威慑研究

# 构建网络时代的威慑稳定

## Deterrence Stability in the Cyber Age

爱德华·盖斯特博士 / 斯坦福大学国际安全与合作中心麦克阿瑟基金核安全研究员（Edward Geist, PhD, MacArthur Nuclear Security Fellow）

2015 年 3 月 19 日，美国网空司令部司令迈克尔·S·罗杰斯海军上将（Adm Michael S. Rogers）在参议院军事委员会作证时宣称，美国需要部署网空进攻能力。他抱怨白宫没有授权网空司令部部署进攻性手段，并对此表示担忧：“最终，纯粹的防御性、反应型战略，既跟不上需要，也极度耗费资源。”他的结论是：“我们需要思考如何提高进攻方面的能力，达到足以威慑的程度。”委员会许多成员呼应这位海军上将的观点。缅因州独立参议员安格斯·金（Angus King）附和说：“我强烈认为发展网攻能力极其重要，”他甚至搬出斯坦利·库布里克（Stanley Kubrick）1964 年的经典电影《奇爱博士》（Doctor Strangelove）来证明这一点：“如果你造出了这台世界末日机器，就必须让世人知道它就在你手中，否则，有这机器又有何用。”[1]

“微妙的恐惧平衡”——兰德公司战略家阿尔伯特·沃尔斯泰特（Albert Wohlstetter）为描述冷战核对峙所撰文章的标题——应该被引用到网空领域吗？“确保相互摧毁”看似一个简单而直觉的概念，但是沃尔斯泰特 1958 年的这篇文章，以此标题向那些把威慑看得轻而易举或者直截了当的人发出了永恒的警告。他告诫说：“世人对威慑稳定的乐观，几乎弥漫全球，要想驱散这种盲目乐观，也许第一步就是要认清，在我方的大量选择和苏联人的多种对策之间，充斥着我们极难分析清楚的种种不确定性和相互作用。”在他的眼中，战略威慑本身远不是所谓的理想终极目的，而是迫不得已必须面对的冷酷现实。虽说威慑构成了“防御政策的基石”，但沃尔斯泰特诚恳提醒说：“这只是一部分，而不是全部，”他并总结指出：“我们对战略威胁的强调已经过了头，战略威胁不可能取代许多它无法取代的东西。”[2]

ICBM = 洲际弹道导弹

继沃尔斯泰特的文章发表之后，美国的防务分析专家们研制出一系列愈加复杂的工具来测量微妙的恐惧平衡。这些演示超级大国之间的核交战可能会如何展开的模型，转而又为威慑稳定研究提供了基础支撑。通过部署即使在遭受精心策划的先发打击之后仍有能力进行毁灭性报复的核力量，美国和苏联都受到威慑，而不敢贸然发动核战争。

这种冷战时代以威慑求稳定的范式，能够适用于网战这个新领域吗？无论前景如何诱人，技术和操作的现实都使它极难实现。尤其是，因为信息的质量问题，类似冷战时代用于评估超级大国之间威慑稳定的战略交换模型，在网络时代也难以开发出来。网空领域和其它领域不同，它与地理空间没有紧密相连，所以建模极度困难，原来明确无误的概念区分，例如“核军事毁伤”（counterforce）目标和“核民事毁伤”（countervalue）目标之间的区分，在这样的建模中变得混沌不清。

* Translated and reprinted with permission from USAF *Strategic Studies Quarterly*, Winter 2015, Vol. 9, No. 4.

这些障碍，既对美国构建可信的网空“确保反应”机制造成严重困难，也对那些企图对美国利益进行网络攻击的潜在敌人带来巨大挑战。虽然缺少这样的建模能力，无法有效模拟网络攻击的效果，美国如能施行合适的政策，保持合适的能力，也可以迫使理性的对手放弃攻击美国的企图，让他们知道发动这样的攻击得不偿失，反而会招致美国毁灭性的报复。因此，为针对网空威胁建立最大程度有效的威慑机制，美国应该为潜在对手制造最大程度的困难。

为达此目的，美国需要建构一套立足技术的全面网空战略，此技术战略必须注重满足几个目标，包括韧存性（尽可能减少敌人网攻得逞而可能造成的破坏）、拒止能力（尽可能降低敌人网攻得逞的几率），和进攻能力。这种战略，如果强大到足以抗衡最老练的国家级对手，那么它也会比威慑战略更加有效地对付那些不会理性计算得失而不可理喻劝阻的非国家行为者。虽然理想情况下，这个框架将覆盖美国政府实体和民间财产两个方面，但其高昂的前期成本，可能会限制联邦政府对执行美国军事行动和保护必要民间基础设施的关键性系统进行初始投资。然而，民营界应该受到鼓励运用类似技术提高其资产的韧存性。在冷战时期，战略核武器的性质使“拒止性威慑”成了无法实现的梦想，相比之下，在网空，美国可以利用技术施行诈敌策略，使潜在对手看到的攻击表面变幻莫测，从而削弱其攻击信心，而达到慑阻目的。

