人员报称通过网络空间解除了对方武装，则在发动风险较大的重大攻击之前用遥控飞行器探测对方系统。

e. **所有 CO 都要求有分支计划来实现类似效果。**由于进攻性网络空间作战（OCO）经常被否且容易失败，因此规划人员必须了解 CO 意图，制定分支计划，进行“曲线救国”。同样，联合参谋人员必须明白，现今的操作系统大多不堪一击。联合部队应做好准备，以免网络空间能力不足时措手不及。

f. **许多网络空间能力并未公开**，以避免暴露漏洞。规划人员若缺乏足够的安全权限就无法整合网络空间能力。要解决这个问题，规划负责人应邀请网络空间专家参与规划团队会议，使其了解计划的目标和意图。这样，一方面，规划人员能够在计划中谨慎地加入机密网络空间能力，另一方面，保证了只有相应权限者和须知人群才能了解内情。[109]

7. **网络空间规划支持。**考虑到 CO 速度，在规划启动后，要进行大量的战前协作，时刻保持警惕，以有效消除作战环境中的冲突因素，协调行动。要达到这种步调一致的效果，关键是保持对网络空间态势的感知并评估所规划 CO 对联合部队的潜在影响，包括 DODIN 的安全状况、正常网络配置的修改或是否检出恶意活动迹象。确定 CO 时间时，应基于实际，评估其所能产生的效果以及是否能支持整个作战环境中的行动。这可能要求尽早使用网络空间能力而非其他能力。成熟的规划人员和作战人员知道作战环境中的

其他行动会如何影响 CO。[110]

III. 作战计划与命令的附录内容—网络空间

1. **为作战计划和命令提供输入。**指挥官和参谋将为作战计划（OPLAN）和命令（OPORD）的附件C（作战）编制附录，描述CO对于主计划或命令中所述行动的支持。该附录应阐述CO支持和目标，讨论CO中的整体作战方针、所需要的支持，并以分段及附件形式介绍具体细节。附录中还应提供同步网络空间时序关系所需的信息，包括约束条件（若有）。下文为附录示例，仅为参考，实际附录中可包含其他信息（见图3-2）：[111]

作战计划/命令附件 C（作战）之附录（网络空间活动）
(U) **参考:***添加网络空间活动的具体参考信息（若需要）*
1. (U) 情况介绍。*提供附件 C（作战）第 1 段未包括或需要展开论述的影响网络空间作战（CO）的信息。*

a. (U) 关注领域。*提供影响网络空间的信息；网络空间会将关注点由本地扩大到全球。*
b. (U) 作战区域。*提供影响网络空间的信息；网络空间会将作战区域扩大到物理活动空间之外。*
c. (U) 敌军。*列出已知和模板化的位置和网络空间部队活动，找出敌方信息系统和网络空间中的漏洞，列出将影响友好行动的敌方 CO，陈述敌方可能会采取的行动方案和敌方网络空间资产的使用。必要时，参照附件 B（情报）。*
d. (U) 友军。*概述上级司令部的网络空间活动计划，列出支持或影响授令司令部或需要协调与额外支持的上级、相邻及其他 CO 资产的计划名称、位置和概要信息。找出影响下级指挥官的友方 CO 资产和资源，发现友军部队网络空间中的漏洞，确定下级指挥官可以合作的国外友军。识别电磁频谱领域（EMS）内的潜在冲突，这对于联合或跨国作战尤为重要。消除频谱分布中的冲突并进行优先级排序。*
e. (U) 跨部门、跨政府及非政府组织。*列出并描述作战区域内可能影响 CO 或 CO 装备和战术部署的其他组织。必要时，参照附件 V（跨部门）。*
f. (U) 第三方。*列出并描述作战区域内外能够影响 CO 或 CO 装备和战术部署的其他组织，包括犯罪组织和非国家支持的恶意组织。*
g. (U) 非军事考虑因素。*描述影响 CO 的非军事方面。必要时，参见附件 B（情报）的附录 1（情报评估）中的表 C（非军事考虑因素）和附件 K（民事行动）。*
h. (U) 附属与分遣部队。*列出附属或分遣部队（仅在需要阐明任务组织情况时）。列出所有临时添加或移除的 CO 资产以及可从上级司令部获得的资源。必要时，参照附件 A（任务组织）。*
i. (U) 假设。*列出所有的 CO 假设。*

2. (U) **任务**。*陈述指挥官的任务，介绍支持主计划或命令的 CO。*

图 3-2 网络空间作战概念附录

基于作战计划和命令附件 C（作战）的附录 12（网络空间电磁活动）的 FM 3-12 部分[112]

3. (U) 执行。

a. (U) 网络空间电磁活动方案。*介绍网络空间和电子战（EW）行动如何支持指挥官的意图和作战方针，确定各作战阶段对部队的优先支持事项，说明网络空间和电子战结果将如何削弱敌方能力、中断敌方网络、达成拒绝效果并欺骗敌人。描述网络空间和电子战攻防措施，按优先级确定目标集和预期效果。介绍网络空间和电子战行动整合的总体概念，列出负责网络空间和电磁活动的参谋小队、分队和工作组，并提供参谋小队、分队和工作组在非 CO 支持活动中形成的网络空间和电子战信息搜集方法。阐述联合行动和非政府合作伙伴及组织的整合计划。必要时，参照附件 C（作战）。本部分旨在提供对网络空间和电子战组成部分的深度观察和理解以及如何在整个作战计划中整合相关活动。建议本附录提供对技术要求的理解。*

本附录重点讨论 CO 整合要求，并根据需要引用对应附件和附录，以减少重复。

(1) (U) 战斗组织。*为合理组织战斗提供指导性信息，包括部队番号、命名和战术任务。*

(2) (U) 其他。*提供规划所需但尚未提及的其他信息。*

b. (U) CO 方案。*说明 CO 如何支持指挥官的意图和作战方针，介绍实施计划 CO 措施的总体概念，描述将联合行动合作伙伴和非政府组织纳入作战的过程，包括网络空间要求和约束条件。识别 CO 相关风险，包括附带损害、暴露、溯源、误伤（对美国、盟国或多国网络或信息）以及或有冲突。阐述哪些活动会阻止敌人和对手活动，严重削弱联合司令部在其作战区域内有效开展军事行动的能力。确定对策和责任机构，列出告警并说明如何监控这些告警。说明 CO 任务将如何破坏敌方计算机网络，降低其性能，中断服务并造成拒绝效果。识别网络空间中的目标集和效果并确定其优先级，说明 CO 如何支持完成行动（若适用）。确定在物理域和网络空间中检测或溯源敌人和敌对行为的计划。确保下属部队进行防御性网络空间行动（DCO）。将网络电磁活动（CEMA）同步给 IO 负责人，将进攻性网络空间作战（OCO）请求递交上级司令部，批准后实施。说明国防部信息网络（DODIN）作战如何支持指挥官的意图和作战方针，将 DODIN 作战与 J-6 同步，利用网络空间分配应用优先级。确保使用网络空间能力，以便在网络空间或通过网络空间实现目标。应考虑到网络降级运营的情况。（根据需要，引用相应附件和附录以减少重复。）*

(1) (U) DODIN 作战。*描述信息战的协调、同步方法以及融入在 J-6 中的支持行动，方便设计、构建、配置、保护、运营、维护和维持网络。必要时，参照附件 H（信号）。*

(2) (U) 防御性网络空间作战（DCO）。描述 DCO 的实施、协调、集成、同步方法以及为保护 DODIN、持续利用友方网络空间能力而采取的支持行动。

图 3-2（续）网络空间作战概念附录

(3) (U) 进攻性网络空间作战（OCO）。*描述 OCO 的协调、集成、同步方法以及为实现实时感知和直接动态活动和响应活动而采取的支持行动。提供目标识别和作战模式信息、利用和攻击功能，并维护情报信息。规定进行 OCO 所需的权限。*

c. (U) 下属部队任务。*列出主命令未涵盖的各下属部队的 CO 任务。*

d. (U) 协调指令。*列出主命令中未涵盖的适用于两个或更多下级部队的 CO 指令。确定并突出显示所有与 CO 相关的交战规则、风险降低控制措施、环境因素、各部队之间的协调要求、指挥官的关键信息需求以及与 CO 有关的友方基本信息。*

4. (U) **保障**。*确定 CO 关键任务的保障优先级，并根据需要提供其他指示。必要时，参照附件 F（保障）。*

a. (U) 后勤。*分段描述与 CO 有关的后勤活动的优先级和具体指示。必要时，参照附件 F（保障）的附录 1（后勤）和附件 P（驻在国支持）。*

b. (U) 人事。*分段描述与 CO 有关的人力资源的优先级和具体指示。必要时，参照附件 F（保障）的附录 2（人事勤务支持）。*

c. (U) 卫生系统支持。*必要时，参照附件 F（保障）的附录 3（卫生系统支持）。*

5. (U) **司令部与信号**.

a. (U) 司令部。

(1) (U) 指挥官位置。*说明关键 CO 领导者的位置。*

(2) (U) 联络要求。*说明部队 SOP 中未涵盖的 CO 联络要求。*

b. (U) 控制。

(1) (U) 指挥所。*说明 CO 相关指挥所的使用情况，包括各指挥所的位置及其工作时间。*

(2) (U) 报告。*列出 SOP 中未涵盖的 CO 相关报告。必要时，参照附件 R（报告）。*

c. (U) **信号**。*解决所有的 CO 相关通信要求。必要时，参照附件 H（信号）。*

图 3-2（续）网络空间作战概念附录

IV. 网络效果请求格式表（CERF）

1. **网络效果。**效果指系统的物理和/或行为状态，是一项或一组活动或其他效果产生的结果。预期效果（Desired Effect）可以理解为支持实现相关目标的条件，反之，不良后果（Undesired Effect）则指阻碍实现目标的条件。指挥官和规划人员在整个 JPP 过程中拟定和持续完善预期效果。在执行过程中，监控贯穿始终，以保证实现预期效果，同时避免不良后果的产生。[113]

a. 指挥官利用 CO 在网络空间内并通过网络空间实现效果，支持军事目标。[114]虽然可以仅通过 CO 产生战术性、操作性或战略性效果，从而实现目标，但指挥官出于协调、同步的目的，多会将 CO 与其他作战行动相结合，完成任务。

b. CO 使用物理域中的链接和节点执行逻辑功能，首先在网络空间中实现效果，然后根据需要在物理域中实现效果。通过精心控制的级联效应，网络空间活动可以让物理域中的活动具有更大的自由度。同样，通过影响电磁频谱（EMS）或物理基础设施，物理域中的活动也可以在网络空间中或通过网络空间产生效果。[115]

c. 由于 CO 通常能够以有线或无线访问实现的虚拟状态远程执行，因此许多 CO 不需要在地理位置上接近目标，而是利用远程操作来实现目的，也就是说，虽然物理区域受限，作战范围却增大了。这里提及的全球作战范围同样适用于红色和灰色网络空间中的区域外行动，以及蓝色网络空间中的内部保护行动。某些 CO 的累积效果会影响到最初目标、联合作战区域（JOA）或单一责任区域（AOR）之外的区域。考虑到跨区域因素以及有限的兵力和能力，有些 CO 通过远程集中执行进行协调、整合及同步。[116]

d. 级联效应或通过目标系统的下级系统传播，或横向传播到同级或向上传播到上级系统。复合效应是各级效果的集合，这些效果或按照预设、或出于偶然而相互作用。附带效果（包括附带损害）是军事行动对非攻击目标的非战斗人员和平民财产

带来的意外影响。根据战略和行动情况，命令或相应交战规则（ROE）或会限制 CO 行动，禁止其导致或仅允许导致少量附带效果。[117]

2. **网络效果请求。**规划和目标定位人员根据指挥官的目标（而非实现目标的能力），在网络空间内并通过网络空间定位并选择攻击目标。重点是促成效果，以完成目标定位任务并实现目标，而非因为具有某项网络空间能力可去使用这项能力。[118]CERF 是部队请求在网络空间内并通过网络空间实现效果的格式表（见图 3-3）。确定了针对目标和关键网络节点的攻击效果后，参谋将填写、提交并跟踪 CERF。该请求将并入联合目标周期中进行处理和审批。联合特遣部队（JTF）、CCMD 和 USCYBERCOM 参谋在处理 CERF 和协调后续网络空间能力方面发挥着关键作用。[119]

网络效果请求格式表（CERF）
第 1 部分：请求单位信息
主司令部：
发送日期/时间：
请求单位：
OPLAN/CONPLAN/ORDER：
任务说明书：
指挥官意图：
指挥官期望的最终状态：
作战方针：
目标（战略/行动/战术）：
战术目标/任务：
第 2 部分：网络空间作战相关信息
目标类型（定时/按需）：
目标优先级（紧急/优先/常规）：
目标名称：
目标定位：
目标描述：
预期效果：
目标功能：
目标重要性：
目标详细信息：*填写相关设备信息，例如类型、操作系统版本和补丁级别、软件、用户数量、活动、作战区域中的友方活动者、周围/邻近/并行设备等。*
网络作战方针：*填写任务、目的、方法和终极目标，同时明确战损评估的情报收集计划，内容包括分配的资源、绩效指标（MOP）、效用度量（MOE）和 MOE 指标。*
目标期望陈述：_____
备注：请提供如下各项（如有）：
（1）攻击时间/效果持续时间
（2）不早/晚于要求时间
（3）触发事件或执行条件
（4）持久化要求（效果须通过重启目标、触发事件等长期存在）
（5）命令与控制要求（效果须能远程打开/关闭）
（6）自毁/自动删除要求（若在规定时间内未再次收到 C2，效果须自行终止）
（7）可溯源等级要求（追溯至 CONUS/USG、错误追溯至 USG 等）
（8）允许的可检测水平（不应被（a）管理员，（b）用户或（c）取证分析师检测出来）
（9）允许的征用水平（低、中、高）
（10）远程监控要求（效果应能由（a）作战人员或（b）JOC 等监控）
（11）基础设施要求（应从特定基础设施/系统/平台启动效果）
（12）可逆性要求（效果应是可逆/不可逆的）

图 3-3 网络效果请求格式表（CERF）[120]
基于附件 C 的 FM3-12

第四章：执行

I. 执行

1. **执行命令（EXORD）。**总统或国防部长（SecDef）授权启动军事行动或其他活动时开始执行。EXORD 或其他授权指令由参谋长联席会议主席（CJCS）按总统或 SecDef 指示发布，以启动或开展军事行动。[121]

2. **执行期间规划。**执行开始后，规划继续，重点放在输出作战命令（OPORD）上（若无）。随着作战的进行，规划通常在三个不同但重叠的时间框架内进行：未来规划、未来行动和当前行动（见图 4-1）。

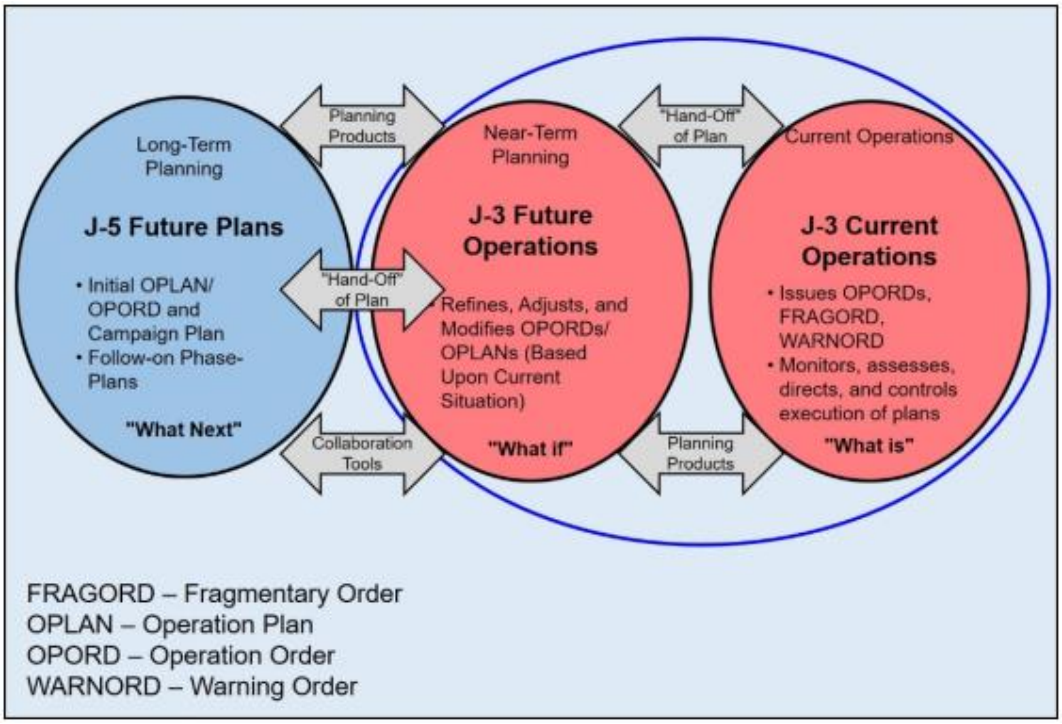


图 4-1 执行期间规划[122]

a. 联合参谋部规划处（J-5）重点关注未来规划。这项工作的具体时间由多种因素决定，包括司令部等级、作战类型、指挥官意愿等。通常，未来规划工作的重点是规划下一阶段行动或当前行动的后续行动。对于具体战役，规划的可能是下一次重大行动或战役的下一阶段。

b. 规划也可能是分支机构针对当前行动进行（未来行动规划）。未来行动规划的具体时间取决于未来规划中列举的因素，但一般比未来规划时间要短。未来规划通常由 J-5 或联合规划小组（JPG）执行，而未来行动规划通常由作战部（J-3）执行。

c. 最后，当前行动规划解决的是与当前行动相关的即时或极短期规划问题。这项工作由联合作战中心或 J-3 完成。

3. 执行期间，监控并度量计划任务的完成情况，了解各目标实现程度，并按原样输入新增数据和信息，以便选择分支或后续（若适用）活动或根据需要修改计划。执行计划并不意味着规划过程结束。参谋可随时重新启动规划周期，接受指导，提供过程审核（IPR），修改计划，决定是否以及何时执行分支或后续活动，或终止行动。针对未来行动的规划将持续进行。[123]

II. 执行期间的网络空间作战

1. **执行。**尽管 CO 规划人员与物理域行动规划人员一样具有相同的作战设计考虑因素和挑战，但在规划 CO 时存在一些独特的考虑因素，例如，由于网络空间中无法预见的关联性，某些 CO 的高阶效应可能更难预测。这可能需要更多的分支和后续规划。此外，网络空间中的许多元素与地理位置相对应，要充分了解对手在网络空间中的部署和能力，不仅要从基础物理网络层而且要从逻辑网络层和网络角色层了解目标，包括系统用户和管理员信息及其与对方关键因素的关系。要规划国防部网络空间的内部行动，国防部信息网络（DODIN）行动和防御性网络空间行动—内部防御措施（DCO-IDM）规划人员需要知悉对手可能攻击的友军或能力、最有可能被利用的 DODIN 漏洞以及对手行动的潜在影响、涉及的任务保障风险，还要了解适用的国内外和国际法律以及美国政府（USG）政策。网络空间的威胁可能来自于国家、非国家团体或个人，他们控制的网络空间不一定位于其所在国的地理边界内，也不一定与其地缘政治影响成正比。在网络空间中，犯罪分子、政治团体甚或资源充足的个人其活动范围和能力可能比许多国家更强大。此外，许多对手在与美国地理位置相关或由美国实体控制的网络空间中执行其网络空间能力。因为上述各因素，CO 规划执行起来颇为复杂。[124]

2. **法律考虑因素。**国防部根据美国国内法律、适用的国际法以及相关的美国政府和国防部政策实施 CO。因此，在 DODIN 范围外作战的 DOD 网络空间部队，经过合理授权，通常仅在灰色和红色网络空间中行动，除非交战规则（ROE）另有规定或根据授权为非军事机构提供防务支持（DSCA）。由于每个 CO 任务均有不同的法律考虑因素，具体适用法律取决于活动性质，例如是进攻性网络空间作战（OCO）或 DCO、DSCA、情报、监视与侦察（ISR）活动、执法（LE）与反情报（CI）活动、情报活动还是保卫国土。在开展 CO 之前，指挥官、规划人员和作战人员需要熟知相关法律框架，以遵守法律和政策。鉴于网络空间的全球属性和国内与国际法的地理定位，应用这些法律和政策可能具有挑战性。在规划和执行 CO 期间，指挥官、规划人员和作战人员须咨询法律顾问（参见附录 A：国防部战争法手册摘录）。[125]

3. **网络空间权力。**特定类型军事 CO 权力由国防部长各项政策（包括国防部指示、指令和备忘录）、总统或国防部长批准的 EXORD 和 OPORD 以及获批执行特定任务的指挥官发布的下级命令赋予。这些权力包括 CJCS EXORD 授予的网络空间作战指令权（DACO），用以协调整个国防部内部的 DODIN 保护工作（见图 4-2）。

美国法典（USC）	标题	关注重点	主要组织	网络空间中的角色
第 6 篇	国内安全	国土安全	国土安全部	美国网络空间安全
第 10 篇	武装力量	国防	国防部	为美军配备、训练人员并提供装备，以便在网络空间进行军事行动
第 18 篇	犯罪与刑事诉讼	执法	司法部	阻止犯罪、逮捕并起诉网络空间犯罪分子
第 28 篇	司法系统与司法程序			
第 32 篇	国民警卫队	美国境内的国防与非军事支援培训及行动	各州陆军国民警卫队、各州空军国民警卫队	国内影响管理（若为联邦义务触发，国民警卫队则被纳入美国法典第 10 篇“武装力量”）
第 40 篇	公共建筑、财产与工程	首席信息官角色与职责	所有联邦部门和机构	制定并执行信息技术获取和安全标准
第 44 篇	公共印刷业与文件	定义针对安全政策的基本机构职责和权限	所有联邦部门和机构	国防部指令 8530.01《对国防部信息网络行动的网络安全活动支持》中规定的活动—即现在所称网络安全活动—的基础
第 50 篇	战争与国防	广泛的军事、外国情报和反情报活动	国防部下属司令部、军队和机构以及情报界机构，由国家情报总监办公室协调行动	通过在网络空间进行军事和外国情报活动来保护美国利益

图 4-2 美国法典赋予的网络空间权力[126]

4. **网络空间部队的指挥与控制。**明确的指挥关系至关重要，可确保部队得到及时有效地使用。CO 同样需要统一的指挥和行动。然而，网络空间部队有时需要同时在全球和战区或联合作战区域（JOA）层面进行行动，因为这种复杂性，CO 须适应传统的指挥与控制（C2）结构。CJCS 根据当前普遍情况，为 CO 建立了两个 C2 模型：正常作战条件下的 C2 和网络空间相关危机或紧急情况发生时的 C2（见图 4-3）。

a. **对全球 CO 的指挥与控制。**CDRUSCYBERCOM 一方面在跨地区和全球 CO 方面接受支援，管理日常的全球 CO，另一方面为一个或多个战区或职能的作战指挥官（CCDR）行动提供支援。接受/提供 CO 支援并不意味着受援/支援司令部在行动之前就无须与相关指挥官协调响应方案了。当行动有可能影响多个国防部部门的完整性和行动准备时，JFHQ-DODIN 要集中协调并指导整体 DODIN 行动和 DCO-IDM。虽然许多行动可能需要分散进行，但是 CDRUSCYBERCOM 作为 CO 的受援指挥官，不仅要保护、管理 DODIN，还要根据命令保护美国的其他重要网络空间资产、系统和职能。

b. **对支援 CCMD 的 CO 的指挥与控制。**CCDR 在其责任区（AOR）或跨区域责任中需要得到 CO 支援，CDRUSCYBERCOM 在必要时提供此等支援。这里的 CO 包括一系列行动，促使战区作战指挥官（GCC）在其 AOR 范围内或职能作战指挥官（FCC）在其跨地区职责范围内达成局部效果。具体而言，这些行动或为 DODIN 特定战区内部的网络空间安全和防御行动，或为外部行动，例如针对特定敌方能力的网络空间利用或网络空间攻击。除了全球网络的各大战区，CCMD 级别的 DODIN 行动和 DCO-IDM 还包括 CCMD 对独立和战术网络以及计算机的专门保护。例如，网络空间中的 CCMD 级别行动包括重新定位能力以增强特定区域内的威胁检测能力、为威胁对手将网络空间部队的活动集中在与特定分支和后续活动相关的区域、激活备用战术网络空间能力从而将友方 C2 转移到更为安全的位置等。当 CCDR 的系统受到攻击而致 DODIN 子网性能降低、遭入侵或失陷时，这种 CO 行动就变得至关重要。在这些行动中，受援 CCDR 通过其 USCYBERCOM CO 综合规划分队（CO-IPE）与相关企业运营中心协调，由 JFHQ-DODIN 和国防信息系统局（DISA）提供支持，恢复受影响网络空间。受援 CCDR 会整合、同步、通常还会指导红色和

灰色网络空间中的 CO 活动（包括交火），通过使用指派、附属或支援性网络空间部队造成其他的杀伤性和非杀伤性效果。CCDR 与 USCYBERCOM CO-IPE 共同开发并协调对此类效果的需求，用于消除冲突，按照优先级执行行动。当 CCDR 建立下级部队（例如联合特遣部队）时，应根据 CCDR 的任务要求以及与 CDRUSCYBERCOM 的协调来确定分配多少网络空间力量支援该下级部队。

5. **网络空间组织与部队。**CCMD 将网络空间能力整合到军事行动中，并与联合部队、USCYBERCOM、军队网络空间部门（SCC）和国防部机构密切合作，构建统一协调的能力。（关于美国的网络空间组织，见附录 B。）[127]

a. **作战司令部（CCMD）网络空间行动支援人员。**CCDR 确定 CO 支援人员的规模并将其组织起来，以有效支持任务和需求。这些人员在 USCYBERCOM CO-IPE 的支持下，在整个规划、情报、作战、评估和准备过程中协调 CO 需求和能力，将 CO 与其他军事行动整合起来，协同作战。此外，CCMD 会根据需要与 USCYBERCOM 合作，在区域内与跨机构和跨国合作伙伴进行协调。CCMD 责任包括：

(1) 将 USCYBERCOM 的输入与 CCMD 的战术和/或构建网络的信息相结合，以开发符合 CCMD 要求的区域/职能性态势感知/通用作战图（COP）。

(2) 若 CCDR 所指挥的 CO 会影响或与其他国防部/其他 USG 网络空间活动或 AOR 内的行动发生冲突，则通过 USCYBERCOM 来协调该 CO 并化解冲突。在规划过程中尽早向 USCYBERCOM 提供有关 CCDR 所规划 CO 的充分信息，以便化解与其他 USG 所进行 CO 的冲突。

b. **USCYBERCOM 网络空间作战 – 综合规划分队（CO-IPE）。**建立 USCYBERCOM CO-IPE 以满足各 CCMD 的要求，并根据需要协助前述三项网络空间任务的规划和协调。USCYBERCOM CO-IPE 直接支持 CCMD CO 并与 CCMD CO 人员整合，作为 USCYBERCOM 和下级司令部（HQ）的桥梁，在战区/战术以及全球/全国层级实现网络空间部队和行动的整合。[128]

c. **任务型部队定制组合（MTFP）。**MTFP 是 USCYBERCOM 定制的支持能力，根据需要，由指派的 CO 部队、补充 CO 支持人员和网络空间能力组成。根据指示，USCYBERCOM 定制部队，在常规支援部队无法满足特定的 CCMD 危机或紧急任务需求时提供支援。各 MTFP 均基于任务建立，为有关 CCDR 提供支援，期限为整个危机/紧急行动期间或直到 CDRUSCYBERCOM 与该 CCDR 协调后重新部署。[129]

d. **联合部队司令部 – 国防部信息网络（JFHQ-DODIN）。**JFHQ-DODIN 与所有 CCDR 和国防部其他部门协调，负责全球 DODIN 行动和 DCO-IDM 任务的行动规划、指导、协调、执行和监督。维持 CDRUSCYBERCOM 与所有 CCDR 为战区/职能性 DODIN 行动和 DCO-IDM 建立的支援关系。JFHQ-DODIN 指挥官受援开展全球 DODIN 行动和 DCO-IDM，CCDR 受援进行 DODIN 行动和 DCO-IDM，将效果控制在其 AOR 或职能任务区域内。JFHQ-DODIN 根据 CDRUSCYBERCOM 的授权对所有国防部部门行使网络空间作战指令权（DACO）。[130]

e. **网络任务部队（CMF）。**USCYBERCOM 的 CMF 团队的主要工作与国防部网络战略的三个主要任务对齐：保护国防部网络并确保其数据安全、支持联合军事指挥官目标、根据指示保护美国的关键基础设施。CMF 团队通过完成下述具体任务来支持这些主要任务：

(1) 网络防御分队（CPF）为 DODIN、指定网络空间以及重要任务提供保护，并帮助网络作战部队做好准备。CPF 包括：

- 网络空间保护小组（CPT）

(2) 网络国家任务分队（CNMF）通过侦察敌方活动、阻止攻击和机动制敌来保卫国家。CNMF 包括：

- 国家任务小组（NMT）
- 国家支援小组（NST）

(3) 网络作战任务分队（CCMF）进行军事网络作战，支持作战司令部。CCMF包括：

- 作战任务小组（CMT）
- 作战支援小组（CMT）

f. **联合部队司令部 – 网络空间（JFHQ-C）。**USCYBERCOM 指定各军种的网络空间部门（AFCYBER、ARCYBER、MARFORCYBER 及美国舰队网络司令部）成立联合部队司令部—网络空间，作为网络空间任务部队的一部分，要求它们为特定作战司令部提供支援。这些司令部提供网络空间领域的专业知识，帮助受援 CCMD 参谋将必要的作战和战术层面的网络空间规划活动纳入作战计划。此外，JFHQ-C 对被称为作战任务小组的战术交火单位进行作战控制（OPCON）。作战任务小组与各自作战司令部内的特定目标集对齐。CCMD 网络空间作战支持人员和 JFHQ-C 通过指导下级作战任务小组，为作战指挥官（或联合部队指挥官（若有））的网络空间作战统一了指挥和行动。

(1) **JFHQ-C 海军部队网络司令部**支持美国特种作战司令部。

(2) **JFHQ-C 陆军网络司令部**支持美国中央司令部、美国非洲司令部和美国北方司令部。

(3) **JFHQ-C 舰队网络司令部**支持美国太平洋司令部和美国南方司令部。

(4) **JFHQ-C 空军网络司令部**支持美国欧洲司令部、美国战略司令部（USSTRATCOM）和美国运输司令部。[131]

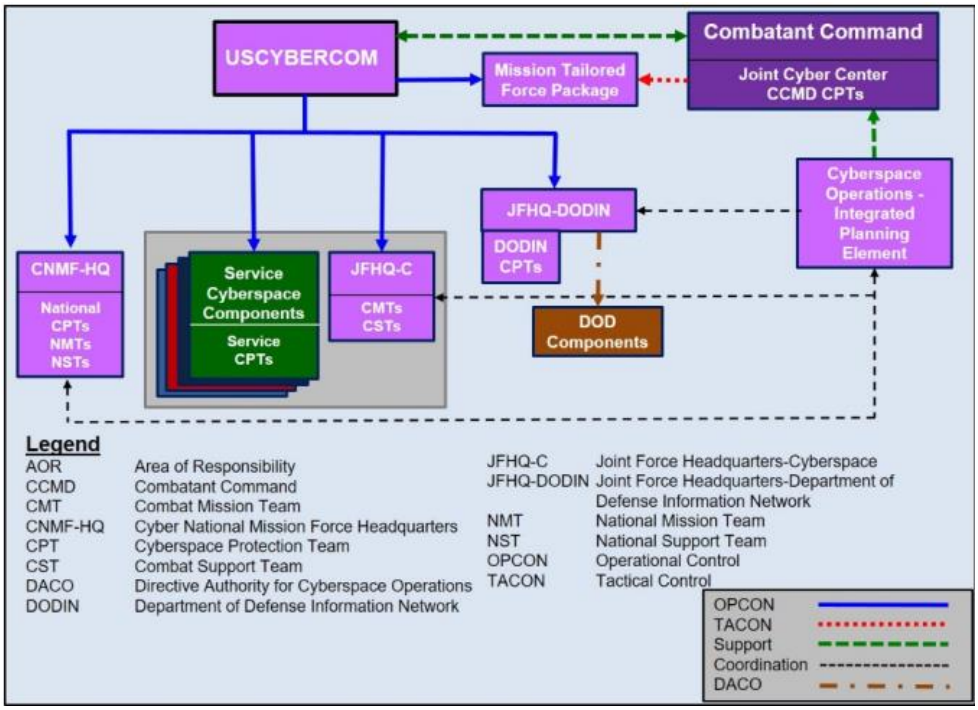


Figure 4-3:危机/应急网络空间指挥与控制

基于 JP 3-12 中的图 IV-4[132]

6. **协调网络空间作战。**考虑到 CO 速度，在规划启动后，要进行大量的战前协作，时刻保持警惕，以有效消除作战环境中的冲突因素，协调行动。要达到步调一致的效果，关键是维持网络空间态势感知并评估所规划 CO 对联合部队的潜在影响，包括 DODIN 的安全状况、正常网络配置的修改或是否检出恶意活动迹象。在网络空间或通过网络空间进行的 CO 冲突化解和协调工作应包括如下类似措施：

a. **化解冲突。**对于 CO，化解冲突指协调网络空间能力的使用，与相关国防部、跨部门和跨国合作伙伴共同制造效果，以确保行动不会干扰、妨碍彼此或以其他方式相互冲突。要在网络空间中实现预期效果并按计划使用能力达到目的，指挥官必须保证本司令部与同一网络空间领域中的其他司令部和机构并无冲突。

b. **电磁频谱（EMS）因素**对 CO 具有重要意义。指挥官利用联合 EMS 行动来协调 CO、空间行动、电子战（EW）、导航战、依赖 EMS 的各种信息搜集方式以及 C2 等。虽然这些活动可与其他信息相关能力（IRC）整合，促进信息行动协调，但 CO、空间行动和电子战行动在发动攻击时通常需要特定的权限。同样，借助于 CO 实现的某些 IRC（例如军事信息支援行动（MISO）和军事欺骗（MILDEC））有自己的执行审批流程。因此，对利用 EMS 的 IRC 进行协调是一个复杂的过程，需要对各种相关政策有精准的预见和了解。

c. **网络空间火力整合。**网络空间攻击能力虽然可以独立使用，但在与其他火力联合时通常最有效。整合网络空间火力包括如下行动：利用基于 EMS 的网络空间攻击破坏敌方防空系统、在敌方领导层的通信中插入信息、破坏敌方太空和地面精确导航和计时系统或影响其性能、破坏敌人 C2 等。网络空间效果可以体现在战略、作战或战术层面，亦可在军事行动的任何阶段，并且可与杀伤性武器协同，最有效地攻击目标。联合火力不一定同时发力，因为为达到最优效果，网络攻击可能安排在杀伤性影响产生之前或之后。每次交战的考虑因素各有不同，具体取决于敌人对网络空间的依赖程度。用来支援的网络空间火力有时充当次要角色，但当用于辅助空中、陆地、海上、空间及特种作战时，又会是任务的关键组成部分。部队若欲在物理领域使用致命武器和其他能力，须知悉预期网络空间效果的类型和时间安排，否则无法最大程度地利用网络空间火力。网络空间火力只有在周密准备、妥善安排的情况下才能产生其他方式无法达到的效果。若安排不当，网络空间火力则会徒劳无益甚或干扰其他任务的有效执行。[133]

