21st Century Defense Initiative
at BROOKINGS

JOHN L. THORNTON
China Center
at BROOKINGS

网络安全与美中关系

Cybersecurity and U.S.-China Relations

李侃如，彼得．W．辛格
Kenneth Lieberthal and Peter W. Singer

February 2012

21st Century Defense Initiative
at BROOKINGS

JOHN L. THORNTON
China Center
at BROOKINGS

网络安全与美中关系

Cybersecurity and US-China Relations

李侃如，彼得．W．辛格
Kenneth Lieberthal and Peter W. Singer

February 2012

作者注：

过去的一年里，美国布鲁金斯学会约翰·桑顿中国中心和21世纪国防计划召集了一个网络安全与美中关系工作组，由两位作者共同组织并主持。研究的动力来自于我们考虑到：1). 很多与网络安全相关的政策议题，尤其是它对于国际关系的影响，已经很显著，而且在今后的几年里，其重要性会快速增长；2). 如果不妥善处理此类议题，他们将成为国际（尤其美中关系中）摩擦的一个主要源头；3). 这个领域的新兴性尤其增加了问题的复杂程度，使网络安全成了全球安全问题中最重要而最少被人掌握的燃点之一。

这次工作组主要聚集了来自私营机构和国家机构，包括美国政府、军队、企业、智库和大学的几十位专家。随着一系列动态的、发展迅速的事件的发生，布鲁金斯的项目不仅旨在研究网络安全的关键议题及它们如何影响美中关系，更旨在解析机构和官僚体系中的弊病，是这些弊病阻碍他们形成良好政策所必须的理解。

工作组并不是要给所有在网络领域影响双边关系的各种问题提供最终的解答。工作组参与者认为首先必须建立一个理解网络领域关键趋势和威胁的框架，这将是思考美中对话如何有效谈论这些议题的基础。工作组特别专注于怎样看待网络空间才有可能带来合作。我们的一个目标是认明建立规范和执行机制的可能途径，这样可能既提高安全保障，又减少美中关系在网络及其他空间蕴含的不信任和潜在危害。

即使华盛顿和北京对接下来怎么走达成共识，这也不能解决所有的网络安全问题。因为它对于从莫斯科到堪培拉的各国领导来说都很重要。网络领域的关键挑战正在于它的全球性和民主性：国家、组织、企业，甚至是个人都可能给全球造成影响。维基解密的朱利安·阿桑奇就是个人重要性的代表，还有小小的爱沙尼亚在网络安全政策讨论中的影响远大于它本身，此类例子都证明了这一点。

美国和中国是网络领域最重要的国家行为者，而且两国在互联网的恰当使用和互联网的未来问题上观点有很大不同。因此我们认为在美中关系这个背景下考虑网络问题可能是发展解决途径的一个有效办法，然后应该更广泛地讨论这些途径，希望最终建立国际规范并实施有效措施尽可能地给网络领域带来更多的秩序和安全。

更重要的是，网络安全波及到其他议题的影响在美中之间比其他任何双边关系中都大。这一方面是因为美中关系在逐渐形成的新世界格局中占有巨大的重要性，另一方面也是因为网络议题在不断损害战略互信和两国民众及精英领导层的态度。如果这种趋势能够通过两国在网络问题上改善合作来逆转，那结果将会是“三赢”：增进美中双边关系；为网络领域的多边合作打下基石；辅助其他重要领域的美中接触，如国际金融、环境等，这都是两国必须学会更好合作的领域。

本文并不是给网络专家的一篇技术性文章，而是希望面向更广大的读者群。我们的目标是使美中两国对网络安全问题感兴趣而不是技术专家的读者们从作品中有所启发，希望对政界、商界以及更广泛的公众都有意义。我们的参考文献既有中国的，也有美国的，我们还刻意避讳随意指责。希望本文，由中英文同时发表，能够协助两国间形成一个关于网络议题的对话，更重要的是推动双方在这个关键事务上有所进展。

本报告是通过作者本身的研究，以及同网络安全与美中关系工作组的讨论而来。本报告仅反映两位作者而非其所主持的工作组的意见。

作者在此对参与网络安全与美中关系工作组座谈会的成员表达感激之意，他们的经验和智慧让我们受益良多。我们也感谢马可基金会和微软公司对这一系列座谈会的支持，以及约翰•桑顿先生对约翰•桑顿中国中心的支持。此外我们要感谢周艾拉对此报告研究的协助和翻译。

摘要

世界上可能没有哪个双边关系比美中关系更能深刻影响未来的国际政治。而在这个双边关系中，没有哪个议题像网络安全一样快速升温，并且在很短的时间内造成了种种摩擦。对于彼此在网络领域行为的不信任正在增加，而且开始给对彼此长期战略意图的估计产生严重的负面影响。

在2010-2011年间，美国布鲁金斯学会约翰·桑顿中国中心和21世纪国防计划主办了一个工作组研究网络安全与其对美中关系影响。本文通过工作组的讨论和更多的研究来为如何考虑网络安全的特征并增进美中在网络安全领域的合作提供建议。

网络领域和美中关系的特点

每个政策议题都有其特点和难处，但网络领域有一系列特征尤其对当前的美中关系和双方就行为规范或合作性实施机制达成共识产生了巨大的挑战。

术语相异

网络安全领域缺少共同的一套词汇，关键术语的定义尚未统一。即使像“信息”和“网络攻击”这种单词在美国和中国的政府内部和政府之间都有着不同的用法。同时，“攻击”分多个种类，但没有统一的方式将他们区别分类。

归属不明

证据确凿地指认恶意网络行为的始作俑者的可能性很小。捕捉他人电脑的操作并用其开展它的主人不经意甚至不知情的活动这种能力使归属问题更为复杂。

攻击优势

至少目前为止，试图穿透网络的这一方比防卫的这一方更有优势。互联网是为了信息共享的便利，不是为防止信息的流通而设计的。历史上，攻守不均衡且偏向攻方的情况将增加恶意和仓促行动的动机，同时也降低双方威慑攻击者、自我保护的信心。

时间概念

政策往往跟不上科技创新的速度，也就不可避免地从根本上比网络领域日新月异的科技进展落后了几拍。另外，从决策角度看，网络安全问题的决策时间实际上是被压缩了。即使完善准备一次网络袭击需要几周甚至几个月的时间，真正袭击成功的时间，仅需几个毫微秒。因此，政府和机构平常决策什么是恰当反应的过程也许在这个问题上根本无关紧要。最后还有数码代沟存在于今天的“天生数码代”，即长大在一个电脑普及的世界里的年轻人，和所有需要去适应电脑的年长的人（称为“数码移民代”）之间。结果是高层的决策者们有着最大的权利，却往往也是最不善于甚至提及网络议题的。

能力分散

在网络领域采取大动作并不需要大规模的人力、财力或物力资源。而且处在这个领域前沿的人可以迅速地学习新能力。史上从来没有哪一种威胁可以像网络领域的威胁这样轻易地扩大其影响。正因为这种扩散性，国家主体和非国家主体在网络世界里的界线往往是模糊的。

建立美中网络安全问题议程

网络领域的以上这些特点使得建立议程改善美中在这个领域的合作更加困难，但并不是没有可能的。任何此类议程必须基于并尊重现实：各政府都会保卫自己运用网络开展间谍活动，并在必要时支持军事行动的能力。此类议程要接受两国政治体系对于网络空间的信息自由观点很不相同，还要考虑到各政府对于网络活动的决策权分散在多个官僚机构，而不是由体制里的某一处协调处理的。最后，此类议程还应尊重一个现实，那就是各种非政府行为者在各国对网络的应用和考虑上也起着举足轻重的作用。

建立这样的议程应该包括以下步骤：

增加接触以应对问题的增长

网络问题在美中官方会议和关键非官方组织的“第二轨道”会议中都有所讨论，但接触的程度远远不及目前手上问题所需。目标应是培养一批人才可以运用同样的词汇，受本国的领导层尊重，而且信任对方的真诚和严肃。

专注于建立共同目标和辨明双方都认为有害的行为

为促进建立相互信心，这些讨论应集中在那些两个社会都认定为犯罪、且没有高度政治性的行为。

考察合作模式

讨论在网络安全问题上应用各类合作模式的利与弊是很有价值的。可能借鉴的类似模式有军备控制谈判，公共卫生、环境生态系统和针对打击国际犯罪与恐怖主义的国际金融体制。

明确表明当今国际互联网体系已建立的规范

让互联网得以平稳运行的规范和协议各式各样且数量可观，但整个系统绝大程度上依赖于各个主体与提供互联网骨干的网络运营商之间的握手协议。两国携手合作将那些广泛接受的规范明确化可以一方面促进彼此的理解和信心，另一方面提供较好的模板去处理复杂的问题。

