CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE
SIIS 上海国际问题研究院 SHANGHAI INSTITUTES FOR INTERNATIONAL STUDIES
WORKING PAPER

2021年4月

关于中美建立网络–核指挥控制与通信系统稳定性的报告

阿里·莱维特 吕晶华 潘可为
鲁传颖 许蔓舒 李彬 杨帆

项目介绍

本研究报告由卡内基专家团队和上研院专家团队合作，并咨询了多名外部专家撰写而成。卡内基团队由潘可为(George Perkovich)、阿里 • 莱维特(Ariel Eli Levite)、吕晶华、凯瑟琳 • 夏勒(Katherine Charlet)、史文(Michael D. Swaine)、怀特 • 霍夫曼(Wyatt Hoffman)组成，并咨询了罗伯特 • 施密德(Robert Schmidle)、约翰 • 戴维斯(John A. Davis)等外部专家。中方团队包括鲁传颖、徐蔓舒、李彬、杨帆，咨询了徐纬地、鹿音、赵武文、康春梅、惠志斌、戴丽娜、沈逸、蔡翠红、郎平、张腾军、赵通、吴莼思、叶江和封帅等专家。作者同样感谢那些虽然没有出现在名单中，但是对报告作出了贡献的研究机构和专家。

上海国际问题研究院网络空间国际治理研究中心简介

上海国际问题研究院网络空间国际治理研究中心是网络安全与国际治理领域的专业智库，旨在跟踪研究全球网络安全形势、各国网络安全战略，推动构建网络空间国际治理机制。网络空间国际治理研究中心成立于 2018 年 12 月，由上海国际问题研究院、中国人民解放军国防大学、复旦大学、南京大学、厦门大学、上海社会科学院等多家单位联合发起。中心服务于我国网信、外交等领域的最高决策机构。

目前，中心已经与联合国机器人与人工智能中心、预防犯罪和刑事司法委员会、美国麻省理工学院、美国卡内基国际和平研究院、美国战略与国际问题研究中心、俄罗斯军事科学院、荷兰莱顿大学等机构开展了机制性合作。

卡内基国际和平研究院简介

卡内基国际和平研究院是由位于俄罗斯、中国、欧洲、中东、印度和美国 6 个政策研究中心所组成的国际组织。研究院创立于 1910 年，在过去的一个世纪以来坚持以促进国际和平为使命。我们通过分析政策和研究新兴政策思路，以及与政府，企业及社会决策者进行直接的交流和合作，以达成这一使命。通过下属各大中心的协同合作，卡内基研究院在双边、区域和全球议题的讨论中综合来自各个不同国家的观点，并带来无可估量的积极影响。

现在，卡内基在北京、贝鲁特、布鲁塞尔、莫斯科、新德里和华盛顿设立了研究中心。各中心的学者都是从各地区脱颖而出，在与世界各地的同事紧密合作的同时用当地语言进行研究和写作。通过这种方式，卡内基帮助各国政府以及国际机构更深入地理解影响决策的因素，并提供新的视角来分析政策问题。

作者简介

阿里·莱维特 卡内基国际和平研究院核政策项目与网络政策倡议，非常驻高级研究员

蔡翠红 复旦大学美国研究中心教授

戴丽娜 上海社会科学院互联网治理研究中心主任

封帅 上海国际问题研究院国际战略所副研究员

潘可为 卡内基国际和平研究院副总裁，肯·奥利维尔和安吉拉·诺梅里尼讲席研究员，主管技术与国际事务项目、核政策项目

惠志斌 上海社会科学院互联网研究中心研究员

约翰·戴维斯 帕洛阿尔托网络安全公司副总裁及联合首席安全官，国防部负责网络政策的前助理副国防部长

康春梅 中国工程物理研究院研究员

凯瑟琳·夏勒 谷歌公司数据治理、政府事务与公共政策主管，曾任卡内基国际和平研究院技术与国际事务项目主管

郎平 中国社会科学院世界经济与政治所研究员

李彬 清华大学国际关系学系教授，曾任卡内基国际和平基金会核政策项目和亚洲项目高级研究员

鲁传颖 上海国际问题研究院网络空间国际治理研究中心秘书长，研究员

鹿音 中国人民解放军国防大学国家安全学院副教授

吕晶华 卡内基国际和平研究院网络政策倡议访问学者

史文 昆西国家事务研究所东亚项目主管，原卡内基国际和平研究院，亚太项目高级研究员

罗伯特·施密德 亚利桑那州立大学网络能力与冲突研究项目顾问，政治与全球研究学院实务教授，冲突未来中心高级研究员，原美国网络空间司令部副司令，退役中将

沈逸 复旦大学国际关系与公共事务学院教授

赵通 清华－卡内基全球政策中心核政策项目研究员

吴莼思 上海国际问题研究院国际战略研究所所长

怀特·霍夫曼 安全与新兴技术中心研究员，原卡内基国际和平研究院，核政策项目与网络政策倡议高级研究助理

许蔓舒 上海国际问题研究院网络空间国际治理研究中心研究员

徐纬地 原中国人民解放军国防大学战略研究所教授

杨帆 厦门大学法学院网络空间国际法研究中心副主任

叶江 上海国际问题研究院全球治理研究所研究员

赵武文 中国工程物理研究院研究员

朱莉欣 西安交通大学网络安全法治研究所教授

前　言

网络对核稳定的影响是当前国际安全领域最具前瞻性和战略性的议题之一。上海国际问题研究院与卡内基国际和平研究院围绕该议题开展联合研究，旨在为核国家之间建立网络与核稳定机制提供参考。

网络攻击已成为核武器面临的重大风险来源，但大国之间对此却未能建立相应的维护稳定机制。网络攻击能够以多种方式削弱战略稳定，核指挥、控制与通信系统的现代化发展，使其与网络空间之间的联系更为紧密。信息技术在强化核战略力量的同时，也给核指挥系统带来日益严峻的网络安全威胁。针对核国家战略指挥控制系统的网络攻击，包括核武器的指挥控制系统和卫星通信系统存在的网络脆弱性、来自第三方的网络威胁、国家间网络空间信任缺失等方面都加剧了网络对核稳定的影响。

由于核武器的特殊性，任何针对核武器的网络安全事故都会导致国家的警惕、焦虑、困惑，削弱国家对于核威慑力量的可靠性和完整性的信心。任何针对核指挥控制系统的网络攻击，受到攻击的核国家都将面临冲突升级和在其核能力受到破坏之前使用核武器的巨大压力。同时，相对于传统核领域大国之间在核威慑、危机管控、冲突升级 / 降级等方面具有的成熟经验，国家对于网络安全对核武器所造成的威胁不仅缺乏全面、准确的认知，对于危机管控和冲突降级的举措也缺乏共识。

鉴于在核大国的安全对话中鲜有关注这种新型威胁，2017 年，上海国际问题研究院与卡内基和平研究院启动了中美网络与核稳定联合研究项目，重点探讨核国家之间达成某种共识和协定的可能性。希望核安全能够唤醒国家决策者对网络安全的重视，希望有核国家能够充分认识到网络攻击的危险性以及各自对这种攻击的脆弱性，从而采取措施降低网络技术引入的核不稳定，防止核战争。

中美是具有核战略能力的网络大国。中美在网络空间有摩擦与分歧，虽然目前双方的分歧呈扩大的趋势，但双方仍然有对话与合作的利益和基础。我注意到，拜登总统在正式就任前曾提出科技政策 5 问，其中包括“如何确保美国科学与技术的长期发展”。习近平主席多次强调，要“最大限度利用网络空间发展潜力，更好惠及 13 亿多中国人民，造福全人类”。显然，在信息技术不断演进发展的今天，避免战争、化解战争风险符合两国利益，这既是大国的国际责任，也是国际社会的共同期望。希望此项联合研究可以促进中美的深度对话和安全合作，建立相应的稳定机制。

这份联合研究报告是一份严谨的学术研究报告，是中美研究团队的共同成果。双方团队历经 4 年的合作，中间召开了 2 次国际研讨会（2018-1-13 上海，2019-3-25 北京）、4 次工作组会议（2017-3-20 华盛顿，2017-6-4 北京，2018-10-24 北京，2019-11-5 北京）、10 多场在线研讨，期间反复征求相关领域专家和政府部门的意见。在英文定稿的基础上，双方的团队逐字逐句进行了翻译、

修订和校对，形成了最终的中英文联合报告。

这份联合研究报告是中美两个重要智库共同发布的一份重要报告，希望能够提高中美两国对彼此安全关切、利益和问题解决办法的相互理解，促进中美关系稳定，推动中美关系的良性发展。相信它对两国政府如何在敏感领域消除分歧，增进共识具有重要的参考价值。在此，我向双方的研究团队表示祝贺，特别感谢卡内基研究团队的 George Perkovich 和 Ariel Levite 不辞辛苦多次往返美中之间，与中方研究团队密切合作。我们希望上研院与卡内基国际和平研究院能够围绕中美网络安全问题继续开展联合研究，为中美关系作出更大的贡献。

陈东晓

上海国际问题研究院院长

尽管中美都希望避免小冲突上升为大灾难的事态升级，也各自或共同为此做出了努力，但军事和国家安全专家正在越来越多地发出警告，称最可能引发中美之间重大（常规或核）战争的诱因是一场急剧升级的小型冲突。而网络行动，无论是中国针对美国还是美国针对中国的，都尤其可能引发对抗局势升级。当一国在其战略性计算机网络中发现入侵行为后，相关官员是很难判定入侵者意图的。这种网络入侵可能旨在防御，以获得对未来攻击的预警；但也可能是攻击性的，作为先导性行动旨在中断或破坏对方与核威慑相关的预警系统和（或）指挥、控制与通信系统。在入侵者意图未知的情况下，防范者在检测到入侵行为后很可能做最坏的设想。而迅速增大的压力，可能促使该方先发实施打击，以防对方的进一步行动导致自己无法或很难再采取这样的打击行动。

这种风险在中美之间尤为突出，因为这两个大国从未像美俄那样，将双方战略关系定义为相互脆弱的关系，也未就如何稳定这种关系达成共识。中美之间核力量及其他攻防能力的不对称性，可能会使中方认为，美国将在某个时间点上试图使中国的核威慑力量失效。而中方为避免这种可能性所采取的行动，特别是在网络空间领域的此类行动，又极可能使美方官员担忧，中国意在抑制美国的核威慑。

当两国中的某一方开始部署卫星、导弹或指挥控制系统等常规与核战争两用的系统时，上述风险还会加剧。一方可能仅仅意在对常规规作战能力采取先发制人或报复行动，但受攻击的另一方则可能认为这些攻击针对的是本国核力量，或至少将影响本国核力量。

此次开创性的研究报告将以中英文版本同时发布，呼吁人们关注这些不断上升的风险。该研究报告是上海国际问题研究院和卡内基国际和平研究院多年合作的独特成果，旨在为中美讨论这些问题提供一个有活力的开放性平台，以克服高涉密性和部门隔阂对分析和交流造成的障碍。该报告

由中美两国团队共同撰写，还旨在克服（至少部分克服）文化和语言障碍，这些障碍也使该领域的相互理解变得非常困难。

报告首先详细说明了值得重点关切的可能情境，并提供了分析相关情境的框架；尔后探讨了中美两国政府、及智库等非政府组织在其鼓励下可以采取的措施，以减少核指挥、控制与通信系统无意中遭受的网络威胁。这些措施可以单边或双边形式实施，可以是互惠式的也可通过谈判实现。报告还为两国相关官员对话交流提供了主题，对话参与者可以是外交官、军官，也可以是网络操作人员、计算机应急反应小组人员，对话的目的是帮助稳定中美关系，并为双方可能希望达成的建立信任措施勾划相关议程。

中美的报告撰写团队都与各自政府的前任和现任专家进行了咨询交流，以确保报告内容与当前的政策和技术现实密切相关。虽然在完成本份报告的进程中两国官方关系显著恶化，但双方研究团队和组织者仍然以建设性的方式，继续聚焦关键目标，即提升对于网络－核背景下两国所面临风险的共同认知，并寻找合作路径以降低风险。双方发现，鉴于涉及重大利益，无论是机制还是个人层面，都能够比较容易地维持合作关系。遗憾的是，在过于激烈的中美两国内部和相互的战略敌对话语环境中，这样的互动已属稀有。

卡内基国际和平研究院衷心感谢纽约卡内基基金会给予的财政支持，使本报告得以发表，并感谢其多年来在帮助减少全球核冲突风险方面与我方开展的密切合作。

托马斯 • 卡罗瑟斯

卡内基国际和平研究院临时主席

目录

报 告 概 述

网络风险对核指挥、控制和通信系统（NC3）造成的威胁，引发了越来越多的担忧。[1] 西方的知名专家们发表了一系列报告和学术论文，对其风险进行了全方位的评估。他们得出的结论是：网络行动可能会或有意或无意地威胁到核系统的各项功能，从而引发高度敌对性的战略互动。这些互动可能会导致危机升级为武装冲突、武装冲突升级为核战争。中国官方和学者未明确讨论这些担忧，但他们运用过往案例（如“震网”事件）强调网络攻击可能破坏核稳定。

鉴于中美两国在减少意外事件、非蓄意性冲突以及阻止事态恶化等方面存在共同利益，卡内基国际和平研究院与上海国际问题研究院召集中美两国专家学者共同开展研究。我们共同的目标是探讨一般性的网络－核挑战，分析 NC3 系统遭受网络威胁的可能场景，并提出两国可以单方或者双方合作采取的措施以降低相关风险。本报告基于公开信息资源，以中英两种语言构建非机密性的共同认知基础，希望由此可为中美两国政府开展更为谨慎的接触提供平台。

本报告首先简要介绍了针对 NC3 系统的网络行动引起担忧的局势背景，即随着中美两国向激烈的“大国竞争”方向发展，双方越来越陷入传统的“安全困境”。不论稳定概念如何界定，中美均质疑对方对战略稳定概念的解释和维持战略稳定的诚意。双方都不认为对方在有意地自我克制，防止采取竞争行为甚至是侵犯性行为。同时，双方也未在建立互信方面做出显著努力。

美国尤其担心中国不会回避在与邻国的领土争端中使用武力，而这些国家当中有许多是美国的盟友国和伙伴国。美国战略学者担心，中国正在增强网络、常规以及核能力，从而破坏美国的延伸威慑保证，阻止其保卫盟友安全。另一方面，中国则主要担心美国寻求更强大的网络、常规以及核能力，从而对中国的核威慑力量进行先发制人打击，削弱中国的报复能力。

中美这些相互冲突的威胁认知，以及两国核武库的巨大差距，使得双方很难找到共同途径并协商具体方案，从而达成双方都能够信任和可以验证的战略稳定。

在网络领域，尽管中美双方直到最近仍保持着对话和合作，但摩擦也在不断增加。出于多方面原因，开展网络间谍、秘密行动和网络攻击的能力显得很有吸引力。网络行动成本相对低廉、非致命、通常很有效也不明显违法。与使用人力间谍和动能武器相比，网络行动的破坏性似乎更小，影响更短暂，整体上的挑衅程度也更弱，因此引发冲突升级的风险更低。网络行动的保密性也会缓解因其运用而带来的风险：遭受攻击一方的公众不会明显感受到袭击，因此也不会公开向领导人施压，要求其做出回应，这使得领导人可以慎重行事。这些原因使得中美两国都在努力提升网络能力，并