7. **网络空间目标定位。**定位目标的目的是将火力（使用武器系统或通过其他行动对目标产生特定的杀伤性或非杀伤性效果）整合和同步到联合作战中。某些 OCO 和 DCO-RA 任务所使用的审批程序仅适用于 CO，同时也可用于联合目标定位周期的多个阶段。因此，CO 规划人员和决策者在定位目标时常将这一程序根据具体情况修改后加以使用。

a. **网络空间目标定位过程。**规划和目标定位人员根据指挥官的目标（而非实现目标的能力），在网络空间内并通过网络空间定位并选择攻击目标。重点是制造效果，完成目标定位任务并实现目标，而不仅仅因为具有某项网络空间能力而去使用它。整合并同步规划、执行和评估是联合目标定位成功的关键。在目标定位过程中，要考虑 CO 的三个基本方面：

(1) 识别哪些网络空间能力可用于打击指定目标；

(2) 知道哪个 CO 方案在某些情况下检出率较低且/或不会造成相关物理损坏因而更优；

(3) 对网络空间目标产生的高阶效应可能会影响 DODIN 部门，包括对联合部队攻击进行报复。

b. **网络空间目标定位挑战。**每个目标都具有不同的内在或后天特征（即物理、功能、认知、环境和时间特征），构成检测、定位和识别的基础。这些特征可用于确定目标系统内的目标值以及对目标进行分类以便今后进行监视、分析、打击和评估。CO 目标定位中的挑战是识别、关联、协调和解除跨物理网络、逻辑网络和网络角色层中多个活动之间的冲突。这要求具有符合 CO 节奏的 C2 能力，以便快速联合受影响利益相关方。

(1) 物理网络层是传输数据的媒介，包括有线（如地面和海底电缆）和无线（如无线电、无线电中继、蜂窝，卫星等）传输装置。它是确定地理位置和适用法律框架的参考要素。

(2) 逻辑网络层提供从目标的物理位置抽象出来且以网络空间中的逻辑位置为参考的另一视角。逻辑位置通常用网络地址（例如 IP 地址）来表示，描述了物理域中的节点如何寻址并相互引用，最终形成网络空间中的实体。逻辑网络层是物理连接最可能丢失的位置。在逻辑层中进行目标定位需要

知道目标的逻辑标识且获得对其的逻辑访问权限才能产生直接效果。

(3) 网络角色层是个人或群体在线身份的集合，同时也是逻辑网络层数据的抽象，在主动识别目标和从属关系以及活动溯源方面对联合部队具有重要意义。创建网络角色是为了将目标的信息分组，以方便分析、交战和上报情报。网络角色会很复杂，各元素分布在多个虚拟位置，通常未与单个物理位置或形式相关联，因此联合部队需要进行大量的情报搜集和分析，以洞悉实情，感知态势，有效定位网络角色。最后，将网络角色与逻辑或物理网络层所使用的功能相关联。

c. **网络空间目标访问。**网络空间部队利用网络空间获取对目标或目标元素的访问权限。获取这种访问权限后，可进行从信息搜集到操控再到目标提名等一系列活动。并非所有访问都对军事行动有用。例如，从实体搜集信息所需的访问级别可能并不足以产生预期效果。在网络空间或通过网络空间获取目标访问权限，这个过程一般需要很长时间。某些情况下，无法进行远程访问，可能需要接近目标。网络空间中的所有目标访问工作都需要根据国家政策与情报界（IC）协调，以便消除冲突，同时阐明 IGL 的潜在问题。如果无法或无需对目标直接访问，有时可通过对相关目标的间接访问来达到类似或局部效果，对预定目标产生高阶效应。有些拒绝服务网络空间攻击便是利用了这种类型的间接访问。

d. **网络空间目标提名和同步。**CO 使用标准的目标提名流程，但目标文件夹应包括目标的独特网络空间信息（如软硬件配置、IP 地址、网络角色应用等）。必须搜集这些数据，这样才能了解和描述网络空间元素与指挥官目标的相关性。有了这些数据，规划人员还能针对特定目标匹配合适的网络空间能力。各军种指挥官、国家机构、支援司令部和/或规划人员为目标定位人员提名目标，方便后者制定并扩充联合目标清单（JTL）。目标一旦进入 JTL，指挥官在收到具有相关目标和交战规则（ROE）的 EXORD 后，就会将目标与组织资产（若在某军种指挥官的指定作战区域内）关联，或者将目标指定给 CDRUSCYBERCOM，以便其他联合部队成员和其他组织采取行动。

e. 时敏目标（TST）。TST 指确定为高优先级的目标，因其对友军构成（或即将构成）威胁或短期内能产生丰厚利润，指挥官决定对其立即开战。大多数情况下，在网络空间中攻击 TST 并非易事，因为它们很可能跨责任区域（AOR），需要进行事无巨细的联合、跨部门和/或多国规划工作。准备在网络空间攻击 TST 时需要在早期规划阶段协调网络空间规划人员、作战人员和受援指挥官之间的活动，这样才更有可能在转瞬即逝的机会出现时有足够的灵活性并获得足够的访问权限。[134]

8. **评估网络空间作战。**通过评估，可衡量联合部队的任务完成情况。指挥官持续评估作战环境以及 CO 进展，并将其与自己的愿景和意图进行比较。衡量目标完成情况并在规划过程中提供及时、相关和可靠的反馈以便在执行期间调整作战，需要将 CO 的预期效果与实际结果进行比较，以确定网络空间部队使用的整体有效性。外部 CO 任务的评估流程始于规划，包括绩效指标（MOP）、火力的效用度量（MOE）、网络空间中的其他效果以及对所属作战行动或目标的贡献。评估 CO 效果的影响要进行典型的 BDA 分析以及评估物理、功能和目标系统组件。然而，网络空间行动的高阶效应往往很微妙，对二阶和三阶效应的评估也不容易。因此，在网络空间并通过网络空间评估火力常常要进行大量的情报搜集和分析工作。[135]

第五章 本土作战

“我们的大部分关键基础设施—金融系统、电网、卫生系统—所在的网络都与互联网相连，这让我们能力大增，但同时也很危险，带来了前所未有的新漏洞。外国政府和犯罪分子每天都在刺探这些系统。”

巴拉克·奥巴马总统[136]

I. 国防部的本土任务

1. **战略。**为支持国家安全战略，国防部（DOD）将着手准备，保卫国土，在军事力量上保持世界先进地位，确保对美国有利的势力均衡，并推进对美国安全和繁荣最有利的国际秩序。[137]

2. **使命。**国防部是抵御传统外来威胁或侵略（例如民族国家常规部队或大规模杀伤性武器攻击）和非国土安全的外部不对称威胁的主导联邦机构。国土安全部是国土安全的主导联邦机构，美国海岸警卫队是海上国土安全的主导联邦机构。根据法律，国防部在国内的使命有两项：国土防卫以及为非军事机构提供防务支持（DSCA）。国防部也提供国土安全支持，必要时需要参加应急防备。

   a. **国土防卫。**国土防卫指按总统指示保护美国主权、领土、国内人口和关键基础设施、抵御外来威胁和侵略或其他威胁。国防部在尽可能远离国土的区域通过侦查、阻止、预防和挫败有关人员的威胁来执行国土防卫。国土防卫在主动分层防御架构中进行，涉及前方区域、中间地带和本国国土。美国北方司令部（CDRUSNORTHCOM）司令和美国太平洋司令部（CDRUSPACOM）司令在各自责任区内（AOR）接受其他所有作战指挥官（CCDR）的国土防卫支援。[138]

   b. **为非军事机构提供防务支持（DSCA）。**DSCA 指由美国联邦部队、国防部文职人员、国防部承包商、国防部各部门资产、后备军和国民警卫队（国防部长在与有关各州州长协调后，根据美国法典第 502 篇第 32 条决定给予支援并请求使用这些力量）应非军事部门请求而提供支援，以处理国内紧急情况、提供执法支持以及展开其他国内活动，抑或是应相关实体的请求对特殊事件提供援助。

   c. **国土安全。**国防部对国土安全行动的支持体现在 DSCA 以及为美国海岸警卫队的海上国土安全提供国防部部队和能力上。国土安全既包含民防、应急、执法、海关、边境管制、移民等传统政府和公民责任，也包含不断演变的威胁和风险。

   d. **应急防备。**应急防备指在紧急情况发生之前采取措施，减少生命和财产损失，并通过国家应急框架（NRF）下的五大防备任务区保护国家机构免遭各类危害。这五大任务区指预防、保护、缓解、响应和恢复。

3. **跨部门/政府协调。**在国内，国土防卫、DSCA 和国土安全需要与跨组织和跨国合作伙伴进行事前和持续协调，以整合能力，促进联合行动。在这种复杂环境中，存在众多跨司法管辖区（联邦、州、地方和部落）的威胁，由不同的利益相关者（例如国际组织、多国伙伴关系、非政府组织[NGO]和私营部门等）共同处理。国防部运筹帷幄，积极准备，与其他美国政府（USG）实体协同行动。（见图 5-1。）[139]

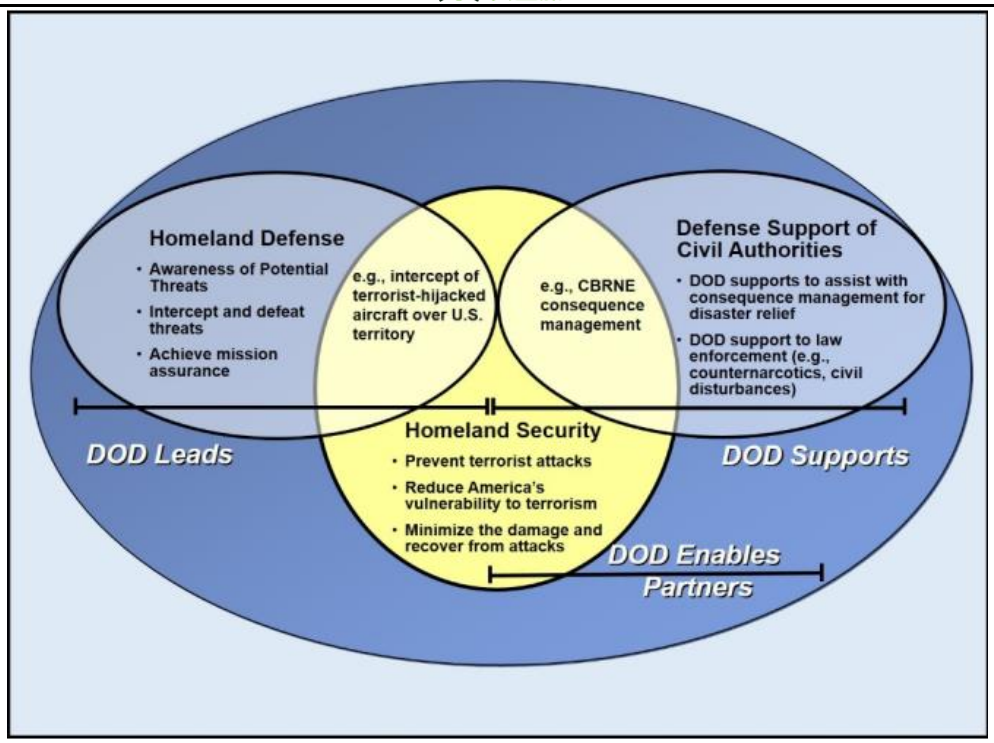


图 5-1 美国的主动分层防御

II. 关键基础设施

1. 国家的关键基础设施提供了支撑美国社会的基础服务，是国家经济、安全和健康的支柱。我们的居家用电、用水、交通工具、购物场所以及与亲友保持联系的通信系统均仰赖于这些关键基础设施。

2. 有 16 个至关重要的关键基础设施部门，其物理和虚拟资产、系统和网络一旦失效或遭到破坏，将会对安全保障、国家经济安全及/或国家公共卫生或安全造成严重影响。第 21 号总统政策令（PPD-21）：《关键基础设施安全和弹性》在全国推行政策，增强和维护安全、有效、弹性的关键基础设施。PPD-21 确定了 16 个关键基础设施部门，指定了联邦政府部门和机构作为行业对口机构（SSA）对其负责：

a. **化工** – 国土安全部
b. **商业设施** – 国土安全部
c. **通信** – 国土安全部
d. **关键制造业** – 国土安全部
e. **大坝** – 国土安全部
f. **国防工业基地** – 国防部
g. **应急服务** – 国土安全部
h. **能源** – 能源部
i. **金融服务业** – 财政部
j. **粮农** – 农业部和卫生及公共服务部
k. **政府设施** – 国土安全部和总务管理局
l. **医疗保健和公共卫生** – 卫生及公共服务部
m. **信息技术** – 国土安全部
n. **核反应堆、材料和废物** – 国土安全部
o. **运输系统** – 国土安全部和交通部
p. **水和废水系统** – 环境保护局[140]

III. 关键基础设施防卫计划

1. **国防部责任。**国防部在关键基础设施保护方面充当两个角色：联邦部门和国防工业基地（16 个国家基础设施部门之一）的行业对口机构（SSA）。在国防部内，负责国土防卫和美洲安全事务的助理国防部长（ASD（HD&ASA））作为主要领导，为这些角色提供政策、指导、监督及资源支持。

ASD（HD＆ASA）下的关键基础设施保护总监负责监督这些职责的日常执行。这两个角色的具体职责如下：

a. **联邦部门。**作为联邦部门，国防部承担着部门和国家责任。部门职责包括国防关键基础设施的识别、优先排序、评估、补救和保护。此外，所有联邦部门和机构在国家层面共同努力，以“预防、制止蓄意破坏、攻击或利用”关键基础设施和关键资源的活动并“缓解”其影响。为实现这一目标，国防部和联邦政府将与州和地方政府以及私营部门合作。

b. **行业对口机构。**作为国防工业基地的 SSA，国防部的职责包括：

(1) 与各相关联邦部门和机构、州和地方政府以及私营部门合作，包括基础设施部门的关键人员和实体；

(2) 开展或促进该部门的漏洞评估；

(3) 鼓励实施风险管理策略，防护对关键基础设施和关键资源的攻击并缓解相关影响；以及

(4) 支持部门协调机制：

- 识别关键基础设施和关键资源、确定防护优先级并协调防护工作；以及
- 促进有关物理和网络威胁、漏洞、事件、潜在保护措施和最佳实践的信息共享。[141]

IV. 国土防卫中的网络空间作战

1. **国防部网络战略。**美国在复杂、互联且日益全球化的作战环境（包括网络空间领域）中开展活动，包括国土防卫。国防部网络战略为国防部网络空间任务设定了五个战略目标。其中之一是做好准备，保卫美国本土和美国的重要利益，避免遭受具有破坏性或毁灭性后果的严重网络攻击。国防部必须与跨部门合作伙伴、私营部门以及盟国和伙伴国家合作，以阻止并在必要时粉碎针对美国本土和美国利益的重大网络攻击。国防部须培养情报、预警和行动能力，以预防高级恶意网络攻击，防止其影响美国利益。根据适用法律和政策，国防部需要获取有关全球网络和系统、对手能力以及恶意软件代理和市场的细粒度、可预测且可操作的详细情报。为了保卫国家，国防部须与政府的其他机构建立伙伴关系，做好准备，进行联合网络行动，以阻止并在必要时挫败网络空间的侵略活动。国防部的重点工作是培养能力，建立流程，做好预案，成功完成这项任务（见图 5-2）。[142]

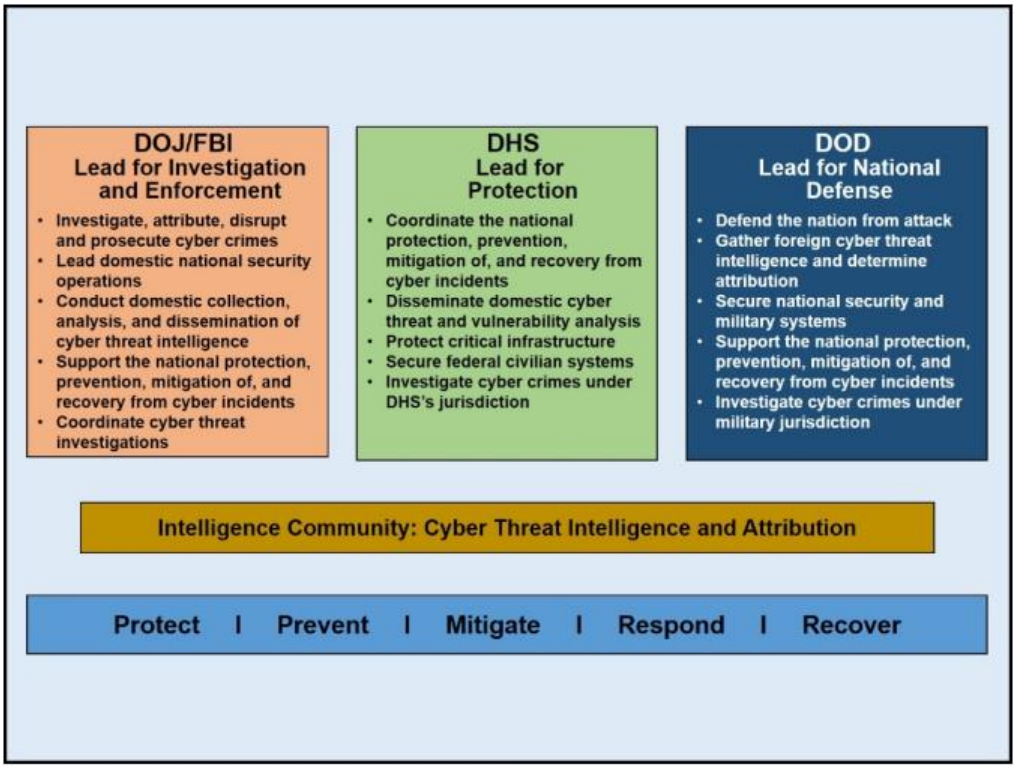


图 5-2 国家网络安全角色与职责

2. **联合行动。**对于网络空间，国家和国际网络的脆弱性和复杂关系要求各级军事、私营部门和其他政府实体密切协调，一致行动。作战司令部（CCMD）的网络空间作战（CO）支援人员、军队

和美国网络司令部（USCYBERCOM）构成军事防务前线。国土安全部在国家层面保护美国的网络空间，为非国防部 USG 网络提供保护，使其免遭网络空间入侵和攻击。在国土安全部内，网络安全与通信办公室（CS＆C）负责保护 USG 网络系统免于网络空间威胁。美国太平洋司令部（USPACOM）和北方司令部（USNORTHCOM）承担着国土防卫和 DSCA 职责，针对 CO 有独特的协调要求，需要其 CO 支持人员与美国网络司令部（USCYBERCOM）合作。[143]

a. USCYBERCOM 同步网络空间作战规划，包括指导国防部信息网络（DODIN）作战和防御，以保护国防部网络以及美国的关键网络空间资产、系统和功能。与参谋长联席会议主席（CJCS）和 CCMD 协调，指导 DODIN 作战和防御。USCYBERCOM 还与其他 CCMD 和相应的 USG 部门和机构协调，以便产生跨 AOR 网络空间效果，应对网络空间威胁。

b. USCYBERCOM 规划、协调、整合、同步和开展进攻性及防御性网络空间作战和 DODIN 防御活动，并根据指示展开网络空间作战，以便在物理领域采取行动，促进己方并抑制对手在网络空间活动的自由度。USCYBERCOM 可以与 USNORTHCOM、USPACOM 和国土安全部合作，通过协调相关 AOR 内的活动并协助分配、提供专业知识和能力来支持与国土防卫相关的网络空间行动。[144]

3. **网络空间作战的指挥与控制（C2）。**

a. **CDRUSNORTHCOM** 负责与 USCYBERCOM 和 USPACOM 协调，防御、缓解并粉碎与 DODIN 无关的针对 USDORTHCOM 和 NORAD 的网络空间威胁。USNORTHCOM 将与 USCYBERCOM 协调，在国土防卫期间规划和执行 CO。最后，地理和职能 CCDR 以及军队负责保护其位于 USNORTHCOM AOR 内、非 USNORTHCOM 负责或所属的网络。[145]

b. **CDRUSPACOM** 负责防御、缓解和粉碎与 DODIN 无关的特定 USPACOM 系统的网络空间威胁。HQ USPACOM 将通过 USPACOM 的 CO 支持人员，与 USPACOM 的各军种司令部、下级联合司令部、联合特遣部队（JTF）、直属单位和其他 CCMD 协调 CO。USCYBERCOM 为 USPACOM 提供网络空间前方支援单位，以支持 CO，并根据需要满足 USCYBERCOM 和 USPACOM 部门之间的联络要求。对于国土防卫，USPACOM 通过 USCYBERCOM 与国土安全部协调，国土安全部的网络安全与通信办公室（CS＆C）将作为主要机构防止 USG 和公共网络受到网络空间入侵和攻击。职能 CCDR 和军队负责保护其位于 USPACOM AOR 内、非 USPACOM 负责或所属的网络。[146]

4. **网络空间行动部队和任务。**USCYBERCOM 的第二个主要任务目标是保护美国，抵御针对美国利益和基础设施的网络威胁。USCYBERCOM 担心的是，有许多此类网络攻击并未构成武力使用，也未涉及武装冲突，但日复一日，会为美国的对手带来战略收益。[147]在网络空间层面保卫国家在技术和政策方面都很复杂。与所有作战司令部一样，USCYBERCOM 仅在总统（若总统不在，则为国防部长）授权后才可依据国际法抵御本国面临的构成“武力使用”的威胁。

a. **网络国家任务部队（CNMF）**的主要任务是打击对手针对美国的恶意网络活动，积极准备，根据指示，对敌方进行全方位的网络空间行动。CNMF 当前正组建一支由国家任务小组（NMT）、国家支援小组（NST）和国家网络保护小组（N-CPT）组成的部队。CNMF 与国家安全局合作，追踪敌方网络攻击者，先发制人，阻止针对美国国家利益的网络攻击。CNMF 还与作战伙伴合作，开发和实施各种能力和作战概念，以便在获得授权后与其他政府和相关私营部门合作伙伴共同进行联合及联盟作战。

b. **举国行动。**在保卫美国关键基础设施的“举国”行动中，USCYBERCOM 只管理一方面的内容。该司令部与下属民事机构合作，帮助保护国家关键基础设施，同时做好准备，在必要时采取军事行动保护国家。司法部主导网络相关调查和执法，而国土安全部则负责保卫国家及网络事件的恢复。USCYBERCOM 现正着手扩大与后备军和国民警卫队的合作关系。警卫队下属的网络响应小组可执行各种任务，以支持州、地方和私人实体（这些实体在其职权范围内独立运作）。最近为鼓励信息共享所做的立法也会促进 USCYBERCOM 和国防部与私营部门的紧密合作，减轻政府和军事系统之外的威胁。联邦政府已建立框架，提供共享信息的官方渠道，并扫清障碍，为美国政府援助私营部门铺平道路。[148]

5. **国防工业基地（DIB）。**国防部作为主导部门，着力提高 DIB 部门的安全性，包括主要部门承包商和主要承包商（无论企业在何国何地）对作战的支持，还将继续推动“全政府”方法以进行风险管理。全球技术供应链影响着国防部企业的各个关键方面，要想有效缓解由此产生的 IT 风险，只

能依靠公私营部门合作。国防部与 DIB 合作，共同提高驻留或经由 DIB 非保密网络的国防部程序信息的安全性。国防部网络犯罪中心（DC3）是国防部自愿网络空间信息共享和事故上报项目的业务联络点。此外，国防部还实施了更为严格的采购条例，要求所有 DODIN 部门的采购都须考虑适用的网络安全政策，以降低联合作战风险。[149]为保护国防部和 DIB 数据的安全，国防部将强化问责和责任制度。国防部将确保政策和相关联邦条例或合同语言要求执行到位，要求 DIB 公司必须向 DC3 上报数据窃取和丢失事件。

a. 国防部将持续评估《国防联邦采购规则补充》（DFARS）中的规则和相关指南，以确保其不断优化，符合已知数据保护标准，包括国家标准与技术研究院（NIST）颁布的标准。

b. 国防部将继续提升公司在威胁信息共享计划（如网络安全/信息保障计划）中的参与度。

c. 作为 DIB 国防承包商网站的安全认证机构，国防安全局将扩充教育和培训计划，为国防部人员和 DIB 承包商提供材料，以提高他们的网络威胁意识。

d. 此外，负责情报的国防部次长办公室将审查关键采购和技术项目的现行分类指导的翔实程度，以保护承包商网络中的信息。[150]

6. **关键基础设施/关键资源（CI/KR）保护。**随着网络攻击越来越多地被用作一种政治工具，国际关系呈现一种危险趋势。脆弱的数据系统为国家和非国家支持的攻击者攻击美国及其利益提供了绝好机会。在一次冲突中，国防部认为潜在对手企图通过攻击美国或盟国的关键基础设施和军事网络获得战略优势。精通复杂技术的攻击者可能会通过攻击公共事业部门的工控系统来影响公共安全，或通过网络入侵篡改健康记录为个人健康带来不利影响。具有破坏性、操控性或毁灭性的网络攻击可导致人员伤亡、财产损失、妨碍政策目标的实现或损害经济利益，会为美国的经济和国家安全带来巨大风险。[151]CI/KR包括对国家的安全保障、治理、公共健康与安全、经济和公众信心关系重大的基础设施和资产。《国家基础设施保护计划》指定国防部为国防工业基地（DIB）的行业对口机构。国防部发布了《国防工业基地网络安全和信息保障计划》且成立了网络犯罪中心（DC3）提供网络空间分析和取证支持。在执行国防和事件响应任务的同时，国防部还为国土安全部和美国政府的其他部门和机构提供支持，确保网络空间CI/KR的所有部门均为实现国家目标提供有力支撑。

a. **国防关键基础设施（DCI）**。DCI隶属于CI/KR，包括为美国在全球范围的军队和作战任务提供规划、支持和维持的国防部或其他部门的资产。地区作战指挥官（GCC）负责防止其责任区内的资产遭遇损失或损毁，与国防部资产负责人、国防部各分部门主管以及关键基础设施部门主要代理机构协调配合履行职责。网络司令部下属的联合部队总部-国防部信息网络（JFHQ-DODIN）是DCI的国防部信息网络（DODIN）的主要代理机构，负责发现DODIN关键基础设施存在的问题、理清问题优先级，以及修复问题等事宜。同样，国防部在必要时会与国土安全部协调配合，为保护国防工业基地提供支持。[152]

b. **国防部对关键基础设施的依赖**。国防部的很多关键职能和行动都依赖通过签约方式获取的商业资产，如互联网服务提供商（ISP）和全球供应链，而国防部及其军队不具备这些资产的直接**管辖**权。此类资产包括云计算架构提供的数据存储服务和应用程序。利用云计算，国防部可在提升业务持续性的同时整合基础设施、利用产品的IT功能并去除冗余功能。然而，若要确保这些活动取得全面成功，国防部下属各部门及行业应了解和制定风险缓解和防范措施，并有效落实这些措施。对商业互联网提供商的依赖主要指国防部与国土安全部、其他跨部门伙伴及私有部门协调合作，这对于构建和维护国防部的信息安全至关重要。国土安全部牵头联合各相关部门对国家关键基础设施的网络空间漏洞进行识别和缓解，国防部为其提供支持。[153]

c. **关键基础设施负责人的职责**。然而，国防部无法对其权利范围之外的组织培养恢复能力。为实现恢复能力从而有效阻断攻击，其他政府机构必须与关键基础设施负责人、运营商及私有部门开展更广泛的合作，开发具备恢复能力的冗余系统阻止潜在攻击。部署有效恢复措施挫败攻击者会使其意识到对美国网络和系统发动网络攻击是枉费心机。[154]

d. **国防部演习计划**。国防部的年度演习计划包括与国土安全部和FBI联合开展应对偶发事件的演习，在伙伴机构带领下，需紧急调配兵力，协助保护关键基础设施。该框架介绍了作

战司令部（CCMD）和各战斗支援部门如何与国土安全部、FBI及其他机构配合，从而加强协作，提升培训和支持力度。[155]网络卫士（CYBER GUARD）开展的作战层面的指挥演习对作战方针（阐述了各州长和国民警卫队副官对关键资产保护的关注）进行了验证。在网络卫士和网络夺旗（CYBER FLAG）开展演习时，作战司令部、整体政府和业界均参与其中，针对国防安全合作局（DSCA）模拟场景（国家的关键基础设施遭遇外来入侵），评估网络能力。在网盾（CYBER SHIELD）开展的演习中，美国网络司令部（USCYBERCOM）与国民警卫局局长的工作协调一致，而在Cyber Prelude的演习中与国土安全部伙伴协同配合。[156]

e. **国土安全部政策**。国土安全部制定了网络支持政策和国内关键基础设施政策，为国家和地方相关部门提供咨询、协调、培训、建议和协助，并为执法、国土防卫和为非军事机构提供防务支持（DSCA）的活动提供支持，协助实现国家目标。[157]

(1) **协调、培训、建议和协助（CTAA）**：国防部的政策规定在以下情况提供CTAA网络支持和服务：向组织提供军事培训、开展活动，以及国民警卫队相关人员使用国防部信息网络、软件和硬件开展国家网络空间活动。国防部的CTAA网络支持和服务不包括：

- 进攻性网络作战或防御性网络空间作战 — 响应行动
- 配合民事执法

(2) **咨询**。除了CTAA培训活动，国防部下属各部门（包括《美国法典》第32卷描述的当值的国民警卫队各分队）可与政府机构、公私事业部门、关键基础设施负责人、国防工业基地和其他非政府机构交换意见，从而保护国防部的信息网络、软件和硬件，提升国防部网络态势感知，满足国防部的任务安全保障要求，最终确保网络安全工作协调一致。[158]

(3) **网络事件响应防护支持（DSCIR）**。国防部的政策规定国防安全合作局的框架提供DSCIR。DSCIR包括直接现场支持、远程支持或二者的酌情结合。DSCIR可由国防部的军警人员、文职人员和承包商人员（包括《美国法典》第32卷描述的当值的国民警卫队各分队）提供。仅在以下两份书面材料提交时才考虑提供DSCIR：

- 关于获得联邦支持的单位知晓联邦支持可能涉及国防部支持（由主导联邦机构提供）的书面确认。
- 关于国防部访问相关信息和信息系统（如相关硬件、软件、网络、服务器、IP地址和数据库）的书面许可。[159]

II. 国土安全部的网络空间职责

1. 国土安全部负责通过保护非国防部的美国政府网络免受网络空间入侵和攻击，从而从国家层面保护美国网络空间，例如，采取措施减少和加固外部接入点、部署主动网络防御措施和传感器以及建立公私伙伴关系，从而支持国家网络安全政策的实施。

2. 国土安全部保护美国政府网络系统免遭网络空间威胁，且与政府、行业、学术界和国际社区合作，将网络安全作为一项国家优先事项，实现责任共担。

3. 根据《2002年国土安全法》和第5号国土安全总统令《国内事件管理》的规定，国土安全部长牵头负责国内事件管理。第41号总统令《美国网络事件协调》规定，国土安全部是网络空间事件发生后进行资产响应的联邦主导机构。关于外界针对国防部信息网络和情报界（IC）网络发起的重大网络安全事件，国土安全部的国家网络安全与通信整合中心为联邦最高领导机构，负责技术援助和漏洞缓解。[160]

III. 司法部的网络空间职责

1. 司法部（包括FBI）牵头开展反恐、反间谍调查以及与政府和商用CI/KR相关的执法活动。司法部负责对外国情报、恐怖分子及国家CI/KR面临的其他网络空间威胁进行调查、挫败和起诉并通过其他方式进行抑制。FBI牵头负责重大网络安全事件威胁的响应活动，但影响国防部信息网络或情报界的事件除外。考虑到恶意网络空间活动传播速度之快，调查针对国防部信息网络的威胁需要司法部和FBI协调配合。

2. FBI还负责国内网络安全威胁信息的收集、分析和传播活动，同时管辖国家网络调查联合工作组（NCIJTF）。NCIJTF是一个多机构中心，负责协调、整合和共享网络威胁调查的相关信息，由来自国土安全部、情报界、国防部和其他相关机构的代表组成。[161]

第六章：网络空间作战（CO）— 案例分析

I. 2008年俄罗斯对格鲁吉亚的攻击

1. **背景**。2008年，俄罗斯通过开展网络空间任务和行动以及配合其他国家权利手段在对格鲁吉亚的战争中取得胜利。我们可以通过分析这一现实事件阐述本文涉及的原则（请参见图6-1）。

图 6-1 2008 年 8 月俄罗斯和格鲁吉亚之间的冲突[162]

a. **跨域协同**。在此次格鲁吉亚与俄罗斯及俄方支持的自称是南奥塞梯和阿布哈兹共和国之间的战争中，俄罗斯和盟军士兵约为35,000–40,000人，并且还有大量空军和海军，而格鲁吉亚士兵人数在12,000–15,000左右且空军和海军实力有限。这次冲突虽持续时间不长且影响不大，但却是史无前例的，因为它开创了配合其他作战领域（主要是陆空作战）开展的网络空间协同攻击的先河。

b. **网络空间情报收集**。俄罗斯在军事行动的数周前发起了网络空间行动。俄罗斯网络情报部门对重要地点进行了勘察，入侵格鲁吉亚的军事和政府网络收集有用数据，为即将开始的战斗做准备。在这段时间内，俄罗斯政府对其网络空间民兵（政府之外的非正规黑客）做了工作安排，让他们辅助作战，为政府的行动打掩护。俄罗斯政府和网络空间民兵针对格鲁吉亚目标进行了攻击演练。

c. **防御性网络空间作战响应行动（DCO-RA）**。俄罗斯还攻击了格鲁吉亚的黑客论坛，防止对方黑客对俄罗斯的网络空间目标采取报复性行动。

d. **拒绝—破坏**。俄罗斯网络空间部队攻击了其军事行动附近的民用场所，目的是在平民中制造恐慌氛围。例如，在戈里镇，俄罗斯在空袭前发动了分布式拒绝服务（DDoS）攻击致使政府和新闻网站瘫痪。对格鲁吉亚的网络空间进行封锁（集中对战术数据链和数据融合中心进行攻击），破坏和中断其决策周期，限制其军事响应能力。

e. **拒绝—中断**。俄罗斯CO部队中断了格鲁吉亚政府、军事和外交方面的通信。

1. **政府和军事通信**。8月7日军事作战期间，俄罗斯政府和非正规部队对格鲁吉亚的政府

和军事网站发动了DDoS攻击，中断了格鲁吉亚军事和政府部门之间的信息传输。

2. **国际通信**。俄罗斯依靠势不可挡的空军实力对格鲁吉亚的数个边境地区进行了武装攻击，对其黑海海岸线进行了两栖攻击，并发动了毁灭性的网络攻击。相比之下，格鲁吉亚却对此毫无招架之力，将全都希望都寄托在战略通信上，即通过向世界发声，揭露俄罗斯的军事侵略和粗暴侵犯，以博取同情。然而，俄罗斯通过有效的网络空间行动使格鲁吉亚政府无法对外传递信息，使他们寻求国际援助的最后希望破灭。

f. **拒绝—破坏（潜在）**：俄罗斯在选取目标时进行了精心策划。例如，俄罗斯并未攻击格鲁吉亚最重要的资产，即巴库（Baku）到苏普萨（Supsa）的石油管道及相关基础设施。这样，俄罗斯就手握这张王牌促使格鲁吉亚决策者考虑尽快结束战争。

g. **操控**。尽管俄罗斯并没有操控格鲁吉亚数据的明确企图，但其CO部队牵引了格鲁吉亚的数据流，将本应在互联网上传输的数据转移到了电话和无线电通信等更为传统的通道上。格鲁吉亚试图以高于信息网络支持的最大速率的速度传输数据，这是因为很大一部分带宽都被网络攻击用作了向网络注入无用数据。在战争初期，网络攻击可有效阻塞格鲁吉亚的整个信息网络，这时候若格鲁吉亚能够采取网络和军事方面的防御措施，快速采取有条理的响应行动，可能会取得最明显的防范效果。[163]

h. 总的来说，俄罗斯的战争策划者将网络空间作战与其外交、信息、军事和经济（DIME）权利因素进行了紧密结合。对于今后准备结合网络空间这一新领域发起冲突的策划者来说，可将俄罗斯和格鲁吉亚之战作为一项案例进行分析。[164]