处理归属问题

归属问题是如此核心，无法长期避免谈及。最好的目标也许是在匿名的危险和对互联网至关重要的行动自由性所带来的优点中寻找一个中间点。

讨论哪些底线一旦逾越会引发冲突

有人提出各国应该继续对各自的冲突升级途径保持模糊，但如果所有行为者能更好地了解哪些行为会引来广面冲突将会十分有益。这不仅能使各国的领导人了解自己国家哪些投资和实力可能不经意地让一场冲突升级，而且能够潜在地帮助一些规范和实施机制的形成，让某些高危行为不在政府考虑之内。

结论

建立更深的互相理解和信任将会是一个困难的过程，需要长时间的不懈努力，共同建构讨论的方式，选择讨论那些最有可能增进对于观念、目标、双方接受的方式、方法的话题。现在发展更良好的美中合作，增进对网络安全挑战的理解是必不可少的。两国如何面对这些议题不仅对互联网、其几亿用户，甚至网络空间之外的全球格局将有着决定性的影响。

序言：网络安全与美中关系的利害关系

世界上可能没有哪个双边关系比美中关系更能深刻影响未来的国际政治；没有其他两个国家能在重大的全球问题上扮演如此主导性的角色，无论是和平与安全，还是金融、贸易，亦或是环境。两国如何处理与彼此的关系不仅仅是影响他们各自政治与经济未来的一个决定性因素，也是全球稳定与繁荣的一个决定性因素。

在中美之间的关系网中，没有哪个议题像网络安全一样快速升温，并且在很短的时间内造成了种种摩擦。仅仅是上个年代，所谓的“网络空间”只不过连接了仅有的几个大学实验室的电脑。而如今，网络在我们整个国际化生活方式的中心，占据了无法估量的重要性。互联网连接了大约四十亿人和五百亿电子设备。全球每年发送90万亿电子邮件，进行2万亿多笔交易，总共传递50万亿Gb（千兆字节）数据。[1] 从商务、传媒到那些给我们的现代生活提供能源和保障的关键性设施都依赖于这个全球化的网络能够安全并稳妥地运行。

对网络安全的忧虑已经很快地移到美中关系的前线。双方的高层决策者和民众尚在试图理解网络领域的基本动力和含义，而网络安全这个议题已经笼罩了美中关系，并严重影响了两国对对方的威胁的认知。[2] 实际上，尽管网络安全是一个全新的议题，它和那些传统上影响中美关系的问题（如贸易、人权、两岸关系、地域性领土争端）同样地具有挑战性。

网络空间之恶的增加是与网络空间之善的利用和规模发展密不可分的，这导致了以上所说的忧虑。全球平均每天新发现五万五千多种恶意软件，每天还有另外二十万电脑成为僵尸（不被其所有者，而是其他用户控制）。这些电脑往往组成一连串包含成千上万甚至以上百万电脑的僵尸网络，由外部控制，用于恶意行为。[3]

比恶意使用互联网行为的数量激增更严重的是网络威胁从由往往源于吸引注意力的个人骇客主导，发展成了由复杂并有组织性的团体主导，其中有国际犯罪组织，还有与主权国家相关的间谍或军事行为。这就导致了网络领域的负面效果和它的正面一样在现实领域造成了迅速的，且常常是不可预计的后果。

互联网虽没有国界，却有越来越多的各国家机构在其中运作，并受到日益关注。从美中关系来说，最近网络领域的趋势是负面活动越来越多。几乎每天都能在媒体上看到对疑似中国攻击美国及盟国的报道，这也是华盛顿政界经常讨论的话题。[4] 2011年，几宗重大的入侵事件把网络问题提高到一个新的层次和公众关注度：美国及盟国政府、军事、企业、大学、非政府组织和智库的网络都在受侵之列。其中最著名的恐怕要数 Shady RAT 攻击，此行动渗透了全球72个政府、国际机构、企业和智库网络。[5]

报道称惊人数量的数据在这些事件中未经许可地被复制并输出。涉及的信息有国家机密、武器科技，有商业知识产权、企业谈判战略，也有高官名流或是普通百姓的私人文件和通讯内容。有人指出如果把所有的损失用金融方式衡量，这将是历史上最大的盗窃案。[6]

即使中国一概否认这些行为，美国的公众及精英都越来越感到虽然来自中国的网络威胁有多面性，其最显著的特征是政府主导。它与普通网络犯罪行为的不同之处在于针对一些非常具体的战略性目标，例如有关中国的决定，具有特殊战略意义的专利技术（人们经常提到的一个例子是普通的网络罪犯入侵美国国家航空航天管理局的航天飞

机得不到很大的回报），还有军事相关的布置和侦察，而且还监视、威胁居住外国的异见者。在对网络安全问题的公众讨论中还提到进入这些网络进行盗窃的同时也有可能为以后进一步的开发和攻击打下了基础。[7]

简而言之，美国对网络安全忧患已经到了白热化的程度，以至于美国国家反间谍执行局2011年的报告里指明说中国是网络入侵者中“最积极和顽固的”。[8] 在媒体中，《经济学人》杂志2010年7月刊的封面把网络攻击刻画成一个笼罩每个美国城市上空的巨大的数码化蘑菇云，这恐怕是再恰当不过的了。与此相似的是在高级政策圈内，恶意软件被称为“大规模杀伤性武器”（参议院军事委员会主席参议员Carl Levin），会“破坏我们的社会”（原国家安全顾问Brent Scowcroft），这意味着美国应该把它当做一个“事关生死存亡的威胁”来对待（参谋首长联席会议主席Mike Mullen）。[9] 很多人把美中在数字领域的关系比作美苏的冷战时代。[10]

虽然正如布鲁金斯的学者指出，这种冷战比喻并不恰当，但对网络安全的忧患却使这种威胁上升到了美苏冷战的等级。[11] 奥巴马总统的2011年《网络空间政策回顾》中指出“网络安全隐患是21世纪最重大的经济和国家安全挑战之一”。[12] 随之而来的是一系列的立法举措和军方伴随着美国网络司令部的成立而启动的全新的网络威慑战略。美国国防部的《网络空间操作战略》虽然没有具体指明某个国家，但是却指向中国为这个领域的威胁来源之一。[13] 该战略试图拟定一个明确针对国家行为体的网络威慑原则，包括给美国留有升级冲突的选择，使得当其感到在网络领域承受沉重损失的时候，可以用传统武力在现实领域反击。

中国的学者和官方当然对以上直接和间接的指控义愤填膺，称其“毫无根据，并反映了冷战思维”。[14] 无论在公开场合还是私下讨论，他们都声称中国的网络体系经受着更为频繁的攻击。[15] 中国公安部指出对中国境内电脑和网站的攻击每年以80%以上的速度激增，而且从数量上来

说，中国是网络攻击的最大受害国。[16] 2011年12月，十几家中国最受欢迎的网络购物、微博、社交和游戏网站受到袭击，导致一亿多网络用户名、密码、邮箱地址泄露。[17]

不仅如此，很多人认为中国的系统比美国的要脆弱很多。[18] 这种说法从某种角度上来说有一定道理，因为大量的中国企业和机构使用盗版软件，这就意味着这些系统无法得到普通软件购买者所享受的针对网络威胁演变而开发的升级保护。有估计表明中国有一千万或者更多的电脑目前为僵尸网络的一部分。[19]

中国官方和学者还声称中国电脑受到的攻击大多数源于美国，约有三万四千来自美国的网络袭击是针对中国的。[20] 虽然具体的数字尚有争议，但难以否认的是大量恶意的互联网活动来自或从美国经过。例如，HostExploit的安全研究员发现世界前50个犯罪活动猖獗的网络运营商中有20家是美国的。[21] 此外，美国政府机构，如国家安全局在网络操作方面很活跃并娴熟。

最后，中方还常常感到全球网络传播领域的不公平性。很多人觉得美国因其在互联网和很多相关网络科技的发展中扮演关键性角色而持续占有过高的优先地位。例如，整个互联网所依赖的13个根服务器中原本有10个在美国境内（其中包括美国政府运营者美国陆军研究实验室和国家航空航天局），另外3个在美国盟国境内（分别在日本、荷兰和瑞典）。另一个例子是ICANN，互联网名称与数字地址分配机构，刚开始的时候是一个美国政府机构，而它担任着主管IP地址这个事关全球互联网稳定、顺畅运行的任务。[22]

不管中方从哪个立场出发，最让人担忧的是此类紧张状态和忧患感与日俱增，难以阻挡。去年的事件把所有这些趋势都放大了，而且网络攻击的规模和复杂程度也大大增加，尤其在Stuxnet（震网）蠕虫病毒上可见一斑。在这个事件中，一个特别开发的蠕虫病毒攻击了西门子数据采集与监控系统，五个伊朗核设施的离心分离机正是依赖此

系统运行的。有人把这一事件看作是防止核扩散的胜利（因为它高度集中地破坏了非法的核武器研究），但美国和中国的网络安全圈内都视之为一个新层次的威胁。[23]