1. 根据公开资源，同时为了便于我们讨论的目的的实现，我们将核指挥、控制和通信系统（NC3）定义为便利和支持核力量行动和协助核武器决策的整个信息和电信设备。需要重点点明的是，NC3 系统还包括辅助系统（如电源），这对其功能至关重要，并可能容易受到网络攻击。核武器国家要求 NC3 系统从早期预警一直到进行核作业的整个流程中均发挥作用。

提升网络能力在国家总体安全态势中的地位。同时，由于双方都非常重视本国的核威慑，他们也都会对对方试图运用网络武器对自己造成威胁的可能性保持高度警惕。

中美虽有理解和努力减少网络－核风险、提升战略稳定方面的共同利益，但以下两个因素阻碍了他们基于这些共同利益采取行动。首先，双方存在深层次的不信任，都没有足够的信心认为双方所给予的保证能够促进稳定。其次，双方在如何开始行动以取得进展的问题上存在分歧。美方坚持认为，如果中方不公开承认拥有攻击性网络能力，也不愿意探讨对这些能力的使用问题，那么双方几乎没有什么可以做的。另一方面，中国则希望美国认识到，美国拥有强大的网络能力，其网络战略可能威胁到中国进行第二次打击的威慑能力。最后，与之相关的一个政治心理因素是，中国官员认为，应当先建立信任然后才能解决具体问题，美国官员则持相反看法，认为具体的行动（通常包括自我克制）是构建信任的主要路径。

基于上述背景，本报告首先描述了各国针对对手 NC3 系统可能直接开展的网络行动。间谍行动位居首位。开展网络间谍行动，可通过渗透到 NC3 系统收集到极有价值的情报，因而吸引力巨大，由此带来的挑战也极为严峻。特别是，预警信息可以了解对手是否以及何时准备进行核打击，是各国都希望获得的情报。获得此类情报，或是使对手相信己方有能力获得此类情报，能够增强威慑。出于间谍目的的网络入侵可用以实施网络攻击，即便行动实施者只意在前者而非后者也是如此。网络行动固有的通用性和潜在的双重用途使“接收方”很难解释行为者动机，也使双方难以预测任何此类行动的影响。NC3 系统体系结构的复杂性、保密性和区隔性，更加剧了网络行动的实施者和目标方准确预测其潜在后果的难度。包括其他国家、恐怖分子、政治颠覆者在内的第三方，也可能会寻求利用网络行动来煽动中美冲突，使局势变得更加复杂。中国或美国也有可能在攻击对方时伪装成第三方（伪旗行动），或通过代理人对对方采取网络行动。

就中美关系而言，还有另外三个因素可能会加剧不稳定和冲突升级。首先是两国指挥控制系统的结构和作战理论差异很大。其次是中美两国政府对双方之间网络能力平衡的认识存在分歧。最后，中美两国正在发展和部署网络力量、常规力量和指挥控制系统，其使用愈发可能与核行动相互交织。无论是有意还是无意这种交织都极具潜在不稳定性。

本报告并未描述网络行动可能引发风险的所有形式，而是试图找出几类场景，能够反映对战略稳定而言最具不稳定性的因素和最令人担忧的风险。以下四类场景尤其值得重视：

1. 针对对方 NC3 系统核心部分进行数据收集的网络间谍活动；

2. 针对对方两用系统或为 NC3 系统提供支持或与其关联的其他环节进行的网络间谍活动；

3. 针对两用（此处指常规和战略）NC3 系统的网络攻击，或是针对为 NC3 提供支持或与其相关联的辅助系统进行攻击、但并无意影响系统核功能的网络攻击；

4. 既严重怀疑对方意图，又对己方 NC3 系统在网络攻击中的脆弱性高度担忧，两者相结合可

能引发的状况。

这些设想可能带来四类在战略上令人担忧的后果：核冲突、无意或意外使用核武器、危机升级、以及长期性的不稳定影响如军备竞赛和随之而来的不稳定危机。这些风险部分源于攻击者和目标国在预先或实时评估网络行动方面所面临的固有困难。第三方行为体可能会制造混乱、加剧危机，以及溯源难题和如双方溯源能力不对称时所产生的影响，都进一步加剧了这些风险。

迄今为止，中美两国都有避免在无意中陷入武装冲突、并致力于防止冲突向核战争升级的意愿。因此，讨论通过单方面或双方合作采取措施，以减少对 NC3 系统的网络威胁是有意义且可行的。即便存在保密限制，且中美互不信任对方意图、在如何应对安全挑战的问题上方法迥异、在网络与核领域存在结构性不对称，也并不改变这一基本判断。

可确信的网络行动决策程序。如果双方对网络行动采取强有力的监管和危机管控程序，就可以降低考虑不周的网络行动造成的风险。相互了解对方的监管方式，也有利于避免夸大双方对对方的威胁认知。评估和管控程序应在以下五个层面运作：

- 内政外交政策监管，由国家强力机关执行；
- 技术监管，以评估网络行动的预期效果和潜在意外后果；
- 行动监管，以确保在获得授权的指挥链内进行有效控制；
- 情报监管，以评估在网络行动或能力暴露时所造成的后果，以及在情报来源、方法和结果预判等方面的潜在损失；
- 法律监管，以考察网络行动与能力是否适用于相关国内和国际法律与协议。

上述所有措施都可以单方面秘密进行。但就这些问题进行双边对话可以获得包括建立信任在内的额外益处。

创造更加稳定和脆弱性更低的战略环境。中美双方正在采取措施实现其核架构与核力量的现代化，包括其 NC3 系统的现代化。两国政府可以采取缓解措施以避免安全困境的最坏影响 -- 或最坏情况的评估。两国政府可以确认并相互沟通，对于感知到的威胁所作的回应中哪些是审慎且起稳定作用的。例如，双方可能出于对自身 NC3 系统受到网络攻击的担忧，都有意增加核武器的数量、多样性和部署方式。双方还可以澄清其意图和作战理论，而在双方寻求降低对备战和核使用限制的情况下，减少核使用与升级的不稳定性和风险。双方开展合作的第三个领域是认识到，开发和部署反卫星、太空战武器和人工智能等新能力，将引起对网络 - 核威胁的担忧，这值得更多的关注。

就限制做出相互承诺。鉴于双方都不认为大规模武装冲突或动用核武器以减少损失具有持久优势，本报告试图探讨一系列措施，以限制对双方 NC3 构成威胁的网络能力和行动。

第一种限制是中美正式承诺不对 NC3 系统的核心进行任何网络渗透。作为启发式的思考，报告提出可采取以下几种形式：1）双方可以就 NC3 系统核心的构成要素达成共识；2）双方可各自选定

其属于 NC3 系统的一些核心要素，并与对方分享该清单；3）在不与对方分享哪些要素构成核心 NC3 的情况下，如一方探测到对方对这些要素的网络渗透时，应即时告知对方，期望入侵者立即停止相关活动并从中撤出。

中方参与者普遍欢迎上述自我克制措施，而美国专家大多认为这种措施不可取或不切实际。但这不能完全否定在内部对上述举述的可取可行之外进行分析、以及促进促进双边讨论的意义。

第二种限制是承诺将针对 NC3 的网络行动置于各国高层领导的授权之下。

第三种值得探讨的限制措施是两国政府可否达成共识，即不以对 NC3 有重要意义的空基战略资产作为行动目标。

第四种限制是两国可承诺对以下行为者进行有效监督和控制，以缓解第三方对 NC3 系统进行网络干预带来的风险：(1) 受两国指挥的，(2) 利用两国领土实施行动的，(3) 运用两国所开发的能力行动的，(4) 可施加重要影响的盟友。美国专家强调了采取这些措施的共同利益，而中国专家则怀疑此类承诺在当前政治环境下的可行性。尽管如此，我们认为这种形式的限制值得进一步考虑和就此开展对话。

开展对话和信息共享。本报告和前述的概要表明，持续的对话和信息共享十分重要。美俄因持续的对话而在战略稳定和危机管控议题上形成共识，但中美之间却没有这样的基础。这尤其令中国感到不安，因为相互的核脆弱性尚未被认为是两国关系的基本条件。这个基础的缺失使得双方很难解决彼此对核态势及网络对核态势威胁的担忧。事实上，两国在是否以及如何讨论军事层面的网络竞争问题上存在相互矛盾的观点，这加大了就网络威胁开展战略稳定对话的难度。

这份报告试图找出在恰当官方议程中亟需关注的三类议题。一是相互了解一方或双方都认为具有不稳定性的和稳定性的措施包括能力建设、决策程序、涉及网络工具的行动和涉及核力量与 NC3 的行动。二是有关进攻性网络行动的潜在利益和风险，特别是当其涉及到网络 - 核关系时。鉴于这些问题的高度敏感性和保密性，这种对话将限于总体和通用的层面上。三是中美双方可探索是否以及如何在和平时期就这些问题进行信息共享。

本报告所涉及的主要议题可以在现有平台抑或是新开启的双边对话中讨论。其中，以下现有的平台可咨利用：

1)“外交安全对话”可作为双方高层官员沟通渠道，表达对彼此政策变化的关切及分享重大进展；

2) 两份“谅解备忘录”可供两军探讨网络行动的基本原则；

3)“中美两军联合参谋部对话”可供中层官员讨论网络力量的能力和意图，以及对 NC3 系统所面临的网络威胁表达关切；

4) 复用在重大网络事件或危机期间建立的高级别官员之间的沟通渠道 ；在特定更高级别官员之间建立的联络渠道可用于在重大网络事件或危机期间进行沟通；

5）两国计算机应急响应小组（CERTs）之间现有的协调机制，可继续作为合作渠道，并可加以扩大从而涵盖具有潜在战略后果的威胁信息；

6）双方国防部门之间现有的热线机制可用于就与 NC3 有关的网络问题进行沟通。

最后，网络行动对 NC3 和战略稳定构成的威胁是如此重要，以致在设计和选择合适路径以理解和应对此威胁的过程中所面临的挑战，都显得微不足道。真正的挑战在于，如何形成克服疑虑、减少猜疑和政治恐惧的意愿，正是这些疑虑、猜疑和政治恐惧使中美两国领导人无法开启必要的行动，使彼此相信建设性的行动将得到回报。本报告旨在列出一系列非机密性的议程以供讨论，澄清其涉及的利害关系，就两国可采取哪些措施扭转危险趋势 -- 特别是那些可危机或冲突在无意中升级的风险的趋势—提出建议。

引　言

近年来，对于网络行动是否会或有意或无意地威胁到核指挥、控制及通信系统（NC3）的功能，全世界的主流专家们都表达了忧虑的态度。他们认为，这一风险将引发消极的战略互动，包括危机可能升级为武装冲突、武装冲突可能升级为核战争的更大风险。[2] 有核国家在发生危机或传统军事冲突时，如果在 NC3 系统中的任何地方发现或怀疑发现有来自外部的网络入侵，即使相关国家的领导人无意升级，也可能引发具有极大升级风险或以其他方式严重破坏稳定的人为反应和技术故障。引发这种互动的可能是冲突双方中的一方，也可能是双方，同时也可以是包括非国家行为体在内的第三方。

表 1：有关网络 - 核风险的现有文献

人们对核系统所受网络威胁的关注近年来与日俱增。2009 年，国际核不扩散与裁军委员会（International Commission on Nuclear Non-proliferation and Disarmament）委托进行的一项研究认为，理论上讲“网络恐怖分子”可以通过网络入侵触发核交战或发射武器。[3] 美国国防部国防科学委员会 2013 年的一份报告警告说，大多数核系统尚未接受顶级网络威胁应对水平的端对端评估。[4] 尽管少有官方层面的正式表态，但多位前军事和国防官员接连公开表达对网络威胁的担忧。例如，美国战略司令部前指挥官詹姆斯 • 卡特赖特（James Cartwright）（退役）上将在 2015 年指出，核指挥和控制系统容易受到网络入侵，其后果可能包括因回应错误的攻击警告而使用核武器。[5] 英国前国防大臣德斯 • 布朗（Des Browne）要求英国政府对英国的三叉戟（Trident）系统进行端对端的网络安全评估，以确保网络攻击不会破坏英国的威慑力。[6] 有充分证据表明，俄罗斯军方和国防官员同样极为关注旨在削弱俄罗斯指挥和控制能力的网络攻击。[7]2019 年 2 月，来自美国、欧洲和俄罗斯的现任和前任高级官员以及几家知名机构共同呼吁进行

2. 最显著的风险存在于美俄、美中、印巴之间。
3. Jason Fritz, Hacking Nuclear Command and Control, International Commission on Nuclear Non-proliferation and Disarmament, 2009. http://www.icnnd.org/Documents/Jason_Fritz_Hacking_NC2.pdf.
4. Defense Science Board, “Task Force Report: Resilient Military Systems and the Advanced Cyber Threats, “Department of Defense, 2013. https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-081.pdf.
5. Robert Burns, “Ex-commander: Nukes on high alert are vulnerable to error,” Associated Press April 30, 2015. https://apnews.com/e970363945364db79dff94240956e2c4.
6. Nicholas Watt, “Trident could be vulnerable to cyberattack, former defence secretary says,” The Guardian, Nov. 23, 2015. https://www.theguardian.com/uk-news/2015/nov/24/trident-could-be-vulnerable-to-cyber-attack-former-defence-secretary-says.
7. See M.V. Ramana and Mariia Kurando “Cyberattacks on Russia—the nation with the most nuclear weapons—pose a global threat,” Bulletin of the Atomic Scientists, Vol. 75, No. 1, 44-50 (2019).