II. 俄罗斯网络空间作战—设计、策划与执行

1. **CO团队**。本节介绍了俄罗斯的CO团队为支持其在格鲁吉亚的行动而规划的设计、策划与执行活动。

2. **网络空间设计活动**。本文介绍的设计理念为CO团队提供了指南，可协助指挥官制定作战方案。

a. **了解网络空间环境**。收到作战策划指示后，CO团队尝试了解作战环境，他们研究了格鲁吉亚、俄罗斯和国际上的环境，重点探讨了物理网络和逻辑网络以及关键人物和团队（请参见图6-2）。

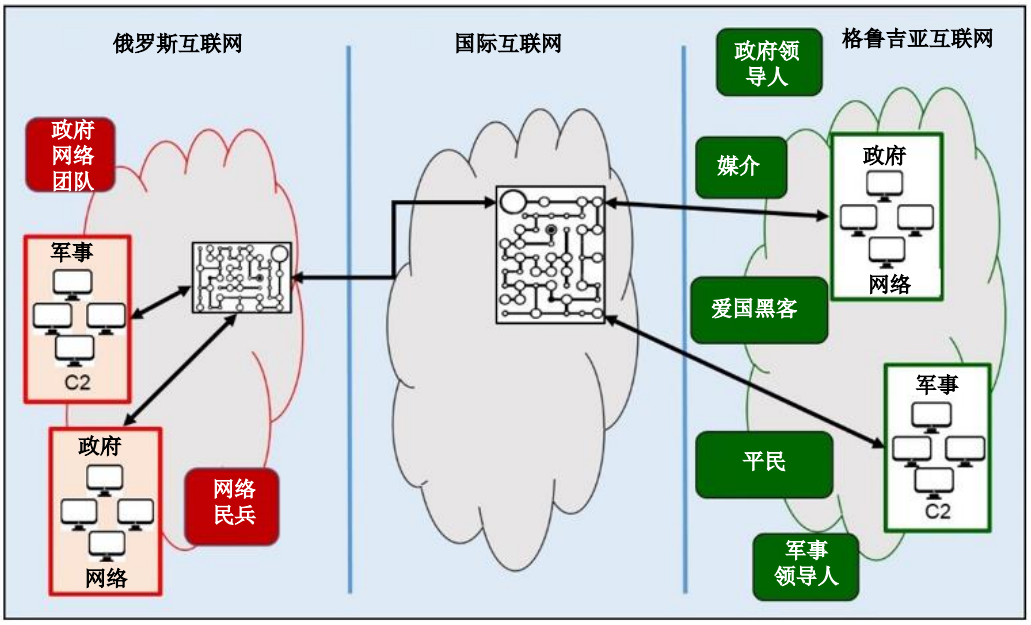


图 6-2 格鲁吉亚、俄罗斯和国际的网络空间环境
（原图出自《联合作战跨域协同》）

b. **了解网络空间中的问题**。明确关键人物、组织和物理和逻辑网络后，CO团队集中精力理

清和了解作战相关问题。他们明确了网络空间挑战、威胁和作战风险，并试图摸清对方的复原和恢复能力。反复出现的CO风险正在失去其匿名性。

c. **制定作战方案**。作战方案阐述了指挥官如何将当前形势最终转化为理想情况。制定作战方案时，指挥官应确保网络空间中以及通过网络空间发起的行动与其他活动协调一致，从而实现最终目标。指挥官可利用作战路线和努力方向展示如何实现最终目标（请参见图6-3）。

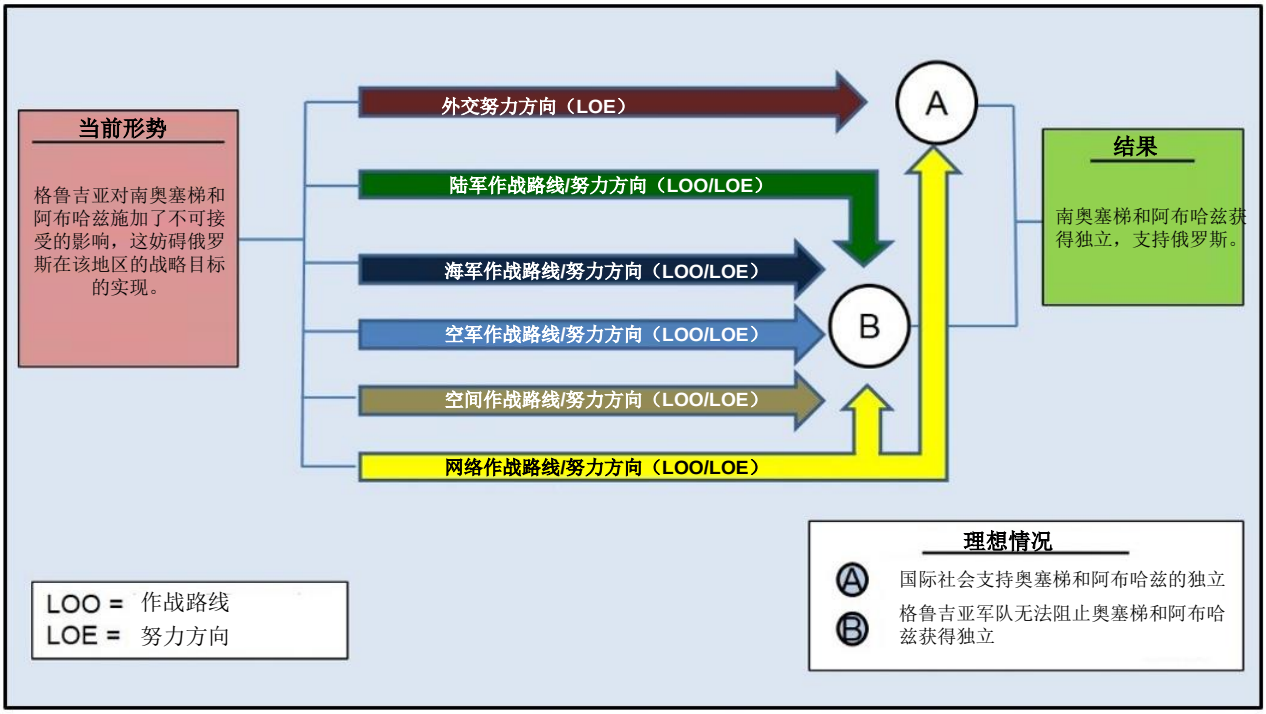


图 6-3　俄罗斯在格鲁吉亚的作战方案
（原图出自《联合作战跨域协同》）

3. **网络空间策划活动**。策划阶段将战略纲要与方向转化为作战计划和行动指示。基于指挥官的作战方案和指导，CO团队将协助参谋制定和分析行动方案，制定计划或指示，而且应进一步分阶段制定CO作战路线和努力方向，将其纳入网络空间作战概念（请参见图6-4）。

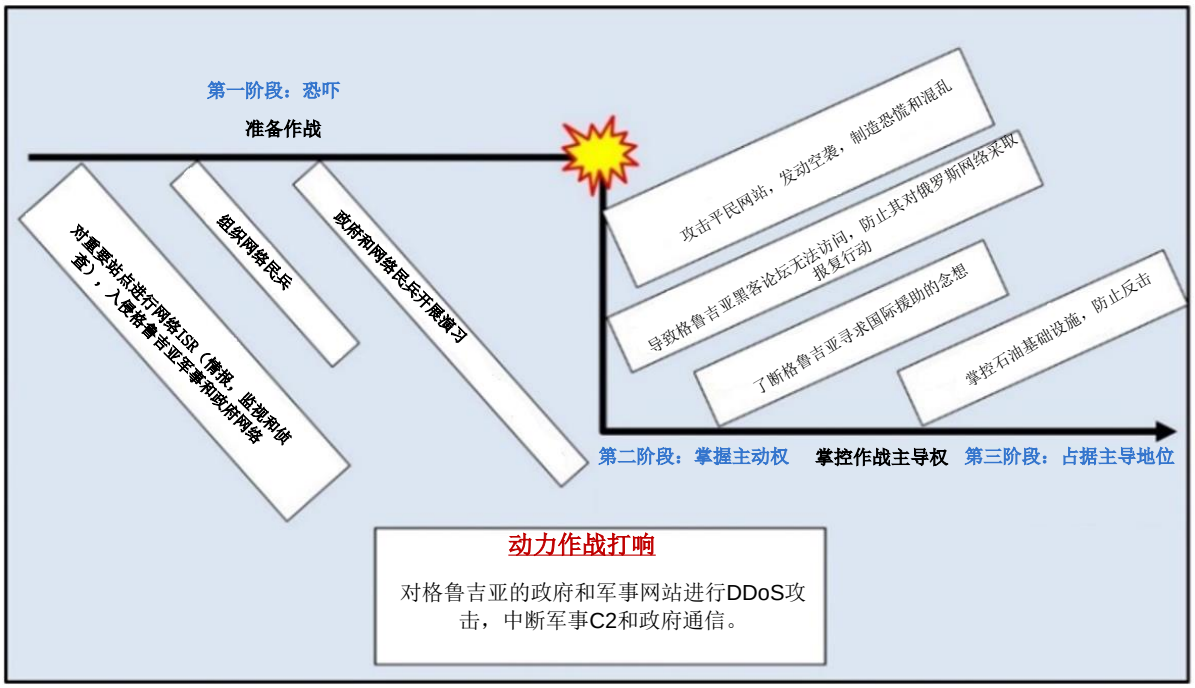


图 6-4 俄罗斯在格鲁吉亚的网络空间作战概念
（原图出自《联合作战跨域协同》）

4. **执行期间的网络空间作战**。在执行阶段仍进行作战规划，开始时侧重于改进当前行动计划和拟定行动命令。在执行阶段，CO团队为未来的计划和行动及当前行动提供支持。

   a. **网络空间影响**。网络空间策划人员应集中精力开展网络空间行动，实现指挥官的目标。CO策划人员应关注战术影响会逐渐累积进而形成总体作战影响。在作战层面，指挥官的参谋负责制定目标和预期效果，并据此为下属拟定任务。在这种情况下，俄罗斯CO团队在通过DDoS和其他技术致使格鲁吉亚政府及军事部门无法有效应对的同时，也保护自身网络，确保匿名行动。这些网络空间攻击效果直接促进了指挥官达成目的和最终结果（见图6-5）。

   b. **确定目标—前置期**。尽早策划网络空间行动至关重要。输出进攻性网络空间作战相关情报通常要比军事行动耗时得多。寻找目标也应比传统方式提前进行，而且应长期作为一项关键任务。在本案例中，俄罗斯网络情报部门对重要站点进行勘察，入侵格鲁吉亚的军事和政府网络，收集有用数据，为即将开始的战斗做准备。此外，网络空间团队在作战前还进行了演练。

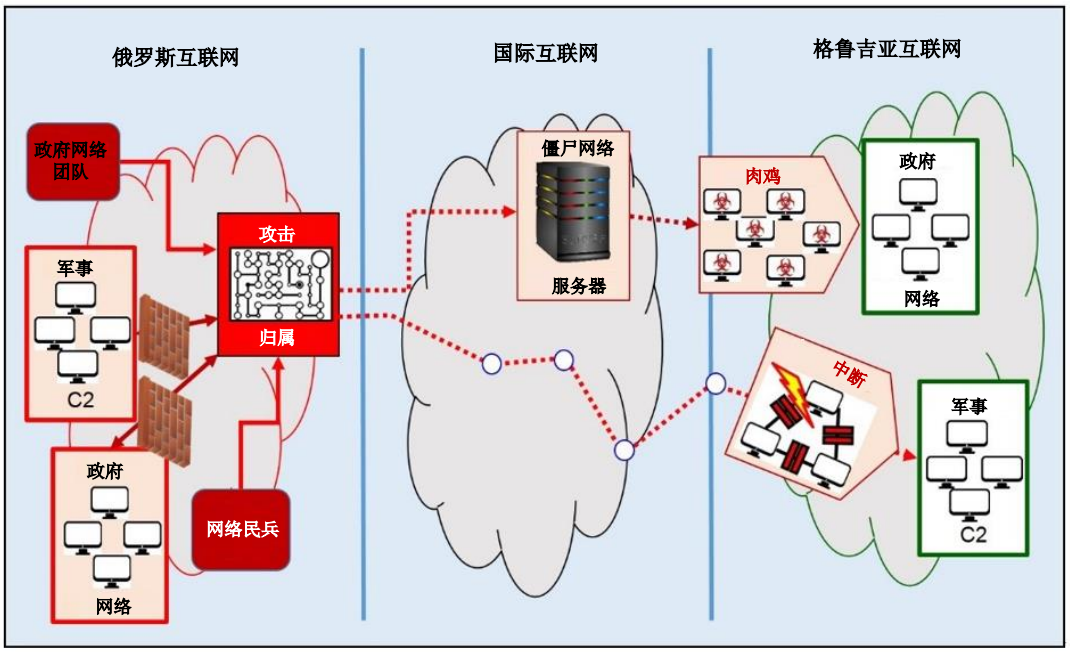


图 6-5 俄罗斯的网络空间影响
（原图出自《联合作战跨域协同》）

c. **目标选定方面的协调与授权**。选择网络空间目标需要多个作战司令部、多部门甚至多个国家联合开展策划协调、合作、评估和情报工作。若要通过网络空间对目标实施打击，网络空间策划者和实施者需在规划前期就与受援指挥官沟通协调，确保可抓住稍纵即逝的机会潜入目标。此外，指挥官应制定流程，快速传播CO目标相关的执行指令。这是因为要联合多部门进行网络空间冲突解除/协调可能需要对具体情况下的特定行动进行联合预审。

III. 格鲁吉亚的防御性网络空间作战

1. 俄罗斯的CO团队在整个冲突过程中一直保持网络优势，致使格鲁吉亚无法成功实施网络防御或反击。这其中很大一部分原因在于格鲁吉亚有着严重的网络缺陷，即在格鲁吉亚的13条对外连接中，超半数均穿过俄罗斯，而且其网站的大部分互联网流量均通过土耳其或阿塞拜疆的互联网服务提供商传输，而很多提供商的流量又通过俄罗斯传送。总之，格鲁吉亚的网络防御过于脆弱且为时太晚。[165]本节将介绍格鲁吉亚CO团队为缓解俄罗斯的进攻性网络空间行动而试图采取的防御性网络空间作战规划和行动（见图6-6）。

a. **防御网络作战**。尽管未能成功，格鲁吉亚的CO团队也曾试图开展信息网络行动（类似于国防部信息网络行动），提升军事网络的安全。他们对信息网络上的信息流进行监控，而且也尝试采取了很多主动措施加固整个防御网络，如配置控制和安装补丁、网络安全措施和用户培训、物理安全和安全架构设计，入侵检测、带宽管理/频谱管理、部署基于主机的安全系统和防火墙以及数据加密。[166]

b. **防御性网络空间行动（DCO）**。格鲁吉亚的CO团队开展了主动和被动的防御性网络空间行动，从而确保其能够合理使用网络空间能力，保护数据、网络、网络中心能力及其他特定系统。

(1) **DCO内部防御措施（DCO-IDM）**。CO团队针对其网络采取内部防御措施，如积极监测外部高级威胁，并应对这些威胁。[167]例如，格鲁吉亚曾试图根据流量来源过滤流量以缓解网络攻击。然而，俄罗斯攻击者由于提前做了充分的情报工作，轻而易举地挫败了格鲁吉亚这一企图。他们通过境外服务器传输流量，屏蔽了真实IP地址，并伪造了虚假IP地址欺骗格鲁吉亚的网络防御过滤器。不过，格鲁吉亚的CO团队为了保护某些政府网站，将其移至了美国境内服务器。[168]

(2) **DCO响应行动（DCO-RA）**。格鲁吉亚的CO团队也采取了有限的DCO响应行动打击俄罗斯政府的CO团队和‘网络民兵’，旨在挫败当前或临近的威胁，从而保护其网络空间防御能力。格鲁吉亚的CO团队企图发起至少一次大型反击，但以失败告终。他们在俄语互联网论坛上利用网络攻击工具和指令欺骗亲俄网络力量，让他们在毫不知情的情况下攻击俄罗斯网站。不过，格鲁吉亚的此次反击对锁定的俄罗斯网站的影响可谓微乎其微。[169]

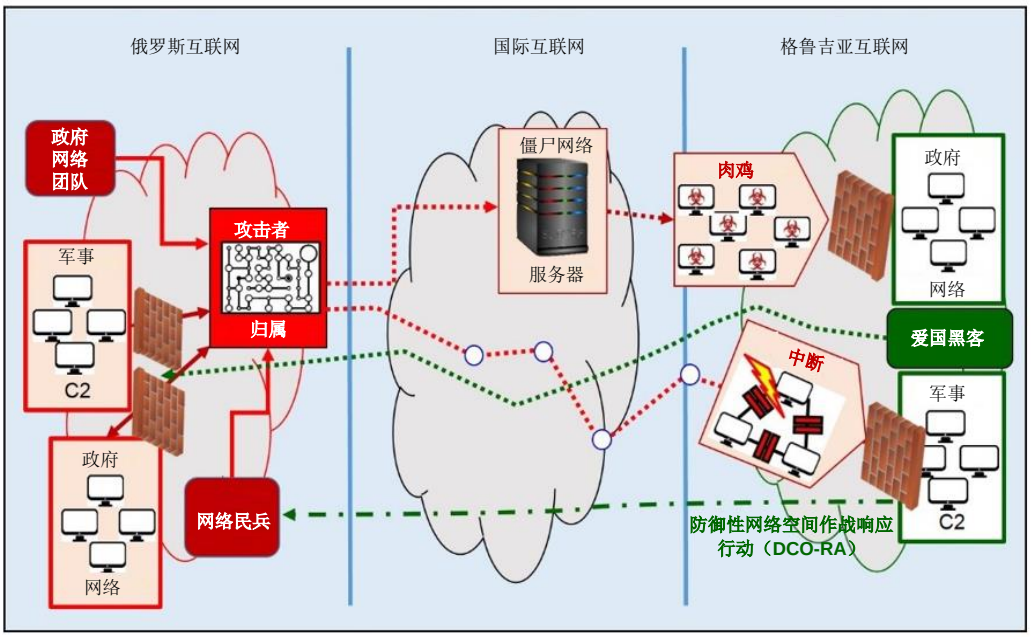


图 6-6　格鲁吉亚的防御性网络空间行动（DCO）
（原图出自《联合作战跨域协同》）

附录 A：美国的战略、指南和政策

附录 A 包括以下几个方面：

I. 美国的战略和政策
- 美国国家网络战略
- 美国国务院的国际网络空间政策战略
- 关于提升网络安全的总统行政命令
- 各部门对有关提升网络安全的总统行政命令的响应

II. 国土安全部安全战略和指南
- 国土安全企业的网络安全战略
- 提升关键基础设施网络安全框架

III. 司法部安全战略和指南
- 2018年司法部长的网络数字工作组报告

IV. 国防部战略
- 国防部网络战略

V. 美国网络法指南
- 国务院对网络空间国际法所持立场
- 国防部战争法手册

I. 美国的战略和政策

A.美国国家网络战略

2018 年 9 月，特朗普总统发布了《国家网络战略》。下文将概括介绍美国的国家安全战略。有关完整报告，请参见以下链接：https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

概述

美国的繁荣和安全取决于我们如何应对网络空间的机遇和挑战。美国的关键基础设施、国防和人民的日常生活都依赖计算机驱动的互联互通的信息技术。随着美国人民生活的方方面面已经越来越依赖安全的网络空间，新漏洞和新威胁不断涌现。《国家网络战略》基于《国家安全战略》和政府前18个月的工作进展制定，介绍了美国如何确保人民持续从安全的网络空间获益，这彰显了我们的原则，保护了我们的安全，促进了我们的繁荣。

我们是如何实现的？

当前，互联网发展迅速，而且网络空间在全球各方面的核心作用日益凸显，这与美国成为世界上唯一的超级大国是相契合的。二十多年以来，美国人民用自己的聪明才智推动了网络空间发展，而网络空间现在又成为美国财富创造和创新的根基。网络空间是美国金融、社会、政府和政治生活中不可或缺的一部分。同时，美国人民时常想当然地认为美国在网络领域一直拥有绝对优势，而且美国人民关于开放、可靠、安全和互联互通的互联网愿景必定会实现。美国人民相信，互联网的发展会促使言论自由和个人自由这一共同愿望在世界每个角落开花结果。美国人民把握住了时机发展通信和商业，而且在自由交流思想方面也取得了显著成果。美国秉持的携手共建开放共享的网络空间，实现互惠互利的愿景得到了世界上多数国家的认同。

然而，我们的竞争对手和敌手却与我们背道而驰。他们自身从开放的互联网中获益，却对其民众访问互联网加以限制和控制，这明显违背了国际论坛提倡的互联网开放性原则。他们以国家主权观为挡箭牌，公然违反其他国家的法律，实施恶劣的经济间谍行为和恶性网络活动，对全球个人、商业和非商业利益集团以及政府造成严重的经济破坏和损害。他们认为美国强大的军事、经济和政治实力的影响被网络空间削弱，而且美国及其盟国和伙伴在网络方面脆弱不堪。

俄罗斯、伊朗和朝鲜肆无忌惮地发动了攻击，损害了美国和国际商业以及美国的盟国和合作伙伴，却没有付出能够阻止未来网络侵略的代价。中国从事网络经济间谍活动，窃取了价值数万亿美元的知识产权。恐怖分子和犯罪分子等非国家攻击者利用网络空间获得利益、招募新人、大肆宣传炒作，并且攻击美国及其盟国和伙伴，而且他们的活动经常受到敌对国家的庇护。随着攻击者发动越来越多更复杂的恶意网络活动，公私实体很难保护其系统的安全。美国的实体目前正面临网络安全挑战，无法有效验证和保护其网络、系统和数据，确保其具备恢复能力，而且也无法检测和应对网络事件和进行恢复。

展望未来

随着新威胁层出不穷且战略竞争步入新时代，我们需制定新的网络战略应对新形势，减少漏洞、阻止攻击者，从而捍卫美国蓬勃发展的时机。网络空间防护在我们战略中是不可或缺的，要实现这一点需要联邦政府和私有部门共同推动技术进步和提升行政效率。同时，美国政府意识到单纯依靠网络空间技术手段无法从根本上解决面临的新问题。若要阻止恶意的网络攻击者防止事态进一步升级，美国必须制定政策让攻击者付出代价。

美国政府正采取行动应对这些威胁，积极适应新的现实情况。美国已制裁了恶意网络攻击者，控诉网络犯罪分子。我们公开了发起恶意活动的攻击者并发布了他们使用的工具和基础架构的详情。我们已要求各部门和机构卸载存在各种安全风险的软件，开始实施问责制，任命各部门和机构的负责人，让他们管理所控制系统的网络安全风险，赋予他们权利，使其提供充分安全保障。

美国政府的网络空间方案以美国一直秉持的价值观作为根基，如个人自由、自由言论、自由市场和隐私等信念。我们一直在践行我们的网络空间承诺，即实现开放、稳定、安全和互联互通的互联网，从而提升和扩展我们的价值观，保护和确保美国员工和公司的经济安全。我们只有重申推动网络空间利害关系的承诺才能实现所期望的未来。

美国政府意识到，美国正在与战略对手、流氓国家、恐怖分子和犯罪网络进行旷日持久的竞争。俄罗斯、中国、伊朗和朝鲜都利用网络空间对美国及盟国和伙伴发起挑战，其疯狂程度超越了任何其他领域。这些敌手利用网络工具损害我们的经济和民主、窃取我们的知识产权，在我们的民主进程中制造纠纷。在和平时期，我们面临针对关键基础设施的网络攻击风险，而且在没有战争危机情况下，这些国家会对美国发起更多网络攻击且持续开发更有效的新型网络武器。

《国家安全战略》概括介绍了以下几点：

(1) 如何通过保护网络、系统、功能和数据保卫我们的国土安全。

(2) 如何通过促进安全的数字经济繁荣发展以及培养强大的创新能力推动美国的繁荣。

(3) 与盟国和合作伙伴共同努力，提高美国阻止利用网络工具实现恶意目的的攻击者的能力，如有必要，对其进行惩罚，从而维护和平与安全。

(4) 广泛扩大美国影响力，宣传关于开放、可靠、安全的互联互通的互联网的关键原则。

只要我们做到以下几点即可成功实现该战略：（1）对网络、系统、功能和数据进行验证和防护，对事件进行检测、响应和恢复，从而有效管理网络安全漏洞；（2）减少或杜绝针对美国利益开展的毁灭性、破坏性或扰乱稳定的恶意网络事件；（3）通过借助网络和非网络手段使攻击者付出代价从而阻止与网络空间负责行为相左的活动；（4）美国已准备好通过利用网络能力实现国家安全目标。

《国家网络战略》基于《国家安全战略》的核心思想编写。国家安全委员会的人员会就合理的资源计划与各部门、各机构和管理和预算办公室（OMB）进行沟通协调，从而实施该战略。各部门和各机构会执行以下战略纲要中规定的任务。

来源：https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf，2018年11月1日。

B. 国务院的国际网络空间政策战略

以下链接是国务院网络问题协调员克里斯托弗•佩恩特（Christopher Painter）2016年5月25日就东亚、太平洋和国际网络安全政策向参议院对外关系委员会提交的报告节选：

https://2009- 2017.state.gov/s/cyberissues/releasesandremarks/257719.htm.

2016年5月，根据《2016综合拨款法案》的规定，国务院向国会提交《国务院国际网络空间政策战略》（简称"战略"）。该战略包括一份关于国务院实施总统发布的《2011网络空间国际战略》的工作报告，还介绍了我们对网络空间负责任国家行为规范所做的推广工作、某些其他国家对该规范的理解、美国面临的威胁、总统可采取哪些工具阻止恶意攻击者以及编写国际规范所需的资源。

尽管该战略中介绍了我们所取得的成功，但我们要实现开放、安全、稳定和互联互通的互联网愿景仍面临一系列政策和技术方面的挑战。很多挑战已在我去年的报告中介绍过，但目前仍未解决。今天，我将着重介绍我们对广泛的国际网络稳定框架所做的推广工作以及其他国家政府部门提倡的互联网观念。此外，我还将花一些时间讨论技术挑战和美国和盟国遭遇的持续恶意网络活动带来的威胁，以及我们可采取哪些工具阻止这些行动。

为营造政策环境所做的外交努力

构建际网络空间稳定框架

国务院以总统的国际网络空间战略愿景为指导与跨部门伙伴协同工作。总统的国际网络空间战略旨在推广国际网络稳定战略框架，从而实现和维持和平的网络环境，让各国充分实现自身利益，方便各国携手防御常见威胁和避免冲突，使各国基本没有任何动机采取破坏性行为互相攻击。

该框架包含三个关键要素：（1）明确全球范围内各国的网络空间行为法规；（2）就和平时期有关负责任国家行为的其他自愿规范达成国际共识并推广这些规范；（3）制定和实施切实可行的信心建立措施，通过减小误判和问题升级风险提高网络空间稳定性。

自2009年以来，负责国际安全环境中的信息和电信领域发展的联合国政府专家组（UN GGE）是联合国为该框架提供支持的一个成果颇丰且富有开创性的专家组。2010、2013、2015年的三篇UN GGE报告中的一致性建议为国际社会制定国际网络空间规范和信心建立措施提供了标准。2016年8月再次召开会议时，联合国政府专家组的工作在我们对该框架大力宣传过程中仍发挥核心作用。

国际法的适用性。对于我们的国际网络稳定框架来说，第一个也是最基本的支柱是当前国际法对网络空间国家行为的适用性。2013年UN GGE报告是一项具有里程碑意义的成就，确认了包括《联合国宪章》在内的现行国际法适用于网络空间的国家行为。2013年的报告强调指出，各国的网络空间行为必须符合现有的国际义务和承诺，这些规定在几十年的和平和冲突时期一直为国家行为提供指导。各国必须履行国际不法行为相关的国际义务。2014–2015年的UN GGE报告在国际法相关问题上取得了进展，明确了《联合国宪章》第51条规定的固有正当防卫权利的适用性，特别强调了武装冲突法的人性、必要性、相称性、区分的根本原则。

负责任国家行为规范。美国正努力针对网络空间内负责任国家行为相关的其他一系列自愿性规范达成共识，明确影响各国的国家和/或经济安全的关键风险领域，指出在和平时期应杜绝这些风险。采取这些稳定措施（即自我约束措施）会极大地帮助防御冲突和实现稳定。美国在全球率先提出制定一系列明确的和平时期网络规范，包括关键基础设施网络安全、计算机安全事件响应小组提供防护以及各国联手处理关于缓解其领土内发起的恶意网络活动的请求。2015年5月，国务卿克里在韩国首尔的一次讲话中突出强调了关于开放安全的互联网的规范。2015年UN GGE报告的最显著成果是推荐了一些和平时期网络行为的自愿性规范，包括美国倡导的概念。

信心建立措施（CBM）。除了我们在法规和自愿性规范方面所做的工作，网络CBM也可能对维持国际网络稳定作出巨大贡献。数十年来，CBM一直用于在国际上关心的其他领域建立信心、降

低风险和提高透明性。以下是网络CBM的例子：透明性措施，如分享国际战略或原则；合作措施，如积极应对某个网络事件或威胁源起方；稳定性措施，如承诺禁止开展某项重大活动。目前，欧洲安全与合作组织和东盟地区论坛正在制定网络CBM，进入了初步实施阶段。2015年，东盟地区论坛就一份涉及未来拟实现的一套CBM的详细工作计划达成了一致。

尽管前面介绍的该框架的多个元素对于美国读者来说无需多言，然而我们必须认识到网络问题对于很多国家来说却是新生事物，而且很多国家对于应如何促进网络稳定持不同观点（在本文后面介绍）。尽管众口纷纭，莫衷一是，而且针对其他问题的外交谈判可能要持续数年或长达几十年，美国及其盟国近些年在推动国际网络稳定战略性架构方面已取得了实质性进展。下面我将举几个去年的进展实例。

美中网络承诺

美国坚决反对利用网络技术窃取知识产权获得商业利益，已就此问题与中方代表交涉多年，让其提起注意。2014年，美国称五名中国军方人员对六家美国实体进行入侵、开展经济间谍以及其他犯罪活动，致使中国暂停了中美网络工作小组。
然而，在习近平主席2015年9月访美期间，中美就网络问题关键承诺达成了共识。以下是关键承诺的内容：

(1) 双方政府同意协调配合，应对其领土内发起的恶意网络活动相关的信息和协助请求进行实时响应；

(2) 双方政府不得或蓄意支持通过网络窃取知识产权谋取商业利益；

(3) 双方政府将共同致力于进一步发现和推广适用的网络空间国家行为规范，组建高级专家组负责解决网络空间的国家安全问题；
(4) 双方政府将建立部长级联合对话机制，打击网络犯罪并解决相关问题。

2016年5月11日，美国在华盛顿召开了第一届高级专家小组会议讨论网络空间国际安全问题，这为中国进一步阐述己方观点以及双方就网络安全国家行为规范和其他主题达成共识提供了平台。国务院带领来自国防部及其他美国政府机构代表组成的美国代表团出席了会议。该高级专家小组帮助我们就国际法和国家行为相关的自愿性网络规范达成了更广泛的国际共识。我们鼓励中国和我们一道敦促其他国家认同G20（二十国集团）等国际论坛提出的原则，而且我们会持续深入地开展这项工作。

为实现习近平主席访美期间达成的其他承诺，中美于2015年12月1日在华盛顿就网络犯罪和其他相关问题首次开展部长级对话。国防部长洛雷塔·林奇（Loretta Lynch）和国土安全部长杰·约翰逊（Jeh Johnson）与中国国务委员郭声琨共同主持了中美就网络犯罪和相关问题开展的首次高层联合对话，增进了相互了解，加强了有关执法和网络保护问题方面的合作。第二次对话定于下月在北京举行。

同时，关于双方政府不得或蓄意支持通过网络盗窃谋取商业利益的承诺，副国务卿布林肯（Blinken）上月对外交委员会全体成员表示，美国正密切关注，确保后续采取行动践行该承诺。

习近平和奥巴马去年举行的高峰会谈集中讨论了具体行动和安排，确保中国对其承诺负责。尽管这些承诺无法完全化解我们与中国在网络问题方面的分歧，但我们已在解决中美双边关系中最棘手问题之一方面向前迈出了一步。

G20 安塔利亚峰会

2015年11月，G20领导人齐聚土耳其安塔利，共同探讨和推动全球经济面临的一系列关键问题。在峰会闭幕之际，G20领导人联合发布了公报，明确支持美国主导的国际网络稳定愿景及其支柱。

此外，G20领导人发表了声明，明确表示“各国均不得或支持基于信息和通信技术（ICT）窃取知识产权，包括商业机密或其他机密商业信息，从而为公司或商业部门谋取竞争优势。” 他们还特别强调了“联合国在制定规范时发挥的核心作用”，着重介绍了UN GGE的工作及其2015年报告。

G20领导人确定了我们的整体框架，指出他们“确认国际法，尤其是《联合国宪章》，适用于基于ICT的国家行为，将共同捍所有国家应遵守基于ICT的负责任国家行为规范这一原则…”

G20领导人发布的公报体现了对我们的网络空间稳定提升方案的大力支持。然而，后续还有很多工作要做。美国将继续与G20国家一道在其他双边和多边合作中发挥作用，推广和宣传关于网络空间负责任的国家行为的政策公告。

欧洲安全合作组织

在美国和其他志同道合的国家的牵头组织下，欧洲安全合作组织（OSCE）的57个成员（包括西方盟国、俄罗斯和其他前苏联成员国），2016年3月就一系列更为广泛的信心建立措施（CBM）达成了共识。这些CBM（包括五项新措施）在OSCE 2013年公布的成员国正在实施的11项措施的基础上构建。