中国军事科学研究院的两位学者发表了一份报告，准确地把这短短一段时间内产生的紧张而令人费解的氛围捕捉下来："网络空间博弈的"龙卷风"席卷全球……给世界带来极大的冲击和震撼，这背后都有美国的影子。面对还仅仅处于热身状态的网络战，各国政府和军队无不担心陷入被动，正紧锣密鼓地加快网络战的备战步伐。"[24]

总而言之，美中对对方在网络领域行为的不信任在增加，而这种不信任很容易波及对彼此的长期意图的广面评估。网络领域与双方不同的关键价值之间的联系使这个问题更为突出：美国方面更重视个人隐私，而中国更重视内部稳定。更重要的是，网络安全问题对美中关系产生潜在危害的大环境是全球力量均衡转移的程度和速度确实存在的不确定性。在这个大问题上的分歧使双方对美中关系前景的焦虑升温，不知道在未来的几十年里这会是一个以相互合作亦或是敌对为主题的双边关系。[25]

传统的两国关系中，能力、弱点和意图的交集决定他们视对方为伙伴还是威胁，因此这个交集含有至高的利害关系。两国的决策者和民众必须面对现实：到目前为止，网络领域的发展给双边关系增加了紧张气氛，而不是加强了双方寻求合作途径以解决共同面对的国际问题的信心。

网络领域和美中关系的特点

每个政策议题都有其特点和难处，而网络安全议题最棘手的地方在于它有很多独特之处使得要取得任何有关规范或者合作的共识都非常困难，更不用说是在中美两国间了。

术语和议题框架

就任何一个登上国际议程的新议题，即使费时费力，都必须发展出一套公认的词汇和概念。无论是贸易谈判还是核武器，这些问题的基本术语往往看起来简单，但要达成共识却非常困难。举例来说，美国代表在美中官员的一次外交会议上第一次运用了“engagement”这个词，中国代表们莫衷一是，不知道美国的意思是“订婚”还是“交战”。[26]

术语问题在网络领域有特殊的难度，它包括特别高科技的专业内容，也包括了一些概念，其基本名词也有可能有着各种复杂的内涵。打个比方说，在美苏谈判中可能对于巡航导弹的准确定义有所分歧，但不会有人否认这是一种武器。而在网络领域，连“信息”是否是武器也没有定论：一边认为有关中东民众抗议的新闻更新，以及社会化网络建立起的跨国际联系不仅仅是良性的，更是人权必不可少的一部分[27]；而另一边却视之为“信息攻击”，企图破坏这些国家的稳定。[28] 相似的，网络恐怖主义也被用于描述一系列活动：恐怖组织在理论上可以用互联网来造成实体的破坏（例如干扰航空控制网络），也有用互联网来招募新的恐怖分子和传播战术和作业性规划。[29]

一个相关的问题就是区分网络领域的活动和目的。往往在讨论网络安全议题的时候，一大批有本质性区别、应分开考量的网络活动都被捆绑在了一起。比如讨论什么可以称得上是“攻击”的时候，不管是私下的还是公开的讨论，一系列各种各样、可行不可行的行为仅仅因为在整个过程的某个部分涉及互联网，就都被称为“网络攻击”。[30]把所有不良的网络行为都作为“攻击”同一而论就好比是因为它们都含有火药的化学成分，把青少年玩的汽水火箭、抢劫犯手中的左轮手枪、反动势力的炸弹和国家军队的巡航导弹所带来的威胁相提并论。

网络攻击从本质上说主要包括发现电脑网络的弱点，入侵这些网络，然后从网络中复制并输出信息，并且/或者在这些网络之间交换信息。问题在于这个简单的概念囊括了一系列各种各样的行为和结果。例如拒绝服务攻击并没有穿透所攻击的系统，而仅是用其他网络（往往通过在世界各地被控制的僵尸网络）发送大量如洪水般的访问请求，让目标系统无法承受而停止运作。这就好比一个房子的门虽然没有被冲破，但因为有太多不请自来的客人堵在门口，使得正式的客人也进不去了。但如此大量的访问请求产生的具体原因可能有很多：可能是网络管理上的无心之失，也有可能是刻意之举，如犯罪勒索（曾有组织以这种袭击作为威胁来进行敲诈[31]）、政治抗议（如不久前“匿名”组织攻击了那些不支持维基解密的公司和机构[32]），甚至可以是在传统战争时的某种战略手段（如格鲁吉亚的网站在与俄国之战中遭到攻击，造成其政府难以与国民或国际方面联系[33]）。此外，这种拒绝服务“攻击”实际上是所有恶意行为中最容易对付的行为之一，而即使如此，它也能作为更广的战略行动的一部分，例如在攻击基础设施的同时实行以倍增攻击效果。

与此同时，那些实际进入目标网络的攻击其目的、后果也可能大相径庭。有些攻击是恶作剧性的，黑客们可能只是炫耀自己的能耐。也有可能是犯罪性质的，例如获得某人的网络身份（私人数据、密码等）用于订购，实施虚假的金钱交易。

特别值得一提的是类似间谍的行动：进入网络系统以开展监视活动并提取信息。这类行为的受害者们从政府外交机构到国际运动员监督组织不等。在这些案例中，被监视和被盗的信息是具有战略性的。这些信息有的是知识产权，诸如可能带来巨大商业甚至国家安全价值的专利产品或设计；有时是某些公司准备的谈判策略，用于往往是国营公司与某个外国公司的谈判。这些攻击的受害者中有设计被别的公司无偿复制的消费品公司，投标策略和钻井机密被盗的石油公司，还有战斗机设计被盗的航空航天公司。[34]总而言之，电子数据生成、储存、传输的广泛使用给国家和私人行为者创造了绝好的间谍机会——而他们也把这些机会利用到惊人的程度。虽然美国的辩论焦点往往集中在对于那种国防部长帕内塔在同意权听证会上提到的“电子珍珠港事件”的畏惧，实际上更严重的问题是长期在经济上被千刀万剐。

最后，“攻击”可能不仅仅包括侵入系统、获取信息，还包括修改里面的信息。在这儿，其目标和后果也是千差万别的：有些破坏可能是仅仅出于恶作剧目的，也有可能是出于政治性的原因而破坏政府机构的网站（正如2001年4月中美海南撞机事件之后发生的那样[35]）。可能是帮助或执行某犯罪行为，如更改权限、用户身份，使得犯罪分子得以通过安全屏障；也可能旨在造成战略性的严重破坏，如损坏他国执行官方制订的自我防卫或者提供公民服务（比如电力输送、医疗保障）策略的能力。虽然没怎么正式试验过，理论上来说，严重的网络攻击可能造成的毁害有：干扰敌方的电力系统和靠电力运行的各种系统（通讯、导航、雷达系统等）；在实际火力攻击的同时通过电子工具使地方系统失灵或自毁造成更大的毁灭力。最让人不安的是那些把基础设施作为目标的攻击，如远程控制大坝水库的门打开，或者关闭地区电网。[36]

这种攻击背后的目的和发起者也同样重要。有人认为在系统中植入恶意软件以降低一个实体设备的运作功能（最著名的例子就是用于伊朗核设施的Stuxnet“震网”病毒[37]）是一种“网络恐怖主义”行为；有人认为这是“网络战

争”行为；也有人认为这是有针对性的强制执行国际规范以减少伤亡的举动，因而是合法行为。[38]对“攻击”的定义因人而异，各方各执一词。

这些有关定义和术语的问题在政策讨论中极为重要。行为者可能在用同样的词语的时候表达的是完全不同的意思（有时是故意为之，比如各组织、机关、公司和个人通过夸大威胁，增加在网络安全上的投资而得益）。[39]但术语问题在国内和国际法中也有很重要的地位。各国之间对犯罪行为的界限划分各异，对于同样的行为的处罚程度也大相径庭。例如自由民主国家往往视互联网为最大限度发挥自由言论的地方，而相对比较专政的国家往往不把言论自由当做一种理所当然的权利。但实际上这个议题远远复杂得多。比如北大西洋公约组织的民主国家在大多数问题上保持很强的一致性，但对于网络犯罪条约，他们彼此之间却难以达成共识。其中一个关键因素就是在很多欧洲国家，否认对犹太人的大屠杀的言论在网上也是禁止的，而在美国却不禁止。[40]

归属问题

在术语问题之外，网络领域还有其他的侧面对美中关系格外重要，并且是要达成任何约定所必须考虑到的。简单地说，这个多变的领域需要人们切实地去看什么行为可以由各机构达成共识并管制，什么行为远远超过了受机构控制的可能。理解这种现实背后的原因，并把注意力放在那些仍然可能施行有效控制的地方是很重要的。也许难度最大的问题要数归属问题。[41]