对话，以解决对 NC3 的网络威胁。[8] 众议院军事委员会（HASC）在 2019 年 6 月提交立法草案，要求美国国会增加对 NC3 的资助，并要求五角大楼制定近期和长期计划和选择，以确保 NC3 网络的弹性。[9] 一些研究从不同层面深入分析了网络 - 核风险。英国皇家国际事务研究所（Chatham House）和“核威胁倡议”（Nuclear Threat Initiative）的报告描述了一系列假想情况，包括对核攻击的错误探查、危机期间的通信干扰、危及核系统的供应链威胁，以及导致未经授权使用核武器的网络入侵。[10] 安德鲁 • 弗特（Andrew Futter）在《黑客炸弹：网络威胁和核武器》一书中描述了网络威胁可能如何破坏“相互确保摧毁”（MAD），并导致“逐渐陷入核不稳定‘加剧’的新时代”，从而引发焦虑和面临需要更迅速使用核武器的压力。[11] 在题为《网络战争与核和平》的报告中，大卫 • 贡佩尔（David Gompert）和马丁 • 李比奇（Martin Libicki）（两位均为供职于美国重要国防智库的杰出网络学者）探讨了革命性数字技术之间的不同关联，并探讨了针对核大国 NC3 的攻击性网络行动可能触发“一触即发”式发射政策，甚至是引发核战争的担忧。[12] 乔恩 • 林赛（Jon Lindsay）在《网络行动与核武器》中，重点研究了针对 NC3 的进攻性网络行动在核危机中引发组织崩溃、决策混乱和误判的可能性。[13] 其他学术研究也阐述了网络行动因具有模糊性和不确定性而在危机或冲突中破坏网络 - 核互动稳定性的可能性。[14] 展望未来，有人警告称，将人工智能和机器学习功能引入 NC3 系统将加剧许多此类风险。[15] 尽管缺乏针对这些问题的官方公开讨论，但一些中国学者也考察了网络攻击与核稳定之间的关系，他们的研究主要从分析以往的案例（例如震网 Stuxnet）入手。[16]

8. “Statement for Cooperation among Governments to Address Cyber Threats to Nuclear Weapon Systems” Euro-Atlantic Security Leadership Group, February 2019. https://www.europeanleadershipnetwork.org/wp-content/uploads/2019/02/EASLG-Statement_Cyber-Threats_FINAL.pdf. The statement added: “increase the risk of use as a result of false warnings or miscalculation, increase the risk of unauthorized use of a nuclear weapon, and could undermine confidence in the nuclear deterrent, affecting strategic stability.”

9. Heresa Hitchens, HASC Adds NC3 Funds; Wants Talks With Russia, China, June 10, 2019 https://breakingdefense.com/2019/06/hasc-adds-nc3-funds-wants-talks-with-russia-china/.

10. Page O. Stoutland and Samantha Pitts-Kiefer, Nuclear Weapons in the New Cyber Age Nuclear Threat Initiative September 2018 https://media.nti.org/documents/Cyber_report_finalsmall.pdf. Beyza Unal and Patricia Lewis, Cybersecurity of Nuclear Weapon Systems: Threats, Vulnerabilities and Consequences Chatham House January 2018. https://www.chathamhouse.org/sites/default/files/publications/research/2018-01-11-cybersecurity-nuclear-weapons-unal-lewis-final.pdf.

11. Andrew Futter, Hacking the Bomb: Cyber Threats and Nuclear Weapons (Washington, DC: Georgetown University Press 2018). See page 124.

12. David C. Gompert & Martin Libicki (2019) Cyber War and Nuclear Peace, Survival, 61:4, 45-62, DOI: 10.1080/00396338.2019.1637122.

13. Jon Lindsay, "CYBER OPERATIONS AND NUCLEAR WEAPONS", NAPSNet Special Reports, June 20, 2019, https://nautilus.org/napsnet/napsnet-special-reports/cyber-operations-and-nuclear-weapons/.

14. See, for instance, James Acton, “Escalation through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of Inadvertent Nuclear War,” International Security Vol. 43, No. 1 (Summer 2018); Erik Gartzke and Jon R. Lindsay, “The Cyber Commitment Problem and the Destabilization of Nuclear Deterrence,” in Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations, edited by Herbert Lin and Amy Zegart (Washington, DC: Brookings Institution Press, 2018); Lawrence J. Cavaiola, David C. Gompert and Martin Libicki, “Cyber House Rules: On War, Retaliation and Escalation,” Survival Vol. 57, No. 1, 81-104 (2015). Paul Bracken “The Cyber Threat to Nuclear Stability,” Orbis Vol. 60, No. 2 (2016). Stephen J. Cimbala and Roger N. McDermott, “A New Cold War? Missile Defenses, Nuclear Arms Reductions, and Cyber War,” Comparative Strategy Vol. 34, No. 1, 95-111 (2015).

15. See, for instance, Mark Fitzpatrick, “Artificial Intelligence and Nuclear Command and Control,” Survival Vol. 61, No. 3 (2019).

16. See, for instance, Xu Longdi, “Cyberattack, Nuclear Safety and Strategic Stability”, in Information Security and Communications Privacy, No.9, 2018; Xu Weidi, “Strategic Stability and its Relations with Nuclear, Outer Space and Cyberspace”, in Information Security and Communications Privacy, No.9 2018; Cui Jianshu, “Modernization of Nuclear Power of the US and Strategic Stability in Cyberspace”, in China’s Information Security, No.8, 2019; Jiang Tianjiao, “Cross Domain Deterrence and Strategic Stability in Cyberspace”, in China’s Information Security, No.8, 2019.

有关网络－核风险的研究均对以下两大主题表示关注。

第一个主题是，由于诸多因素的影响，完全理解和预测 NC3 系统的网络脆弱性实际上是不可能的。这些系统具有内在的复杂性，且这种复杂性与日俱增。这些系统通常是旧（遗留）组件和现代元素的混合，多年反复修改、升级和集成以适应不断变化的需求、技术变革、漏洞修补和现代化。这就使得即使是少部分拥有足够安全许可的个人也很难完全掌握其结构和组成，更不用说找出其中的漏洞。此外，这些系统往往依赖于其他具有双重或多重功能且不具同等安全水平的系统，或是以各种方式与后者相联通，很难完全列出所有这些关联并进行全面评估。随着有核国家逐步将新技术特别是人工智能引入其中以加强预警、侦察和指挥控制，这些系统的复杂程度还在加剧，这可能使得其操作者和对手都更加难以对其全面掌握。

另一个主题是，有关 NC3 以及进攻性网络作战和能力的信息通常都处于高度保密和严格隔离状态。负责不同功能的人员通常只在各自独立的团体中工作，彼此之间最多只是间断的、浅层的沟通，基本谈不上彼此协调。由此造成的结果是，负责 NC3 和网络行动的官员对两者可能面临或制造的风险缺乏充分认知。各个层级的高级决策者可能完全没有意识到这一问题，或是未得到充足的相关信息，当然也没有意识到由此带来的影响。这同样也对各国之间的沟通构成了障碍，其中既包括和平时期的政策宣示，也包括危机升级或冲突期间的意图传递。

上文所述报告未能充分阐述但同样得到普遍关注的另一问题，是第三方的存在可能加剧态势的复杂性。通常而言各方很难非常有信心地溯源网络攻击，更不用说实时溯源。网络技术高超的民族国家可以伪装成其他网络空间行为体并对其他国家发起网络攻击。在 NC3 系统中同样有可能采取这样的行动。据报道，俄罗斯黑客侵入了伊朗的黑客系统并劫持了他们的黑客工具，用以攻击了至少 35 个国家的实体。在有文件披露网络攻击系俄罗斯黑客所为之前，黑客攻击的部分受害者和安全分析人士可能认为攻击是伊朗实施的。[17] 在另一起针对 2018 年奥运会的网络攻击中，据报道攻击者在恶意软件中植入了复杂的“数字指纹”，比如模仿朝鲜恶意软件的伪造元数据，显然是要让调查人员对攻击来源做出错误判断。该攻击最终也被追踪到和俄罗斯行为体有关。[18] 除国家行为体外，恐怖分子和其他非国家行为体会可能假扮成国家来制造危机。

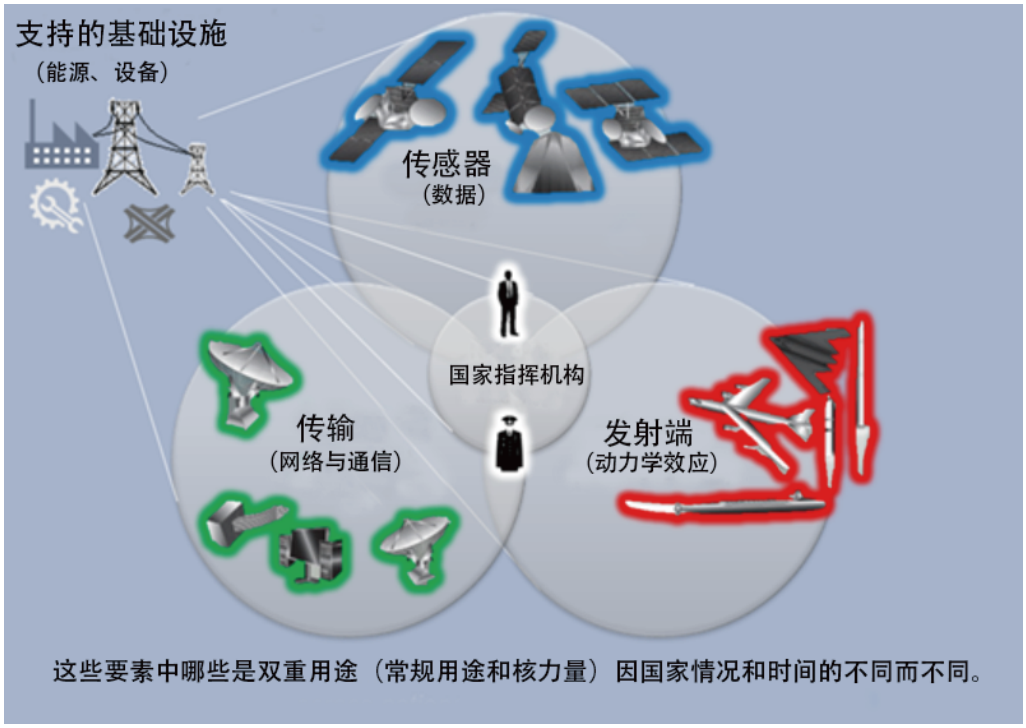
鉴于各行为体在减少事故、意外冲突和减少冲突升级方面的共同利益，卡内基国际和平研究院邀请来自中美两国的专家共同探讨网络－核风险问题，分析针对 NC3 系统构成网络威胁的可能状

17. 美国国家安全局（NSA）与英国国家网络安全中心（NCSC）的联合报告认为，俄罗斯黑客组织“接入并使用了伊朗“高级持续威胁”的指挥控制（C2）体系，用以在与他们利益相关的目标中植入他们自己的工具”。相关行动持续了多年时间。See NCSC and NSA, “Advisory: Turla group exploits Iranian APT to expand coverage of victims” October 21, 2019. https://www.ncsc.gov.uk/news/turla-group-exploits-iran-apt-to-expand-coverage-of-victims; Jack Stubbs and Christopher Bing, “Hacking the hackers: Russian group hijacked Iranian spying operation, officials say,” Reuters October 21, 2019. https://www.reuters.com/article/us-russia-cyber/hacking-the-hackers-russian-group-hijacked-iranian-spying-operation-officials-say-idUSKBN1XO0AK.

18. Andy Greenberg, “The Untold Story of the 2018 Olympics Cyberattack, the Most Deceptive Hack in History” Wired October 17, 2019. https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/.

况，并提出双方可以单方面或合作采取的措施以减缓相关风险。研究的参与者均基于公开信息开展研究。当然，有关网络能力和 NC3 系统的重要细节是高度机密的，且此研究无意对此加以改变。而公开资料已足以为相关专家分析和指明风险、探索管理风险的可能路径奠定基础。

以公开资料为基础，出于研究的需要，我们在讨论中将核指挥、控制和通信系统（NC3）界定为可以为核力量的作战行动发挥促进和支援作用、为核武器相关决策制定发挥辅助作用的整体信息和电信设备。需要强调的是，NC3 还包括相关附属系统（如电力设施），这些系统对核武器的正常运转至关重要，且易遭受网络攻击。对核国家而言，NC3 系统必须保证在从早期预警到核武器运用的全过程中正常运作。为便于说明，我们在此列出系统所需组件的草图。



本报告首先简要介绍了中美关系的背景以及其在网络空间的具体情况，尔后总结了研究参与人员认为可能影响到 NC3 的各种常见网络威胁，并描述了在这些威胁当中被参与人员认为在中美背景下最值得关注和全面应对的几种威胁场景。在探讨这些场景后，本报告探讨了中美两国可以单方面和（或）合作采取的措施，从而减少与这些威胁相关的风险。我们希望邀请两国的专家和官员共同深化对这些问题的理解，思考解决这些问题的建设性方法，并希望在之后将这种努力推广到国际社会层面。当然，是否有意将本报告结论部分所讨论的措施付诸实践，完全由特定核武器国家（本报告中意指中美两国）统筹考虑。

一、战略稳定：背景的重要性

在讨论具体的网络－核关系之前，有必要首先考察针对 NC3 的网络行动受到的关注持续上升的战略（以及国内）背景。通常它会塑造行为体应对具体问题的方法，也会定义可供选择的问题解决方案。基于本报告的目的，这里所探讨的更广泛背景，是指中美双方战略关系的总体性质，以及他们对安全、特别是核态势的总体理解。

定义中美战略稳定面临的一个主要挑战是，与美国和俄罗斯不同，中美两国缺乏对战略稳定的共同界定，且双方关切不同。美国对中国的政策不像对俄罗斯那样基于相互脆弱性（mutual vulnerability）原则。[19] 因此，中国的主要担忧源于这样一种看法：即美国寻求更优越的网络、常规和核能力，以便用来对中国的核威慑进行首次打击，并削弱中国的报复能力。

美国主要担心的不是中国先发制人地使用核武器，而是认为中国不会在与邻国的领土争端中避免使用武力，这些邻国中有几个是美国的盟友或伙伴。在这种情况下，美国担心中国日益增强的网络、常规和核能力是为了阻止美国保护其盟友。

中美两国的担忧都是负面的，这意味着两国都在努力避免因对方的行为造成不利后果。从积极的角度来说，战略稳定意味着双方都不会对对方美方盟友发起军事冲突，且即使冲突爆发也不会认为首先打击对方的战略力量是可行的。

由于两国核武库的巨大差异，中美在对威胁的看法及实现稳定的方式上的不同意见更具复杂性。长期以来，美国一直从平衡俄罗斯的角度来界定其核需求。美国和俄罗斯总共拥有世界上 90% 以上的核武器储备。但美国官员强调，近年来中国的核武库迅速增长，未来十年还将处于继续增长的轨道上。他们表示，这样一种趋势可能在作战层面造成不利影响。

但总体而言，美国对中国的担忧更多地集中在其更广泛的战略行为和意图上。美国观察人士警告称，中国大规模的常规军备建设和军力投射能力旨在阻止美国援助其地区盟友，并削弱后者达成这一目标的常规作战能力。这加剧了美国的担忧，即中国希望单方面改变地区争端的现状——如果有必要的话通过武力——同时努力削弱美国在这些情况下的干预能力和意愿。美国专家和政界人士还对于中国在其他领域的挑衅性行为表达了关切。美国时任国防部长詹姆斯·马蒂斯（James Mattis）在 2018 年美国国防战略（U.S. National Defense Strategy）中则称，“（美国战略）最具深远影响的目标是将我们两国的军事关系置于透明和互不侵犯的道路之上。”[20]

在这种日益恶化的安全环境下，对可能有意或无意地影响 NC3 的网络行动的监管日益受到关

19. Caitlin Talmadge, “The US-China Nuclear Relationship: Why Competition Is Likely To Intensify,” the Brookings Institution, Global China, September 2019, p. 3, https://www.brookings.edu/wp-content/uploads/2019/09/FP_20190930_china_nuclear_weapons_talmadge-2.pdf.
20. Office of the Secretary of Defense, Summary of the 2018 National Defense Strategy of the United States of America. 2018. Available at: https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

注。两国的网络行动操作人员可能都没有充分认识到 NC3 系统的复杂性和敏感性，而且只有那些处于最高层的人才有权限和权力审查这类操作。在这种背景下，美国官员认为中国可能实施或有意或无意地削弱美国 NC3 系统的网络攻击，例如对早期预警卫星进行攻击。他们担心，中国对（包括在网络领域内）军事、情报能力和行动的高度孤立和隔离的管理，将使其高层政治领导人无法对上述行动进行严格监督。那些曾参与过美国政府跨机构有效网络政策审查程序、但未看到中国政府类似政策迹象的美国官员，对此表达的关切尤为突出。

在更大范围上，随着中美关系朝着激烈的“大国竞争”方向发展，他们似乎将要陷入典型的“安全困境”。[21] 双方都感到受到对方的威胁，并采取行动来保护自己。另一方则认为这些行动显然是适得其反、破坏稳定，甚至是具有升级性质的。双方对对方维护战略稳定、克制行动、建立互信的意愿缺乏信心。近年来，由于贸易竞争、对网络相关行为的担忧、相关地区持续的军事建设和胁迫行动，以及普遍的政治对抗，这一问题已经加剧。新型冠状病毒大流行使得两国关系降至 1989 年以来的最低点。

然而，战略稳定将给两国和世界带来重大利益。中美两国在全球数字经济的持续运行和避免全面军事冲突方面有着客观的共同利益。随着时间的推移，他们可以将某些类型的网络行动定义为相互禁止的范围，找到方法让彼此都更确信这些限制将得到尊重。本报告将在第五部分对此进行深入探讨。

21. “Racing toward Tragedy? China’s Rise, Military Competition in the Asia Pacific, and the Security Dilemma,” Adam P. Liff and G. John Ikenberry, *International Security*, Vol.39, No.2(Fall 2014),pp. 52－91.