## 运筹研究和网空领域

“运筹分析”是响应新兴技术而兴起的一门独特学科，出现在第二次世界大战期间，当时新技术不断涌现，给军方带来史无前例的担忧，一如当前新兴的网络能力为军方带来的同样担忧。兰德公司分析家 E.S. 奎德（E.S.Quade）指出：“这种运筹分析的主要推动力是新武器系统的问世，这些武器所立足的技术和以往军事战争经验无关，需要具备新技术知识才能操作。”运筹分析最初主要是针对战术问题，比如，如何最好地利用或干扰像雷达这类新技术；到了战后的年月，逐步演变为“系统分析”，研究专家藉此来评估更加长期的武器研发项目以及其所带来的更高程度的不确定性。在 1950 年代期间，武器系统分析专家们，尤其在兰德公司，开始拓展视野，研究战略和国防政策等影响深远的问题。[3]

核武器在冷战早期的出现，为防务分析家们造成最困惑的新障碍。技术形势急剧演进，各种新技术领域，诸如数字计算，不断把新技术从实验室的设计迅速转变成武器硬件的关键组成部分。而且，对共产主义对手技术能力的最初的不屑一顾，也迅速证明是幼稚的。我们曾经充满信心地预测，苏联需要最少十年或更长才能研发出自己的核武器，这种预测被苏联 1949 年的第一次核试验一举击碎。在 1953 年，苏联成功试验了一枚可运载发射的初级热核武器，甚至领先美国好几个月。苏联积极追求弹道导弹技术，几年之后取得了惊人的回报，在 1957 年 10 月，苏联率先使用 R-7 洲际弹道导弹（ICBM）发射了第一颗人造地球卫星“斯普特尼克”。苏联宣传机器夸耀说：他们的人造月亮证明，苏联政府兑现了布尔什维克“给生活带来神话”的承诺，而在美国，公众恐慌弥漫，人们普遍认为美国正失去技术优势——并可能连带输掉这场冷战。[4]

兰德公司以及其他防务分析家们以美国的智力潜能为武器，来对抗共产主义威胁。他们运用——或者说，在许多情况下构想

出——最新的数学和技术创新，得以管束住超级大国冲突中的问题。系统分析家们不仅把最初为经济和工业管理设计的工具加以改造，用于研究战争和防务问题，还不断启用新方法，诸如蒙特卡洛模拟、线性规划、原始数字计算机等，来“作异想天开之思”——借用未来学家赫尔曼·卡恩（Herman Kahn）的话。[5]

这些智力潮流汇集成一种被称作“造型术”或“建模”的新艺术，此后这种艺术又被用作许多战略思想的基础，常常是意会的基础。“确保摧毁”这类概念依赖的是一种假定，即，我们能够精确模拟核交战的过程，精确到足可预测，只要报复力量足够强大，就能顶住对方精心策划的先发打击而存活。对“多少才算足够”这个一直争论不休的问题，整个战略界的各种人物都利用模型来为自己的回答辩护。到了最后，一整套“威慑稳定”学科都围绕着这类分析生长出来。

“威慑稳定”概念的出现源于 1950 年代后期和 1960 年代早期对于“相互”或“最低”威慑”之价值的讨论。艾森豪威尔政府宣布的“大规模报复”政策认为，美国需要保持压倒苏联的绝对战略优势，才能对其构成可信的威慑性胁迫；相比之下，相互或最低威慑的倡导者则认为：有限的力量，只要可以存活下来，就能劝阻苏联放弃侵略。但这种最低威慑框架，虽然不再要求集结 1950 年代那种规模的军备，并没有明确指出需要多大的报复力量才能有效威慑克里姆林宫。兰德公司的丹尼尔·埃尔斯伯格（Daniel Ellsberg）1960 年发表了一篇题为“战略选择的粗略分析”的颇具影响力的论文，为沃尔斯泰特的威慑概念勾勒出一个明确的格式。埃尔斯伯格的模型通过预测美国和苏联的“首发打击”及“二次打击”战略的“报偿”，旨在帮助阐明美国的哪些政策选择可劝阻苏联放弃首发打击的企图。他指出：“当然了，军事‘态势’、政策，或计划的变化，使得这些［估计的］精确效果难以确定，增加变数，且容易引发争议，”但是“我们仍常可做出粗略的估计，事实上，在选择军事方案时，它们是大多数政策建议的基础。”[6]

埃尔斯伯格的模型为针对威慑稳定进行战略态势分析提供了基础。那个人们孜孜以求的、以多大兵力就足能威慑克里姆林宫的答案，很快在决策者们中取得了共识。尼克松总统在 1971 年宣布：“我们的政策继续是……保持战略充足性，”他将战略充足性定义为“维持我们及盟国无惧胁迫的足够兵力。”进一步，“稳定……也意味着，我方兵力的数量、特征和部署，不会让苏联合理地解释为意图对他们实施瘫痪性攻击。”[7] 然而，究竟需要付出多大代价才能达成这些目的？要想精确预测，事实上困难重重。在 1970 和 1980 年代，大量笔墨倾注于应该如何分析、建模和评估威慑稳定。尽管大家对于威慑稳定框架的总体假设有普遍共识，大致涵盖从最低威慑到兵戎相见的整个战略观念频谱，但随之而来的是喧嚷不休的争论——诸如超级大国的核平衡应如何模拟，我方需要贮备多少枚武器才能镇住苏联的胁迫而又不显出攻击性威胁。[8]