捕获他人电脑并用它来展开一系列电脑的主人都不经意的甚至完全不知情的行动是一种已经发展得很成熟并且非常普遍的能力。（行话中把这种捕获行为叫做“pwn”，意味即占领了对方的电脑）这种攻击往往以僵尸网络的形式出现：连接多台本来并不相关的电脑，让控制者得以运用所有这些电脑的计算和通讯能力实现特定的目的。这种通过秘密连接多台设备而形成的网络能很容易地发展成巨

大的网络。三名并没有经过什么教育的西班牙人就曾用这种方式建立了一个覆盖全球的僵尸网络，据说连接了超过一千两百万台电脑。[42]

在其他案例中，控制者可能只设计去捕捉并操纵一台或少数几台电脑。这时他的目的很有可能是为了更好地隐藏自己的身份。

捕获并利用他人电脑的能力有三个特点尤为重要。第一，这种能力不受地域限制。例如，巴西的某个行为者可以利用俄国和南非的电脑去攻击中国的系统（这里国家名可以用几乎任何国名来替代）。第二，被捕获电脑的主人往往完全不知情，不知道自己的电脑正被远程控制用于恶意行为。第三，在恶意袭击发生后，专业人员通过复杂的分析最多可以确认是哪台电脑发出了攻击。至于那台电脑是否是被远程控制的，被谁控制的，却很难确定。即使那台电脑没有受远程控制，在很多情况下若想确定是谁用了这台电脑，甚至是哪国的人、哪个组织的人用了都很难确定（比如这台电脑是某大学的公用电脑或者在某网吧里）。实际上，即使像中国这种极少数实行网吧实名上网制的国家，追寻归属还是很困难。这是因为国外网络攻击的受害者并没有渠道查看中国网吧记录下的信息，而即使是国内，实名制的真正实施程度在各地也都不相同。这就使得用户信息往往无法获取、或是缺失、被修改了，如果这个用户特别精通技术则尤其如此。此类信息在真正的危机情况中格外重要，但难以及时获取。简而言之，要确认某次攻击的幕后指挥层通常来说是不可能的，而艰难的调查分析也许是解开环环相扣的攻击事件的关键。

不难想象这些困难造成了多么恶性的后果。由于很多人都倾向于认为绝大多数来自中国电脑的恶意行为都是由中国政府幕后主导的，其他国家的恶意分子就会倾向于捕获中国电脑来发动攻击；反之对于美国也是这样。中国的恶意分子也用这种逻辑反驳对他们的指控，说从中国发起的攻击几乎肯定是由其他国家的人操纵的，并把罪名通过对中国的普遍不信任而转嫁中国。这样的转嫁借口同样被用于反驳对美国电脑发出的攻击的指控。

确立共谋关系的难度使归属问题变得更加复杂。即使把某行为追溯到了某一地点，要证明政府担当了主使者或包庇者的正式角色却是难上加难。这和几个世纪以前的海上安全议题有共同之处：那时什么是犯罪性的海盗行为，什么是国家允许的以私掠船巡逻行为之间往往界限模糊。[43] 常常有报道指出政府动员“红客”社群和其他的非政府群体，包括学生甚至网络犯罪集团，就是为了发动直接、有针对性的攻击，而且可以否认政府自己在其中的关系。[44] 因此有些案件需要当地国家政府去调查并惩治恶意网络行为的主谋者时，受害者会感到那个国家中的部分人员实际是自愿的同谋者，或是攻击的策划人，因此并不会协助调查。例如爱沙尼亚受到的拒绝服务攻击事件，很多人相信是俄国的安全机构教唆的，所以俄国必然是不愿意去寻找并制止作案人。[45]

还有一个因素增加了归属问题的复杂性，那就是一个数据包是善是恶一开始并没有办法定夺。（正如一位专家指出的，“数据包并不是洲际巡航导弹。”）域名解析请求可能是正常的登录尝试，却也可能是试图在穿过系统。在后一种情况下，也有可能是合法的域名查询，或是大规模的拒绝访问攻击行动的一部分。此外，恶意软件一旦进入系统，并不带有某些明显的标记说明它是在哪儿开发的，甚至连它的真正目的都不明显。这和裂变物质很不同：各个核反应堆都有特定的“签名”，通常可以让人追踪到原材料的出处。而恶意软件即使被发现了，它具体出自谁手还是不得而知。

寻找 Conficker 病毒（也称刻毒虫）的来源和目的的长期努力很有代表性地诠释了这个问题。刻毒虫是近期历史上最有效的病毒之一，它聚集了全球七百万左右受控制的电脑，其中有英国议会、西南航空公司、法国和德国军队的电脑，还有几十台在中国的电脑。（一个安全专家把它称为“僵尸网络的里程碑”。）后来，随着病毒的大肆散播，调查员们只能从大量的数据中如海底捞针般寻找线索，很难确认其来源。在一次突破性的发现中，他们得知一些编程与乌克兰语的键盘有联系。但即便如此，他们还

是无法下结论说这个恶意软件是来自乌克兰，还是这个线索是故意用来混淆视线的。[46]

攻击具有优势

在任何安全议题上，自我防卫都有一定的优势，它可以降低攻击的有效性，甚至可能制造某种类型的威慑作用以劝阻将来的攻击。网络安全领域的挑战在于试图穿透对方电脑网路的行为者目前为止往往比起防护的这一方占有更大的优势。

互联网在最基本的层面就是用来简化信息分享，而不是防止信息流通的。同样，连接到这个万网之网的大多数产品和系统都没有设计有内嵌的安全成分。相反，这些产品和系统有很多可以被利用的弱点，甚至想要给它们升级或是加补丁都需要信息的流通，不然用户无法知道新威胁的存在和怎样修正它们。

很多人都认为这种趋势必定会持续下去，而且攻击方的相对优势还将加大。能够穿过系统、输出信息而不被察觉或者在察觉前完成所有行动的技术飞速增进。不仅如此，现在还有技术可以把自己所在电脑网络附近的电子设备转换成间谍平台使用。例如键盘记录器就是通过对一台电脑中恶意软件的远程控制来记录这台电脑的键盘按键记录。还有其他的恶意软件可以远程开关受控制电脑或者其他电子设备的摄像头、麦克风等用于监视房间内的情况。[47]2011年10月，有泄露的消息称这种恶意软件已经进入了原本应该处在安全网络中的美国军方无人驾驶飞机系统。[48]

另外，密码保护也变得越来越脆弱。破解技术的发展让拥有高级破解工具的人可以突破除了非常复杂“高安全性”密码之外几乎所有密码。[49]更糟糕的是，在一个网络化的单位，往往有某个管理部门拥有含有全部网络内用户密码的文件，而这些文件本身也能够被破解。

从更大的范围来看，通常人们没有意识到各种用于实现未经许可的访问的方法在迅速增加，而且越来越有效。网络安全环境中一个尤为值得担忧的问题是高级持续性威胁（APT）的增加。高级持续性威胁并不是以前那种随机、速击性的攻击，而是由一个组织锁定某个个人或机构作为目标，然后用复杂程度堪比传统职业间谍的大量资源和技术进行长时间的攻击。高级持续性威胁的特点在于多支拥有各种专长的职业团队联合行动（情报收集、入侵、汲取等）。他们会琢磨清楚攻击目标的内部组织结构、管理系统、行为习惯，甚至于社会关系，分析出哪些是重要任务，哪些不是，有哪些弱点可以攻击。尤其是社交网络，让自我分享变得特别简单的同时也创造了大量关于个人的各个细节的数据。这些数据可以用来开发战略和途径去渗透那些只有网上朋友或是朋友的朋友才能进入的电脑网络。[50]

总而言之，尽管有着非常先进而且广为使用的网络安全防护工具，大多数情况下要防止，甚至只是发现复杂的恶意行为都非常困难。连给电脑网络添加“真空层”这种防范措施也不济事。伊朗那些受“震网”袭击的设备并不是直接连接在互联网上的，而恶意软件仍然进入了这些设备（这就很有可能是有人幼稚地人为带入了软件。[51] 这类事情在美国的国防网络发生过多次，其中有一次用户把在停车库捡到的一个移动优盘直接插到了处在保密网络中的电脑里（据推测，这个移动优盘是国外情报部门放置在车库的）。[52] 因此应该不惜余力地坚持建立用户警惕意识、提高防卫能力并且确认哪些数据丢失、泄露等。但现在网络安全的现实让人们必须要接受防御处在劣势这个事实。连在网络安全领域可称是全球最领先的美国国家安全局也运行在自己的网络已经被渗透的前提下[53]，但世界上其他大多数的机构和用户却还以为自己的网络是安全的。

历史上，当优势的不平衡性偏向攻击这方时，往往增加了发动恶意行为的动机和速度，降低了双方威慑进攻并有效保护自己的信心。这种进攻方较保护方的优势，无论是实际存在还是主观感觉，都会增加不稳定性，使建立互信变得更加困难。[54]