最初的11项CBM侧重于实现透明性和采取机制缓解冲突。例如，一些CBM呼吁参与国提供联络点，可使外国政府发现从其领土发起的网络事件时与之联系，并采取协商调解机制。另外五项CBM更像是协同措施，主要解决关键基础设施网络安全问题和构建公私伙伴关系。

要确保关键基础设施（包括通信部门的设施）的安全性和弹性，需要网络、物理和人类因素的相互配合。由于大部分关键基础设施由私有部门持有，公私伙伴关系对于加固关键基础设施尤为重要。鉴于关键基础设施比较分散，这些工作的开展需要国际协作。今年，我们在继续加强落实之前的CBM的同时将开始实施新措施，而所有这一切都基于我们在该领域以及其他类似论坛与很多国际伙伴进行的合作。同时，我们也希望CBM在OSCM取得的进一步成功会成为说服其他地区性安全组织部署CBM的范例。

除了与政府组织协同工作，国务院还与政府之外的各利益相关方建立了广泛合作关系，这些利益相关方在维护和推动美国提倡的网络安全愿景方面发挥了关键性作用。这些非政府利益相关方往往是我们出席关键会议（进行密切协商）的代表团的一些成员。而且，在重大事件前后，我们通常会与这些利益相关方进行沟通，听取他们的意见，向其传达我们的活动。将来，我们还会与利益相关方群体进行广泛协作，密切关注重大安全会议，如近期在荷兰海牙召开的网络空间全球会议（上次在韩国首尔）。

政策挑战：各方对互联网见仁见智，难有定论

我们落实网络空间战略面临的一大挑战是各方对互联网见仁见智，难有定论。美国和更为广泛的国际社会中的很多国家都支持互联网上流量开放和数据传输，从而促进经济发展、保护人权和推动创新。美国提倡多方利益相关方方案，其中政府、私有部门、民间组织和技术及学术群体可通力配合采取包容、透明、共识驱动的流程解决技术和政策方面的威胁。

中国的全球网络空间治理方案由以下愿望推动：希望维持国内稳定、维护国内网络空间主权、反对其所谓的新兴网络军备竞赛以及网络空间军事化。中国一直倾向于考虑网络信心建立措施，确认国际法适用于网络空间，但一直不愿更为明确地承认武装冲突法和其他战争法规的适用性，因为中国认为这样会使国家利用网络工具作为战争武器合法化。

鉴于此，中国制定了一系列外交政策，强化了中国传统外交政策的核心原则，即不干涉其他国家内政、维护网络空间主权以及不率先使用武器。中国将广泛深入的网络审查制度（包括中国国家防火墙等技术）视为打击破坏稳定的国内外影响的必要措施，而且中国还在国际上推广这一理念。此外，中国还极力推行“网络治理”新手段，特别是制定了新的约束规定限制“信息武器”的开发、部署和使用，加强言论和内容控制，企图替代《欧洲委员会网络犯罪公约》（又称《布达佩斯公约》）框架，提升政府相对于其他利益相关方的作用，还可能赋予联合国对恶意网络活动追踪溯源和响应的权利。美国及其伙伴试图将网络政策重心放在防范网络和网络基础设施面临的威胁以及网络工具导致的其他物理威胁上，而中国还强调了在线内容带来的威胁。除此之外，美国认为所有利益相关方应该能够参与制定互联网相关的公共政策，而中国的一些政策与美国所持的这种观念存在显著差异。

俄罗斯的全球网络空间治理方案侧重于维护国内稳定及“信息空间”主权。尽管俄罗斯与中国和上海合作组织的其他成员联合编写了《行为准则》，然而，随着《布达佩斯公约》招致了很多批评，俄罗斯最终想出台一份新的国际网络公约。

不过，俄罗斯对我们提倡的国际法适用于网络空间国家行为以及出台和平时期国家行为的自愿性非约束规范表示了认同。俄罗斯已承诺同美国联合制定第一套双边网络信心建立措施，且在2013和2016年多边机构—欧洲安全与合作组织中制定第一套网络信心建立措施。

我们采取了一系列外交手段打压其他网络空间政策理念，例如加入多个多边组织、直接双边合作，对各类国家和非国家攻击者提高警惕。下面我将介绍美国目前面临的一些技术挑战和威胁以及我们应对和防范网络事件采取的工具。

应对和防御网络事件

不断发酵的网络威胁

针对美国国家和经济安全的网络威胁在频率、规模、复杂度和严重程度方面一直呈现不断上升态势。2015年引人注目的网络事件包括：1. 医疗保险公司Anthem的IT系统遭遇入侵，造成数百万客户的账户信息泄露；2. 人事管理局的系统遭到非法入侵，导致大约2200万份个人文件失窃；3. 黑客对乌克兰电网发动空前攻击，切断了数十万客户的电力供应。

总的来看，用以支撑美国政府、军事、商业和社会活动的非保密性信息和通信技术网络目前仍面临间谍和中断风险。在我们上月提交的战略中，国务院表示目前任何特定攻击者均有可能对我们发起灾难性攻击。美国情报界预计各种攻击源可能会开展一波儿中低风险的网络行动，会对美国经济竞争力和国家安全带来叠加影响，对美国联邦部门和私有部门的基础设施带来风险，以及侵犯美国知识产权持有人的权利和美国公民隐私。

二月，美国国家情报总监詹姆斯·克莱佩（James Clapper）向美国国会阐述了美国情报界发布的《2016全球威胁评估报告》，称“由于入侵成本相对低廉，渴望获得收益且无需承担严重后果，很多攻击者仍可毫无畏惧地对网络空间进行勘察、开展间谍活动，甚至是攻击。”他特别强调了主要国家攻击者、达伊沙（DAESH）等非国家攻击者以及正在研制和使用网络工具的犯罪分子发起的恶意网络活动，如利用勒索软件进行勒索和借助恶意软件攻击政府网络。

美国情报界将会持续监测在等级和规模上都有所上升的恶意网络活动，通过衡量失窃或删除的公司数据量、泄露的个人身份信息或美国受害者的恢复成本来评估这些活动。由于能够获利，攻击者可能仍有很强动机发动网络攻击和网络间谍活动。

网络威胁应对工具

美国采取整体政府方案应对技术挑战，利用各种国家权力手段和相应政策工具，如依法酌情采取外交、执法、经济、军事和情报手段。

美国认为网络空间威慑最好通过结合“拒止式威慑”和“强加成本式威慑”实现。“拒止式威慑”指通过向潜在攻击者证明美国可阻止其达到攻击目的而削弱其利用网络能力攻击美国的动机。“强加成本式威慑”指威胁恐吓或采取行动惩罚对美国进行恶意网络活动的攻击者，对其强加成本。值得注意的是，采取一刀切的方式阻止或应对网络威胁是行不通的，而应根据特定威胁的特征采取最合适的方式。

总统可利用多种手段进行“拒止式威慑”，例如，利用一系列旨在提升美国政府和私有部门计算机系统的安全和恢复能力的政策、法规、自愿性标准，以及事件响应能力和某些执法权力。

对于强加成本，总统可利用美国政府提供的多种响应方法。

若攻击者的行为难以容忍，可通过外交手段传达给攻击者，寻求盟国和志同道合国家的支持、跟他们进行更广泛合作或寻求他们的帮助，从而解决共同面临的威胁。对友好国家及潜在敌对国家

采取外交措施已成为了美国应对大型国际网络事件的一种常规手段。从长远来看，美国对于网络空间负责任国家行为原则（包括和平时期规范）的推广工作旨在与志同道合的国家达成更广泛共识，为携手应对不负责任的国家行为奠定基础。

我们可借助执法手段调查美国境内和境外的犯罪行为，对恶意网络攻击者进行起诉。国际合作对于网络犯罪调查至关重要，鉴于此，美国在《布达佩斯公约》中提倡实现网络犯罪实体法和程序法国际协调一致，通过G7 24/7网络建立用于维护数据和共享信息的非正式通道，加强援助伙伴关系帮助发展中国家。

经济手段，如金融制裁，可作为更广泛的美国战略的一部分，用于更改、限制和谴责恶意攻击者的网络空间行为。自从2015年1月，总统就制裁朝鲜开展恶意网络活动向财政部长下达了指示。第13687号行政命令的发布在某种程度上是对索尼影视娱乐公司遭遇的挑衅性和破坏性攻击作出响应，而第13722号行政命令及近期签署的2016年《朝鲜制裁及政策强化法案》旨在应对朝鲜对美国发起的重大网络安全损害活动及其他恶意行为。除了授权对朝鲜进行制裁，2015年4月，总统签发了名为《冻结从事重大恶意网络活动人员的财产》的第13694号行政命令，授权对开展恶意网络活动为美国的国家安全、外交政策、经济健康状况或财务稳定造成重大威胁的个人进行制裁。

军事能力提供了一系列阻止和应对恶意网络活动的重要方法。国防部将持续构建网络能力和提升网络防御和威慑状况，例如，国防部正在组建网络任务部队，该部队已开始利用其自身能力保护国防部网络、防止国家遭遇有重大恶劣影响的网络攻击，实现网络空间综合效益，从而为作战计划和应急行动提供支持。此外，今年年初，国防部长阿什顿·卡特（Ashton Carter）称美国军队正在利用网络工具中断达伊沙（DAESH）的指挥控制系统，为其网络带来不利影响。

情报能力也是总统检测、应对和阻止恶意网络空间活动的一项重要手段，尤其是考虑到对此类恶意活动追踪溯源，查明背后动机时面临的特有挑战。

即便有了各种各样的工具，阻止网络威胁仍是一项很大挑战。考虑到网络空间的独有特性，美国将持续对恶意网络攻击者施加更多影响。

能力建设

除了上述手段，美国在该领域的国际伙伴提供的能力和实力也能极大地提升我们应对外国网络威胁和打击跨境网络犯罪的能力。因此，国务院正在与各机构、各部门以及盟国和多边合作伙伴协同配合，为外国政府（尤其是发展中国家）构建网络防御能力，保护他们的网络以及在其境内调查起诉网络犯罪分子。此外，国务院还积极推进援助合作，包括通过双边和多边合作开展联合网络能力建设活动。

例如，2015年，美国和荷兰一道搭建了全球网络专业知识论坛，旨在为各国、国际组织和私有部门提供交流网络能力建设相关的最佳实践和专业知识的全球平台。美国与日本、澳大利亚、加拿大、非洲联盟委员会和赛门铁克公司联合开展了四项网络安全和网络犯罪能力建设活动。此外，国务院还向欧洲委员会、美洲国家组织和联合国网络犯罪全球项目提供援助，向发展中国家提供能力建设支持。很多传统的双边执法培训计划越来越倾向于纳入网络部分，例如培训处理电子证据的调查员和检察官。在我们对其他国家提供的打击知识产权犯罪执法培训中，数字盗窃占很大比重。

能力建设方面的另一个例子：国务院通过国际麻醉品和执法事务局管理全球五所国际执法学院和一家区域培训中心。这六所机构每年为来自全球近85个国家的执法人员提供培训和指导。国际执法学院的培训计划涵盖各种广泛的网络调查培训基础课程和高级课程，由美国特勤局和其他机构的领域专家授课，并与高级刑事司法人员进行政策层面的相关讨论。这可极大地提升国际执法社区联合打击网络犯罪的能力。

国务院将致力于通过持续开展能力建设活动这一行之有效的方式打击国际网络威胁，提升国际网络稳定。

展望未来

目前，全球网络威胁环境快速扩展，人们越来越依赖信息技术，使用的智能设备越来越多，而且很多发展中国家仍处于网络成熟的早期阶段，恐怖分子及其他犯罪分子采取日益复杂的信息技术。可见，网络安全仍是美国面临的一项严峻挑战。因此，国务院推测，在可预见的未来，我们将在网络为主的外交和能力建设方面持续加大投入。

国务院将持续牵头推动各国就当前国际法适用于网络空间国家行动达成的共识，帮助各个国家培养技术能力和出台相关法律和政策为制定某些和平时期政策提供支持，确保他们切实履行在国际网络行为规范的承诺。

来源：https://2009-2017.state.gov/s/cyberissues/releasesandremarks/257719.htm，2018年7月25日。

C. 关于提升网络安全的总统行政命令

2017年5月11日，总统特朗普签发了提升网络安全的行政命令。以下是摘自《白宫新闻通讯》的行政命令概要介绍。如欲了解该行政命令，请访问：https://www.whitehouse.gov/the- press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal:

概况介绍—总统特朗普保护美国的网络基础设施—2017 年 5 月 12 日

“为真正确保美国安全，我们确实要将网络安全作为一件头等大事。”

—唐纳德·约翰·特朗普

美国的网络非常脆弱：美国现在面临来自网络空间的毁灭性攻击。总统正在兑现其竞选承诺，即确保美国安全，尤其是网络安全。

- 对于电子犯罪和外国特工来说，联邦政府是个有利可图的攻击目标，因此多年来一直是网络入侵的受害者。
- 美国关键网络基础设施的网络安全：无论是公共还是私有部门，网络基础设施一直饱受国内外攻击入侵。
- 每天我们都能看到美国大公司遭遇外国威胁入侵的报道。

采取措施加固美国的网络防御：总统唐纳德·约翰·特朗普签署了行政命令采取必要措施修复网络安全漏洞。

- 为确保国防安全，我们着重强调联邦网络安全。
    - 美国当前的政策是要像联邦企业一样管理网络安全风险。
    - 总统要求整个政府采用国家标准与技术研究院（NIST）网络安全框架，确保向私有部门推荐的同等高标准全面落地实施。
    - 该行政命令要求各部门负责人开始规划实现联邦行政部门信息技术的成熟现代化，这是一项完善网络风险管理的长期任务。这项IT现代化工作将由白宫主导，由总统的美国科技委员会牵头实施。
    - 各内阁部长和部门负责人将负责管理管辖范围内的网络风险，确保全面实现问责制。
    - 优化政府的信息系统，在确保安全的同时理出现代化、安全、可行性、成本和创新的优先级。在这方面，总统强调要优先保障共享业务的安全。
    - 具体行动如下：
        - 要求每个部门都采取业界标准的NIST网络安全框架（简称“框架”）管理网络安全风险。
        - 要求所有部门在今后采购时优先考虑共享IT服务，最大限度地符合法律要求。
        - 要求所有部门明确就缓解或容忍网络安全风险作出的决策，包括不及时缓解已知漏洞的任何决策，并输出实施“框架”的行动方案报告，并向国土安全部和管理和预算办公室（OMB）提交该报告。

- 要求国土安全部部长和管理和预算办公室主任评估这些报告的完备性，从而全面衡量联邦政府的整体网络安全风险管理措施是否充分，并提供法律、整合和预算方面的修改意见，从而充分保护行政部门项目。
- 要求国防部长和国家情报总监对国家安全系统采取同等防护措施。
- 授权白宫的美国科技委员会启动联邦IT成熟现代化规划流程，包括向一个或多个统一网络架构和电子邮件等共享服务过渡的技术可行性和成本效益。

- 政府和业界携手，共同保护国家的关键基础设施。
  - 由于私有部门在我国的基础设施方面发挥重要作用，因此，行政命令将更为深入且更具协作性的公私伙伴关系作为威胁评估、检测、防御和缓解的重点。
    - 总统坚持实践出真知的原则，与基础设施提供商协同配合，通过培训等活动提升国家的网络攻击防御能力。
    - 鼓励主动遵守合规要求和协同配合，如联合防御拒绝服务攻击等。
  - 具体行动如下：
    - 制定明确的政策，阐述联邦政府在帮助国家的关键基础设施负责人和运营商管理网络安全风险时可运用的权利和能力。
    - 要求民间、军事和情报机构说明在关键基础设施实体面临可导致灾难性影响的最高攻击风险时可利用哪些法律权利和能力向其提供网络安全风险管理支持。
    - 要求这些机构主动向这些实体提供支持，与他们直接配合，并就联邦政府的网络安全工具包的任何缺陷（如法律、政策或预算缺陷）向他们征求反馈意见和输入。
    - 评估联邦政府为支持市场驱动的风险管理决策而在提升关键基础设施网络安全风险管理做法的透明度方面所做的工作。
    - 召集私有部门解决复杂的物联网网络安全挑战，从应对物联网设备发起的拒绝服务攻击着手。
    - 提升国家对导致长时间断电的网络攻击的响应和恢复能力。
    - 缓解国防部武器平台和国防工业基地面临的网络安全风险，如敏感部门使用的国外产品的相关风险。
- 该行政命令将提升我国的威慑态势，构建国际联盟联合防御全球网络攻击。
  - 白宫、国务院及其他相应联邦机构将持续与其他国家并肩合作，推动实现开放、稳定、安全且互联互通的全球互联网。互联网起源于美国，因此在持续助力全球各国以及世世代代的未来发展时也应反映美国的价值观。
    - 国务院应制定全球网络安全合作战略，简要介绍美国与其盟国的前进之路。
  - 必须解决网络安全从业人员的全球供应短缺。总统承诺制定计划，发现、培养和留住出色的网络安全人才。
  - 不允许其他国家通过网络攻击、间谍或其他恶意行动将我们置于危险境地。
  - 具体行动如下：
    - 制定战略方案阻止攻击者和更好地保护美国人民免受网络威胁。
    - 制定国际网络安全合作战略，概要介绍美国如何采取主动措施且与合作伙伴通力配合打击和阻止恶意攻击者、推广全球网络稳定框架、确保实现开放、安全且互联互通的互联网，促进美国和全球的经济和社会进步与发

展。

- 全面评估美国的公私部门在培养和协助世界一流的军事和民事网络安全人力方面所做的支持工作，并与国外政府在这方面的工作进行对比。

来源—白宫概况介绍：https://www.whitehouse.gov/briefings-statements/president- trump-protects-americas-cyber-infrastructure/，2018年7月25日。

D. 各部门对提升网络安全的行政命令的响应

本节介绍美国的政府部门对特朗普总统的网络安全行政命令的响应。若查看这些响应，请登录国务院和国土安全部的网站：

https://www.state.gov/s/cyberissues/eo13800/
https://www.dhs.gov/executive-order-strengthening-cybersecurity-federal- networks-and-critical-infrastructure

1、关于总统通过国际合作保护美国网络利益的建议（节选）

美国的网络空间愿景和网络空间政策方案

美国的网络安全利益、经济持续繁荣和领先地位以及自由民主价值观的主导地位均取决于我们是否能够确保网络空间的安全、互联互通和恢复能力。美国的创新、经济增长和竞争优势依赖于互联网的全球信任度以及对网络空间中的网络、平台、和服务的安全性和稳定性的信任度。鉴于网络空间的全球性，要实现美国政府的目标必须与其他国家密切协作和配合。相应地，美国将在尊重隐私和防止中断、诈骗和盗窃的同时通过网络空间全球协作促进实现其开放、互联互通和安全可靠互联网的愿景，从而推动创新、沟通和经济繁荣。美国政府旨在通过国际参与确保互联网及其他互联网络和技术仍可成为后人的宝贵工具。

美国的网络空间政策目标

通过与国外伙伴和盟国协调配合而且让利益相关方适当参与，美国旨在通过达成以下五个目标和采取相应措施实现网络空间愿景：

1. 促进国际稳定，减少利用网络空间导致的冲突风险：

a. 推广关于何为可接受和不可接受的网络空间国家行为以及国际法对网络空间适用性的国际承诺。

b. 开展双边和地区安全活动，制定和实施网络信心构建措施。

c. 推广协作框架，支持对恶意国家攻击者和国家支持的恶意活动进行阻止和强加成本。

2. 发现、检测、挫败和阻止网络攻击者；对这些攻击者导致的威胁进行防御、响应和恢复；提升包括关键基础设施在内的全球网络生态系统的恢复能力：

a. 加强信息共享，如通过自动化和计算机安全事件响应团队（CSIRT）渠道；

b. 管理网络危机，有效应对重大网络事件；

c. 加强合作，管理不断演变的国际环境的全面网络风险，增强公私国际协作从而保护关键基础设施，构建恢复能力；

d. 加强全球网络安全教育、培训和员工队伍培养，应对当前和未来的网络安全挑战；

e. 优先考虑强有力的执法合作；

f. 推动军事网络合作；及

g. 进一步加强与合作伙伴和盟国在敏感网络情报问题方面的合作。

3. 支持开放且互联互通的互联网，保护和自由行使人权及保护跨境数据流：

a. 保护多边论坛和国际论坛上对开放且互联互通的互联网的访问（面临安全挑战）；

b. 利用志同道合的国家组成的现有联盟，通过外交协调推动互联网自由；

c. 支持制定国际互联网自由计划，为民间社会组织提供资金支持使其开展技术开发、数字安全培训、政策宣传和应用研究活动。

4. 确保非政府利益相关方在决定网络空间治理方式时发挥至关重要的作用：

a. 提倡采取现有的多利益相关方互联网治理系统管理关键互联网资源，不要引入新的自上而下或政府间互联网治理机制；

b. 支持持续制定、采取和使用基于共识、行业主导且可互用的自愿性技术标准。

5. 提倡构建支持创新和考虑网络空间全球化特性的国际监管环境：

a. 采取一种灵活的风险管理方案，确保全球市场的网络安全；

b. 杜绝使用不正当的市场准入限制，包括数据本地化要求；

c. 为美国企业营造公平竞争的全球市场；

d. 鼓励私有部门创新，防范整个数字化生态系统面临的安全风险；

e. 维持强大且平衡的知识产权保护系统，包括推动创新的同时充分有效地执行知识产权法。

来源—完整报告链接：
https://www.state.gov/documents/organization/282224.pdf，2018年7月25日。

2、关于总统阻止攻击者和更好地保护美国人民免遭网络威胁的建议（节选）

战略方案

通过防御和保护关键基础设施和其他敏感的计算机网络并确保有效缓解恶意网络活动并及时恢复来实现拒止性威慑（Deterrence by Denial）须为美国威慑方法的基础。美国将持续加强努力，阻止攻击者通过开展恶意网络活动获益。

与此同时，美国意识到仅仅通过网络防御并不足以阻止顽固老练的国家资助的攻击者。此外，美国也采取了一项新举措，通过强加成本及其他措施进一步阻吓国家攻击者。

美国进行威慑的最终目的是：

- 让针对美国及其伙伴和盟国的武力型网络攻击长期消失；
- 长时间内显著减少违反美国利益的不同程度的破坏性、非武力型恶意网络活动。

总统已拥有各类网络和非网络方案用于阻止和应对构成使用武力的网络活动，充分显示美国能够对开展此类恶意活动的攻击者强加高额成本对于维护和加强威慑来说至关重要。

对于未构成使用武力的各项活动，美国应在必要时与志同道合的伙伴携手合作对那些

开展重大恶意网络活动损害美国国家利益的外国政府施加迅速、透明，且代价高昂的影响。这种方法包括如下要素：

1. **制定政策，明确美国何时可施加影响**：该政策应说明美国政府判断要阻止的恶意网络活动类型的衡量标准。必须将该政策的要点传达给公私部门从而达成威慑效应。

2. **定义这些影响**：美国应依据其义务和承诺制定一系列方案施加低于武力使用的快速、透明且代价高昂的影响，从而应对需强有力响应的安全事件，避免对威慑效应带来消极意义。制定方案时，美国应评估并尽力降低这些方案的潜在风险和成本。

3. **规划政策，明确如何施加影响**：除了明确要施加的影响，美国应在行动之前、期间和之后进行跨部门政策规划。此规划应涵盖制定相应的跨部门响应规程，有助于确保对各种事件采取一致响应，并协助管控升级风险。

4. **建立伙伴关系**：若我们与合作伙伴共同配合施加影响，将取得更加显著的效果，传达更有威慑性的消息。合作伙伴国家可本着自愿原则在其它国家遭遇严重恶意网络事件时提供响应支持，包括情报共享、溯源分析、事件发生后公开声明提供响应行动支持，和/或实际参与对恶意政府施加影响。

来源—完整报告链接：https://www.state.gov/documents/organization/282253.pdf，2018 年 7 月 25 日。

3、为面临最高风险的关键基础设施提供支持

国土安全部与相关的行业对口机构协同配合，每年发现并维护符合第13636号行政命令《提升关键基础设施网络安全》（基于风险的方法）第9节标准的关键基础设施实体清单。这些实体拥有或运营关键基础设施，遭遇的网络安全事件可能会对公共健康或安全、经济安全或国家安全带来国家或区域层面灾难性影响。

国土安全部与国防部、司法部长、国家情报总监、联邦调查局局长以及相关行业对口机构负责人协调配合，确认联邦政府为符合第9节标准的实体提供网络安全支持的权利和能力。此外，国土安全部及其伙伴让这些实体参与评估如何利用这些权利和能力支持网络安全风险管理工作。

工作过程中的发现和建议已上报给总统，从而为符合第9节的实体提供更好的网络安全风险管理支持工作。以下是具体发现和建议：

- 成立国土安全部计划办公室，加大对符合第9节的实体的支持，加强跨部门支持协调。
- 加强对敏感信息的访问控制；
- 重新评估这一方法，探讨一项更偏向职能的方案用以识别符合第9节的实体。
- 加强事件交流与协调。
- 加强与符合第9节的实体的跨行业信息分享。
- 探讨如何鼓励私有部门合理保护其信息和信息系统，如向政府上报网络安全事件。
- 拟定一份公私合作计划，防御供应链漏洞，减少网络安全厂商的风险。
- 探讨缓解网络风险的新方法。

国土安全部将带领跨部门工作组集中落实这些意见，并让符合第9节的实体参与其中，确保其了解相应计划和可用资源。

来源—完整报告链接：https://www.dhs.gov/publication/support-critical-infrastructure- greatest-risk-section-9-report-summary，2018年7月25日。

4、为市场透明性提供支持

国土安全部和商务部协调配合，评估现有联邦政策和实践是否能充分提升网络安全风险管理做法的市场透明性，重点关注公开上市的关键基础设施实体。在短短的90天内，通过多部门协作输出报告；私有行业进行有限参与；对二手来源的资料进行审查，确保当前的联邦政策和做法能充分提升网络安全风险和风险管理实践的透明性，保证透明制度在推动实现政策目标方面发挥更大作用。审查涉及96个来源的资料及数个联邦政策和实践。相关发现会让我们对透明制度的有效性有深刻了解，揭示当前的联邦政策和做法是否充分，并为后续有关市场透明性和网络安全成效提升的探讨提供参考。

来源—完整报告链接：https://www.dhs.gov/publication/supporting-transparency-marketplace-summary，2018年7月25日。

5、对僵尸网络和其他自动分布式威胁的抗打击能力

国土安全部与商务部密切配合，牵头制定开放透明的流程，识别和推广相关利益方的行动，提高互联网和通信生态系统的抗打击能力，鼓励开展合作，从而实现大幅减少自动的分布式攻击威胁的目标。

《面对僵尸网络和其他自动化分布式攻击威胁，提高互联网和通信生态系统的抗打击能力》报告总结了在减少僵尸网络威胁方面的机遇和挑战，列明了政府和私有部门为减少自动的分布式攻击威胁而采取的相应行动。该报告主要阐述六个主题：

- 自动的分布式攻击是个全球性问题。
- 有效工具已面世，但尚未广泛使用。
- 应在产品生命周期的每个阶段实施保护。
- 需开展安全教育，培养安全意识。
- 应出台更为有效的市场激励措施。
- 自动的分布式攻击是整个生态系统面临的一大挑战。

该报告基于利益相关方和专家的广泛输入编写，明确了关于提升互联网生态系统弹性的五个相辅相成的目标，推荐采取的行动包括，应继续推进或扩展当前活动并采取新举措，如尽力提升软件组件透明性和开展公共宣传活动提升物联网安全意识。

来源—完整报告链接：https://www.commerce.gov/page/report-president-enhancing-resilience-against-botnets，2018年7月25日。

6、针对电力中断事件的响应能力评估

国土安全部也与能源部紧密配合对重大网络事件导致的长时间电力中断的潜在影响范围和持续时间进行评估，检验美国是否充分准备好合理管理和缓解网络安全事件对电力部门的影响以及工作中是否存在不足。我们得出的评估结果是，总体来看，美国已做好充分准备管理大部分电力中断，只有特定区域在对网络攻击的灾难恢复考虑和新威胁应对方面存在不足。

为了弥补这些不足，此次评估过程中，我们简要介绍了提升各级官员的公共传播能力，阐述网络安全技术专业知识和信息共享、以及整合和提高针对此类事件导致的长期中断和潜在后果和影响的规划和分析能力。此外，将网络安全纳入早期系统设计阶段，在这方面投入资金，尤其是小型设施。培养强大的员工队伍会对国家的电力基础

设施提供全面防范支持。

来源—完整报告链接：https://www.dhs.gov/publication/section-2e-assessment-electricity-disruption-incident-response-capabilities，2018年7月25日。

7、美国网络安全队伍培养

商务部和国土安全部对美国过去在培养网络安全队伍方面工作的范围和充分性进行了评估，输出了报告提供相关发现和建议，阐述如何为公私部门的未来网络安全人才的可持续发展提供支持。为此，我们召集了国防部、人力部、教育部、人事管理局、国家科学基金会等相关部门的网络安全教育和队伍培养专家讨论如何增加和扩展人才培养渠道。为征求更广泛意见，我们还召开了公共和国家层面的研讨会并公开发布信息征询函。

商务部的国家标准与技术研究院（NIST）和国土安全部主导的跨部门工作小组将评估结果汇总为报告，提交给总统。该报告包含四个关键发现：（1）需尽快和持续提升美国网络安全劳动力；（2）开展再培训，让更多的妇女、少数群体和资深人士参与其中，从而扩展网络安全队伍的资源池；（3）缺乏初级和中级网络安全教师、高等教育师资以及培训讲师；（4）缺乏网络安全劳动力职位需求、教育和培训计划相关的全面可靠数据。

该报告为解决以上发现提供了5条建议：

- 联邦政府应牵头在全国范围内大张旗鼓地发起行动号召，吸引注意力，调动公私部门的资源，解决网络安全劳动力需求。
- 美国政府应重视和提议对卓有成效的高质量网络安全教育和人力培养计划进行长期授权并划拨充足经费。
- 公私部门应推动学习环境的转型、升级和维持，通过再培训、实操培训、体验式学习和寓学于工相结合的培训方案培养富有干劲的多元化网络安全劳动力，如实行学徒制和实习制、交流研究经验、制定合作教育计划、打造虚拟培训和评估环境以及对网络安全教育和培训提供更大经济援助。
- 公私有部门应采取措施将教育培训与企业对网络安全人员的需求相协调，如利用《国家网络安全教育倡议指南（NICE）网络安全劳动力框架》，制定网络安全职业模型途径，搭建信息交流中心就网络安全员工发展教育、培训和员工发展计划和活动开展讨论。
- 公私部门应制定和采取措施，对接受过教育和培训且能承担网络安全任务的员工数量和质量进行追踪和确认，从而证实网络安全人员投资的效果和影响。

来源—完整报告链接：https://www.dhs.gov/publication/supporting-growth-and- sustainment-nations-cybersecurity-workforce，2018年7月25日。

II. 国土安全部的战略和指南

A. 国土安全企业的网络安全战略

2018年5月15日，国土安全部发布了该战略。以下为《网络安全战略概况介绍》。如欲查看完整文档，请登录：https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf.