人们为衡量超级大国之间的核恐惧平衡，尝试了各种方法，但假定的核武器和投送系统的特征提供了一些共同参考点。尤其是，几乎所有模型都从空间方面分析了投送系统性能和目标生存能力的问题。而且，侦察卫星照片和其他情报数据使得我们有可能估计敌方轰炸机和导弹的数量和大概特征。美国的防务分析专家们就苏联 ICBM 弹头的确切当量和精确度这类问题爆发了激烈争论，但

这些数值的不确定性也都在一个数量级范围内，其中许多对模型输出信息没多大影响。从“百万吨级当量”的度量（即，理论上计算出超级大国核武器产生冲击波超压所覆盖的总面积，把核武器总破坏能力线性化），到更复杂的“核军事毁伤潜能”（即，结合精确度来估计一个核武库对 ICBM 发射井这类坚固目标实施破坏的总体能力），到全面的战略对攻模型（即，用以估计在经受先发打击之后能有多少枚武器可生存下来进行报复打击），分析家们大都认为，核战争其实可简化到以半径和面积来测量。

除了上述共同点之外，战略核力量模型呈现出各种令人眼花缭乱的形式，不过其中有一种，即“充足性模型”，对关于威慑稳定的公开讨论起到了特别大的推动作用。如约翰·巴特勒格和朱迪思·K·格兰奇（John A. Battilega and Judith K. Grange）在 1978 年所言：“战略核力量催生出一类特殊的模型，用以粗略地评定美国战略核力量态势的绝对和相对充足性，而且反过来也可评定外国核力量态势的份量”。这种模型通常归于“静态或准动态有效性衡量”的范畴，其“主要用途”是“为战略均势、威慑、稳定这类概念的讨论提供一个载体。”这两位作者指出：“这类模型的作用随着与核力量的联系发生了独特的演变。”驱动这种演变的因素包括：“对美国战略威慑所达目标的界定（用跟外国对手相对比较的方式）……，动员公众辩论（但用半技术性语言）美国重大核武器计划的需要，……[ 以及 ] 从美国威慑、战略、兵力规模的主要选项加以思考（以能够被人理解但不涉及与核战争有关的历史经验的方式）的需要。”麻烦的是，这种普遍化有时会导致这些模型被用于不一定合适它们的目的，如作者所言：“这些模型有时被用作兵力规划或兵力相互作用有效性的主要或次要衡量标准……但是，应该记住，如此使用的原因，是源于它们作为充足性模型的历史进化。”[9]

虽然威慑稳定和战略充足性的概念对冷战后期的政策辩论有所帮助，但到 1990 年代时，它们的局限性就逐渐暴露出来。从埃尔斯伯格最初框架产生的越来越精细的衍生品，加剧了他在 1961 年就承认的缺陷：需要为各种变量赋值却又无法在现实世界中找到证明此需要的理由。[10] 而且，威慑稳定和战略充足性概念很难转用到冷战后的多极地缘政治格局。在南亚，印度和巴基斯坦作为新拥核国的兴起，提供了一个不符合战略稳定精致数学模型的紧迫现实反例。与冷战时期对峙的两个超级大国不同（双方都害怕对方发动先制核打击），新德里和伊斯兰堡都设想，两国争议边界上的完全能想象得到的常规兵力对抗将引发核冲突。还有另一个早已存在的拥核国中国，使该地区的战略形势更为复杂。行为者的多样化，加上可能出现的各种局面，都使得对这个地区的威慑稳定进行建模极为困难。[11] 这种建模方法在核领域的局限性表明，在把这些方法引入像网战这种新兴竞技场之前，我们应该三思。

## 制作网战模型: 错误但有用

无论是好是坏，我们都无法建造精确估计网空领域威慑稳定的充足性模型，因为网空和常规领域有天壤之别。网空无法以英尺或英里来测量，网战武器的有效性也无法用简单的破坏半径来衡量。网战武器及其潜在目标都没有核武器在冷战期间经历的那种可以预测的演变。定性地说，像 ICBM 这种新武器是在预先警示多年之后才出现，并且通常还在此后好几年时间才真正可投用于实战。进一步，虽然投送系统越来越精准，坚

固目标的生存能力也略有增强，但核武器的毁灭效果保持不变，即使对它们的科学认识一直有不规则的变化。相比之下，令人吃惊的新式网战武器，挟带着前所未见的效果，可能一夜之间就突然冒出来；或者是，一个及时的补丁程序或升级，就可能使精心策划的网络攻击无能为力。网络空间与物理空间的毫无牵连，也使人很难分清核威慑模型中所谓的核军事毁伤目标与核民事毁伤目标之间的区别，也难以限制附带损伤。如“震网”（Stuxnet）病毒案例戏剧般证明的那样，研发一个强大的网战武器，要想不波及计划打击目标之外的其他系统，可能非常困难。鉴于这种种不确定性，的确难以想像如何建造出一个类似的网战模型，能像冷战模型预测超级大国相对核力量那样发挥作用。

但这不是说不可能建造一个网战的综合模型，这种模型可以也应该被建造，不过，网空的定性特征和牵涉到的不确定性，使它们无法提供我们做战略稳定性评估时不可缺少的那种带有信心的预测。正如著名的英国统计学家乔治·伯克斯（George E. P. Box）说过的一句名言：“本质上，所有模型都是错误的，但有些是有用的。”[12] 建造网空冲突模型要克服哪些挑战？这些模型能合理地服务哪些目的？