网络领域的时间概念

“时间”在网络领域是个奇特的概念。以“零日”漏洞攻击为例，它在攻击漏洞时软件开发者本身才发现，甚至都没有发现，那个漏洞。（如果开发者发现漏洞的那天称为第一天，攻击始于这之前，所以名为“零日”。）因此，在恶意软件植入某个网络，与这个软件引发某些可辨认的发展之间可能有或长或短的一段延迟时间。这就使追溯攻击的归属更复杂了。

以“震网”蠕虫病毒为例，据查早在2009年年中，该病毒就已经开始在伊朗纳坦兹(Natanz)核设施生效，但直到2010年6月才被一家白俄罗斯，而非伊朗，网络安全公司发现。其后又花了一个月的时间才发现该病毒是专门设计用来攻击工业流程的，而发现其用途的人是美国的研究员。但即使到了那个时候，研究人员对于它具体的目标是什么还是无法达成一致意见，有的认为目标是伊朗布什尔核电站，还有的认为是印度一颗发射失败的卫星。过了整整一年，也就是在2010年11月，一家德国工业安全公司的研究员和美国网络安全公司的人员终于得出结论：“震网”病毒专门针对伊朗纳坦兹核设施所用的频率转换驱动器（使驱动器的转速忽快忽慢，有效地破坏其生产精炼铀燃料的能力）。[55] 用其中一个研究员的话说，一直到那个时候被攻击的伊朗目标“完全不知道自己正承受着网络袭击”。他们只是一个接一个地更新损毁的离心机，专家说这就正如古代中国的水刑一样慢慢地损毁他们的能力。[56]

网络空间的时间还以另外三种形式给问题造成了很大影响。第一是科技和人们对科技的应用的不断发展进步。信息科技瞬息万变，无论是硬件、软件，还是威胁、反威胁的手段都可能很快就被淘汰了。比方说，大多数恶意软件原来是针对某些系列的电脑设计的，而如今，随着大量的电脑行为转移到移动设备上进行，威胁也接踵而至。

甚至连互联网本身也在进行根本性的转变。它变得愈加个人化，个人用户不只是被动地接受网上信息，也在根

据自己的私人使用需要创造、定制网站，同时在网上更多地暴露了自己。这个转变的推进器有美国的Facebook、中国的人人网此类社交网站，还有推特和中国的腾讯、新浪推出的微博。微博在中国的发展是如此迅速，在2011年底总注册用户数已经达到了五千五百万。[57] 另外，我们的世界正被逐渐再建构成一个“物联网”——越来越多日常生活中的产品和服务，从店里买的食物到家里的电力，都在通过无线射频识别码、智能电网等途径逐渐和网络世界连接起来。

这个迅速的转变从根本上增加了外部行为者得到用户个人信息的能力，其详细程度是以前所不能想象的，这使得他们可以利用网络行为造成对现实世界更大的影响。问题在于网络领域的发展突飞猛进，而政策往往反应较慢（乃至迟滞），因此不可避免地将整个儿慢一个节拍。

在网络领域自然的发展和进步之外，还有大规模扩散。任何新的攻击成功的网络武器往往留在被攻击的网络中，别人可以拷贝使用。很多人因此认为已知威胁不应该公开指认，不然始作俑者（和后来的模仿者）就会知道他们应该改进、换代。[58] 但这样也使得合作寻找解决方案和散播防护措施变得很困难。

第二个时间问题是网络安全领域做决定，至少是政策决定的时间被大大缩短了。政府习惯用日复一日，周复一周，月复一月的时间来斟酌政策。在网络世界，即使完善准备一次网络袭击需要几周甚至几个月的时间，真正袭击成功的时间仅需几个毫微秒。所以政府和机构的正常决策过程对于这个问题可能根本就不相关。这就提高了事先策划和准备的必要性。但是完全自动的反应机制建立在两个前提上：一是准确预测攻击的特性（然后才可能瞬间识别攻击），二是可以微调自动反应使其在一开始识别攻击错误的情况下，自身也不会造成更大的负面影响。从经验上来说，这两个前提都难以成立。[59]

此外，在网络领域还有一个代沟。那就是今天的“天生数码代”，对于年轻人来说，电脑已经在他们长大的环境中，成为他们的世界的自然组成部分了；另一代则是所有年纪比他们大的人，对于他们来说，电脑是需要去适应的，因此称他们为“数码移民代”。

任何年龄段的人都可以在网络领域里活动和操作——实际上，网络领域的最大好处之一就是让用户延伸其实体可及的范围。但这个领域最尖端的创新者往往是来自年轻的这一代，他们成长在网络环境中，与之有深刻的互动，拥有在这个领域开拓新方式的天才。因此，大多数网络安全领域的创新能力掌握在这些年轻人手里，而他们尚未攀爬到一个体制或者机构的高层。换句话来说，那些现在四十多岁的美国或者中国决策者中，很少有人上大学的时候需要用到电脑。即使少数那些用到电脑的人，那时的电脑远不及现在小孩子的一个电脑玩具发达，更不用说连接到互联网了。最高层的那些六七十岁的领导们可能直到工作很久以后才开始接触到电脑，而且他们之中很多人直到今天也只有很少的电脑使用经验。

这种代沟的结果就是往往那些有权利的决策者们是最不习惯去讨论网络这种问题的（在这儿，“网络移民”这个比喻也很有用。当高层领导讨论网络议题的时候常常感到自己是在一个新世界的陌生人，无法掌握这个世界的语言，而因此也很有可能由于怕尴尬或引起误会而沉默不语）。在时间和经验上的不利会影响他们的控制感。在很多情况下，网络问题前线的人往往可以比在领导或者政策发展层面的人做的更多，而且所作的是那些年长的人都无法理解的。另外，很多这些年轻的创新者之所以能够在网络领域如鱼得水，正是因为他们无法适应传统机构的结构和官僚系统。他们的创新力可以在这样的环境中发展，但这也反映了他们常常无法理解或者接受传统上决定是非曲折的程序和模式。

分散化

前面已经提到网络空间既有公共行为者也有私人行为者，这就引申出了分散化和规模的问题。

虽然在网络安全问题上，个人行为者的影响力常常有被夸大的情况（最高级的恶意软件往往需要多个不同方面的专家联手合作，而不是像流行的说法中那样由住在父母地下室的少年黑客开发的），在这个领域，一个小团体的确造成巨大的后果。一位好的编程员和一位精英编程员在编写软件上的差距可能是有天壤之别的。这就意味着政府不能仅仅往这个问题上盲目地投入人力物力。那位发现“震网”病毒的专家就表示说他宁可要自己选择的十个专家，也不要整个美国网战司令部供他差遣。[60] 尽管有人不同意，但事实是小团体、小组织可能有着之前人们无法想象的意义。新的恶意软件可能在全球范围造成巨大损害，但开发、使用它们只需区区几个人就可以。

但最关键的问题不在于这些团体本身的威力，而在他们互享的能力。只要他们愿意，这些团体或个人可以在刹那间把如何制造新的攻击的方法传授给上百万人。举例来说，“震网”病毒可能是由一个专家团队研发制造的，但在它被发现后几周内，一位埃及的网民就在网上发表博客介绍如何制造这个新的网络武器。

大范围的扩散可能通过两种方式发生。很多攻击者直接把发现的新攻击手段拿来用，正如安全专家们所悲叹的，尚有许多基础设施公司没有把“震网”病毒所针对的安全漏洞填补上。[61] 也有其他的攻击者可能从新的网络武器中得到启发，创造出更复杂的进化版本。例如 Duqu 是一个编码类似于“震网”的新病毒，针对微软视窗系统的弱点。很多人称其为“震网之子”，觉得它肯定是由开发“震网”的同一个团队编写的。但虽然两个病毒有很多相似之处，专家发现两者之间有一些关键的不同之处，因此认为它是受启发而创造的，而非“震网”病毒的进化升级。[62]

简而言之，网络领域大规模行动不需要很大的人力、财力、或者物力资源。而且对于处在技术前端的人来说，这个领域的学习是很迅速的。威胁的规模扩大化变得史无前例的简单。

行为者的附属单位问题又增加了行为者的多样性（这也和前面讨论的归属问题紧密相连）。在传统的军事活动领域，军事大国垄断了使用大型武力的可能性；网络领域与之不同，攻击能力通常广泛散布，而且不常常处于某个组织构架中。很多黑客组成虚拟社区，有些有松散的等级结构，有些没有，有些实行固定的会员制。一些由“爱国黑客/红客”发起的攻击行动往往有某个国家支持或至少是默许，而黑客社区往往是跨国界的。例如“匿名”运动，它聚集了各个分散的团体共同决定一系列攻击目标（一般来说是“匿名”组织认为破坏数码自由性的主体：从专政国家到拒绝给维基解密捐款提供服务的信用卡公司不等），然后发动全球的“黑客活动分子”入侵或者/并且打击目标网络。