美国国土安全部的网络安全战略

导言

我们依靠网络空间为日常生活带来便利、提供关键服务和促进经济繁荣。在美国国土安全部，我们相信可实现安全且有弹性的网络空间。国土安全部与联邦政府的关键伙伴、州政府和地方政府、业界和国际社区携手配合，发现和管理国家网络安全风险。《国土安全部网络安全战略》阐述了国土安全部风险管理方案的五个基本点，为履行网络安全职责和利用国务院的各种能力提升网络空间的安全和弹性提供了框架。

为降低国家网络安全风险，我们需采取一项创新方案，充分利用国务院及整个网络安全社区的集体能力。国土安全部将努力深入了解国家的网络安全风险状况，让关键伙伴参与其中从而共同防御网络漏洞和威胁，避免不利影响。我们将持续努力减少和管理联邦网络和关键基础设施的漏洞，提升攻击防御能力，并优先通过执法干预减少网络犯罪活动的威胁。我们将设法缓解已发生的网络安全事件产生的影响。最终，我们会与国际网络安全社区合作，采取以下措施提升整个网络生态系统的安全和恢复能力：1.应对全面挑战，如日益膨胀的全球供应链；2.加强国际合作阻止恶意网络攻击者和开展能力建设；3.加强研发和提升网络员工能力。

通过这些工作，我们会努力为美国人民营造安全和安定的网络空间，确保实现开放、安全、有弹性且互联互通的互联网。

国土安全部的网络安全目标

支柱 1：识别风险

目标 1：评估不断演进的网络安全风险。

我们将了解不断变化的国家网络安全风险状况，据此开展风险管理活动，并理清活动的优先顺序。

支柱 2：减少漏洞

目标 2：保护联邦政府的信息系统。

我们将减少联邦机构的漏洞，确保他们达到合理的网络安全级别。

目标 3：保护关键基础设施。

我们将与关键利益相关方合作，确保合理管理国家网络安全风险。

支柱 3：降低威胁

目标 4：防范和阻止犯罪分子对网络空间的使用。

我们将通过打击跨国犯罪组织和技术熟练的网络犯罪分子减少网络威胁。

支柱 4：缓解影响

目标 5：有效应对网络事件。

我们将通过协调一致的社区级响应活动，尽量缓解潜在重大网络事件的影响。

支柱 5：落实网络安全成果

目标 6：提升网络生态系统的安全和可靠性。

我们将支持各种政策和活动，提升全球网络安全风险管理。

目标 7：加强对国土安全部网络安全活动的管理

我们将统一开展部门级网络安全工作，理清各项工作的轻重缓急。

我们的网络安全战略正在付诸于行动

- 2017年10月，国土安全部发布了《约束性操作指令18-01》，要求联邦机构采取具体措施提升邮件和网络安全，包括引入基于域的消息认证，报告和一致性（DMARC）。
- 2017年“想哭”恶意软件攻击横扫全球期间，国家保护和计划司（NPPD）与其他机构和业界配合，帮助确保美国的医院系统不受影响，并公开发布了技术警报，协助防御者挫败恶意软件。
- 2018年1月，美国的移民海关执法局（ICE）、国土安全调查处（HSI）以及拉斯维加斯的司法部查明了一家名为“欺诈至上”（Infraud Organization）组织的36名成员的职责。该组织是一家基于互联网的犯罪企业，大肆买卖窃取的信用卡数据和身份证件，曾导致了超过5.3亿美元的损失。国土安全调查处对此进行了调查，追回了430万份失窃的信用卡账号。
- 2017年7月，美国特勤局通过协同国际执法活动，抓捕了一名被控运营BTC-e的俄罗斯人。2011年至2017年，BTC-e被指在全球进行了价值40亿美元的比特币交易，用以支持网络犯罪分子进行计算机入侵、身份窃取、勒索攻击、公共腐败和毒品销售。研究人员估计近95%的勒索赎金通过BTC-e进行洗钱。
- 2017年10月，美国海岸警卫队（USCG）成立了网络空间部队办公室，旨在组编USCG网络空间作战部队并为其配备人员、装备和提供培训以及制定有关USCG系统和网络运营、维护、防御和保护的网络空间行动政策，利用网络空间能力发起USCG行动，保护海运系统免遭网络威胁。

国土安全部概况介绍来源：
https://www.dhs.gov/sites/default/files/publications/DHS- Cybersecurity-Fact-Sheet.pdf，2018年7月25日。

B. 提升关键基础设施网络安全框架

2014年2月12日，国家标准与技术研究院（NIST）发布了该框架。以下是执行摘要的一部分。有关该报告完整内容，请参见：https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

执行摘要

美国的国家与经济安全取决于关键基础设施是否可靠运行。越来越多的关键基础设施系统接入网络，日益复杂，成为网络安全威胁的利用因素，置国家安全、经济以及公共安全与健康于风险之中。与金融和信誉风险类似，网络安全风险影响着公司的运营成果。它还会损害组织的创新能力，妨碍其争取并留住客户。

为了更好地应对这些风险，奥巴马总统于2013年2月12日颁布了13636号行政命令《提升关键基础设施网络安全》。命令规定，“美国采取（这个）政策，以提升国家关键基础设施的安全与弹性，建立一个有助于提高效率、激发创新、促进经济繁荣的网络环境，同时保障安全、商业机密、隐私与公民自由。”行政命令要求制订一个针对此种风险的自愿实施的网络安全框架，以确定行业标准与最佳实践，帮助组织管理网络安全风险。为实施该政策，此行在政府与私有部门的共同努力下，本框架出台，采用通用语言阐述了如何基于业务需求高效地应对并管理网络安全风险，但并未对企业提出额外的合规要求。

该框架强调用业务驱动引导网络安全活动，将网络安全风险作为组织风险管理流程的一部分。框架包括三个部分：框架核心（Framework Core）、框架对齐结果（Framework Profile）及框架执行层级（Framework Implementation Tiers）。框架核心包括网络安全活动、结果以及关键基础设施领域内常见的参考文献，为各组织拟定对齐结果提供具体指导。通过使用对齐结果，组织可协调网络安全活动，使之与业务需求、风险容忍度及资源相匹配。框架执行层级是一种机制。利用这种机制，组织可审视并了解自身的网络安全风险管理特点。
行政命令还要求框架提供恰当方法，保证个人隐私与公民自由不受关键基础设施相关组织进行的网络安全活动的影响。流程与现实需求总会有分歧，因此，组织可根据框架制定综合网络安全计划，将隐私与公民自由包含其中。

对于各种规模的组织、不同程度的网络安全风险以及网络安全形势，该框架都能提供风险管理原则和最佳实践，使其提升关键基础设施的安全与弹性。框架整合了当今业界普遍有效的标准、指南以及实践，为当今各种网络安全方法提供了大纲与架构。此外，框架引用了国际认可的网络安全标准，对海外组织也适用，国际合作亦可以此为指导增强关键基础设施的网络安全。

然而，框架并未提供一成不变的方法来管理关键基础设施的网络安全风险。各组织面临的风险各异（威胁不同、漏洞不同、风险容忍度也不同），因而应采取不同方式来实施框架提供的方法。它们应确定哪些活动对于关键服务交付意义重大，并对投资进行排序，把钱用在刀刃上。框架的终极目标是降低网络安全风险，对其进行更有效的管理。

框架作为动态文件会根据业界使用反馈进行持续更新并优化。在实际操作中，框架会不断合入之前的应用经验，形成新的版本。这样，对于动态环境中不断出现的新威胁、新风险与新解决方案，它可以轻松面对挑战，满足关键基础设施业主与经营者的防护需求。

使用本自愿框架可加强我国关键基础设施的网络安全，它一方面可从整体上改善国家关键基础设施网络安全的形势，另一方面可为各个组织提供指导。

来源：https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf，2018年7月25日。

III. 司法部安全战略和指南

A. 2018司法部网络数字工作组报告

以下是《司法部网络数字工作组报告》（2018年7月）的一部分。有关该报告完整内容，请参见：https://www.justice.gov/ag/page/file/1076696/download。

导言

2018年2月，司法部长成立了网络数字工作组，要求该工作组解决两个基本问题：司法部如何应对网络威胁？随着这一重要领域快速演进，联邦执法如何能更为有效地完成任务？
该报告将回答第一个问题。首先，报告明确了美国面临的最紧迫的网络威胁：非法海外影响行动的威胁。第一章介绍了何为海外影响行动以及恶意海外攻击者如何利用这些行动攻击美国的选举等民主进程。
本章最后介绍了国务院关于2018年中期选举的防护工作，宣布了国务院的一项新政策，明确一贯的政治中立原则、尊重法规以及维护海外影响行动披露方面的公众信任。

第二章和第三章讨论了我国面临的其他网络威胁，尤其是网络犯罪威胁，介绍了国务院为应对这些威胁正在部署哪些资源以及我们的工作如何推动美国及全球的法制建设。第四章着重介绍了国务院工作的一个关键方面，其中联邦调查局起主导作用：应对网络事件。第五章将视角转向国内，介绍国务院在网络人才培养和聘用方面的工作。最后，该报告在第六章介绍了对某些优先政策的看法和意见，并提出了工作组的未来工作规划。在未来数月内，国务院将基于初始报告中的发现就国务院如何能更有效地管理日益严峻的全球网络挑战向国防部长提供建议。

来源：https://justice.gov/cyberreport，2018年7月25日。

IV. 国防部的战略与指南

A. 国防部网络战略

2018年9月，国防部发布了网络战略。下面是《国防部网络战略摘要》的导言部分。

有关该报告完整内容，请参见：https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

导言

美国的繁荣、自由和安全取决于是否能确保开放可靠的信息访问。互联网可使我们获取更多知识、使用更多业务和服务，提升了我们的能力，丰富了我们的生活。计算机和网络技术为美国保持军事作战优势奠定了基础，使联合作战队在信息获取方面占据优势、可远距离打击敌方，在全球进行指挥控制。

数字时代的到来也为国防部和国家带来了挑战。我们设法保护的互联网具备开放性、跨国性和去中心化特性，因此存在很多重大漏洞。我们的对手由于不敢对美国及其盟国发生武装冲突，便通过网络空间作战窃取我们的技术、扰乱我们的政府和贸易，挑战我们的民主进程，并且对我们的关键基础设施带来威胁。

我们将与中国和俄罗斯开展长期的战略竞争。这两个国家已将竞争扩展至在网络空间中及通过网络空间持续发起活动，为我国及其盟国和伙伴带来长期战略风险。中国正通过从美国的公私部门机构持续窃取敏感数据，削弱美国的军事优势和经济活力。俄罗斯利用网络信息行动对我国人民施加影响，挑战我们的民主进程。朝鲜和伊朗等其他攻击者也采用了类似的恶意网络活动伤害美国人民，威胁美国利益。从全球来看，恶意网络活动的规模和速度持续上升。由于美国几乎所有核心的民事和军事职能都越来越依赖网络空间，这就使得我国面临的风险难以承受且极具紧迫性。

国务院必须在日常竞争中采取网络空间行动，保持美国的军事优势，捍卫美国利益。我们要重点关注那些会对美国的繁荣和安全带来战略威胁的国家，主要是中国和俄罗斯。我们将发起网络空间行动，收集情报，配备军事网络能力以应对危机或冲突。我们要做好事先防御工作，从根本上中断或中止恶意网络活动，包括那些尚未构成武装冲突的活动。至于那些对美国当前和未来保持军事优势有重大作用的网络和系统，我们要提升它们的安全和弹性。我们将与跨部门、业界和国际上的伙伴携手并进，推进我们的共同利益。

在战争期间，美国网络部队将做好准备与海、陆、空及太空部队协同作战，攻击对方软肋、削弱他们的优势，使联合部队其他小组的工作取得更大成效。同样，对方的军事也越来越依赖联合部队视为作战核心的计算机和网络技术。国务院将利用这一技术依赖性获得军事优势。联合部队将引入攻击性网络能力和创新观念用于整个冲突过程的网络空间作战。

《2018 国防部网络战略》体现了国务院应对这方面威胁及解决《网络安全战略和国防战略》规定的网络空间当务之急的愿景。《2018 国防部网络战略》取代了《2015 国防部网络战略》。

美国万万不能掉以轻心，无所作为：我们的价值观、经济竞争实力以及军事优势均处于日益严峻的威胁之下。我们必须坚决捍卫我们在未构成武装冲突的情况下的网络空间利益，确保我们的网络空间运营商做好充分准备，为联合部队应对危机和冲突提供支持。只要我们的海陆空军队、海军陆战队和文职工作人员时刻做好准备，我们就能取得成功。

网络空间的战略竞争

美国的战略竞争者正在通过开展网络行动削弱美国的军事优势、威胁我们的基础架构，阻碍我们的经济繁荣。国务院必须作出响应，对威胁到美国利益的网络活动进行披露、中断和缓解，从而提升关键潜在目标的网络安全和弹性，与其他部门和机构以及我们的盟国和伙伴密切配合。

首先，我们必须确保美国打赢包括网络空间在内的各领域战争的军事能力。这是我们对美国国家安全的基本要求，也是我们确保抵制对美国及其盟国和伙伴的侵略（包括构成使用武力的网络攻击）的关键所在。国务院必须保护自身的网络、系统和信息不受恶意网络活动侵袭，并在被受命之际，准备好保护非国防部国防关键基础设施（DCI）[1]实体及国防工业基地（DIB）[2]实体运营的网络和系统。我们将提前做好防范工作，中断或缓解针对国务院的网络空间行动，我们将互相配合，提升国防部、DCI和DIB网络和系统的网络安全和弹性。

其次，国务院试图采取主动措施挫败和阻止针对美国关键基础设施发起的恶意网络活动，此类活动可能会导致重大网络事件影响国防部的作战准备或能力。我们在这方面的国土防御任务的主要目标是关注外部行动，采取防范措施在威胁到达目标之前将其阻止。同时，国务院也会配合其他联邦部门和机构为公私部门伙伴提供恶意网络活动描述和警告（I&W）

最后，国防部会与美国的盟国和伙伴并肩协作提升网络能力、扩展网络空间联合作战、加强双边信息共享，从而推进我们的共同利益。

国务院的网络空间目标如下：

1. 确保联合部队能够在竞争性的网络空间环境中完成任务。
2. 开展增强美国军事优势的网络空间行动，提升联合部队的能力。
3. 捍卫美国关键基础设施免受恶意网络活动的攻击，这些活动可单独或作为攻击的一部分导致严重的网络事件[3]。
4. 保护国防部信息和系统免受恶意网络活动的影响，包括非国防部网络上的国防部信息；及
5. 扩大国防部与跨部门、行业和国际合作伙伴的网络合作。

保护可实现美国军事优势的民用资产

国防部必须做好准备保护非国防部所有的国防关键基础设施（DCI）以及国防工业基地（DIB）的网络和系统。我们维持DCI防护能力旨在确保这些基础设施能够持续运行和发挥作用，助力国防部在竞争性网络环境中实现目标。我们与DIB实体进行合作，保护国防部的敏感信息，因为这些信息一旦单独或以汇总方式泄露会削弱联合部队的军事优势。作为DIB的行业对口机构以及DIB和DCI的业务伙伴，国防部将：制定和实施网络安全、恢复和汇报相关标准；接到要求或授权时，准备提供直接援助，包括事件发生之前、期间和之后对非国防部的网络提供直接支持。

尾注：

1.“**国防关键基础设施**”指对于全球范围内的军队和作战的规划、支持和维持起至关重要作用的国防部和非国防部的资产（第3020.40号国防部指令）。

2.“**国防工业基地**”指美国国防部、政府和私有部门为满足军事需求而在全球范围内设立的可进行研发、设计、生产和维护军用武器系统、子系统、组件或部件的工业区（《美国联邦法规》第32章第236篇）。

3.“**重大网络事件**”指计算机网络中发生的或通过计算机网络进行的对美国的国家安全利益、外交关系或经济，或对美国人民的公众信任、公民自由或公共健康与安全可能造成伤害的单个网络事件或一系列相关网络事件（第41号总统政策指令）。

来源：https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF，2018年11月1日。

V. 美国网络法规指南

A. 国务院对网络空间国际法的立场

国际法和网络空间的稳定性

下面是美国国务院法律顾问布莱恩·J·依根（Brian J. Egan）2016年11月10日在加州大学伯克利分校法学院所做报告的一部分。有关完整报告内容，请参见：https://2009-2017.state.gov/s/l/releases/remarks/264303.htm。

今天，我站在有着很多全球最大且最具创新性的信息技术公司的硅谷湾区的对面讨论国际法与网络空间稳定性这一主题非常合适。互联网有覆盖广泛而且计算机与其他互联设备之间的连接日益增多，为全球的个人和社会带来了重大经济、社会和政治利益。此外，越来越多的国家攻击者和非国家攻击者正在培养行动能力和实力，旨在通过网络空间达成其目标。遗憾的是，其中很多攻击者利用其能力开展恶意网络活动，在其他国家的领土上制造影响。重大网络事件（其中很多据称是国家支持的事件）频繁成为头条新闻。

鉴于此，我们很有必要问一句：网络空间连接的风险是否有一天会超越为我们带来的好处？我们如何才能避免网络空间成为导致国家间冲突的不稳定因素？

我认为这一天不会到来，然而我们如何维持网络稳定确保连接持续带来收益仍是个关键问题。要实现这一点，我认为国际法会发挥重要作用。

现有的国际法原则是美国在和平时期和武装冲突期间制定的国际网络稳定战略框架的基础。美国的战略框架旨在实现和维护稳定的网络空间环境，让每个国家和个人均可充分实现自身利益，利用互相合作的优势应对共同威胁，避免冲突，而且各国几乎不会发起破坏性行为或互相攻击。

美国战略框架涉及三大支柱，每个支柱均有助于通过减少误解和冲突升级确保网络空间的稳定：1.全球各国确认当前国际法在和平时期和武装冲突期间均适用于各国的网络空间活动。2.就和平时期负责任网络空间国家行为制定一些其他自愿的非约束性规范，当然这需要各国进行沟通协调。3.制定和实施切实可行的信心建立措施，促进各国之间在网络事务合作。今天，我主要详细阐述其中两个支柱：国际法和自愿的非约束性规范。

国际法

2012年9月，我的前任高洪柱（Harold Koh）曾在美国网络司令部的法务大会上发表过名为“网络空间国际法”的演说。他大篇幅阐述了四年来的网络安全情况，主要回答了以下两个问题：1. 现有的国际法原则是否适用于网络空间？2. 网络空间是否是法外之地，人们可以为所欲为？（为了不让你们的心总悬着，我就提前揭晓答案吧，分别是“是”和“否”）。

这期间，我们取得了很大进步。联合国政府专家组（GGE）解决国际安全背景下的网络问题，是讨论此类问题的主要平台。GGE是联合国秘书长创建的机构，执行联合国大会赋予的任务，即研究国际法如何适用于国家的网络活动等事宜，旨在促进达成共识。2013年，15个国家组成的GGE认同当前国际法适用于国家的网络活动。就在去年，这方面的GGE增加至20个成员国，该专家组在2013年报告的基础上，采取了进一步措施，明确《联合国宪章》第51条规定的固有正当防卫权利的适用性。同时，2015年的GGE报告也明确了武装冲突法规中关于在网络空间开展敌对行为的人性、必要性、相称性、区分的基本原理的适用性。此外，我们最近还达成了双边和多边声明（包括2015年G20国家领导人的联合声明），我们看到各国似乎正在形成这样一个共识，即现有国际法适用于国家的网络活动。

将当前国际法的适用性视为一般事实并非难事，至少对于大多数志同道合的国家是这样。然而，确定法律如何适用于特定网络活动却较为困难，各国也很少公开发表他们在这方面的看法。

美国在这方面做了一些工作，如高洪柱的2012年发言中详细地阐述了国际法适用于网络活动这一观点而且美国遵守联合国政府专家组发布的2014–2015报告，这些资料公开发表在《美国国际法惯例摘要》上。
同时，国防部也经常就这一议题在《战争法手册》上公开发表意见。然而这些远远不够，我们依然任重而道远。

种种原因表明，提升透明性非常重要。当然，国际习惯法来自于各国出于法律义务或法律确信而遵守的广泛一致的做法。由于当前比较缺乏网络活动相关的公共国家实践和法律互信，其他国家设法针对国家法如何适用于网络这一主题发表相关看法，从而填补这一缺口。所有这些工作中，最重要且最全面的当属《塔林手册》项目。尽管该手册是北约协作网络防御卓越中心发表的一项倡议，然而该倡议既非国家牵头，也不是北约官方项目，而是各国律师发起的一项非政府活动，他们着手确定适用于网络战争的国际法，2013年发布了《塔林手册1.0》。该项目组目前正在审查适用于武装冲突之外的未构成使用武力的网络活动的国际法律框架，将在今年年底发布《塔林手册2.0》。

我认为，《塔林手册》项目组显然做了大量细致工作。美国明确赞同该项目的基本观点，即现有国际法适用于网络空间的国家行为。《塔林手册》向多个国际法机构阐述和强调了这一点，作出了宝贵贡献，虽然我们未必完全认同该手册。

同时，各国必须解决这些挑战性问题。非政府组织提出的国际法解读和应用可能无法反映很多或大多数国家的做法或法律观点。若各国对此沉默不言，则会对网络领域带来不可预知的结果，因为他们可能会猜测彼此对于适用的法律框架的看法。在特定网络事件中，这种不确定性可能会使国家产生误解和误判，导致事件升级，最严重时可造成冲突。

为缓解这些风险，各国应在国际和国内平台公开表达对现有国际法如何适用于网络空间国家行为的看法。发生的特定网络事件为各国提供了交流机会，各国对于除特定行为或事件之外的其他方面公开表明立场也同等重要，而且也往往更为容易。公开发布这些观点可有助于明确期望的国家行为，因此可提升网络空间的可预测性和稳定性。这对于以下情况均适用：1.何种法规适用于可构成武力使用或武装冲突情况下发生的网络活动。2. 何种法规适用于除网络冲突情况下不构成武力使用的网络活动。

尽管包括美国在内的很多国家都认为当前的国际法律框架足以管理国家的网络空间行为，不过，各国在具体问题上看法不一，因此非常有必要进一步讨论这些问题、澄清疑问和沟通协调。各国的当前任务是针对当前国际法如何适用这一问题公开表明其立场。

本着这种精神，基于高洪柱2012年的讲话和美国所遵守的UN GGE的2014和2016年报告，我就美国关于某些国际法如何适用于各国的网络空间行为提出另外几条意见，首先从武装冲突期间的网络行动开始，其次明确适用于和平时期国家行为的自愿性非约束规范。

武装冲突时的网络行动

关于武装冲突时的网络行动，我想首先从美军与“伊拉克和黎凡特伊斯兰国”（ISIL）当前的武装冲突中的网络行动谈起。美国国防部长阿什顿·卡特（Ashton Carter）2016年4月告诉国会，美国网络司令部被要求将与ISIL的战争作为其第一次大规模作战行动[…]，目标是摧毁ISIL的指挥与控制，使其无法转移钱财、欺压和控制平民和对外招募。

美国军方在对ISIL开展网络行动时须遵守武装冲突法及其他适用的国际法规定的美国义务，这与美国在武装冲突期间发动其他类型的军事行动一样。若依据武装冲突法这些网络行动构成了“攻击”，必须对这些网络行动应用攻击执行法规。例如，这些行动必须只针对军事目标发起，如计算机、其他联网设备或具体数据（鉴于其性质、位置、作用或用途，这些数据有助于为军事行动作出切实有效的贡献。此外，这些数据若在当时情况下被完全或部分损毁、捕获或失效，会带来明显军事优势）。同时，这些行动必须与区别和对称性需求相符。必须采取可行的预防措施减少对民用基础设施和用户的附带损害风险。在这种网络情况下，冲突各方需评估网络活动对军用和民用基础设施及用户的潜在影响。

然而，并非每次网络行动都能上升到“攻击”层面，成为武装冲突法相关的法律问题。从武装冲突法规角度评估网络活动是否构成“攻击”时，国家应考虑该网络活动是否造成了军事或非军事影响、这些影响的本质和范围、以及该活动与特定武装冲突之间的关联（若有的话）。即使从武装冲突法角度看这些网络行动并未上升到“攻击”层面，武装冲突期间的网络行动也必须符合军事必要性原则。例如，网络行动虽未构成“攻击”但会控制或破坏敌方资产，因而是作战迫切需要的。此外，即使网络行动并未上升到“攻击”层面或并未导致发动攻击的对称性原则规定的伤害或损害，该网络行动仍然应该符合战争法规的基本原则。

除了刚刚介绍的武装冲突法和原则，其他国际法律原则同样适用于美国在武装冲突期间开展的网络行动。时任总统的国土安全和反恐助理的约翰·布伦南（John Brennan）2011年9月在哈佛法学院的讲话中提到，“国际法原则，如尊重国家主权[…]，对于我们单方面[…]在海外领土上的行为起重要约束作用。”下面我将介绍国家主权在网络行动法律分析中的作用。

主权与网络空间

高洪柱在2012年的讲话中表示“各国在开展网络空间活动时必须考虑其他国家的主权，包括武装冲突之外的情况。” 基于这一说法，我想介绍一下关于主权原则与国家网络活动相关性的几个看法。

首先，在其他国家领土上利用计算机或其他联网设备开展的远程网络行动本身并不构成违反国际法。也就是说，国际法并非绝对禁止开展此类网络活动。或许最能体现这一点的是在其他国家领土上的这些活动并没有任何影响或仅有轻微影响。

包括美国在内的大多数国家都在收集海外情报。奥巴马曾表示，“并不单单只有美国”在收集海外情报。而且，总统明确表示，美国同其他国家一样自成立以来一直在收集情报，确保其国家安全和外交政策决策者能够掌握及时、准确和富有洞察力的信息。事实上，奥巴马总统2014年发布了一项指示，澄清了美国收集海外信号情报时遵循的原则。

从几乎每个国家都在全球范围内广泛收集情报的做法看，我们了解到国际习惯法本身并未禁止这些活动。我想在这里提醒一下，由于情报收集未有明确界定，因此，不禁止这些活动就无法解决这一问题，即某个情报收集活动是否会违反国际法的某项条款。

尽管包括网络行动在内的一些活动可能会违反国家的国内法，而这与违反国际法不同，需另当别论。美国高度尊重其他国家制定法规管辖在其领土上的活动的主权权利。蔑视其他国家的国内法可导致严重的法律和外交政策后果。从法律意义上看，若其他国家的特工在美国及全球范围内有此等行为可能面临刑事诉讼和惩罚，例如，从事间谍活动或违反类似美国的《计算机欺诈与滥用法》等国外法规的犯罪活动。从外交政策层面看，我们可以考虑披露这些规程产生的影响。然而，这些国内法和外交政策无法解决该活动是否违反国际法这一问题。
某些情况下，某国在未经其他国家同意的情况下在其领土上开展网络行动会违反国际法，即便是其行动未构成使用武力。这是一个很有挑战性的法律范畴，会带来很多难题。正是互联网的设计可能会导致对其他国家的主权管辖范围的侵犯。例如，在未经许可情况下开展网络行动为违反其他国家主权就是美国政府的律师持续仔细研究的一个问题，这一问题最终会通过各国的实践和法律确信解决。

在这方面，考虑一下我们在明确国际法禁止非法干涉时面临的挑战。从国际法院对尼加拉瓜案情的判决来看，国际习惯法禁止各国针对其他国家依据国家主权原则有权自主决定的各项事宜（如选择政治、经济、社会和文化体制）采取强制性行动。这普遍被视为国际习惯法的一条狭义规定，然而，国家的网络活动可能与此条禁令相冲突。例如，某国开展网络行动影响其他国家举行选举的能力或操控其选举结果是对不干预规定的公然违反。
为提升透明性，国家需多做工作澄清国际不干预法规如何适用于国家的网络空间活动。

很多人可能会问为何国际社会划定法律界限如此重要？更具体地说，为何活动是否违反国际法规事关重大？当然，这非常重要，因为国际社会的国家承诺遵守国际法，包括网络空间活动相关法规。在遵循国际法情况下，各国可携手共进，达成共同目标，如确保网络空间稳

定。国际法针对国家行为制定了约束性规范让各国遵守，同时也为遵约国对违约国进行谴责或召集其他国家共同回应提供了更有力的依据。高洪柱2012年谈到，“若能有效推广合规文化，我们就能获得利益。此外，若能赢得合规美誉，我们采取的行动在全球范围内将获得更高的合法性认知。”确定国际法如何适用于网络空间的国家活动可实现这些目标，就如同这些法规满足国家活动的很多其他关键领域的需求一样。

在结束讨论主权议题之际，我还想解决一个有关国家对网络基础架构及其领土上（而非领土之外）的活动控制权的问题。高洪柱在2012年的讲话中提到，“支撑互联网及网络活动的物理基础设施一般部署在主权领土内且受主权国家管辖。”不过，他继续强调称，“主权国家并非可为所欲为地行使管辖权，必须遵守包括国际人权义务在内的相关国际法。”

这一点很重要，我想在此强调一下。有些国家将国家主权这一概念作为过度监管在线内容的遮羞布，例如，通常以反恐或“反暴力极端主义”名义进行审查和设定限制访问。有的国家会将国家主权这一概念视为对抗外界批评的挡箭牌。

因此，我们在此重申一下高洪柱的观点：国家对其领土内任何事宜（包括互联网使用和访问）监管时都必须履行国际人权法规定的相关国家义务。

毫无疑问，恐怖分子团伙现在已经非常擅长利用互联网及其他通信技术传播仇恨言论、招募新人，以及敦促追随者实施暴力行径。因此，各国政府必须携手打击在线犯罪活动，如非法转账、恐怖袭击策划与协调、犯罪教唆和向恐怖团伙提供物资支持。美国也开展了防止利用互联网实现恐怖主义目的的工作，侧重于打击协助恐怖主义的犯罪活动，如筹措资金、招募新人以及对情绪煽动内容（即使这些内容与我们的核心价值观不一致或相悖）不作限制。

这些工作与对审查互联网或限制其公共访问的更广泛呼声不得混为一谈。甚至有些人建议将网络直接关闭。这些措施对提升安全无益，而且与我们的价值观不符。我们必须维持开放的互联网，让信息和思想自由交流。限制思想交流会阻碍互相理解和互相尊重这一价值观的传播，而后者（互相尊重）正是我们应对恐怖分子团伙散布的仇恨和暴力言论的最有效的一剂良药。

为此，美国认为利用互联网（包括社交媒体）推动恐怖主义及其他犯罪活动这一问题必须通过法律手段解决，尊重每个国家的国际人权义务和承诺，包括言论自由，确保信息自由交流，维持开放自由的互联网。诚然，这样也就限制了煽动恐怖主义暴力的行为。然而，某些审查和内容控制违反了国际人权法，不应由国家介入管理，如只是因为发布了抨击领导、政府政策或意识思想的内容或是因为内容支持某些宗教信仰就彻底封杀该网站。

国家职责和网络空间“溯源问题”

前文已大篇幅谈论了网络空间的国家活动和行动。可能你们中很多人都知道，查明特定网络事件的幕后黑手往往并不容易。这使我联想到了时常引发热烈讨论的网络空间“溯源”问题。

国家和评论员经常从技术角度对溯源问题表示担忧，也就是说，无论通过技术指标还是全源情报，查明事实真相都是个棘手难题，而弄清楚这一点会为国家关于特定网络事件的决策提供参考。还有人对溯源相关的政治决策提出了问题，即考虑国家对于公开发布特定网络事件以及将其他国家视为幕后主使并谴责该事件无法接受的决策。然而，这些溯源相关的技术和政策性讨论应与相关法律问题区别开来。在此次发言中，我将重点从法律角度阐述溯源问题。

从法律角度看，国际习惯法中的国家责任部分明确了行为（包括网络行为）归属于国家的标准。例如，国家机关或国内法授权个人或实体行使国家权力开展网络行动且该机关、个人或实体以此身份行事而由此发起的网络行动归属于国家。

此外，对于非国家攻击者开展的网络行动，若攻击者依据国家的指示、指令或在国家控制之下参与网络行动或事后国家承认和采取了行动，则该网络行动视为国家发起。因此，从法律意义上看，国家若通过代理人蓄意发起恶意网络活动也不能逃避责任。若有信息显示—无论

通过技术手段还是全源情报途径获取—按照国家责任法中规定的标准，网络行为由在法律上属于某个非国家的攻击者发起，则受害国在国际法允许范围内拥有对抗攻击国的所有权利及有权向其寻求补救措施。

国家责任法并没有明确阐述或规定提供法律归属证据。在这种情况下，国家自身查明事实真相，单方面决定网络行动是否来自于其他国家。无需百分百确定攻击来源，而且可能也无法彻底搞清楚。国际法通常规定若国家收集了信息且据此得出了结论，则应在这种情况下采取相应行动。

同时，尽管一些国家持相反意见，我还是想说明一下，国际法未明确规定各国在采取相应行动之前需提供归属证据。当然，若有政治压力，国家可选择披露一些证据，比如旨在方便其他国家协助他们进行谴责。这主要取决于政策的规定，国际法并不做强制要求。

对抗措施及其他"防御性"措施

现在，我们要看一下受害国可采取怎样的措施应对未构成武装冲突的恶意网络活动。首先，国家可采取与任何国际义务冲突的不友好行为，从而影响其他国家的行为。这些行为—称为报复行为—可能包括实施制裁或宣布某外交官不受欢迎等行为。

某些情况下，国家可采取违反国际法的措施应对恶意网络活动。例如，在自我防卫过程中使用武力应对已发生或迫在眉睫的武装攻击。又如，在特殊情况下，国家可发出紧急避险请求，即如果在符合某些条件的情况下，排除了该行为的不法性情况，采取行为是国家应对迫在眉睫的严重危险捍卫其基本利益的唯一方法。

在余下的时间，我将介绍网络空间探讨中备受关注的网络响应类型—对抗措施。国际习惯法中的对抗措施原则规定，若一国对另一国发起国际不法行为，受害国可采取非法措施对付责任国，使其遵守国际义务，如停止国际不法行为义务。因此，采取对抗措施应对恶意网络活动的前提条件是一国向另一国事先发起国际不法行为。与所有对抗措施一样，若实际并不存在国际不法行为引发对抗措施或响应国作了错误的归属判断，采取此类对抗措施可导致响应国违反国际法。因此，不应轻率地采取对抗措施。

此外，根据对抗措施法规，若某国在网络空间或利用网络空间发起国际不法行为，应仅针对发起该行为的责任国采取响应措施，而且该措施必须符合必要性和相称性原则，包括确保对抗措施旨在使责任国遵守其国际义务（例如，停止其国际不法行为的义务），而且应在责任国开始履行其国际业务时停止对抗措施。

一般情况下，对抗措施原则规定，受害国应在采取对抗措施前要求响应国履行其国际义务。换句话说，该原则要求受害国事先提出要求。应根据实际情况评估事先提出要求是否充分，需要考虑到当前的具体情况以及该要求的目的（即受害国向责任国发出通知表明其要求并给责任国提供响应的机会）。

同时，需注意应对一国发起的国际非法网络活动的对抗措施一般为基于网络的对抗措施或非基于网络的对抗措施。具体采取哪类措施应由响应国基于实际情况而定。

关于和平时期负责任的国家行为的自愿性非约束规范

最后，我想简要介绍一下美国的国际网络稳定战略框架的其中一个要素：就和平时期负责任的网络空间国家行为相关的某些其他自愿性非约束规范达成国际共识。

美国已在全球范围内明确并推广以下规范：

- 第一，国家不得通过网络窃取知识产权、商业秘密或其他机密性商业信息或故意支持此类盗窃活动为公司或商业部门提供竞争优势。
- 第二，国家不得通过开展或故意支持在线活动而蓄意破坏关键基础设施或损害对提供

公共服务的关键基础设施的使用。

- 第三，国家不得通过开展或故意支持活动而阻止国家计算机安全事件响应团队（CSIRT）响应安全事件。此外，国家不得利用CSIRT开展在线活动造成损害。
- 第四，若应其他国家要求提供援助，国家应在遵守国内和国际义务情况下联合调查网络犯罪、收集电子证据以及缓解其领土上发起的恶意网络活动。

美国提倡的这四项规范旨在防范各国所关心的国家和/或经济安全面临的特定领域风险。这些规范虽为自愿和非约束性质但可提供国际行为标准，志同道合的负责任国家可依据这些标准阻止攻击者发起恶意网络活动。若能采取这些措施（包括自我约束措施）可极大地有助于防范冲突和维持稳定。随着时间的推移，这些规范或可提供常见标准供负责任的国家发现和应对违反这些规范的行为。随着越来越多的国家承诺遵循这些标准，他们越来越倾向于谴责攻击者发起的恶意活动，并齐心协力对这些活动施加影响。
然而，必须明确区分国际法和自愿性非约束规范。美国确定的这四项规范以及联合国政府专家组的2015年报告均属于自愿性非约束规范。这些规范制定了预期国家行为的标准，这些标准在某些情况下可能与国际法中的行为标准重合。这些规范是对当前国际法的补充，旨在应对国家在武装冲突之外情况发起的某些可能破坏稳定的网络活动。也就是说，国家可能开始将这些非约束性规范中制定的标准视为法律要求，依据这些规定行事，这样这些规范就会逐渐形成有约束力的国际习惯法。因此，国家在确定和决定遵守这些非约束性规范时一定要持谨慎态度。

最后，我想强调几点。首先，虽然网络空间是个新领域，但网络空间内的国家行为与其他领域的行为一样都受现有法律框架（包括国际法）的约束。其次，对于确定当前法律框架如何适用于网络空间这一问题，国家承担主要责任。第三，国家负责公开发布适用的标准。这对于准确理解网络空间及其他领域的国际法至关重要。我希望今天的演讲能进一步推动实现透明性目标，突出强调国际法和国际事务律师在这一重要且有活力的领域发挥的重要作用。

来源：https://2009-2017.state.gov/s/l/releases/remarks/264303.htm，2018年7月25日。

B. 美国国防部战争法手册

以下节选自2015年6月美国国防部发布的《战争法手册》（2016年12月更新）第**16**章“网络作战”。完整内容详见：
https://www.defense.gov/Portals/1/Documents/pubs/DoD%20Law%20of%20War%20Manual%20-%20June%202015%20Updated%20Dec%202016.pdf?ver=2016-12-13-172036-190.