不幸的是，网战模型要求比冷战核战略模型远更复杂精细才能发挥作用。大部分核冲突模型，比如阿森纳交换模型亦即核交战模型（Arsenal Exchange Model），是以两维或三维空间中的交叉概率分布来估计攻击效果。[13] 使用圆形覆盖函数，对投送工具精确度和目标坚固性加以估算，就能方便地生成目标可被摧毁的概率估计。这种运算使用一根计算尺就能进行，在冷战的早些年，通常就是这么做的。用来评估战略稳定性的模型通常完全忽略时间因素。相比之下，网络攻击的效果只有通过依赖关系图的使用才能模拟出来。计算机和网络是网络攻击的明确目标，因为它们是（或者被认为是）连接着攻击者希望干扰、操纵或破坏的某些类型的资源或活动。在数学上，这种系统可以被当作有向图，图中的各条边线代表网络各不同部分之间的相互影响。由于这些影响在时间上只能向前进，所以该系统应该被看作定向非环图，网络中的每个节点用图中表示系统演变每一瞬间的不同位置来代表。此外，这每个节点都有可能根据其内在状态起不同反应。显然，这不是用一根计算尺就能轻易解决的那种问题！[14]

有幸的是，有多种计算方式可以用于建造显示系统对网络攻击反应的模型。只要系统不是过于庞大，就应该可以使用面向对象编程直观地模拟这种依赖关系图。事实上，第一个面向对象的编程语言（即 Simula 语言），就是在 1960 年代为了模拟目的而发明的。一个面向对象的网战模型，其建模者想让它有多精细就可能有多精细，而且只要计算资源允许，想要多大规模就可能有多大规模。这就便于使用这种模型来调研网络攻击、动能攻击和核攻击之间可能的相互作用。虽然有这些吸引人之处，但面向对象的方法很可能需要大量分析师的人力来建造，它也不是唯一可能模拟网战的方法。比如，有限元分析，也许可以加以调整用来模拟某些类型的网络攻击。[15]

网战模型不仅相对更加复杂，而且很可能对用于建模的信息极度敏感。依赖关系图的结构及其节点根据其状态对特殊刺激的反应，很可能导致输出结果出现定性上的巨大差别。核攻击中，一枚核弹爆炸同时摧毁几十个离散目标的可能性极小，与其相比，在

网空领域，瞄准了要害节点的攻击有可能造成该节点及其所有依赖关系顿时瘫痪。然而，任何特定节点的依赖关系——以及它的脆弱部——都极难预先判定。如果没有关于这两个因素的高质量信息，网战模型就不可能具备预测价值。

那么，这些模型能服务什么目的呢？以上特点使网战模型对战区战役的作战规划有潜在用处；但是对制定战略层次上的更广泛的政治 - 军事政策是否同样有用，则不得而知。在战役层次，网战模型即使是建立在纯概念的基础上，也可能有助于研究目的。比如，可以建造这样一种模型，专门用于探索网战与核战或动能打击相结合的多域作战的可能动态演变。通过提供一个具体的框架，用来调查关于这些相互作用如何展开的各种假设，这些模拟能够提供宝贵的启示——即使它们无法预测任何具体作战行动的成败。从中获取的经验教训，可以用来减少美国及其战略伙伴的网络漏洞。借助关于目标系统的充足信息，这种模型也能被用于作战规划，尽管建造模型需要相当大的努力，而且侦察数据的有效期可能有限，这些因素都对建模构成巨大的挑战。

然而网战模型对于战略评估的用处，充其量是靠不住，很可能是有害无益。模型对研究核威慑稳定有用的那些分析类型，转换到网空领域就不太管用。如果有一个类似核战确保摧毁模型的网战版本，决策者绝不敢指望它，因为网战战略模型的建造中实在包含太大的不确定性。此外，实施这样一种模型需要的数据收集，本身就充满了危险性，因为它将需要对美国所有的网络漏洞进行全面评估。假如这个评估，或者甚至只是其中的一小部分，落入敌人之手，其对美国安全的破坏就可能难以估量。

## 网战确保摧毁的不可信性和不可取性

网空进攻战策划中的内在不确定性并没有阻止某些分析家，他们坚持认为，在网空，“进攻是最好的防御”这条陈旧的格言比以往任何时候都适用。富兰克·西卢夫、莎伦·卡达西和乔治·萨尔莫伊拉吉（Frank J Cilluffo, Sharon L. Cardash and George C. Salmoiraghi）在 2012 年的一篇合著文章表示：“尽管美国必须证明它的工具箱里包含只要需要就能拿出来对付敌人的所有必备武器，但迄今为止还没有公开明确的迹象证明，美国已经确凿无疑地取得了网空优势并在积极地争取对其全部掌控。在这种背景下，美国应该考虑进行相当于地面核试验的数字攻击试验吗？”这几位作者声称，这种令人瞩目的手段“不会被草率地摒弃……[因为]只要处理得当（发挥与演习规模相称的巨大影响），也许有助于威慑敌对行为者。”[16]