然而最令人担忧的是类似于地下黑市的恶意软件制造、散播市场，让跨国犯罪组织得以买卖交易专门的网络攻击力量。[63] 和现实世界一样，这些犯罪组织曾被怀疑是在某些政府指使下行动的，尤其是那些间谍和战争行为。

因此网络世界中国家和非国家行为者之间的界限常常是挪移不定，模糊不清的。前面提到的，即使国家行为者也难以对前线的开发新网络技术的编程员进行有效管理这个问题，则更加剧了国家行为者和非国家行为者之间的游移和不确定性。这一方面加深了归属问题的难度，另一方面当某国被指控在网络领域有恶意举动时，给这些国家提供了似是而非的否认借口。

正如在恶意行为者这边没有一个焦点，在处理恶意行为的这一边也是机构分散。有一系列国家和非国家机构提供着某种互联网治理（从互联网名称与数字地址分配机构到国际电信联盟），但没有哪一个组织在国际层面主管互联网。

在国家层面也是一样。美国国家和私人机构的领导们常常提出的一点是中国的决策机制，尤其是网络安全领域的决策机制，对他们来说很不透明。[64] 中国电脑网络的操控相对较不透明，当美国官员或者是私人企业领导想与中国的相应人员联系以协调、合作，或仅仅是互通双方都感兴趣的信息时，不知道具体哪个机构或者个人是恰当的接洽点——有时他们觉得连中国人自己都不清楚。但美国自己的国家网络安全也是如此。有一系列美国机关和部门认为自己是管理网络安全问题的，而他们的能力和管辖权各不相同。各个国家对网络安全的治理并没有很好的协调，而是不成熟、临时性的——这让国家间的合作很不容易。

最后还有一个复杂点在于美中关系从上世纪七十年代开始就是由美国国务院和中国外交部担当主要的部级双边关系管理机构，这也是百年外交惯例自然的一个方面。但在二十一世纪，这种安排就与现代问题的挑战不接轨了。实际情况是这两个机构都对于本国在网络安全领域的政策考量起不到什么作用，对这个问题也没有很深的了解。因而这两个美中关系的传统中间者并无法在网络安全这个重要性迅速提升的议题上起到什么实际作用。

最底线：美中网络安全议程将会是什么样？

世界上所有大国都在其政府的指挥下进行各种形式的网络安全行动，也在其政府流程、军事能力和经济活动中建立了基于网络的性能和要求。因此所有大国都非常关注自己网络活动的安全性和理解其他国家网络活动的能力。

然而在这个空间有大量的不确定性，尤其是美中两国之间。正如上文所述，很多不确定性很难，甚至不可能，大幅度减少。无论是归属问题还是机构管理问题在短时间内都不太可能自动有所解决。所以不难理解在这个领域，猜忌和畏惧会急速增加。

这也不表示单纯聚焦竞争是解决问题的答案，这会愈加加深猜忌和不安全性。两国合作的议程是可能建立的，而且要基于认清以上所述的难点，同时又为美中之间关于网络领域共同举措的严肃讨论提供基础。这个议程可以尊重双方政府运用网络开展间谍活动并在必要时辅助军事行动的能力，可以承认两国政治体制对于网络信息自由的看法截然不同，可以考虑到双方政府关于网络行为的决策分散在很多不同的机构而且整个系统里没有一个中心来协调这个问题，还可以认识到一个现实，那就是各种各样的非政府行为者在该国对网络问题的利用和考量当中占有重要的位置。

增加接触

网络安全在美中官方会议上有所讨论，另外据报道还有少数主要人物之间非官方的“第二轨道”意见交换。[65]但

如今接触的程度不足以处理当前手上的问题。冷战时期，苏联和美国专长于核对话的谈话者有几百人，而且很多领导人对于核领域的术语和概念比较熟悉。与之形成鲜明对比的是现在美国和中国负责在这个问题上接触的人远不及那个数目，而且两国的领导层运用洲际导弹、威慑这些冷战词汇仍然比提及互联网服务提供商和网络安全要适应地多。目标应该是培养一大批运用相同的术语、受领导层尊重而且相信彼此的真诚和严肃性的人才。

对于任何一种努力，都应给予足够的时间去培养相互理解和信任。无论场合是非官方的第二轨道，官方的第一轨道，还是“第1.5轨道”这种新形式（有一些现任政府官员参与的非政府对话），一个好的起始方法是让两边解释自己在一系列关键议题上的看法，提出问题或者开展讨论以增进在这些看法，以及看法背后的前提和经验上的相互理解。

这个阶段并不能仓促进行。要在网络空间逐渐取得共识最重要也是最困难的方面之一就是理解对方的观点和立场——他们的目标、恐惧、疑虑、假设和方法。双方阐明各自的视角是如何成形的可以帮助推进双方做为一个团队来处理一些共同面对的问题——和一些他们可能遇到的最大的阻碍和困惑。设想是把讨论逐渐推往双方可以在谈判桌的同一边讨论怎样处理所遇相同难题的方式，而不要把会议的形式仅限于一种容易引起针锋相对的结构。

最初专注于基本所有国家都认为有害的行为，讨论减轻危害的原则和方法

对可开发、使用的恶意行为建立可信的界限是符合所有国家的利益需求的。由于网络世界跨国性的本质，对于那些被两国都认定为恶意行为的举动（也称“双重犯罪”，因为它被双方承认），两国应该采取行动共同处理。为了有建设性地增进双方的信心，这些讨论应该针对那些没有很多政治成分的行动（例把自由言论犯罪化）。可以讨论的议题包括合作打击未成年人色情或人口贩卖这种犯罪

行为。它们具有典型的犯罪性，而在网络领域又添上了国际特征。因此，一开始针对定义并处理双重犯罪寻找合作途径的讨论和谈判也许能成为一个良好的开端，走向下一步对于彼此目标和忧虑的理解，增进在建立规范行为上的努力，加强相互信赖的基础。

即使讨论的议题逐渐转向比较具有政治性或者有争议的领域，讨论的焦点仍然应该放在共同利益上。举例而言，虽然美国和中国在很多网络安全议题上看法不一致，但两国显然有共同的利益去分辨哪些是网络袭击，哪些是比较温和的行为不经意造成的后果，还有保护事关贸易和经济稳定的信息和通讯。

考察合作的模式

作为国际关系的一个新空间，网络领域有其独特的性质限制了以往任何一种接洽谈判的模式。这并不是说过去的经验不能为前进的道路有所启示。正如美国作家马克·吐温所说的："历史并不重复，但会出现相同的节奏。"

建立互相理解与合作的方式之一是一起详细讨论把现有的可能有用的合作模式运用于网络安全问题有哪些优缺点。其中一种可能有效的模式就是用于军备控制尤其是核武器谈判的第二轨道模式。[66] 它固然有一定的局限性，却有实践证明的效果，也是美国很多决策者有经验的一种模式。它的挑战性在于一方面要认识到中国的决策者并没有同等的经验，另一方面一旦把网络安全和军备控制甚至是贸易谈判相提并论马上就使讨论落入了竞争性的框架。

另一个看待网络安全的方式是把网络领域视为类似生态的系统。它并不是两个行为者之间的竞争，而是一个由很多相互作用甚至竞争的行为者组成的广阔领域，而所有行为者都依赖于整个系统的健康。[67] 在这里，公共健康就是一个更为恰当的比较。这种表述议题的方式就能使双方检查相互的威胁和有哪些合作方式可以在国际、国家或者政府--私人层面达成，以确保整个系统的健康（这也将是

有利于各方的）。例如，一个健康的网络生态环境不依靠于各方增强攻击力量，而是合作致力于信息共享和防御措施，正如抗击传染病一样。

最后，各方也许能够从至今为止在打击恐怖主义融资的努力中汲取经验。正如各跨国银行有责任不处理有可能与恐怖组织有关的交易，互联网服务提供商(ISPs) 作为网络空间的关键中介也有可能通过某些方式为那些基于它们服务的恶意行为负责。这个主张并不是说要把它们等同于作恶，而是摸索在警告国际金融机构停止处理恐怖组织交易的成功（和失败）中有没有得到经验、教训。[68]

合作处理关键原则和途径

如果不就各方怎样看待网络领域的几个关键方面进行某种讨论，建立合作的日程就很难发展前进。这并不需要在各术语、定义这方面达成全面共识。焦点应集中在识别哪些地方可能带来共同认可的原则和途径，而哪些主要问题和原则确实是难以解决。讨论这些顽固领域可以使彼此深入理解那些造成问题困难的原因，如各自潜在假设或者顾虑的不同点，这才能逐渐地在一定程度上增加解决这些问题的可能性，或者至少减轻它们的负面作用。