二、网络维度

自 2012 年以来，网络安全在中美关系中占据着重要地位。两国围绕互联网治理、言论自由、网络商业窃密、大规模网络监控和网络攻击等一系列网络及网络相关问题发生争执。华盛顿和北京在网络安全上的相互指责对双方网络关系的稳定性产生了负面影响。华盛顿指责中国出于商业（包括 APT1 报告[22]）和国家安全（OPM 事件）目的进行间谍活动，北京则反击，斯诺登及其披露的信息表明美国针对中国和中国公司展开广泛网络攻击。两国在安全和商业领域对彼此的态度都明显恶化，导致双方在外交、政治和经济领域的对抗和冲突。人们普遍怀疑和指责中美两国都有操纵供应链或加密设备从而在产品和服务中设置后门的行为，这并无助于缓解两国间的紧张关系。

尽管如此，双方直到最近仍保持着对话与合作。2013 年，奥巴马总统和习主席在美国安纳伯格庄园会晤期间，两国领导人同意通过一个双边工作组就网络问题进行合作。2015 年，两国领导人再次会晤，双方承诺不开展或在知情情况下支持网络商业窃密，并建立了打击网络犯罪高级别对话。2017 年，双方建立执法和网络安全对话机制。[23] 然而，这些充满希望的努力却因两国之间的各种行动、反应、以及对于习奥协议未能得到忠实执行的指责（部分美国智库和网络安全企业）而受挫。如今，两国在网络安全问题上没有任何有意义的讨论，甚至没有任何关于行为准则的共识——无论是明确的还是默认的——来限制所有参与情报收集和攻击性网络行动的行为体。这几年中美两国在网络空间虽然没有发生大规模冲突，但摩擦不断加剧。

双方日益增长的网络能力在其整体国土安全、情报和军事态势中具有特殊的重要性，既是国家权力的象征，又具有操作层面的现实意义。网络空间在情报收集、秘密行动、军事交锋甚至是战争中都已经是占据主导性地位的空间。网络空间力量的运用不仅在冲突期间处于中心地位，在引发冲突（可能在早期使用）及和平时期也是如此。它既日益成为影响认知和行为的媒介，也对物理能力有直接影响。无疑，网络能力对战略稳定特别是核稳定有深远影响。

网络空间的诱惑似乎是难以抗拒的。与常规武器相比，网络工具的获取和操作成本更低。它们提供了巨大的地理覆盖、规模经济和力量投射潜力。它们在很大程度上具有军民双重用途的性质，以极低甚至是零成本从商业应用程序中自然生成。网络行动通常高度保密，从而不必像其他类型行动那样受到审查，并且有更多的方式可以合理地对其予以否认。网络行动受到的正式法律约束和道德约束较少。尽管因网络行动的效应蔓延到其他领域导致升级的风险是存在的，但其仍具有吸引力，因为它们往往不透明，而且不一定会造成明显的物理损害。这些特性可以降低对手以跨域升级

22. The APT1 report, published in 2013 by U.S. cybersecurity company Mandiant, accused the Chinese PLA of a massive cyber espionage campaign beginning in 2006, targeting 141 organizations in the United States and elsewhere. See Mandiant, "APT1: Exposing One of China's Cyber Espionage Units," https://lawfare.s3-us-west-2.amazonaws.com/staging/s3fs-public/uploads/2013/02/Mandiant_APT1_Report.pdf.

23. Details of bilateral dialogues on cyber security can be found at: Lu Chuanying, China-US Cyberspace Relations in the Trump Era, Dec 29 , 2017, https://www.chinausfocus.com/peace-security/china-us-cyberspace-relations-in-the-trump-era.

作为回应的风险。随着人类的操作环境变得越来越数字化，上述特性带来的好处也越来越多。

对于中、美两国对对方 NC3 系统进行网络攻击或保卫自己免受此类攻击的能力，我们并不了解相关细节。但是美国公开承认拥有强大的网络攻击能力，解释拥有这些能力的目的并公开讨论其原则。美国还制定了相关程序，从而依据明确的权限、审查和问责界限使用这些能力，尽管在特朗普政府任内似乎已经对这些能力的使用进行了宽泛的授权。美国政府认为，其他很多国家同样拥有或正在积极发展进攻性军事网络能力，中国在其中无疑处于领先地位。

另一方面，中国公开倡导和平利用网络空间，并坚决拒绝讨论攻击性网络能力和相关条令。中国认为，网络空间稳定的关键是各国放弃使用网络工具实施侵犯性活动和干涉别国内政。中国最新版国防白皮书表示，中国军队将“加快网络空间能力建设，发展网络安全和防御手段，建设网络防御能力。”[24] 这份文件将中国的军事网络力量和能力描述为防御本质的，旨在作为“战略支援”进行防御和反应。中国领导人公开表示希望避免网络军备竞赛和战争，这与中国长期以来表示不首先使用核武器、不寻求外空军事化和对抗的做法类似，这些都与美国在这些领域的立场不同。

这就产生了一个恶性循环：截然相反的方式使中美很难相互理解，更遑论信任。相互理解的缺失使双方很难就网络空间战略稳定进行有意义的双边对话，而此类对话的缺失又使相互理解和信任更难实现。这一现象在探讨网络事件对 NC3 架构的可能威胁时表现得尤其突出和严重，而这种威胁是可能导致事态升级至超出国家领导人预期的程度的。

在此背景下，特别需要关注中国对美网络战略和政策的最新变化的高度忧虑。中国警惕地观察美国的官方文件和公开声明，它们标志着美国在网络空间的战略正在从克制、反应性姿态转变为通过与对手“持续接触”开展更积极的、持续的对抗。[25] 美国国防部的网络战略强调“前置防御”（defending forward），以便“从源头破坏或阻止恶意网络活动”。[26] 除了这些指令上的改变，据报道，2018 年的一项总统指令放宽了对低于“使用武力”级别的进攻性网络行动的审批程序。[27]

国防部官员断言，“前置防御”并未从根本上改变其行动的防御目的。相反，这一概念表明，他们正在不断更新改进方式以打击武装冲突级别以下的恶意网络和信息行动。这种方式也包括与合作伙伴共享信息，而不仅仅是打击外国网络行为体。[28]

---

24. Ministry of National Defense of the People's Republic of China. China's National Defense in the New Era. 2019, p. 9, Available at: http://eng.mod.gov.cn/news/2019-07/24/content_4846443.htm.

25. See U.S. Cyber Command. Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. Cyber Command. 23 March 2018, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010; Paul M. Nakasone, "A Cyber Force for Persistent Operations," Joint Force Quarterly 92 (2019). https://www.459arw.afrc.af.mil/News/Article-Display/Article/1737519/a-cyber-force-for-persistent-operations/.

26. Department of Defense. Cyber Strategy 2018, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

27. Ellen Nakashima, "White House authorizes 'offensive cyber operations' to deter foreign adversaries," The Washington Post, September 20, 2018, https://www.washingtonpost.com/world/national-security/trump-authorizes-offensive-cyber-operations-to-deter-foreign-adversaries-bolton-says/2018/09/20/b5880578-bd0b-11e8-b7d2-0773aa1e33da_story.html.

28. See "An Interview with Paul M. Nakasone," Joint Forces Quarterly Issue 92 (1st Quarter 2019), https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92.pdf.

这些变化在实践中意味着什么还有待观察。但对核心概念的模糊定义以及美国官员传递的含混不清的信息，使得这种新战略可能涉及对中国（和其他国家）系统的常规深入渗透。这将强化中国的观点，即美国在网络空间（和其他领域一样）正变得更加咄咄逼人。中国担心，美国意在威慑和防御的行动实际上可能增加网络危机的可能性，并迫使双方做好要应对最坏情况的准备。这将意味着双方都要扩大、加强和加快网络空间的强势行动，以获得网络空间的安全感。美国对朝鲜导弹系统使用“主动抑制发射”（left of launch）网络行动就是一个例证。尽管该行动针对的目标是物理系统而非网络能力，但它展现了在网络空间实施防范和先发制人的吸引力，也因此而影响了中国人对“防御前置”可能意味着什么的看法。[29]

美国决策者也认同，网络空间给中美关系带来了明显的挑战，但他们在对哪些因素构成了挑战的问题上，与中国的看法截然不同。这种观点上的分歧似乎是根深蒂固的。中国对美国咄咄逼人的网络政策和理论感到担忧，但美国分析人士强调双方有更大的分歧，如国际法如何适用于网络空间、哪些行动可认定为武装攻击，等等。美国还强调有关网络对抗规则的共识严重缺失。中国观察人士承认这些分歧的存在，但认为它们与中美就网络空间战略稳定进行谈判的关联度并不高。

中国和俄罗斯在网络外交上的立场高度同步，加深了美国对中国诚意的怀疑，因此将中国与美国心目中俄罗斯的表里不一相提并论。[30] 在美国看来，俄罗斯一方面呼吁禁止网络战争，一方面即使在和平时期也在从事极具侵略性和欺骗性的网络行为，包括对多个国家的间谍活动、信息行动以及实体毁坏和破坏。由于中国公开支持与俄罗斯相同的正式立场，美国专家担心中国也会有类似作为。

正是在这种背景下，一些美国专家认为，中国不愿谈论其网络能力和监管政策是不诚实的表现，怀疑这是为了掩盖中国对美国进行网络攻击（或至少是做此准备）的意图。他们还担心，中国人在此问题上保持沉默，其实是隐藏了其内部对网络工具的开发与使用缺乏内部审议和政治监督的缺陷。有些美国专家担心，这将使得网络操作人员有相当大的余地，能够更频繁地、非故意地以具有破坏稳定性的方式针对美国使用网络能力。因此，美国专家坚持认为，中国官方承认拥有进攻性网络能力并阐明其使用原则，对于就相互克制和稳定展开有意义的双边对话至关重要。

此外，美国官员认为，如果完全撇开与网络相关的重大问题不谈，很难想象双方能建立起一点点信任。多年来，美国官员和专家一直在谴责中国对信息自由流动的限制及新实施的网络安全法对贸易和商业的“重大不利影响”。[31] 美国司法部起诉、“曼迪昂特”（Mandiant）报告 [32] 及其他报告所披

29. Paul M. Nakasone and Michael Sulmeyer, “How to Compete in Cyberspace,” Foreign Affairs, August 25, 2020, https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity.

30. Nele Achten, “New U.N. Debate on Cybersecurity in the Context of International Security,” Lawfare, September 30, 2019, https://www.lawfareblog.com/new-un-debate-cybersecurity-context-international-security.

31. World Trade Organization, “Communication from the United States: Measures Adopted and Under Development by China Relating to its Cybersecurity Law,” 26 September 2017, https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/S/C/W374.pdf.

32. FireEye Mandiant, “APT1: Exposing One of China’s Cyber Espionage Units,” 18 February 2013, https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

露的中国国内信息政策和持续多年的经济间谍活动，也同样引发美国人的警觉。近年来，美国官员对于中国政府与中国领先科技公司之间的紧密关系反复表达关切（尽管他们并未公开提供证据支持其观点）。他们认为，这种政企关联不仅对美国也对其他国家构成了安全风险。

中方官员一直谴责美国利用网络对中国开展大规模网络监听，[33] 坚决反对美国对于中国政府与科技公司关系紧密的指责，并谴责美国在缺乏证据的情况下抹黑中国互联网企业，[34] 借助“清洁网络计划”对中国企业开展无理由的单边打压。[35]

中国还强调，中美必须先建立信任，才有可能在透明度和其他具体问题上取得进展。在中方看来，如果彼此对对方的意图没有信任或信心，那么要求了解有关对方能力的信息只是另一种间谍手段。即使双方交换了某些信息，也不会认为这是可信的或者是愿意提供真正有意义的细节。

在本报告的研究过程中，中国专家多次对美国一方面敦促中国参与全面双边对话、另一方面又不断采取指控解放军军官和逮捕中国科学家等敌对行动表示失望。这些研究人员和其他人士都认为，美国的这类行动向中国发出了混淆不清的信号，只会削弱信任的基础，而这正是进行有意义的对话所必需的。[36] 例如，在美国起诉五名解放军军官后，2013 年成立的网络安全工作组就停止了。中国专家进一步指出，“（在军事和情报领域）互信的缺乏可能导致低强度的冲突”。[37]

这些在双边对话性质和机制问题上相互冲突的观点，长期以来阻碍了双方在大多数紧张领域取得进展，而非仅限于网络领域。美国总体上倾向于把分歧化解成具体问题，首先着手应对最紧迫和最具风险的实际问题，以此作为建立信任的途径；而中国则反复强调，如果信任不存在，在这些实际问题上的努力都是没有意义的。中国强烈主张应把重点放在战略意图上，因为如果能够消除不信任，那么所有其他具体问题都将迎刃而解。

毫无疑问，中美之间的信任问题比本报告讨论的问题要广泛和深入得多。但在此指明这一点尤为重要，因为各方都有强烈的技术和作战动机，在对方目标最脆弱、自身设施最完备的冲突初始时期使用进攻性网络能力。这是经典的“要么使用，要么失去”（use it or lose it）在网络空间的演变。信任问题还可能导致军备竞赛不稳定甚至是危机不稳定。长期存在的不信任和安全困境将使两国官员和专家都以极度的猜疑心态看待彼此的行为，并将政策和态势的变化解读为以胁迫和先发制人为目的。