眼下普遍的倾向是沿循冷战时期为描述超级大国核对峙特征而设计的框架，但把网络安全问题也如此概念化的倾向实在不着边际，因为，冷战核战略家们从来就把那些预示世界末日的种种可能性视为不受欢迎的东西。美苏两国的科学家们都耗费了九牛二虎之力，企图研发出可信的防卫核攻击能力，但都在不可逾越的技术障碍面前败下阵来。于是迫不得已，退而选择以威慑求安全，于是美苏两国领导人不得不彼此拥抱。

在核领域中，威慑因其特征而成为一个次中求好的选项——网络攻击也具有类似的特征吗？有些官方评估就做出这样的结论。国防科学委员会在 2012 年曾说：“网空威胁是严重的，其潜在后果在某些方面类似于冷战的核威胁。”委员会认为，“当前网络攻击”的特征是“能够造成足以使政府失去对国家

控制的大规模破坏，”它断言，有些对手有这样的能力并可能得逞，如果他们“投入大量资金（几十亿）和时间（数年）的话，就真正可能在我们的系统——包括那些原本防御坚固的系统——中制造出漏洞。”幸亏“这种能力如今仅限于几个国家，比如美国、中国，和俄罗斯。”委员会声称，“由于不可能万无一失地保护我们的系统免遭［这种］威胁，威慑必须是降低风险总体策略中的一个要素。”[17]

然而，也有些同样权威的评论和报告对当前网络攻击的可能性和后果提出不同的看法。国家情报总监詹姆斯·克莱佩（James Clapper）2015 年 2 月 26 日向参议院武装部队委员会报告说，虽然“美国国家安全与经济安全面临的网空威慑在频率、规模、技术含量、影响严重性等方面都在上升……，但是，还谈不上具体有谁能对美国发起灾难性的攻击，这样的可能性目前还微乎其微。”克莱佩表示：“我们也在前瞻未来，不过绝对看不到那种瘫痪整个美国基础设施的‘网络末日’。”克莱佩所预见的，不是由俄罗斯或中国策动的一场数字大灾变，而是“随着时间的推移，一系列持续不断的、来自多方面的、低级到中级程度的网络袭击，可对美国经济的竞争力和国家安全增添累计成本。”[18] 如果在可见的未来并无大灾变之忧，那么，还有必要追求确保摧毁的网战能力吗？

无论如何，即便敌人图谋发动重大网络攻击，也难以克服上述的建模挑战。任何网络攻击图谋者，若想导致美国政府失去对国家某部分的控制，几乎肯定需要对多重系统同时发起技术复杂的攻击，很可能是配合针对关键目标的火力打击。然而，策划如此复杂的攻击首先需要整合大量的可靠情报，情报收集将困难重重，建模演绎战局变化更是谈何容易，对手如何对其攻击成功几率建立足够信心？以此看来，大概只有极度绝望或极度鲁莽的对手——亦即那些无惧威慑、不可理喻的亡命之徒——才敢如此铤而走险。因此，美国一位最有经验的建模专家保尔·K·戴维斯（Paul K. Davis）的见解并不令人意外，他在兰德公司的一份工作文件中说：“威慑本身是战略思维的脆弱基础。”他认为：“从目前的现实来看，指望威慑却敌就好比抓救命稻草。威慑手段必须是战略的一部分，但战略的焦点应落在别处。”[19]

## 网空战略以技术却敌

如果基于确保摧毁的威慑不可作为美国网空战略的核心，那什么是核心？幸运的是，我们在模拟网空进攻作战有效性的艰辛努力中所碰到的根本性障碍，同样也困扰着我们的潜在对手。美国可以高瞻远瞩，开发出另一种战略，这就是从技术上尽量强化潜在攻击者面对的这些障碍，率先阻止其发动网络攻击。我们可以双管齐下，一方面提高美国系统的韧存性，另一方面采取各种措施阻止和迷惑敌人收集情报的努力，使这些国家和非国家对手失去信心，迫使他们放弃这种疯狂网络攻击的图谋。

早在 1970 年，斯蒂芬·T·波索尼和 J.E. 普耐尔（Stefan T. Possony and J.E. Pournelle）就提出担忧：苏联没有仿效美国，他们追求的是“技术战略”，有可能不费一枪一弹就能赢得超级大国之间的竞争。尽管苏联的经济和技术处于劣势，但它有能力把较有限资源中的较大份额集中用于军事研发，并且寻找机会直接盗窃西方技术，凭此作为，克里姆林宫可能建设出一支更优越的兵力——尤其是如果美国仍然自满自得的话。波索尼和普耐尔把“技术战”界定为“直接地、

目的明确地运用国家技术基础和由此基础产生的具体进步，来达到战略和战术目的。”他们宣称：“真正的技术战争，在于把任何火力形式的使用降到最低程度。”[20] 他们强调：“和所有战争一样，技术战争也需要一个深思熟虑的战略，”因此建议说，这种战略的目的应该是“使敌人对抗你的每一步行动，并被你牵着鼻子走。”[21] 美国应该采取这种“技术战略”，来对付二十一世纪的网空威胁。这种战略应该包含三个基本要点。第一，“提高韧存，防卫自身”，即通过提高抵抗敌人打击的能力而保护美国关键性基础设施。第二，“加强拒止，劝阻敌人”，即通过增加潜在对手的情报收集与分析难度，把他们对美国网络资产实施攻击的计划极度复杂化。第三，“建设网攻，实力慑阻”，但决不可将此步骤作为单独的威慑手段，因为如果对手也采取上述类似步骤的话，此等威慑就难以信赖。相反，建设全面网攻能力是为服务两个目的。其一，美国必须牢固掌握“最先进”的网空进攻技术，藉以确定韧存能力和拒止能力中的必要手段。其二，我们需要具备网攻能力来配合美国的常规、太空和核行动防御计划。