另外，即使一开始在最有争议的领域无法达成任何共识，双方也可能对就这些领域里一些隐含的忧虑找到共鸣。例如，即使双方对什么行为称得上是“攻击”有很多异议，但如果能在某类攻击目标的定义上达成一致也很有益。两方如果同意什么是“关键性基础设施”，那么将会使保护这些设施比损坏它们更容易。[69] 这与核武器控制谈判相类似，两方有很多意见不同，但有共同的利益去控制那些增加先发制人的动机或者破坏双边关系稳定的武器，例如分导式多弹头武器（MIRVs）。[70] 虽然在战争情况下，所有大国都可能希望通过网络攻击破坏对方的关键性基础设施，但同时它们有共同的利益去促进这个领域以“防御主导”。类似的，宣布“不首先使用”（正如中国在核武器问题上的立场）也将有益于建立互相间的信心。[71]

明确表明当今国际互联网体系已建立的规范；寻找合作途径处理低层次违规行为

让互联网得以平稳运行的规范和协议各式各样且数量可观，但整个系统绝大程度上依赖于各个主体与提供互联网骨干的网络运营商之间的握手协议。合作将那些广泛接受的规范明确化可以一方面促进彼此的理解和信心，另一方面提供较好的模板去处理复杂的问题。

在现有普遍的网络系统规范上达成了基本一致后，就可以设计更好的方式去合作处理网络空间低层次的违规行为，例如无所不在的垃圾邮件相关问题。[72]垃圾邮件在高层决策者听起来好像只是妨害，但实际上这是阻塞互联网，使其无法以最大程度给所有用户，无论国籍，提供沟通、创新便利的主要原因之一。从更适切于网络安全的角度来说，高等级的威胁常常伪装成低等级威胁来获取准入权。这也是进攻优势的一个重要方面。即使是保护较先进系统（如关键性基础设施、国防承包商、或国家机构）的人也表示他们在垃圾邮件和低级蠕虫等普遍性问题上花的时间、精力和金钱远远比对付高级持续性威胁所花的要多得多，虽然后者特别针对它们的秘密，而且有可能造成严重得多的威胁。因此，发展有效的途径合作处理低级威胁可带来广泛的回报。

把注意力集中在归属问题上

归属问题是如此核心，无法长期避免谈及。有越来越高的呼声要求在匿名的危险和对互联网至关重要的行动自由性所带来的优点中寻找一个中间点。比如，很有可能已经有技术和政策可以建立一个机制用来确定甲消息和乙消息是同一个人发出的（这对于确认和辨别恶意行为很有用），而不知道那个人究竟是谁。即使无法充分处理归属问题，单是讨论这个问题，它带来的后果和怎样面对它对于增进相互理解和信任也是重要的。

讨论哪些底线一旦逾越会引发冲突

和网络犯罪领域一样，在网络战争领域，若能够在哪些行为可能引发更广的冲突上达成一致将对各方都有利：不仅是让双方知道，以免投资或使用那些无意中会急速升级冲突的网络能力，也是试图培养某些规范和实施机制以弃这些危险行为于不用。任何类似协议——甚至只是洽谈的过程——也能促进相互理解，减少不信任，降低两国面对任何威胁的征兆就轻率反应的可能。

冷战中有一些例子说明了“底线”不明确造成的问题。1962年，美国和前苏联之间没有就各自对对方的核武器放置在什么区域以及什么行为会造成危机升级进行有效的沟通。也就是说，双方都不满对方发展这些核能力，但在运用过程中非故意地（美国把导弹置于土耳其，前苏联将导弹置于古巴）大幅度提升了关系的紧张程度，刺激产生了比预期激烈得多的反应，其后果就是古巴导弹危机。当时的竞争已经带来了极大的不安定，以至于险些导致热核战争。

现在，美国和中国在网络领域的方针都有意模糊，正类似于五十年代后期和六十年代的情况。例如，美国国防部2011年发表的网络战略宣布实行一个新的方针，提出可以用其他领域的相似反应措施来应对网络领域的恶意行为。[73] 这个方针也被称为“对等”方针。[74]从某种角度来说，这种灵活性自然有其道理，但从两国竞争的视角来看就会产生问题。把“网络”和“动能”换成“传统（武器）”和“核（武器）”，就能看出这个新方针从本质上来说和给古巴危机铺路的六十年代“灵活反应”核震慑方针大同小异。中国的网络战略就更加不透明了，正如当年美国领导眼中的前苏联的核战略一样。

也许难以置信，但即使在争执最大的领域，就各自行为的底线达成协议也是有可能的。例如，当今很多国家支持的网络恶意行为往往或多或少和间谍情报有关。但即使是冷战最紧张的时期，美国中央情报局（CIA）和前苏联

国家安全委员会（KGB）在应避免哪些行为上也达成了非正式的协议。两方都不希望对方偷窃到自己的机密，但这两个机构互通明确了一组应当避免的行为和目标，以免两方在间谍领域的竞争升级到更严重的层面。(75)

简而言之，没有人可以指望所有的不合都能简单解决，或者两方会放下各自的核心利益或价值，或者某些行为准则不会随着事态演变而变化，但目标是要能够有效地传达各方的利益和价值。很多人相信这将对双方都有利，因为它可以帮助他们各自的威慑战略。正如前美军参谋长联席会议副主席，推进美国网络安全战略的关键人物，James Cartwright元帅（现已退役）所说："你不能指望一个秘密的东西起威慑作用。因为如果不知道它在那儿，它就不吓人。"(76)

最重要的是向两方明确哪些行为的轨迹会被视为逾界，引起严重的关系紧张，并导致两方都不愿看到的后果。也就是说，即使不可能达成正式协议，双方通过严肃的讨论来开始对各自的底线——哪些是不能接受，会迅速升级为危机的网络行为——进行交流也有着很大的价值。这种讨论的重要性在于能够给决策者提供信息，了解对方有哪些合理的顾虑，也潜在地看清某些可能领向冲突升级的途径，从而避免。

讨论底线和升级途径还有一个关键的附带好处，那就是使各政府内部对网络安全问题提增有益的关注。这可以使领导者不但对对方国家的考虑有所了解，同时也更了解自己的机构和相关非政府机构在做什么，会带来什么结果。这是目前双方的高级决策者关注不够的地方。

结论

美中双边关系是全球最重要的关系之一。双方都从互联网的稳定运行中大大受益。但网络安全议题很有可能成为双边摩擦的一个主要来源。这个将全世界紧密相连的科技将可能造成拆开这两个国家的危险。

就现有的情况来说，华盛顿和北京必须开始建立基础以加大彼此相互理解、合作，发展应对网络安全种种问题的共同规范。当然，这种双边努力不应影响到各种类似的多边举措，但关注双边对话可能有很高的价值。

没有人可以指望这些问题能在短时间内解决。任何网络领域的讨论必须考虑到这个议题相对来说是崭新的（连关键概念的术语都没有完全标准化），两方政治中缺少有效的协调机制，还有双方现有的对彼此在这个领域的动机和行为的高度怀疑态度。网络空间用于间谍行为的潜能如此之大，要达成合作协议去管理这部分问题是不现实的。那些关于价值的严重分歧也是如此，例如公民自由言论到什么程度政府可以认为它是破坏稳定的。网络领域的确有种种棘手的特征，但并不在任何程度上削弱了建立更多理解和合作的重要性。相反，这应使人对于目前发展合作途径和共同规范上的失败更为不安。

建立更大程度的相互理解和信任将是一个艰难的过程。这需要长时间的不懈努力，共同建构讨论的

方式，选择讨论那些最有可能增进对于观念、目标、双方接受的方式、方法的话题。这条道路对于美国和中国专家、领导来说都会是困难的，但没有什么重要的东西可以不费吹灰之力就得到。

而且这个努力应该马上开始。中国有一个成语，叫做“冰冻三尺，非一日之寒”，与英语里面“罗马不是一天建成的”这个说法相似。这些古老的说法仍然是对的，在快速发展的网络领域尤其如此。

美中关系对互联网、其几亿用户，乃至网络空间之外的全球格局都有着举足轻重的影响。若两国立志于走向一个更积极的未来，那在今天面对网络安全的挑战至关重要。

ENDNOTES

(1) "Security in Embedded Devices," McAfee presentation, June 22, 2011.

(2) Richard D. Fisher, Jr. "Cyber Warfare Challenges and the Increasing Use of American and European Dual-Use Technology for Military Purposes by the People's Republic of China (PRC)," Testimony before House Committee on Foreign Affairs, Oversight and Investigations Subcommittee, Hearing on "Communist Chinese Cyber-Attacks, Cyber-Espionage and Theft of American Technology." April 15, 2011; Larry M. Wortzel. "China's Approach to Cyber Operations: Implications for the United States," Testimony before House Committee on Foreign Affairs, Hearing on "The Google Predicament: Transforming U.S. Cyberspace Policy to Advance Democracy, Security, and Trade." March 10, 2010. 沈逸, "网络安全与中美安全关系中的非传统因素 (Cyber Security and the Non-traditional Elements in Sino-U.S. Relations)," 《环球视野》 322 (4, 2010) http://www.globalview.cn/ReadNews.asp?NewsID=22733.