---

33. Ministry of Foreign Affairs of PRC, Foreign Ministry Spokesperson Zhao Lijian's Regular Press Conference on October 21, 2020, https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1825675.shtml.
34. Ministry of Foreign Affairs of PRC, Foreign Ministry Spokesperson Zhao Lijian's Regular Press Conference on August 18, 2020, https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1807193.shtml.
35. Ministry of Foreign Affairs of PRC, Foreign Ministry Spokesperson Hua Chunying's Regular Press Conference on December 10, 2020, https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1839270.shtml.
36. Lu Chuanying, China-US Cyberspace Relations in the Trump Era, China-US Focus, December 2017, https://www.chinausfocus.com/peace-security/china-us-cyberspace-relations-in-the-trump-era.
37. Ibid

三、网络-核威胁：需要特别关注的场景

正是在上述背景下，两国都担心对方军队会采取可能威胁 NC3 的网络行动。以下三种场景尤其值得关注：

首先，在常规对抗之前可能会在网络空间采取早期的预防性甚或先发制人行动，而这种行动可能会在无意中对核资产及核指挥与控制基础设施产生影响。其次，在常规冲突爆发后可能出现网络攻击，其目的可能是为了防止出现核升级，但可能会在无意中导致核升级。第三，网络行动的巨大威胁，会造成对方对核力量安全性、生存性和可靠性的强烈焦虑，从而触发更高的警戒状态和其他防御措施。这些都可能会导致事故和失误，或者被对方误解为具有进攻意图的行为。这三种场景都可能产生意想不到的可怕后果。

有充足的理由认为，国家（尤其是拥有核武器的国家）可能会针对某个对手的 NC3 实施网络行动。通过网络行动，国家可以得到有价值的情报、及时提供有关核攻击（或非核攻击）的早期预警，以及确保对方并未准备发起此类攻击。事实上，具有极高精度的情报，还可以判别核预警（在被对方探量到的情况下）是更具防御性还是更具攻击性。

一些国家还可能认为网络行动有助于慑止对手使用核武器。以可被探查到的方式对对手的 NC3 实施网络侵入，或者在事后有意披露相关信息，对手对于其自身系统可用性（availability）、完整性（integrity）和机密性（confidentiality）的信心可能被削弱。即使因网络行动而暴露出来的漏洞得以被修复，受影响一方仍会担心，还有其他漏洞存在或是有可能被发现和利用。由此，该方可能被劝止采取威胁性措施。

在极端的情况下，网络行动也会削弱对手使用其核武器的能力。如果仅在战术层面采取行动，那么与对核武器系统的核或常规攻击相比，以网络行动对系统实施降级所带来的升级风险较低。用以攻击 NC3 的网络能力与收集相关情报的能力在很大程度上是互通的。从内部对系统进行深度侦查是实施攻击的必要前提，正如一位经验丰富的网络操作人员所说，“当你进入系统，你就成功了”，接下来很多事情都可能发生。

由此带来的问题是，对此类网络入侵行动背后的动机很难准确解读。网络工具的设计者和操作者几乎不可能对工具的效果有百分百的把握，更不可能充分认识到这些工具将如何影响接收方的认知。目标国核设备的操作者和领导者对入侵动机的评估可能更加不确定。他们可能想立即知道：这些结果是源自自然发生的技术故障、灾难或事故，还是有敌意的攻击？如果是后者，是谁实际上（不仅仅是表面上的）发起了攻击，是谁授权此次行动，哪些系统受到了影响以及受到何种影响，攻击的目的是什么，以及对方是否意在制造更大的损伤？即使是旷日持久的调查也很少能就上述问题给出确定的答案。

双方都无法充分认识到网络攻击能力的使用对被攻击的核心系统和辅助系统有何影响，更不用说对攻击者并不知晓但实际波及到的那些参与核支援任务的系统有何影响（考虑到核系统的高度机密性，后一种情况非常可能出现）。如果像一些人所认为的那样，两国在探查和正确溯源网络行动的能力方面存在明显的不对称性，那么决策制定的合理性和质量就会受到更多复杂因素的制约。

进一步加剧上述不确定性的另一个因素是，两国开发和运用网络能力与核力量的各机构之间在信息、行动管理、政策监督和决策制定等领域的深入整合方面可能存在差异。如本报告第一部分所述，网络操作者可能并不充分了解，更不用说理解和把握对手复杂而高度机密的 NC3。因此，他们也无法准确告知领导人其所建议或实施的网络行动可能有何后果。

中美两国核力量在架构和理论方面的差异也影响到各自指挥与控制系统的脆弱性，这些脆弱性反过来又会影响中美是否有意愿以及如何攻击对方 NC3，以及各自如何防范这些威胁。

如果中国认为美国正寻求针对中国核威慑的“主动抑制发射”（left of launch）网络能力，[38] 那么中国可能把任何对其系统的网络入侵视为美国对其核威慑力量的蓄意攻击，即使其无法确定网络入侵背后的实际源头和意图。中国甚至可能感受到必须实施网络侦察的压力，以试图了解美国可能有何计划。同样，如果这种侦察活动被美国探查到，美国官员对其威胁性和侵犯性的看法可能会高于中方的实际意图。最后，中美核力量与核理论的巨大差异也阻碍了双方准确理解对方的 NC3。双方可能都无法很好地理解对方的 NC3 是如何与常规力量相结合的。这些都增大了网络行动在无意间影响到极具敏感性系统的风险。

对中美间网络实力平衡的不同看法可能会加剧这些风险。中国专家似乎坚信，在中美网络冲突中，中国在双方网络冲突中将是实力较弱和较有限的一方。这种看法可能会让中国更加担忧自己是否有能力监测、溯源或挫败美国对其 NC3 的潜在入侵。中国核力量当前的扩充和多样化可以增强中国的二次打击能力，这将有利于增强稳定性。但另一方面，如果新的核力量最终导致其更易遭受网络渗透，那么这些新力量非但不能让中国领导人放心，反而会增加他们的焦虑感。

中国官员认为，美国同行理解中国在这个问题上的普遍看法，即其规模小得多的核武库并不适宜对美国实施率先打击。不管中国的网络攻击是否会减缓或阻碍美国的核行动，这一点都是勿庸置疑的。中国的网络操作者则进一步假定，美国能够充分认知到，中国无意抵消美国的核威慑。因此，他们可能会低估网络侦察及其他活动会无意中引发升级风险的可能性。而如果美国防务分析人士并不像中方那样认为中国在网络空间上要弱得多（或是真的奉行不首先使用核武器政策），这种风险就更大了。鉴于美国分析人士认为中国在网络空间及其他领域的行为都具有挑衅性，如果美国在其 NC3 中探查到中国的网络行为，就会将其视为严重威胁。

38. 译注：“主动抑制发射”战略最初是由美国陆军和海军将领在 2014 年的备忘录中提出，他们希望国防部高层能对“弹道导弹防御”（BMD）战略进行调整，不再单纯地依赖拦截弹进行防御。简单地说，“主动抑制发射”是指在敌方发射前击败威胁的能力，包括非动能能力、激光武器甚至网络攻击武器。

核与非核设施的日益整合是不稳定和冲突升级的另一个潜在来源。[39] 未来几年，随着美国投入巨资以提高其总体指挥和控制能力，美国将很可能对以往各军种独自拥有和运用的能力加以整合。至少 NC3 的部分功能将很可能被纳入多域指挥和控制体系（Multi Domain Command and Control）。美国国防部已经开始就建立“全域联合指挥和控制”（Joint All-Domain Command & Control, JADC2）而做出广泛努力，据报道该体系将连接和整合所有军种和所有作战领域的传感器和通信系统。虽然这一概念仍处于开发阶段，国防部官员已表示它将与 NC3“相互交织”。[40] 这引起了人们的担忧，即对手将更加难以将核与非核的 C3 能力区分开来。这种情况在今天的中国可能已经比较普遍。美方猜想，中国的常规导弹与核导弹可能已经在共用一个指挥和控制系统。一个普遍认同的看法是，火箭军（原第二炮兵）具有双重职能。至少包括超视距雷达在内的一些中国早期预警装备，可能用于核操作与非核操作。

现在不可能确切地预知这种常规与核的整合对于中美网络 – 核态势有何影响。但值得担忧的是，美国各军种、核与网络指挥机关以及文职官员对于这种发展趋势会如何影响中国对威胁的认知可能没有清晰的了解，更谈不上充分的感知。同样，他们的中国同行可能也没有完全意识到中国现有的联合指挥和控制会如何影响美国的看法与计划制定。另外一个需要关注的问题是，网络当中节点越多，潜在的网络漏洞就越多，就越难以准确地判定对手旨在破坏何种能力。与此同时，两国还都越来越依赖于卫星等多用途设施，来同时为常规和核力量提供通信和早期预警支持。

总之，网络行动可能因多种方式引发问题。即使是最复杂、最有针对性的网络行动也可能产生意想不到的影响，包括扩散到其他系统并造成附带损害。[41] 潜在的、不可预见的连锁反应并不局限于技术系统，破坏数据或系统、引发对核力量控制的不确定感，同样可能造成决策者思维上的混乱和不稳定。遭受网络入侵行为的一方面临着实时评估网络入侵来源、意图、影响和含义的巨大挑战。区分技术故障和网络攻击也是一项耗时的工作，可靠的溯源耗时更久。因此，在高度的战略不信任的背景下，危机或冲突中影响核系统的任何网络事件，都可能引发焦虑、困惑与恐慌，相关当局也将面临极大的决策压力。

本研究的主要目的并非探讨所有可能的情况，也不希望仅限于描述“问题”。我们试图提出减少和管控风险的实用建议，以服务于双方在战略稳定方面的共同利益。以此为目的，我们希望针对那些在 NC3 内外部的（有意或无意的）网络行动，找出可能导致军备竞赛、危机升级甚至核冲突的几类场景。针对这些场景也许可以设想出无数种变化，但我们的目标是更为简洁地找出最具不稳定性的

39. James M. Acton, “Escalation through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risk of an Inadvertent Nuclear War,” *International Security,* vol. 43, no. 1 (Summer 2018): 56-99.

40. Colin Clark, “Nuclear C3 Goes All Domain: Gen. Hyten,” Breaking Defense, February 20, 2020, https://breakingdefense.com/2020/02/nuclear-c3-goes-all-domain-gen-hyten/.

41. 在网络空间的背景下，评估一项进攻行动的复杂性的关键指标是机密性、合理的可否认性、准确性，有保证的效果及其及时性，以及避免附带损害。

因素，进而明确指出中美两国都希望降低的、最令人担忧的不稳定风险，之后回归我们的主要目的即探索降低此类风险的可行方法。

（一）NC3 的功能

在确定要关注哪些场景时，清楚界定任何 NC3 架构都可以提供的基本功能是非常有益的。[42] 根据我们的理解，这些功能包括：

1、保证在任何时候对所有核力量和战略行动进行有效监管和专属控制；

2、在所有场景下为决策、规划和行动提供支持；

3、对即将到来的攻击及时发出预警；

4、为各指挥层级提供态势感知；

5、确保系统与国家指挥机关之间有效且安全的通信联络；

6、依要求适应和支持所有的维护、升级、安全和保证操作；

7、抵御所有的破坏和颠覆行为，维护指挥层级之间以及跨指挥层级的信息与指令的可靠传输；

8、维持与核武器的敏感性相称的高标准安全、安保和保密。

数字安全事件（或攻击）通常被归类为会影响“AIC 三要素”的事件，后者即硬件、软件、网络以及数据的可用性（availability）、完整性（integrity）、机密性（confidentiality）。本报告聚焦影响 NC3 组件、产品和服务之可用性、完整性和机密性三要素的网络事件，探究其可能造成的潜在影响。这些事件包括以下一种或多种情况（并不互斥）：

1、国家指挥中枢、早期预警系统与 NC3 其他部分之间的通信，或是 NC3 与作战单元之间的通信被切断或扰乱，削弱上述机构对最高指挥当局指令的反应能力和可信度；

2、数据的保密性（可能在所有级别）受到破坏，从而扭曲决策并将核力量置于危险境地；

3、用于预警、决策制定、响应以及操作控制的数据之完整性（可能在所有级别）受到破坏和操纵，从而削弱态势感知、破坏警报与响应进程。

4、运载机制或平台瘫痪或被破坏；

5、对系统与程序的可靠性乃至整个核武库的信任出现动摇，导致高度紧张，影响战略和战术层面的选择与应对；

6、在发现对这些系统的攻击后，针对嫌疑攻击者发起或对等或升级的报复或回应；

7、对自身安全度的高估（如果攻击未被发现，或攻击被提前发现并化解）。

（二）需特别关注的四种具体情景

如前所论，蓄意削弱、瘫痪和（或）破坏 NC3 的网络行为毫无疑问会带来严重的甚至是极为严峻

42. See also John R. Harvey, “U.S. Nuclear Command and Control for the 21st Century” NAPSNet Special Reports, May 24, 2019, https://nautilus.org/napsnet/napsnet-special-reports/u-s-nuclear-command-and-control-for-the-21st- century/.