为了提高我们自身以及民用网络系统的韧存性，军方应与民间企业联手，通过长期合作，减少易被敌对网络攻击利用的漏洞。想排除所有漏洞固然不可能，但毕竟可以减少潜在对手攻击的目标选择，从而有助于加强美国安全。我们有充分的理由相信，安全软件和硬件研制所遇到的困难，在根源上主要是体制和文化上的障碍，而不是技术性障碍。我们的许多较陈旧的代码库是建立在过去的时代，当时根本不可能想象到眼下出现的这些安全挑战；传统的软件开发惯例，更多着眼于控制成本和如期完成任务，而不是强调关注安全。起初，国防部虽然拨款资助方法研究，以证明开始于 1960 年代的程序的正确性，但其之所为对美国防务部门或民营界开发自身系统的方式几乎没有影响，部分是因为这种研究需要几十年时间才会出成果。研究人员原来希望开发某种技术，能够适用于用现有编程语言编写的软件，却发现，要想证明用 FORTRAN 这类语言编写的即使是最一般程序的正确性，也难如登天。事实表明，要想编制出能证明正确的软件程序，将需要以另一种模式进行编程和硬件工程。学术研究人员在 1970 年代着手开发这种技术，几十年来虽在理论和实施上缓慢演进，却仍未达到可实用的程度。并且，一直到最近之前，我们很少需要安全系统和安全软件。虽然军方为了某些应用而寻求这些技术，但民间不情愿为看似完全多余的功能付出额外的成本。既然防务市场基本排外，既然成本控制问题无所不在，广大民营界自然缺少热情来生产价格可负担的安全系统和软件，或是开发这种生产所需的人力资源和技术。幸运的是，有充分理由相信这些障碍可以被克服。

由于意识到当前的方法不能充分满足美军的未来需要，国防高级研究计划局在 2012 启动了一个项目，旨在依据像定理证明这种形式化方法来开拓性地创造硬件和软件的安全结合。这个项目被称为“高可靠性网络军事系统，”其目的是“开创构建高可靠性物理网络系统的技术，高可靠性的定义是指功能上正确且能满足合适的安全与安保性能。”[22] 作为示范，该局研发了一个遥控四轴无人飞行器，其安全程度如此之高，以至于组成“红队”的黑客耗费了六周时间研究完整的源代码之后，也未能找到任何漏洞。[23] 这个绝技显示，充分安全的软硬件不一定是白日梦想，但是需要沿循另一个非常不同于常规的开发

过程。要想使这种技术得到普遍采用，即使仅出于防务目的，也将需要建立一整套全新的系统开发文化，包括用截然不同的思维方式培训大批程序员和工程师。这个转变过程将艰难而昂贵，但是可能是保护美国资产免遭日益复杂的网络攻击的唯一途径。

民营界现在也越来越注重运用正规方法减少网络漏洞风险。技术产业面临着针对商业利益的网络攻击所引发的严峻经济赔偿责任，投入了越来越多的资源，从质量上改善软件工程技术，从而大大减少了这种漏洞的发生率。比如，莫兹拉基金会（Mozilla Foundation）就积极开发出了 Rust，这个系统编程语言的目的是把程序员从经常给软件带来严重安全漏洞的人工记忆管理中解脱出来。[24] 另一种有前途的方法是使用像 Haskell 这种功能性编程语言，其特点在于迫使软件按照严格的数学形式编写，而保障建立起确保正确行为的非常规程序。这类功能性编程虽然与大多数程序员熟悉的命令式编程非常不同，但吸引了安全研究人员越来越多的关注，因为它编排的软件可望大幅度减少安全漏洞数量。[25] 国土安全部正在进行一些项目，旨在鼓励更加安全的软件开发做法，而国防部——凭借其广泛的购买力——可以帮助加速这些技术的开发和采用，并更换漏洞频现的陈旧代码。[26]

硬件的弱点和漏洞常常是由类似的遗留问题和工程疏忽所导致，其之弥补有时更具挑战性。美国的民用网络基础设施，是在目前这类司空见惯的安全威胁出现之前，从最原始的设计技术上逐步发展起来的。几十年之后的今天，基础网络中遗留下来的陈旧技术，成为敌人注目和利用的各种漏洞，美国的许多系统可能因此被攻陷。要过渡到本质上更安全的技术，其过程不仅漫长而且具有高度扰乱性，可能需要从根本上重新构建互联网的技术基础概念，但从长远看，也许是保护美国利益的必要之举。因此，国防部应该资助这些努力，开发出本质上更加安全的网络硬件供自己使用，并且鼓励民营界做出类似的努力，不仅保护支持军事行动的民用系统，从根本上说，也是保护整个美国。