第 16 章 网络作战

章节目录

16.1 概述 本章介绍战争法和网络作战，论述如何将战争法原则应用于较为新颖的网络能力和网络领域。

根据政策，美国已寻求国际合作，试图阐明如何将现行的国际法及标准（包括战争法原则）应用到网络作战[1]中。

战争法究竟如何应用到网络作战中尚无定论，该领域的法律仍处于发展阶段，尤其是随着新的网络能力的出现，各国都会据此形成自己的观点[2]。

16.1.1 网络空间领域。根据规定，美国国防部已将网络空间视为一个作战领域，武装部队必须能够像在陆海空和太空领域[3]一样进行防御和作战。

*网络空间*可定义为“由相互依赖的信息技术基础设施和驻留数据网络构成的全球信息环境，包括互联网、电信网络、计算机系统、嵌入式处理器和控制器”[4]。

16.1.2 网络作战描述。网络空间作战可理解为“应用网络空间能力以在网络空间或通过网络空间实现目标”[5]：（1）使用网络能力，如电脑、软件工具或网络；以及（2）主要目的是在网络空间或通过网络空间实现目标或效果。

16.1.2.1 *网络作战示例*。网络作战包括使用计算机中断计算机或计算机网络运行、导致计算机或计算机网络拒绝服务、降低计算机或计算机网络的性能、破坏计算机或计算机网络或其中的信息。网络作战可作为先遣行动在目标区域先于主要行动展开，为实现主要的攻击目标做好准备。例如，网络作战包括侦察（例如绘制网络）、占领支援位置（例如获取关键关键网络系统或节点的访问权限）和预先部署能力或武器（例如植入网络访问工具或恶意代码）。此外，网络作战可用于获取与特定军事目标无关的国外情报，例如了解技术发展或获取有关攻击者军事能力及意图的信息。

16.1.2.2 *非网络作战行动示例*。网络作战一般不包括仅使用计算机或网络空间，而不以在网络空间或通过网络空间实现目标或效果为主要目的的活动。例如，使用计算机网络辅助指挥和控制的行动、使用空中交通管制系统的行动，以及利用计算机广泛传播信息的行动，这些通常都不能视为网络作战。那些以对手的网络空间能力为目标，但未在网络空间或通过网络空间实现目标的行动都不能视为网络作战。例如，即使可以在网络空间内实现军事目标，轰炸网络枢纽或干扰无线通信均不能视为网络作战。

16.3 网络作战 – 术语解释。国防部关于网络作战的原则和术语在持续演进中。

16.3.1 *修饰性的"网络"与"网络空间"比较*。当用作修饰语（例如网络攻击、网络防御、网络作战）时，"网络"和"网络空间"通常可以互换使用。

16.3.2 *网络攻击或计算机网络攻击*。在讨论网络作战时，"攻击"一词常用于口语表达，指的是各种不同类型的敌对或恶意网络活动，如网站篡改、网络入侵、窃取私人信息或中断互联网服务。

因此，"网络攻击"或"计算机网络攻击"未必是用于在敌对行动[6]期间应用攻击规则的"攻击"。同样，"网络攻击"或"计算机网络攻击"也未必是触发国家根据开战正义原则[7]（*jus ad bellum*）而发挥其固有自卫权的"武装攻击"。

16.2 战争法在网络作战中的应用。

某些战争法规则可用于网络作战，尽管它们是在网络作战出现前制定的。在缺乏更具体的战争法规则或其他适用规则的情况下，战争法原则为武装冲突中的网络作战提供一般性指导。

16.2.1 将具体的战争法规则应用于网络作战。某些战争法规则可用于网络作战，尽管它们是在网络作战出现前制定的。

战争法确实预见技术创新并考虑到现有规则要适用这些创新，包括网络作战[8]。战争法规则之所以能够适用于新技术，是因为这些规则通常不针对特定的技术手段。例如，攻击规则与攻击所使用的武器类型无关。因此，网络作战可根据其性质应用不同的战争法规则。例如，若网络攻击的物理后果等同于投放炸弹或发射导弹所造成的物理损害，则网络攻击同样应遵守与使用炸弹或导弹[9]攻击相同的规则。

由于可产生各种影响，网络作战可能会带来具有挑战性的法律问题。例如，网络作战可能是非暴力对抗手段或方法（如信息收集），需要按照非暴力战争手段和方法[10]规则进行管理。有的网络作战会产生攻击效果，需要按照实施攻击[11]的规则进行管理。此外，特定网络作战行动可能会视为对敌方财产的侵占或破坏，因而产生法律挑战，应进行评估[12]。

16.2.2 将战争法原则作为网络作战的一般性指导。当没有具体的适用规则时，战争法原则成为战时一般性行为指南，包括网络作战期间的行为。例如，根据人道主义原则，在网络作战中必须避免为实现合法军事目的而造成不必要的苦难、伤害或破坏[14]。

某些网络行动显然既具有独特的能力和效果[15]。这些行动可能与使用传统武器的攻击所产生的影响截然不同，并且这些不同的影响会导致不同的结论[16]。

16.3 网络作战与开战正义原则。

根据战争法中诉诸武力相关条款（即开战正义原则）[17]，网络作战可能会出现问题。

16.3.1禁止进行构成《联合国宪章》第2（4）条所述非法使用武力的网络行动。《联合国宪章》第2（4）条规定，"各会员国在其国际关系上不得使用威胁或武力，或以与联合国宗旨[18]不符之任何其他方法，侵害任何会员国或国家之领土完整或政治独立"。特定情况下，网络作战构成《联合国宪章》第2（4）条和国际习惯法[19]中所指的武力使用。例如，当网络作战效果等同于传统物理手段实现的效果时，若后者视为开战正义原则下的武力使用，则这种网络作战也会视为使用武力。网络作战包括：（1）引发核电站熔毁；（2）在人口稠密地区上游打开水坝，造成破坏；或（3）破坏空中交通管制服务，导致坠机[20]。同样，削弱军队后勤系统从而削弱其执行和维持军事行动的能力的网络作战也会视为根据开战正义原则[21]而使用武力。除了网络作战效果，其他因素也会用于决定网络作战是否构成开战正义原则下[22]的武力使用。

根据《联合国宪章》第2（4）条和国际习惯法规定的构成武力使用的网络作战必须有适当的法律依据，避免违反开战正义原则中关于诉诸武力[23]的禁令。

16.3.2 和平时期的情报与反情报活动。国际法和由来已久的国际规范适用于网络空间

[24]中的国家行为，和平时期的情报和反情报活动的合法性问题必须逐案考虑。网络作战与传统的情报和反情报活动相似时（例如，单纯为了获取信息而非法入侵计算机网络），一般会依据国际法[25]同等对待该种网络作战。美国通过网络空间开展此类活动时要考虑国际上长期认可的制约因素，包括将这些活动视为敌对行为[26]的可能性。

16.3.3 应对敌对或恶意网络行动。《联合国宪章》第51条承认自卫权是一个国家的固有权利，肯定其成员国在面临或即将面临构成武装攻击的网络作战自卫权[27]。根据国家政策，美国认为，在必要时，将像对其他威胁一样对网络空间中的敌对行为做出反应[28]。

根据《联合国宪章》第51条之规定，在行使国家自卫权以应对武装攻击时采取的措施必须立即向联合国安理会[29]报告。

16.3.3.1 *武力使用与武装攻击*。长期以来，美国一直主张固有的自卫权可用于对抗任何非法使用武力的行为[30]。因此，任何对某国非法使用武力的网络行动都可能引起为了自卫而采取必要和同等行动的权利[31]。

16.3.3.2 *对网络攻击的网络响应没有法律要求*。只要满足必要性和比例要求，法律上没有规定对网络武装攻击自卫响应时必须采取网络行动的形式[32]。

16.3.3.3 对不构成武力使用的敌对或恶意网络行为的响应。虽然根据开战正义原则不构成武力使用的网络行动不允许受害国家使用武力[33]进行自卫，但这些受害国家有理由采取必要和适当的非武力行动，例如外交抗议、经济禁运或其他报复行为[34]。

16.3.3.4 网络作战溯源与自卫。在应对敌对或恶意网络攻击时，溯源是一个实际的难题，因为与其他类型的攻击[35]相比，攻击者更容易在网络空间中隐藏或伪装活动或身份。无论攻击源自他国或他人[36]，国家都有权对通过网络空间发起的武装攻击采取必要、对等的自卫措施。

16.3.3.5 美国法律规定的应对敌对网络行为的相关机构。是否行使固有自卫权由国家领导决定，因为这些决定关乎国家在国际法下的权利和义务。例如，在美国，通常由总统做出此类决定。

美国军队的常规交战规则规定，美国武装部队可以对敌对行为或敌对意图（包括在网络空间或通过网络空间实施的此类行为）采取自卫行动[37]。

16.4 网络作战与中立法

中立法在某些网络作战中可能很重要。例如，根据中立法，交战国必须尊重中立国的主权[38]。由于网络空间的相互关联性，以一国的网络信息基础设施为目标的网络攻击可能会对未参与武装冲突的另一国产生影响[39]。

16.4.1 使用中立国通信基础设施的网络作战。中立法规定了使用中立国的通信基础设施的情况。某些情况下，这些规则可适用于网络作战。

根据一般规则，若使用中立国的通信基础设施，中立领土不得作为双方交战国的作战基地[40]。特别是，交战国禁止在中立国领土上安装任何用于与陆、海交战部队通信的装置，或禁止纯为军事目的而使用武装冲突前在中立国领土上安装的此类装置或未开放的公共信息服务[41]。然而，仅通过中立的通信基础设施（若这些设施是公正提供的）传输信息一般不构成违反中立法，交战国有义务避免这样做，中立国也有义务防止此类情况发生[42]。之所以制定该条规则，是因为让中立国去审查或筛查用于战时通信的公共通信基础设施是不切实际的[43]。因此，例如，不会禁止交战国通过中立国用于公共信息服务的网络基础设施进行传输信息，而且中立国也没有义务禁止此类通信。该条规则还适用于以下情况：通过中立的通信基础设施传送的信息被归为网络武器，或在交战国造成破坏性影响（但对中立国没有破坏性影响）[44]。

16.5 网络作战与交战正义原则

本节介绍开战正义原则和网络作战。

16.5.1 为应用攻击规则而发起的攻击性网络行动。若网络行动构成攻击，则必须使用与发动攻击相关的战争法规则来规范这些网络行动[45]。例如，此类行动必须符合区分性和比例性要求[46]。

例如，摧毁敌方计算机系统的网络攻击不能针对民用基础设施，如证券交易所、银行系统和大学计算机系统，除非测试证实，在当时的情况下，这些计算机系统被用于军事目的[47]。必要情况下，战争可能会要求立即进行不构成攻击但能够夺取或摧毁敌方财产的网络行动[48]。

16.5..1. *评估网络作战过程中的附带伤害或损坏*。比例原则禁止此类攻击：预期会造成附带的平民死亡以及民用物体损坏的攻击，而且这些损失超出了预期的直接军事目标[49]。

例如，将此禁令应用于网络作战时，评估网络攻击对非军事目标的计算机（例如不具有军事意义但可以与有效军事目标的计算机联网的个人及民用计算机）的潜在影响是非常重要的[50]。

需要注意的是，网络作战过程中造成的附带伤害或损坏若很轻微或不太严重（例如造成的不便或临时中断），在按照比例原则评估是否禁止攻击时可以忽略[51]。例如，若对军事目标的网络攻击偶然对平民互联网服务造成了轻微、短暂性中断，一般不需要进行比例性分析[52]。此外，由这种中断而造成的交战国经济损失（例如交战国的民用企业无法开展电子商务），通常也不需要考虑比例性分析[53]。

即使构成攻击的网络行动预计不会造成过多附带伤亡或损坏因而不会根据比例原则禁止，冲突方仍需采取切实可行的预防措施，限制这些网络行动造成的伤亡和损害[54]。

16.5.2 根据战争法不构成“攻击”的网络行动。不构成攻击的网络行动不受攻击规则限制[55]。网络行动不构成“攻击”的因素包括其造成的效果是可逆、短暂的。

通常不构成攻击的网络行动包括：

- 篡改政府网页；
- 造成轻微、短暂的互联网服务中断；
- 短暂中断、禁用或干扰通信；以及
- 传播宣传。

根据战争法，此类行动一般不视为攻击，因此一般不需要针对军事目标，可能会针对平民或民用物体。但是，除非出于军事必要性，此类行动不得针对敌方平民或民用物体[56]。并且，此类行动应符合战争法的一般性原则[57]。

例如，即使网络行动不是“攻击”，或者不会造成任何按照比例原则评估攻击必要性时须考虑的伤害或损坏，也不应给平民或中立人士带来不必要的麻烦。

16.5.3 采取可行预防措施的责任与网络行动。冲突方必须采取切实可行的预防措施，以降低对平民和其他受保护人员和物体造成附带伤害的风险[58]。发起网络作战的冲突方应采取预防措施，尽量减少其网络活动对民用基础设施及用户带来的危害[59]。

采取可行预防措施的义务在网络作战中的重要性大于其他战争法规则，因为相较于其他战争法规则，该项义务适用的活动范围更广泛。例如，采取切实可行的预防措施以降低意外伤害风险的义务适用于攻击方，即使按照比例原则该攻击不会被禁止[60]。此外，即使非攻击方也有义务采取切实可行的预防措施，因为该项义务也适用于受攻击方[61]。

16.5.3.1 *可用于降低对平民或民用物体造成伤害风险的网络工具*。某些情况下，具有软杀伤或可逆效果的网络行动有助于最大程度地降低对平民造成的不必要伤害[62]。在这方

面，网络能力在某些情况下可能比动能武器更可取，因为带来的效果是可逆的，而且能够在没造成任何破坏性杀伤效果的情况下实现军事目标[63]。

与其他预防措施一样，决定使用哪种武器需要考虑多种因素，包括效能、成本和“脆弱性”。也就是说，一旦使用后可能会被对手制定出防御措施，则该武器在未来会成为一件无效的网络工具[64]。因此，与特殊动能武器（例如产生附带伤害少于其他动能武器的精密制导武器）一样，网络能力通常不是法律允许的唯一武器类型。

16.5.4 禁止在网络作战期间不当使用标志。根据战争法，某些标志不得不当使用[65]。这些禁令也适用于网络作战。例如，不允许进行网络攻击或试图利用促成非敌对关系的通信（如战俘交换或停火[66]）来破坏敌方内部通信。同样，禁止伪造来自敌方国家元首的信息，谎称国家部队已签署停战协定或停火协议[67]。

另一方面，限制使用敌方旗帜、徽章和制服，仅将其用于具体的视觉对象；不限制使用敌方代码、密码和口令[68]。因此，将网络流量伪装成来自敌人计算机的流量或在网络作战时使用敌方代码，这些都是允许的。

16.5.5 使用平民支持网络作战。与非网络作战一样，战争法并不禁止各国使用平民支持网络作战，包括直接参加战斗[69]。

根据GPW，授权陪同武装部队成员的非武装部队成员也会成为战俘[70]。这包括在军事装备操作方面具有特殊技能并支持和参与军事行动的平民，如军事机组人员中的平民成员[71]；还包括授权陪同武装部队的平民网络专家。

直接参与战斗的平民不受保护，也会成为攻击对象[72]。

16.6 对具有网络能力的武器的法律审查。

国防部政策要求对武器或武器系统的采购进行法律审查[73]。该项政策包括审查具有网络能力的武器，以确保它们本身不被战争法所禁止[74]。然而，并非所有网络能力都会构成武器或武器系统。美国军事部条例规定了哪些网络能力需要法律审查[75]。

战争法并不阻止开发新型网络武器。战争法对于特定类型武器的习惯禁用源于国家及法律确信某种类型的武器是非法的；新式武器或采用新技术的武器并不意味着非法[76]。

虽然哪些问题需要进行法律分析取决于所评估武器的特点，但对具有网络能力的武器的获取或采购进行法律审查很可能是评估该武器是否属于滥杀滥伤武器[77]。例如，若一种破坏性的计算机病毒被编程至民用互联网系统中进行不可控制的传播和破坏，该病毒就会被当作是一种滥杀滥伤武器而被禁止[78]。

尾注：

1 例如，请参见美国向联合国政府专家小组提交的《国际安全背景下信息和电信领域的发展》（2014-15），1（“然而，挑战并不是现有的国际法是否适用于网络空间中的国家行为。2012 至 2013 年，政府专家小组确认称，国际法确实适用，而且对于规范国家在这一领域的行为至关重要。挑战是决策者须考虑哪些因素以确定如何在网络活动中应用现行国际法。不过，历史上，通过协商和合作，各国多次成功地将现行法律体系应用于新技术。美国一直认为，所有国家都将受益于稳定的国际信息和通信技术环境，其中现行国际法是网络空间中负责任国家行为的基础。”）；2011 年 5 月，巴拉克•奥巴马（Barack Obama）发表了《网络空间国际战略：网络世界的繁荣、安全和开放》。（“制定国家网络空间行为准则不需要重新制定国际习惯法，也不会使现有的国际准则过时。” 在和平和冲突时期指导国家行为的国际准则同样也适用于网络空间。尽管如此，网络技术的独特属性要求特别说明如何应用这些准则，以及必要的理解补充。关于如何在网络空间中应用这些准则，我们将继续努力达成国际共识。其中，很重要的第一步是将对于和平公正的国家间行为的广泛期望应用于网络空间。”）；2011 年 11 月，美国国防部发表了《国防部网络空间政策报告》：根据《2011 财政年度国防授权法案》的国会报告（第 934 节，7-8）（“美国积极参与网络空间负责任的国家行为规范的制定，明确指出，根据美国政策，指导国家行为的既定国际规范同样适用于网络空间。其中，运用武装冲突法的基本原则对实现这一愿景至关重要，尽管网络空间的独特性可能需要在某些领域进行澄清。”）

2 美国国防部法律顾问，《信息战中国际法律问题评估》（1999 年 11 月第 2 版），《美国海军战争学院国际法研究》第 76 卷（2002 年转载，459, 464 - 65）（“通常，只有开始感觉到后果时，国际社会才会协商条约，处理问题。这并不完全是坏事，因为解决方案可以根据实际发生的问题进行调整，而不是根据一系列假设的可能性进行调整。然而，这会产生一个后果，即由此产生的法律，无论是国内法律还是国际法律，可能会受到事件性质的剧烈影响而加速法律进程，同时还会受到相关政策和政治因素的影响。... 同样，我们可以对国际法律体系如何应对信息战做出一些有根据的猜测，但实际采取的响应措施可能在很大程度上取决于事件引起全国关注的程度。若信息战技术被视为另一种不会对国家利益造成重大威胁的新技术，法律不会有重大变化。若信息战被视为是对国家安全和公民福利的巨大威胁，则更可能采取行动，通过法律手段限制或禁止信息战。这些是国家领导人在当今信息时代决定是否使用信息战技术时应考虑的因素，但还应该了解的是，未来事件的进程往往超出政治家的控制。

3 美国国防部副部长威廉·J·林恩三世(William J. Lynn III)发布《防护新领域：五角大楼的网络战略》（2010 年 9/10 月）（“根据条令，五角大楼已正式承认网络空间为新的战争领域。） 尽管网络空间是人造领域，但它对军事行动的重要性和海陆空、太空一样重要。因此，军队必须能够防护网络空间，并进行网络空间作战。”）

4 联合条例 3-12，网络空间作战，GL-4（2013 年 2 月 5 日）（“网络空间指全球信息环境，由相互依赖的信息技术基础设施和驻留数据网络构成，包括互联网、电信网络、计算机系统、嵌入式处理器和控制器。”）

5 联合条例 3-0，联合作战（2011 年 8 月 11 日）（“网络空间作战”。使用网络空间能力的主要目的是在网络空间中或通过网络空间实现目标。）

6 参见 16.5.1（为应用攻击规则而发起的攻击性网络行动）。

7 参见 16.3.3（应对敌对或恶意网络行动）。

8 2012 年 9 月 18 日，美国国务院网络空间国际法法律顾问高洪柱（Harold Hongju Koh）在网络空间司令部跨部门法务大会上发表演讲；2012 年 12 月被哈佛国际法杂志（网络版）转载。（“网络空间不是法外之地，任何人都不得毫无约束地开展攻击活动。这并不是第一次发生技术变化，国际法必须应对这些变化。特别是，由于冲突工具不断演变，国际人道法或武装冲突法预测到了技术创新，并认为现有规则可适用于这些创新。”）。

9 2012 年 9 月 18 日，美国国务院网络空间国际法法律顾问高洪柱（Harold Hongju Koh）在网络空间司令部跨部门法务大会上发表演讲；2012 年 12 月被哈佛国际法杂志（网络版）转载。（“在分析网络行动是否构成使用武力时，多数评论员关注的是网络事件造成的直接人身伤害和财产损失是否与动能武器所造成的直接人身伤害和财产损失相似。例如，直接导致伤亡或重大破坏的网络活动很可能被视为使用武力。... 只要稍加思考你就会意识到这是个常识问题：若网络攻击的物理后果起犹如投下炸弹或发射导弹那样严重，那么它同样应被视为使用武力。”）

10 参见 5.26（非暴力手段和作战方法）。

11 参见 5.5（实施袭击、轰炸和其他攻击的规则）。
12 参见 5.17（侵占和破坏敌方财产）。参见 2.1.2.2（战争法原则作为一般性指导）。
14 参见 2.3（人道主义）。
15 2012 年 9 月 18 日，美国国务院网络空间国际法法律顾问高洪柱（Harold Hongju Koh）在网络空间司令部跨部门法务大会上发表演讲；2012 年 12 月被哈佛国际法杂志（网络版）转载。（“我还留意到一些明确的案例，恶意网络行为的物理效果可以与军事行为的效果相媲美：例如，投放一颗炸弹可能会毁堤淹民，但从远程计算机插入一行恶意代码同样能轻易达到这样的效果。然而，众所周知，有些网络行动无法与军事行动类比，这要求我们对“武力”的确切含义进行深入思考。” 1999 年 11 月，国防部法律顾问办公室，《关于信息战中国际法律问题的评估》（第 2 版），2002 年被《美国海军战争学院国际法研究》（第 76 卷）转载。（“在与适用于传统武器的法律进行类比推理的过程中，必须始终牢记：计算机网络攻击的含义可能与传统武器攻击的含义截然不同。这些不同的含义会产生不同的结论。”）
16 参见 1.11（开战正义原则）。
17 U.N. 《联合国宪章》第 2（4）条。
18 2012 年 9 月 18 日，美国国务院网络空间国际法法律顾问高洪柱（Harold Hongju Koh）在网络空间司令部跨部门法务大会上发表演讲；2012 年 12 月被哈佛国际法杂志（网络版）转载。（“某些情况下，网络活动可能构成《联合国宪章》第 2（4）条和国际习惯法中所指的武力使用。”）
19 2012 年 9 月 18 日，美国国务院网络空间国际法法律顾问高洪柱（Harold Hongju Koh）在网络空间司令部跨部门法务大会上发表演讲；2012 年 12 月被哈佛国际法杂志（网络版）转载。（“经常被引用的构成使用武力的网络活动包括：（1）触发核电站熔毁的操作，（2）在人口稠密地区的上游打开水坝造成破坏的操作，或（3）禁用空中交通管制造成导致坠机毁的操作。”）
20 1999 年 11 月，国防部法律顾问办公室，《关于信息战中国际法律问题的评估》（第 2 版），2002 年被《美国海军战争学院国际法研究》（第 459、483 卷）转载。（“即使被攻击的系统是非机密的军事后勤系统，对这些系统的攻击也可能会严重威胁到国家安全。） 例如，在一个国家用于管理军事燃料、备件、运输、部队动员或医疗物资的计算机系统中，破坏数据可能会严重影响该国的军事作战能力。总之，后果可能比使用的手段更重要。”）
21 2012 年 9 月 18 日，美国国务院网络空间国际法法律顾问高洪柱（Harold Hongju Koh）在网络空间司令部跨部门法务大会上发表演讲；2012 年 12 月被哈佛国际法杂志（网络版）转载。（在评估事件是否构成在网络空间中或通过网络空间使用武力时，我们必须评估所有可能的因素，包括事件背景、攻击者（意识到网络空间溯源的挑战性问题）、目标和地点、影响和意图。
22 参见 1.11.3（禁止某些使用武力）。
23 参见 16.1（概述）。
24 1999 年 11 月，国防部法律顾问办公室，《关于信息战中国际法律问题的评估》（第 2 版），2002 年被《美国海军战争学院国际法研究》（第 459、518 卷）转载。
25 2011 年 11 月，美国国防部，《国防部网络空间政策报告》：根据《2011 财政年度国防授权法案》的国会报告（第 934 节，6-7）。
26 2012 年 9 月 18 日，美国国务院网络空间国际法法律顾问高洪柱（Harold Hongju Koh）在网络空间司令部跨部门法务大会上发表演讲；2012 年 12 月被哈佛国际法杂志（网络版）转载。（“问题 4：国家是否可以行使自卫权对计算机网络攻击做出响应？回答 4：可以！”） 《联合国宪章》第 51 条中承认国家自卫权，在面临或即将面临构成武装攻击的计算机网络攻击时，各国有权行使自卫权。”）；2011 年 5 月，巴拉克•奥巴马（Barack Obama）发表了《网络空间国际战略：网络世界的繁荣、安全和开放》。（“自卫权：《联合国宪章》赋予各国正当的自卫权，面临网络空间侵略性行为时，各国均有权自卫。”）
27 2011 年 5 月，巴拉克•奥巴马（Barack Obama），《网络空间国际战略：网络世界的繁荣、安全和开放》。（“必要时，美国将像应对我们国家受到的其他任何威胁那样应对网络空间的敌对行为。各国都有固有的自卫权，并且我们认识到，通过网络空间实施的某些敌对行为，将迫使我们根据对军事条约缔约伙伴的义务采取行动。我们保留根据国际法适当使用所有必要的外交、信息、军事和经济手段的权力，以便保护我们的国家、我们的盟国、我们的伙伴和我们的利益。在此过程中，我们将在动用军事力量之前尝试所有替代方案；我们将仔细衡量采取行动的代价和不采取行动的代价；我们的行动方式将反映我们的价值观并强化我们的合法性，在任何可能的时候寻求广泛的国际支持。”）
28 参见 1.11.5.6（向联合国安理会报告）。
29 参见 1.11.5.2（使用武力与武装冲突）。

30 2012 年 9 月 18 日，美国国务院网络空间国际法法律顾问高洪柱（Harold Hongju Koh）在网络空间司令部跨部门法务大会上发表演讲；2012 年 12 月被哈佛国际法杂志（网络版）转载。（在此，我只举一个例子，长期以来，美国一直认为，国家固有的自卫权适用于任何非法使用武力的行为。在我们看来，只要使用了致命武力，就是"武装攻击"，就会有暴力响应。但这并不是说，所有非法使用武力都会触发使用任何武力的权利——响应必须是必要的、相称的。"）

31 2012 年 9 月 18 日，美国国务院网络空间国际法法律顾问高洪柱（Harold Hongju Koh）在网络空间司令部跨部门法务大会上发表演讲；2012 年 12 月被哈佛国际法杂志（网络版）转载。（"没有法律规定对网络武装攻击的响应必须采取网络行动的形式，只要响应满足必要性和相称性的要求即可。）"

32 1999 年 11 月，国防部法律顾问办公室，《关于信息战中国际法律问题的评估》（第 2 版），2002 年被《美国海军战争学院国际法研究》（第 459、482 卷）转载。（"挑衅和响应均不涉及使用武力的情况下，普遍承认一国国际法下权益受到侵害时可对攻击国家采取反制措施。） 例如，1978 年的仲裁裁定：在法国暂停美国飞往巴黎的商业航班后，美国有权暂停法国飞往洛杉矶的商业航班。对反制措施原则的讨论通常将违反条约义务或国际法一般原则（实际上，不涉及使用武力的报复）的反制措施与报复行为（可能是不友好、甚至是破坏性的行为，但不违法任何国际法律义务）区分开来。和自卫一样，反制措施的使用也应遵循必要性和相称性要求。"）

33 参见 18.17（报复行为）。

34 2011 年 11 月，美国国防部，《国防部网络空间政策报告》：根据《2011 财政年度国防授权法案》的国会报告（第 934 节，4-7）。（"促进网络空间爆炸式增长的互联网技术协议，同时也提供一些匿名措施。我们的潜在对手，包括国家和非国家攻击者，都清楚地了解这一动态，试图利用溯源挑战构筑战略优势。国防部认识到，阻止恶意攻击者进行网络攻击很复杂，因为难以核实发起攻击的位置以及需要在大量潜在攻击者中识别出真正的攻击者。"）

35 美国向联合国政府专家组提交的《国际安全背景下信息和电信领域的发展》（2012-2013）,2（"正如美国在 2010 年提交给 GGE 的报告中所指出的，以下既定原则适用于武装攻击背景（无论是否通过网络空间发起）：面临即将发生或实际的武装攻击时，无论是国家攻击者还是非国家攻击者，均可行使自卫权"）。

36 参见 1.11.5.4（针对非国家攻击者的自卫权），美国参谋长联席会议主席指示 3121.01B，美国部队交战常设规则/使用武力常设规则，6b（1）（2005 年 6 月 13 日）（"部队指挥官始终保留对敌对行为或敌意进行自卫的固有权利和义务。除非部队指挥官另有指示，军人可针对敌对行为或意图进行个人自卫。"）

37 参见 15.3.1（中立权）。

38 2012 年 9 月 18 日，美国国务院网络空间国际法法律顾问高洪柱（Harold Hongju Koh）在网络空间司令部跨部门法务大会上发表演讲；2012 年 12 月被哈佛国际法杂志（网络版）转载。（"国家在网络空间开展活动时必须考虑其他国家的主权，包括武装冲突之外的主权。支持互联网和网络活动的物理基础设施一般位于主权领土内，受领土主权国管辖。由于网络空间具有互联互通的性质，攻击一个国家的网络信息基础设施可能会对另一个国家产生影响。每当一个国家打算在网络空间开展活动时，都必须考虑其他国家的主权。）

39 参见 15.5（禁止使用中立国领土作为活动基地）。

40 参见 15.5.3（禁止在中立国领土上建立或使用交战通信设施）。

41 参见 15.5.3.1（不禁止交战国使用中立设施）。

42 《陆战时中立国及中立国人民之权利和义务公约》（"这里谈及的是属于中立国或公司、个人的电缆或装置，这些电缆或装置用于新闻传播，具有公共服务性质。不得强迫中立国限制或禁止交战国使用这些通信方式。若非如此，则会这里谈及的是，因为在实施控制方面存在很大困难，更不用说电报通信的保密性和快捷性了。英国代表团通过雷勋爵阁下（his Excellency Lord Reay），明确指出"中立国拥有通过其陆地电报线路、海底电缆或无线设备传输信息的自由，但并不意味着有权使用或允许使用这些设备，明确援助交战国一方。该想法极为公正，得到了委员会的一致同意。"）

43 美国国防部发表了《国防部网络空间政策报告》：根据《2011 财政年度国防授权法案》的国会报告（第 934 节，8-7）（2011 年 11 月）。（"在未取得对等'飞越权'的前提下，通过中立第三国拥有及/或位于其境内的基础设施在互联网上运输网络'武器'的合法性问题。关于'络武器'网的定义，目前尚未达成国际共识。通常，开发恶意代码的成本较低，并且网络空间中参与者的数量和种类繁多，使得发现和跟踪恶意网络工具变得困难。在这种情况下使用的大部分技术本质上都具有双重性，软件只要稍作改动就能被用于恶意用途。"）；1999 年 11 月，国防部法律顾问办公室发表了一篇《关于信息战中国际法律问题的评估》（第 2 版），2002 年被《美国海军战争学院国际法研究》（第 459、489 卷）转载。（"不必担心那些领土或通信系统用于传递破坏性信息的国家的反应。若只涉及国家的公

共通信系统，过境国通常不会意识到信息的传输。即使意识到信息传输并将消息追溯到美国，也没有任何既定的国际法原则认为这是违反规定的。如上所述，即使在国际武装冲突期间，国际法也不要求中立国限制交战国使用其公共通信网络。各国普遍同意在商业或互惠基础上免费使用通信网络。因此，使用某国的通信网络作为电子攻击通道，不会像使用军用飞机穿越其领空那样侵犯主权”。）

44 参见 5.5（实施袭击、轰炸和其他攻击的规则）。

45 参见 5.6（攻击目标区分）；5.12（相称性——禁止可能造成过度附带伤害的攻击）。

46 参见 5.7（军事目标）。

47 参见 5.17.2（敌方财产—军事必要性标准）。

48 参见 5.12（相称性——禁止可能造成过度附带伤害的攻击）。

49 2012 年 9 月 18 日，美国国务院网络空间国际法法律顾问高洪柱（Harold Hongju Koh）在网络空间司令部跨部门法务大会上发表演讲；2012 年 12 月被哈佛国际法杂志（网络版）转载。（“众所周知，信息和通信基础设施通常在国家军队和私有社区、民用社区之间共享使用。战争法要求，不得使用民用基础设施保护军事目标，这也适用于网络领域。然而，开战正义原则规则如何运用于网络空间内？武装冲突各方需评估网络攻击对非军事目标计算机（例如不具有军事意义但可能与有效军事目标计算机联网的私人、民用计算机）的潜在影响，。在进行必要的相称性审核时，各方还需考虑对使用这类基础设施的平民造成的危害。然而，可能会有一些实际情况需要进行周密、基于事实的法律分析。”）

50 参见 5.12.2（危害类型—人员伤亡和损坏）

51 Cf. 哈佛大学人道主义政策和冲突研究项目，《适用于空战和导弹战的国际法 HPCR 手册评注》，28（A.1.E.7）（2010 年）（“”攻击”的定义还包括“软杀伤”攻击（即不涉及能量物理转移的攻击，如某些计算机网络攻击）；见规则 1（m）），导致人员死亡或物体损坏。不容置否，根据国际冲突法，“软杀伤”作战能否上升至“攻击”高度是有争议的。专家组一致认为，‘攻击’一词不包括造成不便的计算机网络攻击（如暂时拒绝互联网访问）。”）

52 参见 5.12.2（危害类型—人员伤亡和损坏）

53 参见 16.5.3（采取可行的预防措施和网络作战的责任）。

54 参见 5.5（实施袭击、轰炸和其他攻击的规则）。

55 参见 5.3.2.1（军事上必要的非暴力措施）。

56 参见 16.2.2（将战争法原则作为网络作战的一般性指导）。

57 参见 5.3.3（采取可行的预防措施保护平民及其他受保护人员和对象的积极义务）。

58 美国向联合国政府专家组提交的关于在国际安全背景下信息和电信领域发展的报告（2012-2013），4（“战争法还要求交战国充分考虑军事和人道主义因素，采取一切切实可行的预防措施，以避免和尽量减少对平民和民用物体造成附带伤亡和损害。若在武装冲突中涉及信息技术，冲突各方应采取预防措施，尽量减少此类网络活动对民用基础设施及用户造成的伤害。”）

59 参见 5.11（攻击中应采取的可行预防措施，以降低对受保护人员和物体的伤害风险）。

60 参见 5.14（受攻击一方在攻击中应采取的可行预防措施，以降低对受保护人员和物体的伤害风险）。

61 参见 5.11.3（选择武器装备）。

62 美国向联合国政府专家组提交的关于在国际安全背景下信息和电信领域发展的报告（2012-2013），4（“导致非动能或可逆影响的网络作战是一个重要工具，可以最大限度地减少对平民造成不必要的伤害。在这方面，网络能力在某些情况下可能比动能武器更可取，因为它们的影响是可逆的，而且能够在不产生任何杀伤性破坏效果的情况下实现军事目标”。）

63 1999 年 11 月，国防部法律顾问办公室发表了一篇《关于信息战中国际法律问题的评估》（第 2 版），2002 年被《美国海军战争学院国际法研究》（第 459、490 卷）转载（“当一个国家有能力采取渐进式自卫措施时，这种技术能力就会产生某种影响。有人可能会辩称，拥有这种能力的国家在应对攻击时应将伤害降至最低。这无异于说，“只要可能造成潜在的意外损害，拥有精确制导弹药的国家就必须使用这些弹药”的观点。支持这种观点的国家寥寥无几，而美国更是强烈反对。人们普遍认识到，附带损害的风险只是众多军事考虑因素之一，计划攻击的军事当局必须平衡这些因素。一个显然要考虑的因素是，若一支军事力量长期受制于“只要可能造成潜在的附带损害，就必须使用精确制导弹药政策的制约，它很快就会耗尽这些弹药供应。同样地，军事当局必须能够权衡所有相关的军事考虑因素，从而选择出针对计算机网络攻击的自卫响应措施。”）