的风险。网络间谍活动和网络攻击之间的模糊界限、网络攻击潜在的传染和连锁效应（即超出预定的攻击或破坏目标），以及持续存在的对于侵入者及其意图的不确定性，使网络行动极易在无意中引发不稳定。这里有四种情景值得特别讨论：

第一种情景涉及旨在收集对手 NC3 核心部分相关数据及核心部分所储存数据的网络间谍活动。一旦间谍活动被发现，目标国可能会认为，对手在己方 NC3 建立据点，侦查和提取信息，这些是对方即将向武装冲突升级、甚至可能攻击己方核力量的前奏。

第二种情景同样涉及网络间谍活动，不同在于其对象是两用系统或为 NC3 提供支持或与其关联的其他环节，而这种关联有可能是并没有被网络行动发起者（或是网络行动对象国政府）充分认识到的。潜在目标包括：两用 C3 系统，特别是早期预警设施、电力供应或其他提供支持的辅助系统。虽然其敏感性低于第一种情景，但这种行动同样可被视作即将进行攻击、特别是对核力量进行攻击的征兆和准备工作。

第三种情景涉及的是针对两用（此处指常规和战略）NC3 的网络攻击，或是针对为 NC3 提供支持或与其相关联的系统进行攻击、但并无意影响系统核功能的网络攻击。潜在目标可能包括：两用 C3 系统，特别是早期预警设施、电力供应或其他辅助系统。无论网络行动实施者意图如何，此类行动都可能影响到目标国的核运作，或者至少目标国会解读认为有此意图。

第四种需要探讨的情况是，有时一方既对另一方意图有严重猜疑，又对己方 NC3 在网络攻击中的脆弱性高度担忧，两者相结合导致反应过度和危机升级。技术故障、对事件的误判或是人为失误都可能被认为是网络攻击（或至少在短期内如此认为），或是触发导弹攻击即将到来的错误预警。随着人工智能算法被应用到 NC3 中，这种情景发生的可能性正在增加。各国因担忧其核力量的脆弱性而采取措施，但这可能反而加大危机不稳定性的风险，相关的例子包括“预警发射”或将发射权预先赋予地区指挥机构。

（三）针对 NC3 的（实际发生或所察觉到的）网络行动的潜在后果

网络行动可对美、中或二者一起直接制造战略影响，其影响可能是正面的，也可能是负面的。不管行动是否真实发生，对网络行动的担心和预期都可能产生战略影响。同样，如果中国或美国误以为行动是针对他们的，或者对正在发生的事件或行动做出误判，战略后果都可能随之产生。

网络行动的显著特征使上述所有这些场景都有可能发生。所察觉到的网络行动的目标方可能对此不以为意，但鉴于核安全与安保的极端重要性，这种可能性相对较低。因此，此处重点关注的是，如目标方感到不得不采取反制措施将产生什么后果。

当然，此类行动也有可能阻止对手做出可能导致冲突升级的反应。正是这种可能性促使处于敌对状态的竞争对手制造出本文所涉及的威胁，也使我们难以说服他们完全排除此类行为。此外，由于实施威慑的个人和机构都意在防止出现战争（及战争发生时的升级），很难使之愿意放弃他们认

为可能需要依赖的能力。为了鼓励他们在实施此类活动时尽力保持克制，并使他们在确实投入此类活动时保持极度审慎，充分理解此类行动所带来的风险就非常有必要。另外，行动的潜在后果可能将大大超过他们认为能够从威慑中获得的益处。

由上述情景引发的后果有四大类在战略上尤其令人担忧：

1. **核冲突。**如目标国观察到针对其 NC3 的（无论是真实的还是误判的）网络攻击，并断定必须立即使用自己的核武器以防之后丧失使用核武器的能力，就可能引发这一后果。将早期预警和通信系统的故障错误解读为“攻击即将发生”，会引发同样的情况。

2. **无意地或意外地使用核武器。**在系统故障情况下，失效的 NC3 会阻止指挥官撤回对使用核武器的预先授权、更改可能引发升级的指令、制止未授权使用核武器的行为。如流氓行为体能够接触到 NC3 或核力量，也可能导致这些后果。

3. **危机升级**可能以多种方式发生。网络行动的影响可能会在无意中从非核目标传播到 NC3 目标。网络行动背后的意图可能被错误地归因或理解，并产生错误认知，即一国的核力量正受到攻击或对手已对本国发射核武器。技术故障和人为失误可能被误认为是对手网络行动所造成的影响，但事实上这只是失误、事故或故障。最后，在关键系统或信息并未被破坏的情况下对其失去信心，或者反过来，对已受破坏的系统或信息仍然盲目信任，都可能影响决策。

4. **长期不稳定性影响。**其中最有可能的是军备竞赛和随之而来的危机不稳定，此外可能在对对 NC3 丧失信心时为弥补不足而采取行动的压力，如采取预先授权使用核武器、将人工智能纳入分析和决策体系等行动。而最不利的影响可能来自于对己方核威慑可靠性失去信心。

在我们看来，中美在短期内可以应对解决的最重要风险是那些因疏忽或在无意中制造的影响，尽管这并非两国网络－核稳定面临的最大挑战。由于第三方行为体可能制造混乱和加剧危机、溯源难题和双方溯源能力不对称、攻击者和目标国预先或实时评估网络行动影响面临固有困难等因素，这些风险出现的可能性更高，纠偏难度也更大。[43]

43. 这里提到的三个原因，即网络空间的第三方行为体、溯源难题、攻击者和目标对网络行动的评估能力，在本报告的其他部分有具体阐述。

四、加强战略稳定和缓解网络－核风险的可能措施

本报告在探讨过程中所形成的一个基本共识是，中美两国应当并且可以共同采取行动，降低网络－核风险并增强其稳定性。虽然两国间的不信任感日益加剧，但这并不必然阻止他们合作以建立信心，从而避免在网络空间或通过网络空间采取有可能破坏稳定的行动。**特别是，两国都希望避免在无意中陷入武装冲突，并致力于防止其向核战争升级，虽然美国并不排除在极端情况下率先使用核武器。**因此，中美两国从事战略、核与网络研究的诸多专家都认为，除最极端的情况之外（甚至即使那时也是如此），两国都不可能通过破坏对方有效使用其核力量的能力而获益。

本报告拟提出两国可以单方采取或是以互惠的、和（或）双边的方式来采取多种措施，以增进在网络空间的稳定信任。这些措施包括：加强中美战略稳定的总体措施、与两国网络政策及核武库结构与能力相关的措施、以及直接加强两国各自 NC3 的稳健性和弹性以抵御网络威胁的具体步骤。本节所列各种值得期待的政策、规则和沟通形式，均旨在缓解严重关切并增进信任。

（一）可确信的网络行动决策程序

如本报告引言所述，网络安全涉及多种行为体、技术和现象，他们广泛分布在国家和国际层面的不同经济体与政府的各个领域当中。协调所有部门的决策制定通常是一个艰难的过程，而不同层级的操作者和决策者可能也并未充分认识或预见到其网络行动可能会溢出并影响其他领域。官员们可能不明白为什么他们自己的能力或行动会看似对他者构成威胁，以及是如何构成威胁的。他们可能也无法评估因他者对其行为做出反应而可能形成的连锁效应。在这样一个复杂的技术和政治－官僚环境下，每个人都很容易夸大他者所构成的威胁。

无论对网络稳定是否有一致的定义和理解，中美两国都可以通过各自的单边网络政策和决策制定，使己方受益并惠及对方。网络行动固有的风险和不确定性意味着，对网络行动进行强有力的监督和风险管理，既有利于实现各自利益也符合共同利益。为此，可以采取适应两国各自独特情况和治理安排、既满足保密和区隔要求又允许实施评估和控制程序的措施。

我们推荐在以下五个层面澄清监管措施：

1、由国家强力机关执行的**内政外交政策监管**，以便充分考虑国内外行为体在发现针对自身的网络行动时可能做出的反应；

2、**技术监管**，包括技术层面的得失评估，以考察一旦行动中所使用的技术能力被发现并被用于针对其他目标（包括在本国领土内的目标）时所产生的意外后果。这种监督还应在（可确信的低／中／高层级）进行评估，以确保网络能力所产生的技术后果或影响与预期相符，而不会产生升级或级联效应等意外影响。

3、以适当责任、问责和指挥控制程序为基础的**行动监管**，以确保能够在获得授权的指挥链内进

行积极的控制。

4、**情报监管**，包括情报层面的得失评估，以考察在网络行动或能力被发现或暴露时所造成的后果，以及在情报来源、方法和结果预判等方面的潜在损失。

5、**法律监管**，包括对网络行动与能力的两类法律审查，以考察其适用于《国际武装冲突法》和其他可适用国际国内法律协定的情况。

此类监管安排无疑会降低因网络行动考虑不周而造成的风险。如将其用于监管可能影响 NC3 的网络行动，也将有助于增强稳定性，因为那些对相关信息了解全面的高层领导人往往会努力减少因错误或无知而导致升级、之后不得不向政治对手及其国内民众和世界进行解释的可能性。这些措施都可以单方面和秘密进行。此处所探讨的这种可以秘密实施的单边行动，同样会带来因谨慎而产生的益处。

如果中美就此展开双边对话，则可以带来额外的裨益。可以乐观地认为，这有助于让双方官员相信，即使在不泄露机密的情况下也可以持续开展有意义的讨论。这有助于两国的官员和专家建立新的平台以交流对这些问题的看法。两方至少可以借此向对方表达关切，并介绍己方所实施的内部监管安排。其关键在于，要让对方都确信，己方只有在获得极高层级的批准后，才会实施对 NC3 有潜在影响的网络行动。

（二）创造一个更加稳定和更低脆弱性的战略环境

中美两国都在采取措施以实现其核架构与核力量的现代化，包括 NC3 的现代化。除众多其他措施之外，两国都寻求加强该系统的安全性、可靠性和弹性以强化整体威慑。这些努力有两种互为补充的逻辑和目标：一是稳健性，即通过各种手段使核武库和 NC3 免受网络攻击，包括隔离专用的核系统、强化基础设施和系统；二是弹性，即从网络攻击中平稳且快速地恢复的措施和能力，如激活备用通信渠道和指挥所、增加电力供应和其他必要供应的冗余。

以此为背景，首先有必要再次强调两国的现代化努力之间所固有的不对称性。对中国来说，现代化的主要驱动力可能是对美国威胁的担忧；而对美国来说，其在核领域的首要（尽管不是唯一的）关切是俄罗斯。无论美国意图如何，中国都不会对美国的现代化感到放心，因为中国确信，美国对军力及 NC3 的现有及规划中的强化措施都远超出网络安全需求，将提升对中国发起先发制人核打击的作战能力。此类作战行动可能摧毁中国的核威慑或至少使其失效，或是削弱中国的核报复能力。正如一位参与本报告的中国专家所说，“任何旨在抵消或降低对方核能力的弹性努力，都将被视为威胁或是可能导致不稳定。我们应当鼓励以增强自身网络防御为目标的弹性措施，包括隔离、改进供应链安全、备份。”这部分解释了为何中国不愿展开对话。按照传统的观点，中国核能力与核战略的模糊性有助于抵消美国的优势。

无论是否能就这些问题展开有意义的持续对话，对中国和（或）美国以多种方式调整其核力量、

理论、作战计划以及 NC3 从而提升稳定性和弹性时的潜在风险与收益，都需要认真加以考察。我们在此将简要介绍本项目参与者对这些可能措施的看法。

1. 增加部署的数量、多样性和方式

这一选项主要与中国相关，因为美国庞大的核武库主要是为了与俄罗斯抗衡。如果美俄于 2021 年 2 月在《新削减战略武器条约》(New START Treaty)预定失效后停止核军控，那么可以想象，美国和俄罗斯也都将增加核武器的部署数量。[44] 目前没有明显的迹象表明，美俄正出于对其 NC3 受到网络攻击的担忧，而增加核武器的种类和部署方式。

美方认为，中国的核力量要小得多且主要依靠陆基运载系统，但目前正在提升其相对有限的海基弹道导弹发射能力，中国可能出于种种原因决定增加核武器的总体数量，并加大在空基和海基运载方面的投入。尽管这种决定可能增强他们对己方二次核打击能力生存性的信心，但尚不清楚，这是否会显著降低其整体核威慑之于网络攻击的脆弱性，以及如果会，将降低到什么程度。如上所述，这在很大程度上取决于供应链、质量控制以及美国如何看待这些变化。

相应的，本项目有研究者认为，中国某些谨慎的应对措施可以起到稳定作用，并应被视为稳定措施。例如，通过降低 NC3 对网络要素的依赖规模和程度，加强核武器系统的安保与安全，提高 NC3 的修复能力；更多地引入备份的辅助系统，如电力供应；支持国家创新和并购，以提高关键信息通信技术的自给水平；维持 NC3 较低的互联网接入程度。

2. 放松对预备措施与核武器使用的限制

美国一直寻求对敌方核力量实施先发制人的网络打击、常规打击或核打击的能力，并且怀疑中国是否会在实际冲突中信守不首先使用核武器的承诺。我们和本项目的其他参与者认为，由于可能有错误信息和(或)分析，放宽对核武器使用的限制将加剧不稳定性，导致使用核武器与升级的风险增大。更佳的安全战略应是加强对过早或错误使用核武器的限制。如能以谨慎的方式提高 NC3 的安全性、稳健性和弹性，将有助于实现这一目标。

澄清意图和原则也会有所裨益。例如，美国已宣称，将考虑使用任何可使用手段来应对网络入侵。可以想象，这为美国以核攻击来回应对其 NC3 的网络攻击奠定了基础。[45] 可以推理认为，该举措意在强化威慑，以阻止网络攻击和对关键资产(特别是 NC3)的网络渗透。然而，其他国家会担心，美国可能在没有准确（或公开共享）溯源的情况下贸然发起核攻击。这可能会促使其中一些国家有更大的意愿，强化、扩大核武库或是放松对使用核武器的限制。这也可能促使他们对美国的核武器系统开展网络间谍活动，以便能够探查美国何时可能准备发起先发制人式攻击。而这反过来又会推动

44. 译注：《新削减战略武器条约》是美俄削减核武器的双边条约，2010 年 4 月签署，2011 年 2 月 5 日正式生效，有效期为 10 年，经双方同意可延长 5 年。2019 年 8 月，美国正式退出《中导条约》，《新削减战略武器条约》成为美俄之间仅存的军控条约。目前，美俄就《新削减战略武器条约》的谈判分歧很大。

45. Office of the Secretary of Defense, 2018 Nuclear Posture Review. February 2018, https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF.

美国采取更激进的威慑政策，从而助长恶性循环。

我们不知道美国是否已在实际上放松了对核使用的限制，以应对可能出现的网络威胁。这种可能性引起了中国的担忧，从而加大或降低对冲突的威慑，或避免无意中的升级。这种挥之不去的不确定性使得双边对话的必要性更加突显。双方可以直接向对方表达自己的关切、看法和意图，说明为什么对方的担忧可能是缺乏依据的或者至少是被夸大了。例如，一方可以郑重地向另一方保证，不打算采取众多措施来加快核武器的发射速度，如为导弹安装核弹头、将发射权预先授予战区指挥官、实施预警即发射（launch on warning）核攻击，等等。中美也可能考虑以某些措施对冲网络攻击对 NC3 构成的威胁，如预先授权军事指挥官在核指挥通信系统遭到破坏时使用核武器。对此类行为的预期收益、风险和方式，我们已在其他文献中加以讨论，在此不再赘述。[46]

3. 新能力的开发和部署

可以想见，反卫星或太空战武器等新能力的开发和部署，也可能引发对网络－核威胁的担忧。在使用此类新武器时，可能通过网络攻击或者其他破坏方式，削弱 NC3 的完整性和可靠性。之前我们已经提到，中国对美国最新的网络空间“持续交手”（persistent engagement）政策表示担忧，认为这可能削弱中国的二次打击能力。除网络对 NC3 的直接威胁之外，在此我们也意在提醒，有必要关注两用 C3 资产所面临的更广泛挑战，并建议在未来的中美战略稳定对话中应涉及这些问题。

另一个需要关注的领域是人工智能的应用。如果人工智能被贸然应用于预警和指挥控制系统，因错误或其他意外导致升级的风险可能增加。将新的漏洞或潜在缺陷带入系统中的新软件、硬件和（或）实践，都可能增加事故或意外升级的风险。（要理解增强 NC3 稳健性和弹性的措施如何会加剧风险，可以关注苏联在 20 世纪 70 年代末、80 年代初开发、测试甚至可能实际部署的“死亡之手”系统或“周长”系统，这些系统允许在极端情况下自动发射核武器。[47]）

（三）相互承诺自我限制

在某些情形下，中美两国可能对限制针对 NC3 及其他指挥控制系统的网络行动毫无兴趣。如其中任何一方的领导人已决定进入大规模的武装冲突，甚至考虑使用核武器以防失败，那么他们可能会希望在冲突早期就使用这些武器。抑或，如果他们打算打一场升级战，那么同样会希望如此行动。所幸，无论是美国还是中国，都并不认为此种情形具有潜在的可持续优势。相反，双方都希望在不陷入武装冲突的情形下寻求获得相互竞争的或是彼此冲突的利益。在这一共同战略利益的驱动下，可以认为中美在短期内需着力应对的风险，主要是因冲突意外升级而导致核武器的使用。因此，有必要为两国提供充分的建议，使他们能够通过谈判和／或采取单方面措施，限制可能威胁对方 NC3 的

46. Peter Feaver & Kenneth Geers, “‘When the Urgency of Time and Circumstances Clearly Does Not Permit…’: Pre-delegation in Nuclear and Cyber Scenarios,” in Understanding Cyber Conflict: 14 Analogies, ed. George Perkovich & Ariel E. Levite (Washington, D.C.: Georgetown University Press, 2017).