为了阻止潜在对手轻易进入关键性系统，美国可以布设假情报和噪音迷雾，来掩蔽有关已知或可疑漏洞的准确信息。对那些特别被关注的系统，如军事指挥控制系统和民用电网，不妨制造大量模仿其网空印迹的诱饵阵，虽说不见得总是有效，但亦无坏处。这些伪装系统，如果设计巧妙，可以做到非常逼真，足可迷惑潜在网络攻击者，使他们以为已经潜入了目标——同时为这些对手灌输精心准备的假信息，或者诱骗他们远离真实漏洞，或者纵容他们犯错而暴露自己的身份和意图。[27] 黑客面对众多诱饵阵，就不得不费力辨别真假，从而大大增加他们为发动复杂网络攻击所必需执行的技术侦察的难度。美国还可以通过采取技术措施，提高“真实”攻击表面的变化速率，是以加强此策略的效果。若用这种方式隐蔽所有系统，耗资将过于庞大，也会排挤掉合法的网络流量；但是，防务界可与民营界建立伙伴关系，共同建造必要的技术基础，因为民营界也有昂贵资产需要保护。

最后，鉴于潜在对手越来越多地使用信息技术，美国应该发展网空进攻能力，来配合其他领域的军事行动，并找到和弥补美国的漏洞。在未来的冲突中，我方如果能够利用敌人的网络漏洞来破坏其设施，就可以在战胜敌人的同时有效减少生命和财产损失。进一步，如果不具备与潜在对手相当的最先进网空进攻能力，那么挑战我们自己系统的

红队也就无法将自身质量提升到可接受的水平。虽然美国应发展网攻能力，但不可以威慑为核心目的来发展。因为网络空间的特定性质，对危机的升级控制构成一些无法逾越的障碍。如果没有可靠的模型来评估不同国家的网空进攻能力和互相之间的相对实力，如果无法预测网络攻击的效果，那么威慑稳定的概念在网空就没有意义。★

## 注释：

1. Ellen Nakashima,“Cyber Chief: Efforts to Deter Attacks against the U.S. Are Not Working”[ 网络首席官：威慑努力效果不彰，未能遏止针对美国的网络攻击 ], Washington Post, 19 March 2015, http://www.washingtonpost.com/world/national-security/head-of-cyber-command-us-may-need-to-boost-offensive-cyber-powers/2015/03/19/1ad79a34-ce4e-11e4-a2a7-9517a3a70506_story.html.
2. Albert Wohlstetter, The Delicate Balance of Terror [ 微妙的恐惧平衡 ], (Santa Monica, CA: RAND, 1958), http://www.rand.org/about/history/wohlstetter/P1472/P1472.html.
3. E. S. Quade, Systems Analysis and Policy Planning: Applications in Defense [ 系统分析与政策规划在国防中的应用 ], 参看“引言”部分 , (New York: Elsevier, 1968), 2-3.
4. 关于“斯普特尼克”卫星发射之后引发的“导弹差距”恐慌，参看 Peter J. Roman, Eisenhower and the Missile Gap [ 艾森豪威尔与导弹差距 ], (Ithaca, NY: Cornell University Press, 1995).
5. 关于兰德公司的早期历史，参看 Bruce L. R. Smith, The RAND Corporation: Case Study of a Nonprofit Advisory Corporation [ 兰德公司：一家非营利性咨询公司的案例研究 ], (Cambridge, MA: Harvard University Press, 1966). 关于兰德公司在冷战早期的核战争研究，参看 Fred Kaplan, The Wizards of Armageddon [ 世界末日的巫师们 ], (Stanford, CA: Stanford University Press, 1983).
6. Daniel Ellsberg, The Crude Analysis of Strategic Choices [ 战略选择的粗略分析 ], (Santa Monica, CA: RAND, 1960). Ellsberg 这份兰德报告的缩略版以“战略选择的粗略分析”为名刊登在 American Economic Review 51, no. 2 (May 1961): 472-78.
7. Richard M. Nixon, Public Papers of the Presidents of the United States, Richard Nixon: Containing the Public Messages, Speeches, and Statements of the President 1971 [ 美国总统尼克松的公开文件：包括总统 1971 年的公开信息、演讲和声明 ], Washington, DC: Government Printing Office, 1972), 310.
8. 尽管这两位军备控制的拥护者都曾利用 Ellsberg 的框架支持自己的论点，但到 1970 年代早期，就出现了对其基本假设的攻击。例子请见 Douglas E. Hunter,“Some Aspects of a Decision-Making Model in Nuclear Deterrence Theory”[ 核威慑理论中一个决策制定模型的某些方面 ], Journal of Peace Research 9, no. 3 (1972): 209-22.
9. John A. Battilega and Judith K. Grange, eds., The Military Applications of Modeling [ 建模的军事应用 ], (Wright-Patterson AFB, OH: Air Force Institute of Technology Press, 1981), 245-46.
10. 有关这一精辟论述的一个重要例子是 Glenn Kent 和 David Thaler 研发的首发打击稳定性模型。 Glenn A. Kent and David A. Thaler, First-Strike Stability: A Methodology for Evaluating Strategic Forces [ 首发打击稳定性：评估战略力量的方法 ], (Santa Monica, CA: RAND, 1989). 有关 Kent/Thaler 模型的评论 , 参看 Stephen J. Cimbala and James Scouras, A New Nuclear Century: Strategic Stability and Arms Control [ 一个新的核世纪：战略稳定与军备控制 ], (Westport, CT: Praeger, 2002), 1-23.
11. 对这个主题的最新评估，参看 Michael Krepon and Julia Thompson, eds., Deterrence Stability and Escalation Control in South Asia [ 南亚的威慑稳定和升级控制论文集 ], (Washington, DC: Stimson Center, 2013).
12. G. E. P. Box and N. R. Draper, Empirical Model-Building and Response Surfaces [ 经验性建模和响应面 ], (New York: John Wiley and Sons, 1987), 424.
13. 同注释 9，第 283-289 页。
14. 同注释 9，第 381-400 页。具有这些特征的模型是在冷战期间设计的，是以评估美国指挥、控制和通信（C3）系统的生存力。历史上的例子包括：最小基本应急通讯网络（MEECN）和战略司令部，由美国空军用来评估通往战略轰炸部队的 C3 链接。