64 参见 5.24（某些标志的不当使用）。

65 参见 12.2（非敌对关系中的诚信原则）。

66 1999 年 11 月，国防部法律顾问办公室发表了一篇《关于信息战中国际法律问题的评估》（第 2 版），2002 年被《美国海军战争学院国际法研究》（第 459、473 卷）转载。（欺骗：对作战船只或飞机而言，发射医疗船只或飞机的约定识别信号以避免受到攻击似乎很有吸引力，但这种行为将构成战争罪。） 同样，计算机“变形”技术也可用来制作敌国元首图片，宣告其部队已签署停战协定或停火协议。若违背事实，这也将构成战争罪。”）

67 参见 5.23.1.5（敌方代码、密码和口令的使用不受限制）。

68 参见 4.15.2.2（通过雇佣参与敌对行动）。

69 参见 4.15（授权陪同武装部队的人员）。

70 参见 4.15（授权陪同武装部队的人员）。

71 参见 5.9（直接参与敌对行动的平民）。

72 参见 6.2（国防部武器合法性审核政策）。

73 2012 年 9 月 18 日，美国国务院网络空间国际法法律顾问高洪柱（Harold Hongju Koh）在网络空间司令部跨部门法务大会上发表演讲；2012 年 12 月被哈佛国际法杂志（网络版）转载。（“各国应对武器进行法律审查，包括具有网络能力的武器。例如，这种审查应分析某一特定能力是否属于滥杀滥伤，即未按照区分和比例原则使用。针对武装冲突背景下的武器使用，美国政府应至少开展两个阶段的法律审查：首先，评估新武器，判断新武器的使用是否是战争法所禁止的；第二，审查使用武器的行动，确保每一项行动均符合战争法规定”。）

74 参见，例如陆军部条例 27-53，《根据国际法进行武器合法性审查》（1979 年 1 月 1 日）；海军部长指令《海军部实施和运营国防采办系统和联合能力集成与发展系统》（2011 年 9 月 1 日）；空军部指令 51-402，《武器与网络能力的法律审查》（2011 年 7 月 27 日）。

75 参见 6.2.1（新武器审查）。

76 参见 6.7（滥杀滥伤武器）。

77 美国向联合国政府专家组提交的关于在国际安全背景下信息和电信领域发展的报告（2012-2013），（“不能瞄准特定军事目标或使用效果无法控制的武器，在本质上均属于滥杀滥伤；根据武装冲突法规定，这类武器都是非法的。在传统动能武器背景下，这类滥杀滥伤武器和非法武器包括生化武器。鉴于网络的互连特性，一些网络武器因为使用效果无法预测或控制而被界定为滥杀滥伤；在民用互联网系统中不加控制地传播破坏性病毒也可能认定为滥杀滥伤。战争法中禁止使用此类工具发起攻击。）”

来源：
https://www.defense.gov/Portals/1/Documents/pubs/DoD%20Law%20of%20War%20Manual%20-%20June%202015%20Updated%20Dec%202016.pdf?ver=2016-12-13-172036-190,

2018年7月25日。

附录 B：美国网络空间组织

附录 B 包括：

I. 美国国务院
   - 网络事务协调员办公室

II. 国家情报总监办公室
   - 网络威胁情报整合中心（CTIIC）

III. 美国国土安全部
   - 网络安全和基础设施局（CISA）

IV. 美国国防部
   - 国家安全局（NSA）
   - 国防部首席信息官（DOD CIO）
   - 国防信息系统局（DISA）

V. 联合组织
   - 联合频谱中心（JSC）
   - 联合通信系统支援单位（JCSE）
   - 美国网络司令部（USCYBERCOM）

VI. 军队组织
   - 美国军方网络司令部（ARCYBER）
   - 美国海军陆战队网络空间司令部（MARFORCYBER）
   - 美国海军舰队网络司令部/美国第十舰队（FCC/C10F）
   - 美国空军方网络司令部/第 24 师空军
   - 美国海岸警卫队/指挥、控制、通信、计算机、情报、监视、侦察与信息技术（C4ISR&IT）

I. 美国国防部 – 网络事务协调员办公室

1. 通过与其他各国合作，美国国务院领导美国政府努力建设开放、互通、安全可靠的信息和通信基础设施，以支持国际贸易和商务，加强国际安全，促进自由言论与创新。
2. 为了更有效地实现美国在《网络空间国际战略》中所描述的网络空间利益，2011 年 2 月成立了网络事务协调员办公室（S/CCI）。
3. S/CCI 收集了美国国务院在处理网络问题时涉及的很多部门，其职责包括：
   - 协调国务院在网络问题上的全球外交事务
   - 在这些问题上，担任国务院与白宫、联邦部门和机构的联络人
   - 就网络问题和事务向国务卿与副国务卿献计献策
   - 在网络问题上担任公共和私营部门实体之间的联络人
   - 协调国务院内处理该领域事宜的地区与职能机构的工作
4. S/CCI 的协调功能涵盖所有与网络相关的问题，包括安全、经济问题、言论自由，以及互联网信息自由传播。

来源：http://www.state.gov/s/cyberissues/，2018年7月25日。

II. 国家情报总监办公室 – 网络威胁情报整合中心

网络威胁情报集成中心（CTIIC）是国家情报总监办公室下属的四个跨部门中心中最新成立的一个，负责整合有关威胁美国国家利益的情报。根据总统备忘录，美国国家情报总监（DNI）于2015年成立CTIIC，旨在针对影响美国国家利益的外来网络威胁进行IC分析，确保在联邦网络社区中进行信息共享，并支持运营商、分析师和决策者及时了解重大网络威胁和威胁源起方。

使命。CTIIC的使命是促进对影响美国国家利益的外来网络威胁的了解，为联邦网络中心、部门和机构以及决策者的决策提供参考。CTIIC整合来自网络防护、情报和执法部门的信息；促进信息共享；主导对网络威胁的社区分析；支持跨部门规划，制定针对网络攻击的全政府方法。CTIIC发布发布情报产品，将当前网络威胁与具体情境相结合，并对攻击者使用网络手段实现其战略目标的能力和动机提供集成IC评估。

职责。根据总统备忘录，CTIIC主要履行五项职责：

- 对外来网络威胁或影响美国国家利益的网络事件相关情报进行综合全源分析。
- 支持联邦网络中心，为其提供完成各自使命所需的情报。
- 监督情报共享能力的开发和实施，以增强对外来网络威胁和事件有关的情报的共享态势感知。
- 若有必要，尽量降低恶意恶意网络活动指标以及情报渠道中包含的相关威胁报告的保密级别，以分发给美国政府和美国私营部门实体。
- 促进和支持跨部门合作，利用所有国家权力工具，包括外交、经济、军事、情报、国土安全和执法活动，制定和实施协调计划，以应对威胁美国国家利益的外来网络威胁。

组织结构。CTIIC 侧重于感知、分析和机会这三方面：

- 当前情报部门建立对包含上下文信息的重要外来网络威胁的共享态势感知。
- 分析集成部门对外来网络攻击者、威胁和事件进行综合全源分析。
- 威胁机会部门支持并促进不同机构间利用国家权力工具开发方案。

来源：https://www.dni.gov/index.php/ctiic-who-we-are，2018年7月25日。

III. 国土安全部 — 网络安全和基础设施安全局（CISA）

2018年11月16日，特朗普总统签署《2018年网络安全和基础设施安全局法案》。这项具有里程碑意义的立法提升了国土安全部内前国家保护和计划局（NPPD）的使命，成立了网络安全和基础设施安全局（CISA）。

- CISA 领导全国人民保护关键基础设施免遭当今威胁，同时与各级政府和私营部门的合作伙伴合作，以防范未来不断变化的风险。
- CISA 的名称让人们对其职责一目了然，因而可促进与合作伙伴和利益相关方的合作能力，并聘请到顶级网络安全人才。

CISA 的职责是什么？

CISA负责保护国家关键基础设施免遭物理和网络威胁。为了实现这一使命，政府和私营部门组织之间需要展开广泛有效的协作。

全面的网络防护

- CISA 的国家网络安全和通信集成中心（NCCIC）向联邦政府、州政府、地方政府、部落和地区政府、私营部门和国际合作伙伴提供全天候的网络态势感知、分析、事件响应和网络防御能力。
- CISA 提供网络安全工具、事件响应服务和评估能力，以保护支持联邦文职部门和机构基本运作的网络。

基础设施恢复能力

- 通过在私营和公共部门之间建立可信的合作伙伴关系，CISA 协调安全和恢复能力工作，并向联邦利益相关方以及全国基础设施所有者和运营商提供培训、技术援助和评估。
- CISA 通过国家风险管理中心为美国关键基础设施提供综合的全风险分析。

紧急通信

- CISA 加强了各级政府的公共安全互联互通，提供培训、协调、工具和指导，帮助全国各地的合作伙伴发展其应急通信能力。
- CISA 与全国各地的利益相关方合作，开展广泛的全国性宣传活动，以支持和提高应急响应提供者和相关政府官员在发生自然灾害、恐怖主义行动和其他人为灾害时保持通信的能力。

来源：
https://www.dhs.gov/CISA?utm_source=hp_slideshow&utm_medium=web&utm_campaign=dhs gov，2018年11月27日。

IV. 国防部

A. 国家安全局/中心安全局（NSA/CSS）

使命。国家安全局/中心安全局（NSA/CSS）为美国政府提供密码指导服务，包括信号情报（SIGINT）和信息保障（IA）产品和服务，助力计算机网络作战（CNO），使美国及其盟国始终具有决策优势。

中心安全局（CSS）向军事密码学社区提供及时、准确的密码学支持、知识和协助。它促进了国家安全局和武装部队的密码部门之间的充分合作，并与高级军事和文职领导人部门，处理并响应与军事有关的关键问题，以支持国家和战术情报目标。CSS协调和制定有关NSA/CSS信号情报和信息保障任务的政策和指南，以确保军事一体化。

美国国家安全局（NSA）的信息保障（IA）使命不同于任何其他美国政府实体。国家安全指令（NSD）授权NSA保护国家安全体系，包括处理机密信息或对军事或情报活动至关重要的系统。信息保障在履行这一职责方面具有关键的领导作用，并与政府、行业和学术界合作执行信息保障任务。

信号情报（SIGINT）。国家安全局负责向国家决策者和军队提供外国信号情报。SIGINT在国家安全中发挥着至关重要的作用，通过向美国领导人提供关于保卫国家、拯救生命和推进美国在全球的目标与联盟方面所需的关键信息。

- SIGINT 是指从外国目标所使用的电子信号和系统（如通信系统、雷达和武器系统）中衍生的情报。SIGINT provides a vital window for our nation into foreign adversaries' capabilities, actions, and intentions.
- 国家安全局的 SIGINT 使命仅限于搜集有关国际恐怖分子和外国势力、组织或个人的信息。国家安全局在收到情报需求部（包括美国政府行政机构的所以部门）提交的正式需求后，按照要求提供情报。

网络安全。国家安全局在美国网络安全方面的职责主要体现在其信息保障使命上，即管理国家安全体系。国家安全体系指包含机密信息和对美国军事或情报任务至关重要的美国系统。国家安全局有多项职能帮助政府保护这些系统，例如审批与国家安全体系安全相关的标准、技术、系统和设备。此外，国家安全局在促进美国网络安全方面地位独特，因为它还拥有外国信号情报使命。这两项使命相辅相成，加强了国家安全局检测和预防网络威胁的能力。国家安全局聘请了信号情报、信息安全和计算机网络防御和漏洞利用方面的专家。他们为国家安全局提供端到端的新视角，包括恶意网络活动、敌对外国势力活动和网络最佳实践。通常，国防部和情报界的合作伙伴需要这方面的专业知识，帮助政府缓解威胁并保护网络安全。最后，国家安全局通过与行业和学术界开展合作研究（如国家安全局技术转让计划和安全科学倡议或项目），提升网络安全状况。

国家安全局还通过国家安全局网络演习（NCX）和网络安全学术卓越中心等项目，帮助培养下一代网络专业人员的技能。

军事支持。国家安全局是美国国防部的组成部分，是一个战斗支援机构。支持世界各地的美

国军人是国家安全局所做的最重要工作之一。

- 我们通过信号情报活动为军事行动提供情报支持，而我们的信息保障人员、产品和服务则确保军事通信和数据的安全且不受敌方控制。
- 我们为作战人员和其他部队人员提供无线及有线安全通信，无论他们身处何地。我们的信息保障任务还包括制定并打包保护国家武器系统安全的代码。
- 此外，我们制定了通用协议和标准，便于我方军队与盟国、北约和世界各地的联合部队进行信息共享。互通性是联合作战和演习成功的关键。
- 为了支持军事用户，国家安全局已将其人员分派至所有主要军事司令部及全球范围的美国军事基地。国家安全局将分析师、语言学家、及工程师等人员派驻到阿富汗和其他敌对地区，为前线作战人员提供可执行的 SIGINT 情报和信息保障支持。我们部署的许多人员都在密码服务组工作，为作战司令部或总部提供专门支持。然而，自 2000 年代中期以来，国家安全局人员还同时在密码支持小组工作。这些小组被分派支持较小的部队（如旅级战斗队），确保他们获得完成特定任务所需的情报和信息保障产品及服务。这些小组使国家安全局能够促进美国全球密码事业最大程度地发挥其全部能力。
-

客户与合作伙伴。美国政府、军方和许多盟国能够顺利完成任务，都依赖于国家安全局在外国信号情报和信息保障方面的专业知识。国家安全局的客户范围很广，上至最高级别的政府（如总统办公室、国务院和参谋长联席会议），下至处境危险的小战斗队。国家安全局提供7x24全天候服务，确保客户及时获得完成任务和保护国家所需的关键情报和信息保障产品和服务。没有任何机构可独立完成这些任务，所以，国家安全局与国内外政府均有合作关系。

来源：https://www.nsa.gov/about/ 和 https://www.nsa.gov/what-we-do/support-the-military/，2018年7月25日。

B. 国防部首席信息官（DOD CIO）

使命：DOD CIO是国防部长的首席助理和高级信息技术顾问，其职能包括监督多个国家安全和国防业务系统、管理信息资源和提升效率。DOD CIO负责与国防部信息工作有关的所有事宜，包括：

- 通讯
- 频谱管理
- 网络政策与标准
- 信息系统
- 网络安全
- 定位、导航和时间安排政策
- 支持国防部指挥和控制的国防部信息工作

该组织包括四名副职和指派人员：

指挥、控制、通信和计算机（C4）和信息基础设施能力（IIC）副首席信息官（DCIO C4&IIC）。提供与 C4&IIC 相关的政策、方案和技术问题方面的专业知识和广泛指导，以整合和同步整个国防部的通信和基础设施项和工作实现和维持国防部的信息主导地位。

信息事业副首席信息官（DCIO IE）。负责整合国防部政策和指导，为国防部人员、组织和国防部任务伙伴创造信息优势。DCIO IE专注于提供领导、战略和指导，基于单一、安全、可靠的国防部IT架构和关键赋能能力，营造联合信息环境。

资源与分析副首席信息官（DCIO R&A）。负责帮助 DOD CIO 管理国防部的信息技术开支，确保每一分钱都花在刀刃上，并确保作战人员拥有完成任务所需的工具。

国防部2018财年的IT和网络空间预算申请额将近420亿美元，其中包括作战、指挥、控制和通信系统、计算服务、企业服务（如协作和邮件）以及业务系统。

网络安全副首席信息官（DCIO CS）。DCIO CS也是国防部的首席信息安全官（CISO），负责确保国防部的网络安全计划内容明确并得到妥善执行。国防部还负责与其他联邦机构、联盟伙伴和行业调整网络安全标准、政策和程序。

来源：http://dodcio.defense.gov/和http://dodcio.defense.gov/About-DoD-CIO/，2018年7月25日。

C. 国防信息系统局（DISA）

概述：DISA是国防部的战斗支援机构，由8000多名军人和文职人员组成。该机构提供、运行并确保指挥控制和信息共享能力以及可从全球各地访问的企业信息基础设施，为联合作战人员、国家领导人及军事行动中的其他任务和联盟伙伴提供直接支持。

使命：为联合作战人员开展国防部信息网络（DODIN）活动确保在所有作战领域的杀伤力，保卫国家。

愿景：在网络空间领域，成为联络和保护作战人员方面值得信赖的提供商。

目标状态：通过高性价比的基础设施和计算，随时随地提供对服务和数据的可靠、可扩展以及可控的访问服务。

DISA的任务伙伴支持：作为信息技术（IT）作战支持机构，DISA致力于向国家作战人员、国家领导人、任务和联盟伙伴提供企业级IT能力及服务。

国防信息系统局局长也是国防部信息网络联合部队总部（JFHQ-DODIN）的指挥官。JFHQ-DODIN负责指挥和控制（C2）防御性网络作战。

DISA为任务合作伙伴提供数百种IT支持和服务能力。我们的在线服务目录中包含这些功能：https://www.disa.mil（点击顶部导航栏上每类服务链接访问）。无论需要哪种IT服务或支持，DISA均能获取相关服务并提供托管、支持、工程及测试服务。

此外，为了优化国防部世界级的企业基础设施，DISA致力于提供企业服务、统一能力和移动性方案，以支持国防部随时随地采取行动。通过企业安全架构、智能计算方案和其他领先的IT机遇，DISA仍致力于扮演好IT提供商的角色，以满足防御需求。

DISA组织工作人员以最佳方式支持白宫、五角大楼、各军种、作战司令部、国防和联邦机构以及全球联盟伙伴的领导人及其合作伙伴，并与他们展开合作。

通过白宫通信局（WHCA），DISA向总统、副总统及其工作人员和美国特勤局提供直接的电信和IT支持。

DISA在五角大楼也占有重要地位，在联合参谋支持中心（JSSC）有支援小组，为参谋长联席会议主席、武装部队高级成员、由各军种高级军官组成的参谋长联席会议、联合参谋部提供直接支持。

指挥、控制、通信、计算机/网络（C4）联合参谋部通信参谋（Joint Staff J6）代表联合作战人员，支持C4需求验证和能力开发过程，同时确保参与联合作战的系统的互通性。随着企业服务的开发和发布以及企业信息基础设施的增强，国防部会逐步简历联合信息环境（JIE），在此过程中，J6会与DISA合作。

DISA设有现场办公室，与10个统一作战司令部驻扎在一起，并直接为其提供支持。

DISA通过其国防部企业计算中心（DECC）、国防信息技术契约组织（DITCO）的外勤办事处和特殊任务中心（如联合互通性测试司令部）提供国防部信息技术支持。此外，DISA负责运行DISA指挥中心（DCC），该中心保持对所有网络作战和DISA提供的基础设施、计算和企业服务的态势感知。该中心确保为DISA的所有任务伙伴提供持续优质的客户服务。

指挥链：DISA直接向国防部首席信息官（CIO）负责。国防部首席信息官办公室是国防部信息资源管理政策和监督的主要权力机构，包括与信息技术（IT）、网络防御和网络作战有关的事务。国防部首席信息官通过搜集、处理和传播不间断的信息流来支持国防部任务，以此获取并保持信息优势。国防部首席信息官对国防信息系统局局长进行授权、指导和控制，并代表本组织向国防部长（美国总统的主要顾问）报告所有国防事务。

联合信息环境（JIE）：国防部会逐步建立联合信息环境，因此各组成部分之间的界限就会

模糊化。建立JIE的矩阵型组织指明了部门的技术方向。当前组织包括参谋长联席会议（JCS）、副首席管理官办公室（DCMO）、国防部首席信息官、联合参谋部通信参谋（Joint Staff J6）、美国网络司令部（CYBERCOM）、各军种、情报界和国民警卫队。

JIE的管理由JIE执行委员会执行。该委员会由国防部首席信息官、联合参谋部通信参谋和网络司令部指挥官三人共同担任主席，他们同时也是行动发起人。

在执行中，有三条线：治理、作战和技术同步。DISA负责JIE的技术方面并领导JIE技术同步办公室（JTSO）。JTSO包括机构工作人员以及来自各军种、情报界和国民警卫队的代表。

来源：http://www.disa.mil/About，2018年7月25日。

V. 联合组织

A. 联合频谱中心（JSC）

联合频谱中心（JSC）是国防频谱组织（DSO）的现场司令部，拥有在频谱规划、电磁环境效应（E3）、信息系统、网络安全、质量保证、建模与仿真以及作战等领域领先的专家，为军事部门和作战司令部（CCMDS）提供完整的频谱相关服务。JSC在应用电磁环境数据库和分析工具方面拥有丰富的经验，能够协助获取和运营通信电子资产。JSC可提供专业知识和服务，确保可有效使用电磁频谱。

JSC提供频谱规划指导、系统集成、系统脆弱性分析、环境分析、测试和测量支持、运营支持和频谱管理软件开发等服务。

JSC为频谱规划、新式武器和传感器系统开发的频谱认证提供支持，并为联合司令部、军事部门和国防机构提供培训和作战支持。这些服务也可用于联邦政府和地方政府活动。此外，其他国家可通过对外军事销售（FMS）渠道获得援助。为了国家安全，JSC可为美国各个行业提供这些服务。

JSC 分支/服务：

网络安全和质量保证（J2）提供信息保证、技术和非技术网络作战专业知识，并监督所有DSO频谱能力和开发工作。J2还为DSO的应用程序开发和总体质量保证流程提供验收支持。

作战支援（J3）为作战司令部提供通信电子和电磁作战空间支持以及联合频谱干扰解析支持。

电磁环境效应（E3）工程（J5）通过以下方式向国防部首席信息官（DOD/CIO）、联合参谋部、各军队和其他国防部部门提供E3工程和频谱保障性（SS）技术支持：（1）管理国防部E3计划和政策制定；（2）联合能力获取支持；（3）联合E3军械计划；（4）国防部电磁兼容性标准；（5）E3和SS培训与意识。

信息系统（J6）作为企业系统和服务的客户支持顾问，向DSO和JSC提供IT支持，确保任务得到执行。J6运行和维护高级IT环境，以支持与频谱相关的软件应用程序的部署和保障。

频谱企业服务（J7）可提供联合、动态、快速响应和敏捷的频谱管理企业服务和能力，以支持作战人员的需求。全球电磁频谱信息系统（GEMIS）项目办公室开发并提供可为国防部提供支持的企业能力和服务。

应用工程部（J8）提供量身定制的工程支持和指导，使国防部和军队能够在预期的电磁环境中，主动规划、设计、获取和操作频谱相关系统。

来源：http://www.disa.mil/mission-support/spectrum/About-Us/Joint-Spectrum-Center，2018年7月25日。

B. 联合通信支援单位（JCSE）

联合通信支援单位是分配给联合赋能司令部和美国运输司令部（USTRANSCOM）的下级司令部。它为多达40人的联合特遣部队（JTF）提供途中、初始进入或早期进入通信支持，支持友好环境和非友好环境。此外，JCSE还具备必要的技能，支持更大型的联合特遣部队总部和两个联合特种作战特遣部队（JSOTF）总部，用户人数在40至1500不等。

使命：一旦接到命令，JCSE立即部署，按照指示向区域作战司令部、特种作战司令部和其他机构提供途中、早期进入、可扩展的C4支持；一旦接到命令，JCSE在72小时内提供额外C4服务，以支持更大型CJTF/CJSOTF总部的全谱作战。

组织：JCSE是联合司令部，由一个总部支援中队（HSS）、一个通讯支援分队（CSD）、三个现役中队、两个空军国民警卫中队和一个陆军预备役中队组成。

其中，三个现役中队（第一、第二和第三联合通信中队[JCS]）以及HSS和CSD的总部均位于佛罗里达州麦克迪尔空军基地。

- 陆军预备役中队（或第四 JCS）总部也位于佛罗里达州麦克迪尔空军基地。
- 空军国民警卫中队是佛罗里达州和佐治亚州空军警卫队的组成部分：
- 第 290 联合通信支援中队（JCSS）来自佛罗里达州空军警卫队，总部位于佛罗里达州麦克迪尔空军基地。
- 第 224JCSS 来自佐治亚州空军警卫队，总部位于佐治亚州不伦瑞克。

核心能力：JCSE的核心能力是能够按照运输司令部（USTRANSCOM）的指示为应急作战提供通信支持。这是JCSE的独特功能。有了JCSE，您将能够领略到满足当今作战需求的最新技术。我们是一支战术部队，在战术、作战和战略层面上拥有罕见的能力。作为应急任务的一部分，我们为多达40人的联合特遣部队（JTF）提供途中、初始进入或早期进入通信支持，支持友好环境和非友好环境。

此外，JCSE还具备必要的技能，支持更大型的联合特遣部队总部和两个联合特种作战特遣部队（JSOTF）总部，用户人数在40至1500不等。

为了满足这一广泛的任务需求，JCSE拥有一支专业部队，成员都是训练有素、部署迅速的通信专家，他们具备最新形式的网络和通信技能。我们的组织灵活多样，由现役部队和预备役部队组成。我们是整个部队的模范，各部门经常一起演习和部署，从而形成一支能够适应各种任务和工作的有效团队。

来源：http://www.jcse.mil/index_n.htm，2018年7月25日。

C. 美国网络司令部（USCYBERCOM）

使命：USCYBERCOM计划、协调、整合、同步和开展以下活动：指导国防部特定信息网络的作战和防御；准备并在接到指示时开展全谱军事网络空间作战，以便采取全领域行动，确保美国/盟军在网络空间中的行动自由，并阻止对手拥有这种自由。

关注点：USCYBERCOM有三个重点关注领域：保卫国防部信息网络（DODIN、为作战指挥官在世界各地执行任务提供支持、增强国家抵御和应对网络攻击的能力。

USCYBERCOM可统一网络空间作战方向，增强国防部的网络空间能力，并整合和加强国防部的网络专业能力。USCYBERCOM可提高国防部操作弹性可靠的信息和通信网络、应对网络空间威胁的能力，以及确保网络空间访问的能力。USCYBERCOM正在设计网络部队结构、培训要求和认证标准，使军队能够建立起执行各自任务所需的网络部队。USCYBERCOM还与跨部门和国际伙伴密切合作，执行这些关键任务。

组织：USCYBERCOM利用军队网络部门的部队执行任务。

- 第 2 集团军–陆军网络司令部（ARCYBER）
- 空军 24 师–空军网络司令部（AFCYBER）
- 美国第十舰队–舰队网络司令部（FLTCYBER）
- 美国海军陆战队网络空间司令部（MARFORCYBER）

部队：USCYBERCOM的组织概念包括133个网络任务部队（CMF）团队：

- 网络国家任务分队通过观察敌方活动、阻止攻击和机动作战而致胜，保卫国家。
- 网络作战任务分队执行军事网络作战，支持作战司令部。
- 网络防御分队保卫国防部信息网络，保护优先任务，并为战斗准备网络部队。

USCYBERCOM联合网络任务部队（CMF），共同支持联合部队. 具体而言，在USCYBERCOM网络联合部队总部的框架下，CMF各小组重点关注对作战司令部的日常支持：

- MARFORCYBER 支持美国特种作战司令部（USSOCOM）
- ARCYBER 支持美国中央司令部（USCENTCOM）、美国非洲司令部（USAFRICOM）和美国北方司令部（USNORTHCOM）
- FLTCYBER 支持美国太平洋司令部（USPACOM）和美国南方司令部（USSOUTHCOM）
- AFCYBER 支持美国欧洲司令部（USEUCOM）、美国战略司令部（USSTRATCOM）和美国运输司令部（USTRANSCOM）

来源：https://www.cybercom.mil/，2018年7月25日。

VI. 军队组织

A. 美国陆军网络司令部（ARCYBER）

美国陆军网络司令部是直接向陆军部总部（HQDA）报告的作战级陆军部队。根据美国网络司令部指挥官的授权，ARCYBER指挥官对陆军部队实施作战控制。ARCYBER是主司令部，负责按照战略司令部指挥官或美国网络司令部指挥官的指示和授权进行网络空间作战（进攻性网络空间作战、防御性网络空间作战和国防部信息网络作战）。ARCYBER组织、管理、部署和维护陆军网络部队开展网络空间作战，并提供培训、人员、设备和资金。

使命。根据授权或指示，指导和执行综合性的电子战、信息和网络空间作战，以确保在网络空间和信息环境中的行动自由，并阻止对手拥有这种自由。

愿景。

- 一支能够积极作战，保护国家网络、数据和武器系统的部队
- 一支能够在网络空间内和通过网络空间对敌方产生影响，实现指挥官目标的部队
- 一支为未来战斗设计、构建和提供综合能力的部队—包括网络空间战、电子战和信息战

组织。

陆军网络部队单位包括：

美国陆军网络企业技术司令部（**NETCOM**）领导国防部信息网络（DODIN）陆军部分的全球行动，确保在网络空间中的行动自由，同时阻止对手拥有这种自由。

第一信息作战司令部（陆地）通过以下方式向陆军和其他军队提供信息作战支持：

- 可部署支援小组
- 对立部队支援
- 后方支援规划与分析
- 专业培训

第780军事情报旅（网络）是美国陆军情报与安全司令部的主要下属司令部，作战控制权归美国陆军网络司令部所有。它开展网络空间作战并传送信号情报，实现网络空间作战效果，以获得和保持陆军及联合需求的行动自由，同时阻止对手拥有这种自由。

来源：http://www.arcyber.army.mil/，2018年7月25日。

B. 美国海军陆战队网络空间司令部（MARFORCYBER）

使命

1. 作为美国网络司令部指挥官的海军陆战队服务部门的指挥官，海军陆战队网络空间司令部指挥官（COMMARFORCYBERCOM）代表海军陆战队的能力和利益；就海军陆战队部队的合理使用和支持向 CDRUSCYBERCOM 提供建议；协调部署、使用以及重新部署附属部队的规划和执行。
2. COMMARFORCYBERCOM 支持全谱网络空间作战，包括规划和指导海军陆战队企业网络作战（MCEN Ops）、支持海军陆战队、联合部队和联军的防御性网络空间作战（DCO），以及规划和指导（在获得授权情况下）联合部队和联军的进攻性网络空间作战（OCO），以便在所有作战领域实现行动自由，并阻止敌方部队拥有这种自由。
3. COMMARFORCYBERCOM 对海军陆战队网络空间战大队（MCCYWG）和海军陆战队网络空间作战大队（MCCOG）实施直接作战控制，以支持任务需求和各项任务。
4. COMMARFORCYBERCOM 还兼任联合部队司令部网络司令部（JFHQ-C）/海军陆战队司令部（JFHQ-C/Marines）的指挥官。JFHQ-C/Marines 向 OCO 的作战司令部提供支持，并在接到指示时通过附属网络空间部队开展网络空间作战。JFHQ-C/Marines 负责附属网络空间部队的指挥、控制和战术指导。
5. 下属单位。

海军陆战队网络空间作战大队（MCCOG）执行海军陆战队国防部信息网络（DODIN）行动和海军陆战队DCO，以增强跨作战领域的行动自由，同时阻止敌方通过网络空间降低或破坏这一优势。

海军陆战队网络空间战大队（MCCYWG）负责组织、训练、装备、提供行政支持、管理指派部队的战备状态，并向USCYBERCOM推荐认证并介绍网络任务部队（CMF）小组。MCCYWG按照COMMARFORCYBER的指示规划和实施全谱网络空间行动，以支持服务、作战指挥、联合部队及联盟的需求。

来源：http://www.candp.marines.mil/Organization/Operating-Forces/US-Marine-Corps-Forces-Cyberspace-Command/，2018年7月25日。

C. 美国舰队网络司令部/美国第十舰队（FCC/C10F）

作战—美国舰队网络司令部/美国第十舰队（FCC/C10F）作战人员指挥网络空间作战，在确保网络空间行动自由的同时，威慑和击败入侵。然而，作战并不局限于网络空间，因为FCC/C10F是海军除网络和网络作战之外的密码/信号情报、信息作战、电子战和空间能力的中央作战机构。

- 美国舰队网络司令部（FCC）是美国网络司令部的海军司令部和国家安全局/中央安全局下属的海军服务密码司令部。舰队网络司令部还作为二级司令部直接向海军作战部长负责。
- 美国第 10 舰队（C10F）是舰队网络司令部的作战部队，通过类似于其他作战指挥官的特遣部队结构来执行任务。在这一角色中，通过位于马里兰州乔治米德堡的海上作战中心，C10F 提供作战指导，执行对指派部队的指挥和控制，从而支持在网络、信息作战、电子战、密码/信号情报联合和空间领域的海军任务或联合任务。

舰队网络司令部

使命：舰队网络司令部的使命是规划、协调、整合、同步、指导和开展全面的网络空间作战活动，以确保海军在网络空间所有作战领域内的行动自由，并阻止敌方海军拥有这种自由。

愿景：舰队网络司令部的愿景是在网络空间及通过网络空间、电磁频谱和太空展开作战，确保海军和联合/联军的行动自由和决策优势，同时阻止对方拥有这种自由和优势。通过追求卓越以及加强与美国政府、国防部、学术界、行业以及国外合作伙伴的联合，我们终将赢得这些领域的胜利。

第十舰队

使命：第十舰队的使命是计划、监测、指导、评估、通讯、协调和执行作战行动，实现指挥和控制，并通过以下方式为下属部队的成功创造条件：

- 作为美国舰队网络司令部的编号舰队，对美国舰队网络司令部指派的部队实施作战控制。
- 通过网络空间、太空和电磁频谱向全球海军指挥官指导和交付所需的战术和作战效果，确保在美国舰队网络司令部指定任务区域内成功执行任务。

来源：http://www.public.navy.mil/fcc-c10f/Pages/home.aspx和http://www.public.navy.mil/fcc-c10f/Fact%20Sheets/FCC-C10F%20Fact%20Sheet%202014.pdf，2018年7月25日。

D. 美国空军方网络司令部/空军24师

该司令部有三个不同的角色和职责。每个角色和职责都有一套独特的权限和命令链。

空军网络角色：指挥官利用空军网络部队支持美国网络司令部（USCYBERCOM），以规划和执行整个空军信息网络（AFIN）、国防部信息网络（DODIN）和其他关键网络领域的全谱网络空间行动。

空军24师角色：指挥官直接对空军作战司令部指挥官负责，并在空军内部负责组织、训练和装备网络部队和能力，以支持联合任务、联盟任务和军事任务。空军24师还为空军网络（AFNET）、空军网络安全（AFNET-S）以及其他指定的网络领域提供网络安全服务。

联合部队司令部网络司令部角色：指挥官受托负责规划和执行（根据总统和/或国防部长的命令）进攻性网络空间行动，以支持作战指挥官。

空军24师共有5600多人,他们开展网络空间作战或提供全天候支持，其中包括大约3250名军事人员、900名平民和1400名承包商。约有1100名空军预备役部队人员转到空战司令部（ACC），他们来自现有的空军预预备役部队，以及与第688网战联队、第67网战联队和空军网络作战有关的空军国民警卫队。