47. David Hoffman, The Dead Hand: The Untold Story of the Cold War Arms Race and Its Dangerous Legacy (New York: Random House, 2014).

网络能力和/或行动。

当然，本项目的参与者也承认，鉴于两国关系高度紧张，对单方面采取建设性限制措施在政治上的可行性需要存疑。双方可能都意图展示自己的能力和意愿以示威慑，从而阻止对方走得太远。双方可能都认为，公开做出克制承诺可能被视为软弱，或至少在政治上被如此解读，而这将削弱威慑和战争准备。他们也可能担心，如对方突然改变既定路线，或是正在准备挑起或升级冲突，这种克制会使他们无法提前做好充分准备。尽管如此，我们仍认为，现在应当认真考虑这些措施，以便在政治和战略条件许可时尽快逐步落实。下文旨在阐述本项目所分析的几项限制性措施。

1. 承诺不对核心 NC3 系统进行网络渗透

我们尝试探讨了中美正式承诺不对核心 NC3 系统进行任何网络渗透是否有吸引力和可行性。各国政府自然会有意继续寻求有关对方核力量的信息。但中美两国可以下定决心，在开展情报活动时均不通过对核心 NC3 系统的网络渗透来收集信息，无论这种活动是有意地、直接地针对核心 NC3 系统，还是旨在从其他系统扩散到核心 NC3 系统。他们还可以做出保证，会采取额外的谨慎措施，防止其他网络行动因扩散而对 NC3 核心系统造成意外影响。这种承诺可以增强稳定性，减少误判风险——如第三方的网络渗透被误解为其中一方试图针对另一方的 NC3 开展行动。

要落实这一承诺有多种可供选择的方案，哪种方案更具可行性和吸引力，部分取决于双方愿意在多大程度上透露己方认为属于核心 NC3 架构的要素。下述选项所追求的目标和实现的难度依次递减。

1）双方就核心 NC3 系统构成要素的通用描述达成共识，列入禁止网络渗透的清单。其中可能包括以下一个或多个要素：指挥和控制站、早期预警系统（卫星、雷达）、核武器和运载系统，这些要素彼此之间及它们与国家领导人之间的联系，以及为各要素提供支持的必要基础设施（电源）。

2）两方可各自选择确定哪些属于核心 NC3 系统的，并与另一方分享清单，以表明己方认为应禁止网络渗透的要素。双方均应知会对方，但所列清单不必以对等（或完全对等）为前提。如果一方同意这一方案，但选择不告知对方哪些要素属于其核心 NC3 系统的组成部分，那么就意味着它接受对方可能在无意中闯入这些系统而并未违反承诺。

3）双方同意采取极度谨慎的措施，避免在网络渗透中将对方核心 NC3 系统当作目标，但并不彼此分享核心 NC3 系统的具体构成要素。如一方探测到对 NC3 系统某些要素的网络渗透，认为这些要素对于 NC3 系统至关重要，且攻击溯源至对方，则应告知其所怀疑的入侵者，此活动已进入己方 NC3 系统。后者应停止相关活动并立即撤退，除非它愿意以对方认为可信的方式解释其行为。如果被怀疑采取网络渗透行动的一方对该活动并不承担责任，则应帮助对方识别活动的实施者。

4）上述限制网络渗透活动的一项或多项承诺仅适用于和平时期。中国和/或美国可以明确表示或者暗示，如果发生实际战斗，所有先前的承诺都将中止。

中方参与者普遍认为，美国有能力也有意愿对中国的两用常规 NC3 系统进行网络渗透和攻击。美国长期存在和近期采取的政策均表明，如果战争爆发，美国倾向于这样做。因此，他们普遍赞赏上述自我克制措施，认为这将减少中国的压力，使其不寻求增加核武库的数量和多样性、提高核力量警戒水平。他们还认为，中国不倾向于对美 NC3 系统实施网络行动，因为他们对中国目前是否与美国有同等的发动类似有效攻击的能力表示怀疑。

对于中国专家欢迎美国采取此类限制措施的种种理由，美国专家认为要么不可取，要么不切实际。他们担心的是，这种限制可能会削弱美国的威慑力。这些专家认为，中国将是引发冲突的一方，因此美方不愿自我削弱网络能力，而且正在制定规划，以削弱中国通过使用常规导弹和 / 或核导弹升级冲突的能力。这进一步证实了中国专家们的担忧，即与单纯的常规或核打击相比，美国针对指挥和控制系统的网络行动可能更不易可察觉且更有效。美国专家的另一担忧使得问题更为复杂，即如果美国承诺实施此类限制，中国是否会做出类似的承诺并履行承诺。

总之，中美两国中的任何一方都极难让对方相信，己方正在遵守这些规定，并证实另一方也在这样做。因此，美国专家普遍对该建议的可行性持怀疑态度。但这并非完全否定该建议的价值，因为它有助于激发思考，且我们可以不时重新审视与这些方案及其排序相关的利益交换分析。

有鉴于上述考虑，美国专家建议两国采取更温和的措施来应对风险。例如，美国应该让网络和核力量的操作者和政策制定者参与深入的分类评估，探讨美国针对中国 NC3 系统的网络行动可能制造或加剧哪些风险。此类研究应着眼于恶意软件传播到预定目标以外的系统所可能产生的意外后果，以及其他可能被中国同行误解的措施。更进一步，上述人员者应开展桌面演练，探索和更好地了解相关互动态势，以及如何避免那些高度危险和 / 或具有高度可能性的情况。虽然中国在上述领域的同行会有与美方不同的假设，但有理由认为，开展类似的内部分析和桌面演习，以了解网络间谍活动和对美 NC3 系统可能攻击的意外后果，也会使他们从中受益。这些行动可帮助中美两国做好准备，以确定和实施己方认为恰当的单方面限制措施，并就相关问题展开双边对话。

与此同时，作为临时性措施，中美有关专家和官员可以探讨，如宣告对方干扰 NC3 系统有效运作的任何企图都将被视为对安全的严重威胁，对两国是否有益及是否可行。更进一步，他们还可以宣布，他们理解对方也持相同看法。要传达这样的看法，可以由两国的最高级别官员私下沟通。这样做的额外意义在于，这表明相关机构已就这些问题向其高级领导人做了充分介绍。

2. 承诺仅最高权力机构可授权针对 NC3 开展网络行动

从上述讨论可以看出，如果中美宣布，在冲突中以包括网络行动在内的任何方式蓄意攻击核武器及其 NC3 系统的决定，都应像核武器使用一样由最高权力机构授权，中美网络 - 核稳定性将得以增强。虽然对核武器和 NC3 系统的攻击一直是由最高权力机构授权的，但以网络手段采取的行动是否包括在内尚不明确。考虑到网络行动可能产生意想不到的后果，这样的承诺对于双方减少猜疑、

建立信任可能都是有意义的。有助于达成或确认该谅解的一个办法是，阐明高级领导人（直至总统/国家元首一级）应对其控制下的网络力量采取的有关行动负责，即使没有得到明确授权。

3. 承诺不以空基战略资产为目标

在太空和反太空战争中使用网络手段会带来极其危险和复杂的挑战。美国明确寻求对俄罗斯、中国和其他国家保持“太空优势”。[48] 俄罗斯和中国试图对此加以阻止。由于 NC3 系统以多种方式依赖于空基资产，太空和反太空战争很有可能损害该系统，特别是与导航、预警和通信有关的功能。鉴于网络能力可用于太空战，这种互动关系也对网络－核稳定构成挑战。

因此，有必要探讨，中美能否就太空和反太空战争部分规范达成共识，以防止对空基战略/早期预警资产的某些或所有攻击。这可以只适用于网络手段，也可排除针对此类资产的所有手段。它也可以只适用于特定类型的攻击，如禁止欺骗攻击（spoofing）但允许干扰（jamming），以最大程度地降低触发错误警报或因无法生成可靠态势感知而产生恐慌的风险。与排除对所有 NC3 系统的攻击相比，这样的承诺在范围上更有限，但可能更具适用性。其原因在于，它不需要任何一方划定 NC3 的边界，也不需要说明单一或两用系统的用途。此外，承诺排除所有形式的攻击，将可避免在哪些构成合法攻击载体或工具保持模糊。

4. 承诺限制第三方网络活动

两国专家均完全同意，第三方因素会给双方的网络－核互动带来极度其不稳定的影响。其中共有六种可能：第三方可伪装成中国或美国，对另一方实施网络行动；中国或美国可伪装成第三方攻击对方（伪旗行动）；中国或美国可以运用代理对对方实施网络攻击。在以动能方式进行攻防时，第三方不会有这样的机会操纵危机和冲突。中美应同意，对具有以下一项或多项特征、可破坏稳定的第三方网络活动实施有效的监督和控制：

- 在他们指导下的行动；
- 利用他们的领土实施的行动；
- 运用他们所开发的能力的行动；
- 他们能够施加较大影响力的盟国的行动，以及可能引发涉及中美的危机或使危机升级的盟国的行动。

美国专家们强调，降低第三方风险的措施符合中美共同利益，且美国将把中国的此类措施视为有意义的信号，将有助于在两国之间建立信任。中国专家则质疑此类承诺在当前政治环境下的可行性。然而，有必要在此提及该建议，以备未来政治环境有助于推动达成此类谅解时提供参考。

---

48. United States Space Command, Vision for 2020 (Peterson AFB, CO, February 1997), https://thecommunity.com/vision-for-2020; “Remarks by President Trump at a Meeting with the National Space Council and Signing of Space Policy Directive-3,” Executive Office of the President, June 18, 2018, https://www.whitehouse.gov/briefings-statements/remarks-president-trump-meeting-national-space-council-signing-space-policy-directive-3/.

（四）对话和信息共享

显然，由于缺乏有关网络空间负责任行为的有意义对话，更不用说达成相互谅解，两国难以采取行动降低风险。如前面反复提到的，由于网络与核行动的互动具有极度的隐秘性和敏感性，这一问题就更为显著。

在美俄的经验中，战略稳定对话有助于双方建立共同的基础，以调整各自的行动，正确解读对方在危机期间发出的信息。而中美在对抗和误判风险不断增大的情况下仍然缺乏这样的基础，令人十分担忧。

华盛顿之所以拒绝将相互脆弱性作为中美战略稳定的基础，原因之一是美国提供延伸核威慑以保护其亚洲（及北约）盟友的安全。这些盟国担心，如果中国能够以核武器威胁美国的存在，美国将不太可能在与中国的冲突中保护他们。这些盟国以及美国越来越担心，可用以投送力量的中国常规军力的迅速发展，及中国在该地区为维持军事存在而日益显著的努力，将削弱美国对其地区盟友的安全保障，并拒止美军进入该地区及在该地区自由行动。

美国虽然很明显不愿使用核武器，但必须考虑在中国与美盟国发生冲突时采取此类行动的可能性。必要时美国将首先利用网络和常规军事力量，对中国的核报复力量进行先发制人的攻击。但美国在最极端的情况下也有可能使用核打击。[49] 对中国核能力进行“有限毁伤”的攻击，旨在为美国及其盟国的常规部队提供时间和空间，从而在所设想的冲突早期阶段将中国推回，使其无法获得预期收益。[50]

中国可能会把不首先使用核武器政策等承诺视为对其邻国及盟国的一种保证。事实上，中国坚称其核使用条令要比美国克制得多。[51] 中国相对较小的核武库规模与这一原则相符，也使得针对美国或俄罗斯实施有限毁伤（先发制人）战略显得不切实际。取而代之的是，中国寻求拥有足够的能力，以确保在面对美国可能威胁时保证其核威慑的生存能力，并能对美国施加严重的报复性毁伤。然而，美国专家认为此类不首先使用的承诺存在问题且不可验证，因此认为坦诚对话意义更为重大。他们还怀疑这样的政策是否能反映中国的真实意图及在冲突中的可能行动。

美国观察人士发现，很难缓解中国因美核态势而对战略稳定产生的担忧。例如，华盛顿在《2019年导弹防御评估》(2019 Missile Defense Review) 中做出官方表态，称其导弹防御并非旨在抵消

---

49. 美国国防部发布的报告详细阐述了《2018 年核态势评估》（NPR）为什么及如何界定美国不排除使用核武器可能性的“极端情况”并进一步指出“通过威慑阻止对盟国及所部署美国力量进行有限核打击”是当前最为紧迫的核威慑挑战。参见：Office of the Under Secretary of State for Arms Control and International Security, U.S. State Department, “Strengthening Deterrence and Reducing Nuclear Risks: The Supplemental Low-Yield U.S. Submarine-Launched Warhead”, April 24, 2020, https://www.state.gov/wp-content/uploads/2020/04/T-Paper-Series-4-W76.pdf.

50. Elbridge Colby, “The Need for Limited Nuclear Options,” in Challenges in U.S. National Security Policy: A Festschrift Honoring Edward L. (Ted) Warner, ed. David Ochmanek & Michael Sulmeyer (RAND Corporation, 2014). Available at https://s3.amazonaws.com/-files.cnas.org/documents/The-Need-for-Limited-Nuclear-Options-Colby-Chapter1.pdf.

51. See, for instance, Li Bin, Tong Zhao, eds., Understanding Chinese Nuclear Thinking, Carnegie Endowment for International Peace, 2016, https://carnegieendowment.org/files/ChineseNuclearThinking_Final.pdf.