15. 有限元分析在工程学方面普遍用来分析复杂的问题。它的工作原理是把一个偏微分方程（PDE）的复杂系统，细分为能够被偏微分方程的简单子集概略估算的更小的子域。有限元分析在科学和工程学方面的某些应用表明，它也许是模拟某类网络袭击的有效方法。比如，模拟传染病传播技术的使用，可能类似于恶意软件在异机种系统中的传播。例子见 Joshua P. Keller, Luca Gerardo-Giorda, and Alessandro Veneziani, "Numerical Simulation of a Susceptible-Exposed-Infectious Space-Continuous Model for the Spread of Rabies in Raccoons across a Realistic Landscape"[ 表现浣熊狂犬病在实际环境中传播的易受感染的 - 显性 - 传染性空间 - 连续模型的数值模拟 ], Journal of Biological Dynamics [ 生物动力学杂志 ] 7, Supplement 1 (2013): 31-46.

16. Frank J. Cilluffo, Sharon L. Cardash, and George C. Salmoiraghi, "A Blueprint for Cyber Deterrence: Building Stability through Strength"[ 网空威慑的蓝图：通过实力建立稳定 ], Military and Strategic Affairs 4, no. 3 (December 2012): 15-16.

17. Department of Defense Science Board, Resilient Military Systems and the Advanced Cyber Threat [ 具备韧存性的军事系统和先进的网空威慑 ], (Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, 2013), 2, 6.

18. James R. Clapper, director of national intelligence, "Statement for the Record Worldwide Threat Assessment of the US Intelligence Community Senate Armed Services Committee"[ 美国情报界就全球威胁评估向参议院武装部队委员会的发言记录 ], 26 February 2015, http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf.

19. Paul K. Davis, "Deterrence, Influence, Cyber Attack, and Cyberwar"[ 威慑、影响、网络攻击，以及网战 ], (working paper WR-1049, RAND, June 2014), 1.

20. Stefan T. Possony and J. E. Pournelle, The Strategy of Technology: Winning the Decisive War [ 技术战略：打赢决定性战争 ], (Cambridge, MA: Dunellen, 1970), 4, 8.

21. 同上，第 5、15 页。

22. John Launchbury, "High-Assurance Cyber Military Systems (HACMS)"[ 高可靠性军事网络系统 ], Defense Advanced Research Projects Agency, (DARPA), http://www.darpa.mil/program/high -assurance-cyber-military-systems.

23.Kathleen Fisher, "Using Formal Methods to Enable More Secure Vehicles: DARPA's HACMS Program"[ 使用正规化方法保障更安全载体：国防部先进研究项目局的高可靠性军事网络系统计划 ], (presentation, Tufts University, 16 September 2014), http://wp.doc.ic.ac.uk/riapav/wp-content/uploads/sites/28/2014/05/HACMS-Fisher.pdf.

24. Mozilla Foundation, "The Rust Programming Language"[Rust 编程语言 ], http://www.rust-lang.org/.

25. David Terei, Simon Marlow, Simon Peyton Jones, and David Mazi ē res, "Safe Haskell"[ 安全 Haskell 编程 ], Proceedings of the 5th Symposium on Haskell, September 2012, 137-48.

26. Department of Homeland Security, "Build Security In"[ 建设安全系统 ], https:// buildsecurityin.us-cert.gov/. 国土安全部也管理 "连续诊断和缓解项目"，该项目旨在为 "联邦部门和机构持续不断地提供鉴定网络安全风险的能力和工具，根据潜在影响优先处理这些风险，使网络安全人员能够首先缓解最严重的问题。" 参看 Department of Homeland Security, "Continuous Diagnostics and Mitigation"[ 连续诊断和缓解项目 ], 14 September 2015, http://www.dhs.gov/cdm.

27. "Social engineering" -- manipulating individuals to divulge sensitive information -- is a critical part of many cyber-attacks, but disinformation could mislead adversaries into compromising themselves. "社会工程学" — 即巧妙地控制个人使其泄露敏感信息 — 是许多网络攻击的关键组成，但是假情报可以误导对手使其自身跌入陷阱。"

爱德华・盖斯特博士（Edward Geist, PhD），是斯坦福大学国际安全与合作中心的麦克阿瑟核安全研究员，曾是兰德公司的斯坦顿核安全研究员。他获得北卡罗来纳大学的历史学博士学位，在《冷战研究杂志》、《俄罗斯评论》、《斯拉夫评论》，和《医学史公报》上发表过文章。