组织：空军24师由一个综合作战中心（OC）（624OC）和两个联队（第688、67网战联队）组成。

> 位于德克萨斯州圣安东尼奥-拉克兰联合基地的**第624作战中心**受空军24师司令部领导。它接受美国网络司令部的命令和任务分派，并为第24空军下属部队分派任务，执行广泛的网络任务，为空军和联合部队指挥官提供支持。第624作战中心管理网络指挥和控制任务系统武器系统。
>
> **第67网战联队**总部位于德克萨斯州圣安东尼奥拉克兰联合基地。它是空军最新的战斗联队，是作为空军网战的执行机构，利用网络空间漏洞评估/猎手武器系统生成、规划和维持战斗力。其员工由来自三个作战大队的2000名空军士兵、平民和承包商组成，在全球七个地点共拥有26家单位。他们为空军、作战司令部和国家机构提供网络作战、防御、攻击和漏洞利用的服务。
>
> **第688网战联队**总部位于德克萨斯州圣安东尼奥拉克兰联合基地。它执行网络空间能力开发、测试和评估等不同任务；开发和验证网络战术；将网络集成至空军作战中心培训任务中；聘用网络防护团队防护国防部重点网络和系统免受威胁；控制空军网络和信息作战正式训练部队。第五作战通信小组位于佐治亚州罗宾斯空军基地，接受第688网战联队的领导。

来源：https://www.afcyber.af.mil/，2018年7月25日。

E. 美国海岸警卫队

指挥、控制、通信、计算机、情报及监视、侦察&信息技术（C4ISR&IT）

使命。加强指挥、控制、通信、计算机、情报、监视、侦察和信息技术在执行海岸警卫队任务中的价值；根据海岸警卫队的战略目标、任务和客户需求，制定企业战略、政策和资源决策。

目的与目标。C4ISR&IT的五大战略目标为：网络空间作战、高效信息管理、技术创新、治理和组织卓越。

目标1：网络空间作战。通过预防C4ISR&IT安全事件（如网络攻击和入侵，以及加强C4ISR&IT安全缓解与恢复），提高任务效率。预防、缓解和恢复目标可支持目的达成：

1.1 预防：根据美国联合信息环境、国防部和国土安全部政策，通过适当的保护措施和程序保护海岸警卫队的网络空间，并确保信息的机密性、完整性、可用性和隐私性，从而增强 C4ISR&IT 网络安全。
1.2 加强整个海岸警卫队的信息安全。
    1.2.1 OSC 转换为国防部服务器加固指南。
    1.2.2 制定 IT 关键基础设施和关键资源的优先级列表。
    1.2.3 建立信息保障计划。
1.3 缓解：提高海岸警卫队及时发现和响应 C4ISR&IT 事件的能力，同时尽量减少系统中断，并提高海岸警卫队执行任务的能力。
1.4 计算机网络防御（CND）能力。
1.5 恢复：部署和指派适当的 C4ISR&IT 资源，以快速恢复海岸警卫队系统和数据。
1.6 移动指挥中心（MCC）开发。
    1.6.1 应急卫星通信。

来源–2015-201财年战略规划：https://www.dcms.uscg.mil/Portals/10/CG-6/FY15-19_C4ISRandIT_Strategic_Plan.pdf?ver=2016-12-05-161842-567，2018年7月25日。

术语表

本文中大部分术语来自《国防部军事及相关术语词典》（截至 2018 年 6 月）。其他网络空间术语来自《网络作战与网络恐怖主义》、《DCSINT 手册 1.02》（2005 年 8 月 15 日）和美国计算机应急准备小组（US-CERT）网站。

责任区（AOR）–与作战司令部相关的地理区域。在该区域内，作战指挥官有权计划和执行作战行动。

战场毁伤评估（BDA）–包括对物理损伤和功能性损伤的评估，以及对使用致命或非致命军事力量而造成目标系统损害的评估。

CCDR–作战指挥官（Combatant Commander）。

CCMD–作战司令部（Combatant Command）。

CCMF–网络作战任务部队（Cyber Combat Mission Force）。

CERF–网络攻击效果请求格式表（Cyber Effects Request Format）。

CJCS–参谋长联席会议主席（Chairman of the Joint Chiefs of Staff）。

CCMF–网络任务部队（Cyber Mission Force）。

CMT–作战任务小组（Combat Mission Team）。

CO-IPE–网络作战整合规划部门（Cyberspace Operations-Integrated Planning Element）。

命令与控制（C2）–在完成任务过程中，指挥官对指派和附属部队行使权力和指挥权。

指挥官的关键信息需求（CCIR）–是指由指挥官提出的信息需求，对及时决策至关重要。

作战方针（CONOPS）–一种口头或图形陈述，清楚、简洁地表达出联合部队指挥官计划完成的任务以及如何利用现有资源去完成。

反情报（CI）–是指为了外国势力、组织或个人或其代理人、国际恐怖组织或活动而收集的信息和开展的活动，或代表外国势力、组织或个人或其代理人、国际恐怖组织或活动而收集的信息和开展的活动，目的是为了识别、欺骗、利用、破坏或防止间谍活动、其他情报活动、破坏或暗杀。

行动计划（COA）–是指：1、个人或单位要完成的一系列活动。2、为完成任务而制定的计划。3、联合作战规划过程中的行动计划开发环节的产品。

CPT–网络空间防护小组。

网络安全–是指对计算机、电子通信系统、电子通信服务、有线通信和电子通信（包括其中包含的信息）的防护、保护和恢复，以确保其可用性、完整性、认证、保密性和不可否认性。

网络空间–指全球信息环境，由相互依赖的信息技术基础设施和驻留数据网络构成，包括互联网、电信网络、计算机系统、嵌入式处理器和控制器。

网络作战–是指确保使用网络空间能力，以便在网络空间或通过网络空间实现目标。

网络空间优势–是指部队在网络空间中的优势程度，利用这种优势，该部队及其相关的陆、空、海、网络空间部队可在给定时间和地点安全、可靠地开展作战，而不受敌方的禁止性干扰。

数据挖掘–是指使用计算机筛选个人数据、背景以识别某些行动或请求项的方法。

防御性网络空间行动（DCO）–是指被动和主动网络空间作战，旨在保持利用友好网络空间的能力和保护数据、网络、网络中心能力和其他指定系统的能力。

DCO 内部防御措施（DCO-IDM）–是指根据授权在国防部信息网络内进行的有计划的防御措施或活动，包括积极探查高级内部威胁以及对这些威胁的内部响应。

DCO 响应活动（DCO-RA）–是指为保护国防部网络空间能力或其他指定系统而在被保护网络之外进行的有计划的防御措施或活动。

拒绝服务攻击（DoS）–旨在破坏网络服务的网络攻击，一般通过每秒数百万次的请求拖垮系统，导致网络速度变慢或崩溃。

国防部信息网络（DODIN）–DODIN是一套全球互联、端到端的信息功能和相关流程，根据需要为作战人员、决策者和支持人员搜集、处理、储存、传播和管理信息，包括自有和租用的通信和计算系统和服务、软件（包括应用程序）、数据、安全服务、其他相关服务和国家安全系统。

DISA–国防信息系统局。

网络作战指挥权（DACO）：向国防部国防部所有部门发布命令和指令，执行全球国防部信息网络作战和防御网络空间作战内部防御措施的权利。

分布式拒绝服务（DDoS）–是指使用大量计算机同时攻击目标的网络攻击。这种攻击不仅会发出更多的请求使目标过载，而且从多个路径发动DoS会使回溯异常困难，几无可能。很多时候，蠕虫被植入计算机以创建僵尸，这样，攻击者便可在用户不知情的情况下使用这些机器参与攻击。

DoD–国防部

国防部信息网络（DODIN）行动–是指设计、构建、配置、保护、运营、维护和维持国防部网络的行动，目的是为国防部信息网络提供长期的信息保障。

电磁频谱（EMS）–指电磁辐射从零到无穷大的频率范围，分为26个指定波段，按字母顺序排列。

电磁频谱管理–是指通过操作程序、工程程序和管理程序来规划、协调和管理电磁频谱的使用。

电子攻击（EA）–是电子战的一个分支，使用电磁能、定向能或反辐射武器攻击人员、设施或设备，目的是削弱、压制或摧毁敌人的作战能力，该种攻击视为一种火力形式。

电子战（EA）–是指利用电磁能和定向能控制电磁波谱或攻击敌人的军事行动。

电子邮件欺骗–是指向用户发送电子邮件，将真实发件人伪装为其他来源。

执行命令（EXORD）–是指：1、参谋长联席会议主席根据国防部长的指示发布的命令，目的是执行总统发起军事行动的决定。2、按照指示发起军事行动的命令。

防火墙–是指使财产远离破坏的屏障。

GCC–战区作战指挥官

黑客–是指高级计算机用户，他们花费大量时间，利用计算机努力寻找IT系统中的漏洞。

黑客行动主义者–他们是黑客和激进主义分子的结合。他们的活动通常具有政治动机，可通过行为来识别这种动机，例如他们可能会用反信息或虚假信息来篡改对手网站。

信息环境–是指搜集、处理、传播信息或根据信息采取行动的个人、组织和系统的集合。

信息作战（IO）–在军事行动中，综合利用与信息有关的能力，并与其他作战方略一起，在保护自己的同时影响、干扰、破坏或获取敌方和潜在敌方的决策。

IPR–过程审核。

情报–是指：1、搜集、处理、整合、评估、分析和解释有关他国、敌对或潜在敌对势力或因素、或实际或潜在作战区域的现有信息的产物。2、可产生上述产品的活动。3、从事这些活动的组织。

情报需求（IR）–是指：1、需要搜集信息或生成情报的一般或具体缘由。2、为填补司令部对作战环境或威胁部队在知识或理解上的空白而提出的情报需求。

情报、监视和侦察（ISR）–是指一种同步和集成传感器、资产的规划和操作以及处理、开发和分发系统的活动，直接支持当前和未来的行动。这是一项综合情报和作战功能。

J-1–联合参谋部人力与人事局；人力资源处。

J-2–联合参谋情报局；情报处。

J-3–联合参谋作战局；作战部。

J-4–联合参谋后勤局；后勤处。

J-5–联合参谋战略规划局；战略规划处。

J-6–联合参谋通信系统局；指挥、控制、通信和计算机系统参谋处。

FJHQ-C–联合部队司令部网络空间。

JFHQ-DODIN–联合部队司令部—国防部信息网络。

联合火力分队（JFE）–是一个可选的参谋分部，它向作战部提供完成火力规划和同步的建议。

联合部队指挥官（JFC）–该通用术语适用于作战指挥官、二级联合指挥官或联合特遣部队指挥官，他们授权对联合部队行使作战指挥权或控制权。

联合综合优先目标列表（JIPTL）–是指由联合部队指挥官批准和维护的优先目标清单。

联合作战情报环境准备（JIPOE）–联合情报组织用来生成情报评估和其他情报产品的分析过程，以支持联合部队指挥官的决策。

联合规划程序（JPP）–由一系列分析性的逻辑步骤构成，用以解决问题、检查任务，以及开发、分析和比较替代行动方案（COA）、选择最佳COA、形成计划或命令等。

联合作战区（JOA）–是指由战区作战指挥官或下属联合指挥官定义的陆地、海洋和空域。联合部队指挥官（通常是联合特遣部队指挥官）在这些地域执行军事行动以完成特定任务。

联合目标列表（JTL）–是指选定目标的综合清单。对这些选定目标没有任何限制，并且它们在联合部队指挥官的作战区域内具有重大军事意义。

联合目标协调委员会（JTCB）–由联合部队指挥官组成，负责完成广泛的目标监督职能，包括但不限于协调目标信息、为目标选择提供指导、同步以及确定优先事项，并完善联合一体化优先级目标列表。

联合特遣部队（JTF）–由国防部长、作战指挥官、二级联合指挥官或现有联合特遣部队指挥官成立并指派的联合部队。

键盘记录器–这是一种软件程序或硬件设备，用于监视和记录用户的每次键入。

作业线（LOE）–在联合作战规划的背景下，根据目标（因果），通过将多项工作和任务联系起来，努力创建作战条件和战略条件。

作战线（LOD）–是指确定部队相对于敌人内部或外部方向的线，或在时间和空间上相关的节点和/或决策点将行动与目标相连的线。

逻辑炸弹–这是一种程序例程，通过重新格式化硬盘或在数据文件中随机插入无用数据来销毁数据。

恶意软件–是指专门设计用来破坏系统的软件，如病毒或木马。

有效性度量（MOE）–是指用于评估系统行为、能力或作战环境变化的标准，可用于测量最终状态的实现、目标的达成或效果的产生。

性能度量（MOP）–是指用于评估与衡量任务完成情况的标准。

军事欺骗（MILDEC）–是指为了故意误导敌方军事、准军事或暴力极端主义组织决策者而采取的行动，从而使敌方采取有助于完成任务的特定行为（或不作为）。

军事信息支援**作战（MISO）**–是指将选定的信息和指标传达给外国受众的计划性行动，以影响他们的情绪、动机、客观推理，并最终影响外国政府、组织、团体和个人的行为，从而有利于发起者实现目标。

导航战（NAVWAR）–是指有计划的防御和攻击行动，目的是通过协调利用太空、网络空间和电子战行动，确保定位、导航和定时信息的安全。

非保密互联网协议路由器网络（NIPRNET）–是指美国国防部使用的全球多段网络。

进攻性网络空间作战（OCO）–是指在网络空间或通过网络空间使用武力营造影响力的网络空间行动。

作战命令（OPORD）–是指指挥官向下级指挥官发布的指令，以实现行动的协调执行。

作战计划（OPLAN）–是指：1、为应对实际发生的和潜在的突发事件而制定的军事行动计划。2、完整详尽的联合计划，包含对作战方针的完整描述、适用于该计划的所有附件以及分阶段的部队及部署数据。

作战环境（OE）–是影响功能使用的条件、环境和影响因素的综合，是指挥官决策的重要参考依据。

作战环境准备（OPE）–在可能或潜在的作战区域开展活动，以准备和塑造作战环境。

勒索软件–这是一种恶意软件，用于感染并限制对计算机的访问，直到支付赎金为止。勒索软件有多种传播方法，但大多利用网络钓鱼邮件或软件中未修补的漏洞。

后方支援–从非前沿部署的组织处获取产品、服务和应用，或部队、设备或材料的过程。

交战规则（ROE）–由主管军事当局发布的指示，规定美国部队发起和/或继续与其他部队作战的各种情况和限制。

保密 IP 路由网络（SIPRNET）–采用高速互联网协议路由器和大容量国防信息系统网的全球秘密级数据包分组交换网络。

信号情报（SIGNT）–1、它是一种情报类别，包括所有通信情报、电子情报和外国仪器信号情报中的一种或多种，情报的传输方式不限。2、由通信信号、电子信号和外国仪器信号衍生而来的情报。

嗅探器–旨在帮助黑客和/或管理员从其它计算机处获取信息或监控网络的程序。这类程序查找某些信息，可将信息存储供以后检索，也可将信息传递给用户。

垃圾邮件–互联网上未经请求的产品和服务广告，专家估计这类广告约占电子邮件的50%。

间谍软件–是指在个人或组织不知情的情况下搜集信息的技术。间谍软件可作为软件病毒或以安装新程序的方式进入计算机系统。广告软件是被设计用于广告目的的软件。广告软件通常也可以被认为是间谍软件，因为它们都包含跟踪和报告用户信息的组件。

特种作战部队（SOF）–是指由国防部长授命专门组织、训练和武装的现役和预备役部队，执行和支持特种作战。

TTP–策略、技术与过程。

时敏目标（TST）–联合部队指挥官确认一个或一组需要立即做出响应的目标，因为它是有利可图、机会短暂的目标，或对友军构成（或即将构成）危险。

木马–这是一种程序或实用程序，可伪装为正常程序，如屏幕保护程序。但是，一旦安装，它就会在后台执行某个功能，例如向其他用户开放目标计算机的访问权限或从目标计算机向其他计算机发送信息。

病毒–用于感染、破坏、修改计算机或软件程序或使计算机或软件出现其他问题的软件程序、脚本或宏。

蠕虫–这是一种破坏性软件程序，包含能够访问计算机或网络的代码，一旦进入计算机或网络内，便可通过删除、修改、分发等数据操控方法来破坏该计算机或网络。

僵尸机–是指被某种恶意软件劫持用于帮助黑客执行DDoS攻击的计算机或服务器。

关于在线的军事相关术语词典，请访问：
http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf

约瑟夫·邓福德（Joseph F. Dunford）将军，和约瑟夫·邓福德将军一起认识当今全球安全挑战（2016 年 3 月 29 日），内容详见美国国际战略研究中心的网站首页（2016 年 4 月 1 日）：http://csis.org/files/attachments/160329_Meeting_Today%27s_Global_Security_Challenges_with_General_Joseph_F_Dunford.pdf。

美国参谋长联席会议，美国国防部军事及相关术语词典（华盛顿特区：美国参谋长联席会议，2018 年 6 月），60。

布雷特 T.威廉姆（Brette T. Willams），联合部队季刊（2014 年第 2 季、总第 73 期）,联合部队指挥官网络空间作战指南。

美国参谋长联席会议，联合规划，联合条例（JP）5-0（华盛顿特区：美国参谋长联席会议，2017 年 6 月 16 日），xvi。

JP5-0，xi。

P5-0，xiii。

美国参谋长联席会议，网络空间作战，JP3-12（华盛顿特区：美国参谋长联席会议，2018 年 6 月 8 日），xii-xiii。

JP3-12，vii-viii。

JP3-12，x。

JP3-12，xvii。

JP5-0，xxi。

JP5-0，IV-7。

JP5-0，IV-6–7。

JP5-0，IV-8。

美国总统唐纳德·J·特朗普（Donald Trump），美国国家安全战略（华盛顿特区：白宫，2017 年 12 月），II，https://www.whitehouse.gov/wp-content/.../2017/12/NSS-Final-12-18-2017-0905.pdf（2018 年 7 月 9 日）。

美国国家安全战略，12-13。

美国国家安全战略，18-23。

美国国家安全战略，32。

美国国家安全战略，40-41。

美国国防部长詹姆斯·N·马蒂斯（James N. Mattis）,《美国国防战略概要：增强美国的军事竞争优势》（华盛顿特区：国防部），1，https://www.defense.gov/Portals/1/Documents/pubs/2018-National- Defense-Strategy-Summary.pdf（2018 年 7 月 9 日）。

美国国防战略概要，3。

美国国防战略概要，6。

美国国防部长詹姆斯·N·马蒂斯（James N. Mattis），2018 年网络防护战略概要（华盛顿特区：国防部，2018 年 9 月），3–6，https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF（2018 年 11 月 1 日）。

P5-0，IV-9。

JP5-0，IV-9。

美国国务院，给总统提建议：通过国际合作保护美国的网络利益（华盛顿特区：国务院），1–3，https://www.state.gov/s/cyberissues/eo13800/281980.htm（2018 年 7 月 9 日）。

JP5-0，IV-10。

美国参谋长联席会议，联合作战中的跨域协同，JP5-0（华盛顿特区：美国参谋长联席会议，2016 年 1 月 14 日），49-50。

本杰明·C·雷泽尔（Benjamin C. Leitzel），网络跳弹：风险管理和网络空间作战（宾夕法尼亚州卡莱尔：美国陆军战争学院战略领导中心，2012 月 7 月）。

《联合作战中的跨域协同》，50-51。

美国陆军部，《网络空间与电子作战》，战地手册（FM）3-12（华盛顿特区：陆军总部，2017 年 4 月 11 日），1-14。

JP3-12，I-3。

JP3-12，I-4–5。

JP3-12，I-5。

JP5-0，IV-14。

JP3-12，I-11。

JP3-12，I-12。

美国国家情报总监丹尼尔·R·科茨（Daniel R. Coats），2018 年美国情报界全球威胁评估报告，美国参议院特别情报委员会（华盛顿特区，2018 年 2 月 13 日），4–5。

丹尼尔·R·科茨（Daniel R. Coats），《2018 年美国情报界全球威胁评估报告》，6。

美国国家情报总监詹姆士·R·克拉柏（James R. Clapper），全球网络威胁评估报告，美国众议院常设情报委员会（华盛顿特区，2015 年 9 月 10 日），4。

“大陪审团对 12 名俄罗斯情报总局官员进行起诉，指控其参与干扰 2016 年美国总统大选活动”，内容详见司法部网站首页：https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers- hacking-offenses-related-2016-election （2018 年 7 月 16 日）。

美国网络司令部司令迈克尔•S•罗杰斯（MICHAEL S. ROGERS）海军上将在美国参议院军事委员会听证会上的讲话（华盛顿特区，2018 年 2 月 27 日），5-6。
丹尼尔·R·科茨（Daniel R. Coats），2018 年美国情报界全球威胁评估报告，6。
“中国商人承认与人合谋入侵美国国防承包商系统窃取敏感军事信息”，内容详见美国司法部首页：https://www.justice.gov/opa/pr/chinese-national- pleads-guilty-conspiring-hack-us-defense-contractors-systems-steal-sensitive（2017 年 5 月 26 日）。
“联邦调查局通缉令”，内容详见美国联邦调查局首页：https://www.fbi.gov/wanted/cyber/huang-zhenyu/view（2017 年 5 月 26 日）。
詹姆士•R•克拉柏（James R. Clapper），全球网络威胁报告，2。
美国网络司令部司令迈克尔•S•罗杰斯（MICHAEL S. ROGERS）海军上将在美国参议院军事委员会听证会上的讲话，4-5。
丹尼尔·R·科茨（Daniel R. Coats），2018 年美国情报界全球威胁评估报告，6。
“联邦调查局通缉令”，内容详见美国联邦调查局首页：https://www.fbi.gov/news/stories/2016/march/iranians- charged-with-hacking-us-financial-sector（2017 年 5 月 26 日）。
“曼哈顿美国检察官宣布指控 7 名伊朗人，指控其代表伊斯兰革命卫队赞助的实体对美国金融部门进行协调网络攻击活动”，内容详见美国司法部首页：https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney- announces-charges-against-seven-iranians-conducting-coordinated（2017 年 5 月 26 日）。
美国国家情报总监詹姆士·R·克拉柏（James R. Clapper），全球网络威胁评估报告，美国众议院常设情报委员会（华盛顿特区，2015 年 9 月 10 日），3。
丹尼尔·R·科茨（Daniel R. Coats），2017 年美国情报界全球威胁评估报告，1。
丹尼尔·R·科茨（Daniel R. Coats），2017 年美国情报界全球威胁评估报告，6。
丹尼尔·R·科茨（Daniel R. Coats），2017 年美国情报界全球威胁评估报告，6。
美国网络司令部司令迈克尔•S•罗杰斯（MICHAEL S. ROGERS）海军上将在美国参议院军事委员会听证会上的讲话，6。
詹姆士•R•克拉柏（James R. Clapper），全球网络威胁报告，4。
丹尼尔·R·科茨（Daniel R. Coats），2018 年美国情报界全球威胁评估报告，6。
丹尼尔·R·科茨（Daniel R. Coats），2018 年美国情报界全球威胁评估报告，6。
“联邦调查局通缉令”，内容详见美国联邦调查局首页：https://www.fbi.gov/news/stories/2016/march/two-from- syrian-electronic-army-added-to-cybers-most-wanted/two-from-syrian-electronic-army-added-to-cybers-most-wanted（2017 年 5 月 26 日）。
“联邦调查局通缉令”，内容详见美国联邦调查局首页：https://www.fbi.gov/wanted/cyber/firas-dardar（2016 年 4 月 1 日）。
“两名叙利亚电子军成员因涉嫌参与针对美国的黑客攻击阴谋而受到美国当局指控”，内容详见美国司法部首页：https://www.justice.gov/usao-edva/pr/two-members-syrian-electronic-army-indicted-conspiracy（2018 年 7 月 9 日）。
丹尼尔·R·科茨（Daniel R. Coats），2018 年美国情报界全球威胁评估报告，6。
丹尼尔·R·科茨（Daniel R. Coats），2018 年美国情报界全球威胁评估报告，2。
丹尼尔·R·科茨（Daniel R. Coats），2018 年美国情报界全球威胁评估报告，2。
“联邦调查局通缉令”，内容详见美国联邦调查局首页：https://www.fbi.gov/wanted/cyber/igor-anatolyevich-sushchin（2017 年 5 月 26 日）。
丹尼尔·R·科茨（Daniel R. Coats），2017 年美国情报界全球威胁评估报告，2。
“36 名被告因涉嫌参与跨国犯罪组织造成网络犯罪而被起诉，涉案金额高达 5.3 亿美元”，内容详见美国司法部首页：https://www.justice.gov/opa/pr/thirty-six-defendants-indicted-alleged-roles-transnational-criminal-organization- responsible（2018 年 7 月 9 日）。
“曼宁 20 项罪名全部成立，但‘通敌罪’不成立”，内容详见美国陆军部首页：http://www.army.mil/article/108143/Closing_arguments_heard_in_Pfc_Manning_trial/（2017 年 5 月 26 日）。
“美国司法部向香港提出协助引渡爱德华·斯诺登（Edward Snowden）的请求”，内容详见美国司法部首页：https://www.justice.gov/opa/pr/justice-department-statement-request-hong- kong-edward-snowden-s-provisional-arrest（2017 年 5 月 26 日）。

美国核管理委员会前雇员承认曾试图在能源部计算机上进行网络钓鱼攻击，内容详见美国司法部首页：https://www.justice.gov/opa/pr/former-us-nuclear-regulatory-commission-employee-pleads-guilty-attempted-spear- phishing-cyber（2017 年 5 月 26 日）。
“佐治亚州联邦政府承包商被指控将机密材料发送至一家新闻机构。”，内容详见美国司法部首页：https://www.justice.gov/opa/pr/federal-government-contractor- georgia-charged-removing-and-mailing-classified-materials-news（2018 年 7 月 9 日）。
美国陆军部，网络作战与网络恐怖主义，DCSINT 手册 No. 1.02（堪萨斯州利文沃思堡：美国陆军训练及战略思想司令部，2005 年 8 月 15 日），I-8–11。
美国计算机应急准备小组，勒索软件，内容详见 US-CERT 首页：https://www.us- cert.gov/security-publications/Ransomware （2017 年 5 月 26 日）。
美国陆军部，网络作战与网络恐怖主义，II-8–11。

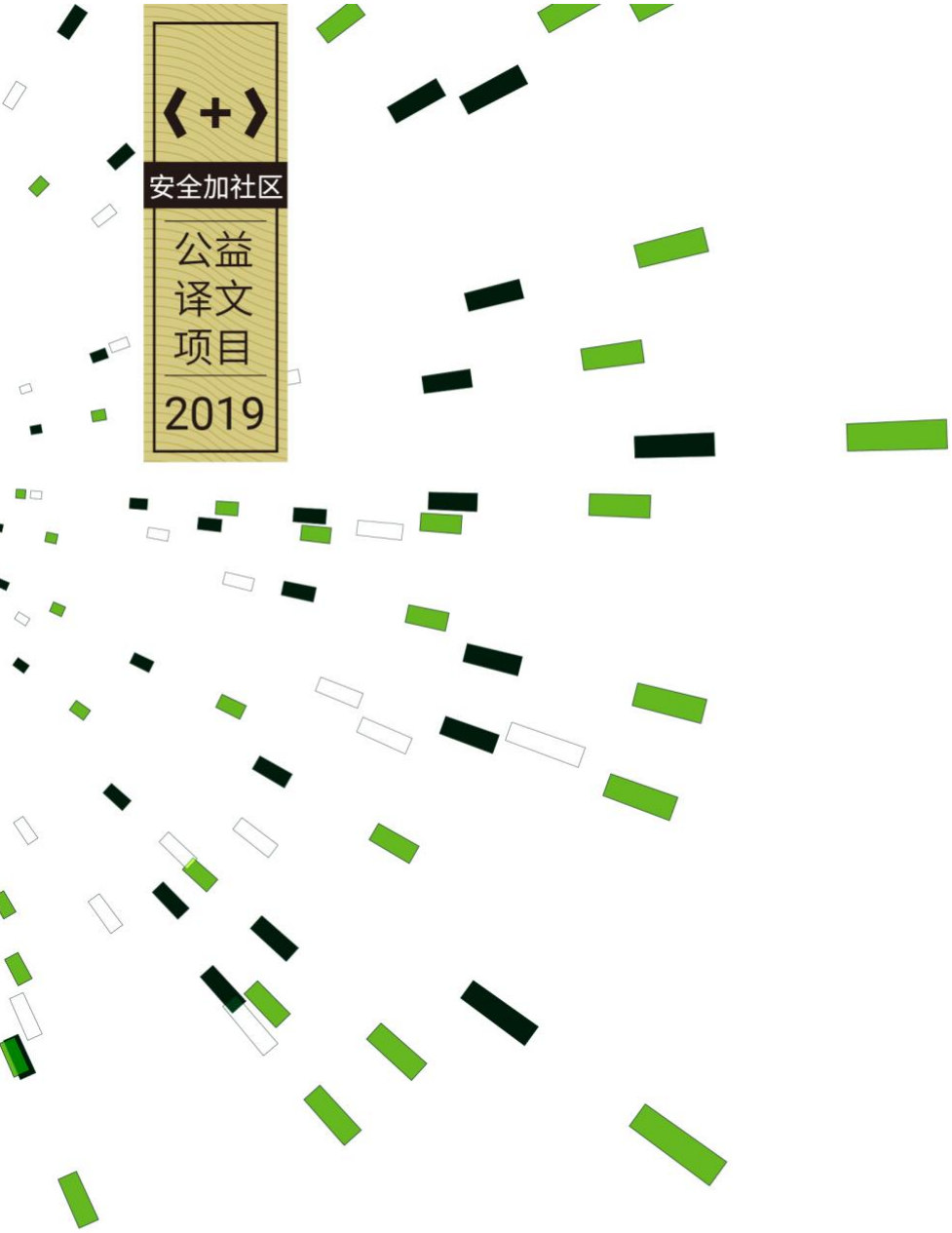
JP5-0，IV-15–16。
JP3-12，IV-2–3。
JP5-0，IV-16。
JP3-12，II-9–10。
美国国防部，国防部科学委员会专责小组报告：弹性军事系统与高级网络威胁（华盛顿特区：美国国防部，2013 年 1 月）备忘录，17–18。
JP3-12，II-2–5。
JP3-12，II-3。
JP3-12，II-5–7
JP5-0，IV-17。
JP3-12，IV-23–24。
JP5-0，IV-17。
JP3-12，IV-7。
JP3-12，IV-9。
JP3-12，IV-20。
JP5-0，IV-17。
JP3-12，IV-1。
JP5-0，xiii。
JP5-0，V-2。
JP5-0，V-4–49。
JP5-0，V-2。
JP3-12，IV-1。
JP5-0，V-4。
战地手册 3-12，3-14–15。
JP5-0，V-4。
战地手册 3-12，3-15–16。
JP5-0，V-20。
战地手册 3-12，3-16–17。
JP5-0，V-31–46。
战地手册 3-12，3-17–20。
JP5-0，V-49–50。
JP3-12，3-20。
美国陆军部，战地情报准备，陆军技术出版物 2-01.3/海军陆战队参考条例 2-3A（华盛顿特区：陆军部总部，2014 年 11 月），9–12。
JP3-12，II-10–11。
JP3-12，IV-6。
联合作战中的跨域协同，55–56。
JP3-12，IV-18。
战地手册 3-12，B-2。
战地手册 3-12，B-3–6。
JP5-0，IV-21–23。
JP3-12，x。
JP3-12，I-2。
JP3-12，I-12。
JP3-12，IV-3。
JP3-12，IV-10。
战地手册 3-12，C-1–2。

战地手册 3-12，C-4。
JP5-0，xvii。
美国参谋长联席会议，联合特遣部队总部，JP3-33（华盛顿特区：美国参谋长联席会议，2018 年 1 月 31 日），IX-8。
美国参谋长联席会议，作战设计规划者手册（华盛顿特区：美国参谋长联席会议，2011 年 10 月 7 日），IX-2–3。
JP3-12，IV-1–2。
JP3-12，III-11。
JP3-12，III-3

JP3-12，III-7。
JP3-12，IV-17。
JP3-12，IV-11–17。
JP3-12，III-6。

美国网络司令部，所有网络任务部队均具备初始作战能力（马里兰州米德堡：美国网络司令部新闻发布，2016 年 10 月 24 日），1-3。
JP3-12，IV-14。
JP3-12，IV-19–20。
JP3-12，IV-8–10。
JP3-12，IV-21。
美国总统巴拉克·欧巴马（Barrack Obama），奥巴马总统在斯坦福大学网络安全与消费者保护峰会上的演讲，2015 年 2 月 13 日。
美国国防战略概要，4。
美国参谋长联席会议，国土防御，JP3-27（华盛顿特区：美国参谋长联席会议，2018 年 4 月 10 日），vii–viii。
JP3-27，I-1–3。
关键基础设施部门，内容详见美国国土安全部主页：https://www.dhs.gov/critical-infrastructure-sectors（2017 年 5 月 26 日）。
美国国防部受保护的重要的基础设施计划，内容详见负责政策的副部长网站首页：http://policy.defense.gov/OUSDPOffices/ASDforHomelandDefenseGlobalSecurity/DefenseCriticalInfrastructureProgram.aspx（2017 年 5 月 26 日）。
美国国防部网络战略（华盛顿特区：国防部，2015 年 4 月），14。
JP3-27，II-3。
JP3-27，II-13。
JP3-27，II-8。
JP3-27，II-12。
美国网络司令部司令迈克尔•S•罗杰斯（Michael S. Rogers）海军上将在美国参议院军事委员会听证会上的讲话稿（2018 年 2 月 27 日），12。
美国网络司令部司令迈克尔•S•罗杰斯（Michael S. Rogers）海军上将在美国参议院军事委员会听证会上的讲话（华盛顿特区，2017 年 5 月 7 日），7-8。
JP3-12，I-13–14。
美国国防部网络战略，23。
美国国防部网络战略，2。
JP3-12，III-2。
JP3-12，I-12–13。
美国国防部网络战略，10–11。
美国国防部网络战略，22。
美国网络司令部司令迈克尔•S•罗杰斯（Michael S. Rogers）海军上将在美国参议院军事委员会听证会上的讲话稿（2018 年 2 月 27 日），16。
美国国防部网络战略，22-23。
美国国防部，政策备忘录 16-002，为军事训练及国民警卫队使用国防部信息网络和软硬件进行本州网络安全活动而提供的网络支持和服务（华盛顿特区：国防部，2016 年 5 月 24 日/延期备忘录 2018 年 3 月 1 日），1–2。
美国国防部，指令型备忘录（DTM）17-007，关于网络事件响应防护支持的暂行政策与指南（华盛顿特区：国防部，2017 年 6 月 21 日），2–3。
JP3-12，III-10–11。
JP3-12，III-11。

联合作战中的跨域协同，4。
美国空军中校 E•林肯•邦纳三世（E. Lincoln Bonner III），21 世纪联合作战中的网络力量，联合部队季刊第 74 期（2014 年第 3 季度）：105。
联合作战中的跨域协同，4。
21 世纪联合作战中的网络力量，联合部队季刊第 74 期，104-105。
JP6-0，ix。
JP6-0，I-7。
21 世纪联合作战中的网络力量，联合部队季刊第 74 期，106。
21 世纪联合作战中的网络力量，联合部队季刊第 74 期，105。



网络安全公益译文项目旨在分享国外先进网络安全理念，将网络安全战略性文档翻译为中文，促进国内安全组织在相关方面的思考和交流。该项目由安全加社区发起，安全加社区是国内的网络安全社区，社区欢迎网络安全人士的加入，并致力于交付网络安全问题的解决能力。

安全加