俄罗斯或中国的核心核力量。[52] 但大多数中国专家并不认为这样的推断特别令人信服。美国不断努力增强以常规、核力量以及弹道导弹防御系统、或许还有网络行动发动第一次打击的能力，使得中国观察人士对华盛顿所宣称的防御意图持怀疑态度。中国（和其他国家）的观察人士还指出，美国的言论和政策随着新政府的上台而频繁变化，使得人们很难理解美国的意图并相信它的保证。谨慎的规划者自然会觉得，他们必须对美国现有的和正在寻求的能力做最坏假设。即使美国接受相互保证毁灭（MAD）作为与中国战略稳定的基础，也很难让中国放心。中国观察人士强调，“MAD 本身（是）一种咄咄逼人的思维方式”，与防御性的“中国的核政策不符”，后者使得中国将“核能力维持在国家安全所需的最低水平”。[53]

在网络领域，中国指出，过分强调网络安全，特别是在军事领域，将阻碍信息和通信技术在社会经济发展中的应用。中国号召其他国家，不要“放弃努力”使“网络空间去军事化和去武器化”。[54] 用中国研究人士徐培喜的话来说，“我们制定规则正是因为我们希望网络空间不再成为一个战场。”[55] 一些资深中国专家对对讨论有关网络作战的军事条令持否定态度，他们指出在网络空间应用武装冲突法存在技术困难。他们认为，最基本的出发点应是在网络主权等核心问题上达成共识，否则有关网络军事透明度和理论的讨论对于维护两国网络稳定将毫无意义。他们还以赞赏的态度提及 2015 年 9 月奥巴马总统在一次演讲中的发言，即如果网络成为竞争领域，美国将做好获胜准备，但美国更愿意制定避免网络冲突的基本规则。[56] 显然，他们更希望美国能聚焦于制定规范以应对攻击性网络行动。

而另一方的美国主要专家则认为，中国宣称致力于建设完全和平、合作的网络空间，要么是幼稚、要么是“两面派”，或者两者兼而有之。他们认为，如果中国愿意和美国一起，承认其军事网络能力并解释其目的和理论，实现稳定的几率将得以提升。这样的做法可为有意义的对话奠定基础，探讨管理约瑟夫 • 奈所说的“合作性对手”应达成哪些有关责任和问责的原则，并进而商议如何应对可能影响 NC3 系统的潜在网络行动。本项目的美国参与者也承认，美国能够而且应该采取更多措施来澄清自己在这一领域的政策，并努力保持就这些政策进行沟通时的连贯性和一致性。

我们认为，中美两国必须找到恰当的官方途径，就三个主要议题进行对话。首先，双方可以就一

52. 美国国防部在《2019 年导弹防御评估》报告中乐，“美国导弹防御能力的规模，将依据有效保护美国本土免受流氓国家进攻性导弹威胁的需求而定。美国依赖于核威慑来应对大规模且更为复杂的俄、中洲际弹道导弹能力”。参见：Office of the Secretary of Defense, 2019 Missile Defense Review. 2019. Available at: https://www.defense.gov/Portals/1/Interactive/2018/11-2019-Missile-Defense-Review/The%202019%20MDR_Executive%20Summary.pdf.

53.Ministry of National Defense of the People's Republic of China. China's National Defense in the New Era. 2019, p. 9. Available at: http://eng.mod.gov.cn/news/2019-07/24/content_4846443.htm.

54.Xu Peixi, Nine Areas of Disputes in the Debate on International Cyber Norms, https://ceipfiles.s3.amazonaws.com/pdf/CI-ISS_Nine+Areas+of+Dispute+in+the+Debate+on+International+Cyber+Norms+-+full.pdf.

55.Xu Peixi, Nine Areas of Disputes in the Debate on International Cyber Norms, https://ceipfiles.s3.amazonaws.com/pdf/CI-ISS_Nine+Areas+of+Dispute+in+the+Debate+on+International+Cyber+Norms+-+full.pdf.

56.https://obamawhitehouse.archives.gov/the-press-office/2015/09/14/remarks-president-town-hall-fort-meade.

国认为或者两国均认为不稳定的措施、以及双方都认为有助于稳定的措施达成共识。例如，为了缓解中国的担忧，美国可以澄清，它确实承认自己无法成功摆脱在中国核报复面前的脆弱性，然后寻找具体的方法向中国保证，它确实计划依于这一认知行事。反过来，美国是否愿意限制其与中国的军事竞争，将在很大程度上取决于中国能否表明其理解下述观点，即战略稳定要求不使用武力或实际行动来改变领土现状或单方面界定陆地、海洋或空中边界。

为了减少因网络行动对 NC3 系统构成威胁而可能造成的焦虑和不稳定，双方还需要举行专家级别的会谈，更广泛地讨论相关问题。他们可能希望探讨的问题之一，是他们对 NC3 系统脆弱性的担忧，以及常规武器运载系统和核武器的指挥控制一体化是如何增加非有意升级风险、特别是源于网络攻击的风险的。预期专家们应当探讨的另一个问题是，核和常规设施之间的模糊界限、以及特定类型导弹防御系统的引入，会如何打破战略平衡。[57] 对此，双方也有可能希望讨论彼此所感受到的对方在核态势、核部署和核试验项目等方面的变化。[58]

除表达担忧之外，此类对话还可以探讨各方是否可以共同采取措施来降低这些风险。可能采取的措施涵盖从政策声明到建立有关演习和部署的信任措施、到最终限制各种进攻性和防御性系统的数量。

另一个在此可能讨论的领域是，中国的核武库和现代化建设总体缺乏透明度，这是美国的主要关切之一。中国可能不愿就这些问题进行对话，因为传统观点认为，保持模糊有助于抵消美国优势。然而，一些参与本项目的专家更接受另一种观点：能力较弱的一方如透明度低，可能会导致能力较强的一方在冲突中反应过度。就中国而言，它可以寻求提升美国在弹道导弹防御计划和能力方面的透明度。我们认为，在这些问题上的分歧本身可能是中美网络－核关系对话中的有益议题。

对话可以讨论的第二类议题，是进攻性网络行动、特别是在网络－核互动背景下的潜在利益和风险。该对话应作为一种进行战略分析而非交换政治指控的平台。在中国已公开承认其拥有军事网络能力（就本质而言该能力可用于攻击）的前提下，我们认为就交流设置先决条件是不明智的。通过对话，有利于彼此澄清哪些类别的克制措施对于战略稳定最重要。它可能包括双方如何看待网络行动，包括哪些行动将被视为升级，以及双方可能如何尝试发出愿意降级或后撤的信号。这有助于防止危机或冲突的无意升级。

---

57. James M. Acton, Is It a Nuke?: Pre-Launch Ambiguity and Inadvertent Escalation, Carnegie Endowment for International Peace, 2020, https://carnegieendowment.org/2020/04/09/is-it-nuke-pre-launch-ambiguity-and-inadvertent-escalation-pub-81446.

58. 鉴于中国依赖于有限核力量，美国发展和部署可有效、可靠地打击中国装备核弹头导弹的导弹防御系统，必然引进北京更大的担忧。然而，迄今为止美国所试验和部署的导弹防御并不具有可靠的有效性。与美国不同，依据报道，中国并未在和平时期将其陆基与空基核力量置于警戒状态以实现在数分钟内发射。中国海基核力量的运用战略目前尚不清楚。然而，随着中国开展部署使用战略核潜艇进行威慑巡逻，其将面临更大的压力，要求在巡逻潜艇上安装核弹头。这至少在技术上将缩短从决策发射核武器到实际发射之间的时间间隔。这也将使之前既有的 NC3 架构的复杂性进一步加剧。更多相关细节可参见：Tong Zhao, Managing the Sino-American Dispute over Missile Defense, August 11, https://warontherocks.com/2020/08/managing-the-sino-american-dispute-over-missile-defense/; Tong Zhao, China Wants More Nuclear-Armed Submarines. Should Everyone Be Worried?, October 22, 2018, https://carnegietsinghua.org/2018/10/22/china-wants-more-nuclear-armed-submarines.-should-everyone-be-worried-pub-77546.

最直接的是，中国可以在适当的双边平台中，就其网络及其他相关能力的内部流程与监管的性质加以说明。当然，我们也期望美国以积极姿态做出类似回应。中国还可以谈及那些被认为破坏稳定的活动（例如使用致盲激光），这些活动加剧了人们对其意图和组织的广泛担忧。

原则上，中美还可就和平时期某些类别信息的共享达成谅解甚至是明确的协议。例如，可共享符合共同利益的网络威胁情报。诚然，这种信息共享不会对网络－核关系产生直接影响，也不一定适用于直接对抗场景。然而，建立规范并促进其有效实施这一进程的存在本身，就有助于为应对双边网络－核挑战营造更具建设性的氛围。理想情况下，这种双边联络渠道还应提供一种可能，使双方可在特定情况下（危机期间）交换有关警报和相互保证的信息。

虽然中美两国参与本项目的研究人员在原则上都认可这种信息共享的潜在价值，但并不清楚可以交换何种信息，且怀疑在目前的政治环境下是否可行。尽管如此，他们均同意对目前双方计算机应急响应小组（CERTs）之间的渠道加以拓展，以共享更多可能产生战略后果的威胁信息。另一种选择是将当前中美综合对话框架内“执法及网络安全对话”（Law Enforcement and Cybersecurity Dialogue）的一部分加以功能化，使之成为实时响应机制。尽管将广泛的网络相关信息双边交流制度化和商定共同的克制准则存在固有困难，以及如前所述在如何建立互信方面存在长期分歧，该项目的所有参与者一致认为，中美两国应尽快就 NC3 系统面临的网络风险展开对话。其中一些对话可能与我们之前提议的对话重叠，即双方就网络威胁、网络稳定以及网络战略与政策的总体看法和关切进行沟通，但其中一部分应聚焦于 NC3 面临的风险与应对措施。通过对话，还有助于相互沟通各自为避免在无意中升级为核战争而制定实施的政策和做法，从而为解决彼此的关切开辟道路。

本项目的美国参与者从不同的政治和战略角度得出共同的看法，即这种对话是及时、必要和有价值的，有助于降低本报告所探讨的风险，并为中美危机管理铺平道路。他们还表示，这份非机密报告还可为讨论某些现阶段因过于敏感而使政府无法阐明的问题奠定基础。中国参与者基本同意这一建议，但也持一定保留态度，因为他们认为美国是更强大的一方，可能会从这些问题的对话中获得更大优势。美国专家了解这一担忧，尽管他们认为这缺乏依据。因此，这份报告的价值之一可以是找出两国政府官员可以商讨的问题，而不必把它们作为官方立场或关切提出。

如果中美两国均认为对话必要且可行，那么作为起步就应考察哪个平台最有利于展开此对话。现有的联络渠道可能适合于某些类别的信息交换，同时也可以建立新的机制来应对其他问题。下列平台值得考虑：

－现有的“外交安全对话”（Diplomatic and Security Dialogue）可作为双方高层官员沟通渠道，表达对彼此政策变化的关切以及分享各自能力或政策的重大进展。

-2014 年中国国防部和美国国防部签署的两份谅解备忘录（MOUs）为两军对话提供了可能平台，即“重大军事行动相互通报机制”和“海空相遇安全行为准则”。两国军方可以探讨，是否可将后

者扩展至网络行动基本行为准则。

- 另一项于 2017 年建立但于 2018 年中止的机制是双方 J5（战略、政策和规划）部门间的联合参谋对话。该机制第一次会议以危机管理为主要议题。如得以恢复，将可作为更详细讨论网络力量的能力和意图的平台，中层官员亦可在此对 NC3 系统面临的网络威胁表达各自的关切。

- 为在重大网络突发事件或网络危机期间进行沟通，已经在特定更高级别官员之间建立的联络渠道是最有用平台，可防止误解、协调应急响应措施或向对方告知可能针对重大网络攻击采取的应对措施。

- 两国计算机应急响应小组之间现有的协调机制可继续作为一般合作的主要渠道，并可加以扩大，以涵盖具有潜在战略后果威胁的信息。

- 中美国防部门之间的现有热线可以用于危机沟通。它似乎非常适用于沟通与 NC3 有关的网络问题。

需要考虑的一个问题是，如何确保外交协调的适当参与。一种可供选择的建议是，提前指定外交沟通渠道，在发生可疑攻击或第三方干扰时就攻击溯源进行交流，包括澄清中国 / 美国没有参与所怀疑的网络行动。

结束语

本报告是中美两国战略事务专家多年对话的成果，双方在此期间广泛探讨了他们认为可能将两国引向极不可取方向的互动态势。最初，他们并不确定能否在非政府机制下对这样一个微妙和敏感的议题进行有意义的探讨，更不用说双边讨论了。因此，开始时他们谨慎地探讨了两国政府是否有必要的知识储备和兴趣来支持像这样的非官方专家级别研究小组。在得到了两国政府将欢迎此类研究项目（但并未事先承诺赞同其研究成果）的保证后，双方专家一起拟订了该研究的主题、范畴，并就实施该项目的方式达成共识。

随着时间推移，与会者清楚地认识到，在两国内部和两国之间的网络与 NC3 互动确实带来了难以解决且极度严峻的挑战。本报告力求描述和解释这些挑战。对此的探讨颇为冗长，反映了参与者对 NC3 系统所面临网络威胁所做的相当严峻的评估，以及他们认为这些威胁（尚未）被广泛理解的基本看法。这些挑战的形成，源自两个高度专业化、秘密、相互分隔、持续演化的领域的相互交叉。这两个领域的人员之间很少进行严肃的系统性交流。此外，在相互竞争、某些领域甚至彼此冲突的背景下，中美两国在网络与核领域的操作者和政策制定者均做好了一旦有需要就针对对方展开行动的准备，这使得两国间形成相互谅解难上加难。我们希望，通过本报告第一部分的介绍，可以表明两国都迫切需要对网络与 NC3 的互动进行审慎、全面的审视，并为双方在不损害机密信息或过度破坏各领域间隔的前提下进行通用分析奠定基础。

报告第二部分讨论了中美可各自应对这些风险和挑战的方式，并希望双方可以就此合作。专家们已经指明，为什么此处所讨论的一些措施很难在双边层面实现（至少在开始阶段是如此）。双方对彼此意图的极度不信任，根深蒂固的以某些特定方式应对安全挑战的倾向，以及中美在网络和核领域的结构性不对称，共同导致了这一结果。美国主要关注与俄罗斯的竞争，也使中国对美国所构成威胁的看法更为复杂，同时限制了华盛顿缓解中国顾虑的能力。尽管如此，本项目的参与者依然认为，有多种方法可以开展有意义的合作，以应对核武器和网络武器相互交叉所固有的风险，特别是与双方极其敏感的 NC3 系统相关的风险。

本项目参与者认为，这项研究充分表明，中美在避免武装冲突及冲突升级为核冲突方面有足够大的共同利益，因此有可能彼此合作，以达成降低网络对 NC3 系统的威胁这一共同目标。他们认为，对双方而言最可行的开展方式是，首先进行内部考察、头脑风暴、建立模拟团队和开展桌面演习，并将相关情况通报两国最高领导人。这一进程本身可能立即产生效益，因为它有助于缓和中美之间在总体战略问题和特定 NC3 领域事务中的一些摩擦。

随之，双方可做好准备，在特定对话者之间谨慎开展双边对话。对话可建立在一个或者多个现有制度化双边对话渠道的基础上。其目的是：帮助双方更好地理解各自的关切、理念和政策，并建

设性地应对至少部分关切；如初步双边对话证明有益，且中美间更广泛的政治关系得以改善，那么双方还可就如何防止在网络－核领域采取最不利于稳定的行动设计一些自我限制和彼此限制的措施，并相互达成共识。

上海国際问题研究院
SHANGHAI INSTITUTES FOR INTERNATIONAL STUDIES

195-15 Tian Lin Road Xuhui Shanghai | 54614900 | www.siis.org.cn