(3) Marc Brown, "Embedded Device Security in the New Connected Era," *Electronic Engineering Journal*, accessed Sept. 26, 2011, http://www.eejournal.com/archives/articles/20110818-windriver/.

(4) 例如2011年8月起对日本最大的国防承包商，包括三菱重工等，的攻击；谷歌等34个公司在2011年1月受到的攻击，引发了谷歌从中国的推出；1月加拿大政府系统受到的黑客袭击；6月国际货币基金组织的受侵。 Hiroko Tabuchi, "U.S. Expresses Concern About New Cyberattacks in Japan," *New York Times*, September 21, 2011, http://www.nytimes.com/2011/09/22/world/asia/us-expresses-concern-over-cyberattacks-in-japan.html. http://www.nytimes.com/2010/01/13/world/asia/13beijing.html?pagewanted=all. Greg Weston, "Foreign Hackers Attack Canadian Government," CBS News, Feb 16, 2011, http://www.cbc.ca/news/politics/story/2011/02/16/pol-weston-hacking.html. David E. Sanger and John Markoff, "I.M.F. Reports Cyberattack Led to 'Very Major Breach'," *New York Times*, June 11, 2011, http://www.nytimes.com/2011/06/12/world/12imf.html.

(5) David E. Sanger and John Markoff, "I.M.F. Reports Cyberattack Led to 'Very Major Breach'," *New York Times*, June 11, 2011, http://www.nytimes.com/2011/06/12/world/12imf.html

(6) Ibid.

(7) Michiko Kakutani, "The Attack Coming From Bytes, Not Bombs," *New York Times*, April 26, 2010, http://www.nytimes.com/2010/04/27/books/27book.html?pagewanted=all.

(8) Office of the National Counterintelligence Executive, "Foreign Spies Stealing US Economic Secrets in Cyberspace," October 2011, available at http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.

(9) Nominations of Vice Admiral James A. Winfield, Jr., and Lieutenant General Keith B. Alexander Before the Senate Armed Services Committee, 111th Congress, available at http://armed-services.senate.gov/Transcripts/2010/04%20April/10-32%20-%204-15-; Karen Parrish, "Mullen Offers 40 year Perspective on Social, Military Issues", American Foreign Press Service, September 23, 2011.

(10) 例如，前美国国家安全顾问 Brent Scowcroft 在一个采访中称冷战与网络安全问题"相似程度吓人"。David Ignatius, "Cold War Feeling on Cybersecurity," *Real Clear Politics*, August 26, 2010, http://www.realclearpolitics.com/articles/2010/08/26/cold_war_feeling_on_cybersecurity_106900.html.

(11) Noah Shactman and PW Singer, The Wrong War," Government Executive, Oct. 15, 2011 http://www.brookings.edu/articles/2011/0815_cybersecurity_singer_shachtman.aspx

(12) Ronald Deibert, "Tracking the Emerging Arms Race in Cyberspace," *Bulletin of the Atomic Scientists*, January/February 2011 vol. 67 no. 1, p. 1-8 available at http://bos.sagepub.com/content/67/1/1.full

(13) Department of Defense, Strategy for Operating in Cyberspace, July 2011, available at http://timemilitary.files.wordpress.com/2011/07/d20110714cyber.pdf

(14) Jiang Yu, a representative of the Chinese MFA, as quoted in "Also China Denies Pentagon Cyber-Raid," http://news.bbc.co.uk. September 4, 2007.

(15) 例如据《中国日报》报道，外交学院一位国际安全专家Su Hao讲到："China was accused time and again for launching cyber attacks abroad but there was never any solid proof. Actually, China has become a victim of such repeated claims," "Nation needs 'more Internet security'" *China Daily*, Dec. 29, 2010.

(16) Ai Yang, "Nation needs 'more Internet security'" *China Daily*, Dec. 29, 2010.

(17) Lea Yu and Xuyan Fang, "100 Million Usernames, Passwords Leaked," *Caixin Online*, December 29, 2011. http://english.caixin.com/2011-12-29/100344138.html.

(18) "2011年6月2日外交部发言人洪磊举行例行记者会, " accessed September 26, 2011, http://vancouver.china-consulate.org/chn/fyrth/t827448.htm. 张召忠, "中国服务器网络安全面临很大威胁 (China's Servers Network Security Faces Great Danger)," 新华社, May 18, 2010, http://news.xinhuanet.com/mil/2010-05/18/content_13511986.htm. "专访国家互联网应急中心:中国是黑客攻击的最大受害国,"新华社, January 22, 2010, http://news.xinhuanet.com/politics/2010-01/22/content_12859136_1.htm.

(19) Shaun Waterman, "China Open to Cyber-attack," T*he Washington Times*, March 17, 2011, accessed September 26, 2011, http://www.washingtontimes.com/news/2011/mar/17/china-open-to-cyber-attack/?page=all. "著名IT杂志称：中国已成为黑客攻击热门目标 (Famous IT Magazine Claims: China is a Heated Target for Hackers)," 人民网, accessed September 2, 2011, http://it.people.com.cn/GB/42891/42894/3308326.html.

(20) "中国是"间谍软件 "最大受害国 美国攻击最多," 新华社, April 10, 2009, accessed September 26, 2011, http://news.xinhuanet.com/mil/2009-04/10/content_11163263.htm.

(21) Noah Shachtman, "Pirates of the ISPs," Brookings Cybersecurity Paper, June 2011, http://www.brookings.edu/~/media/Files/rc/papers/2011/0725_cybersecurity_shachtman/0725_cybersecurity_shachtman.pdf

(22) "谁掌控了我们的服务器," 《国际金融报》, August 20, 2009, 2. http://paper.people.com.cn/gjjrb/html/2009-08/20/content_323598.htm.

(23) "The FP Survey: The Internet." *Foreign Policy*, September/October 2011. P 116
吴正龙, "震网的警示," 《解放日报》, February 10, 2011, 4.

(24) 叶征、赵宝献, "网络战，怎么战？" 《 中国青年报 》, P 09, June 3, 2011. http://zqb.cyol.com/html/2011-06/03/nw.D110000zgqnb_20110603_1-09.htm

(25) 程群, "奥巴马政府的网络安全战略分析," 《现代国际关系》 01, 2010: 11-16.

蔡翠红, "试析" 9·11 "后美国国家信息安全战略," 《美国问题研究》, 00, 2006. James A. Lewis, "Cyber Security and US-China Relations," *China U.S. Focus*, July 6, 2011, accessed September 26, 2011, http://www.chinausfocus.com/peace-security/cyber-security-and-us-china-relations/. Adam Segal, "The Role of Cyber Security in US-China Relations," *East Asia Forum*, June 21, 2011, accessed September 26, 2011, http://www.eastasiaforum.org/2011/06/21/the-role-of-cyber-security-in-us-china-relations/.

(26) King Jr., N. and J. Dean, "Untranslatable Word in U.S. Aide's Speech Leaves Beijing Baffled; Zoellick Challenges China To Become 'Stakeholder'; What Does that Mean?" T*he Wall Street Journal*, Dec. 7, 2005.

(27) Hillary Rodham Clinton, "Remarks on Internet Freedom, " January 21, 2010, http://www.state.gov/secretary/rm/2010/01/135519.htm.

(28) Dmitri Alperovitch, and Ralph Langner. Transcript of "Deterrence in Cyberspace: Debating the Right Strategy with Ralph Langner and Dmitri Alperovitch." Washington, DC, September 20, 2011. 作者引用与中国外交部的讨论，讨论中中方表示Facebook 上散布谣言，引起社会不稳定的，在中国可被视为网络攻击。

(29) 美国联邦调查局把恐怖分子运用信息化科技和运用互联网的恐怖主义袭击区分开，只有后者才算"网络恐怖主义"。而Evan Kohlmann 把定义扩大了，因为他认为网上的恐怖主义社区和现实生活中的有很大的重叠性。Keith Lourdeau, "Testimony before the Senate Judiciary Subcommittee on Terrorism, Technology, and Homeland Security," February 24, 2004, http://www2.fbi.gov/congress/congress04/lourdeau022404.htm. Eben Kaplan, "Terrorists and the Internet, " Council on Foreign Relations, last modified January 8, 2009, http://www.cfr.org/terrorism-and-technology/terrorists-Internet/p10005.

(30) 例如 William Lynn, "Defending a New Domain," *Foreign Affairs*, Oct. 2010, http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain

(31) "Germans Fear Cyber-crime as Digital Blackmail Grows," *Reuters*, June 30, 2011, http://in.reuters.com/article/2011/06/30/idINIndia-58011620110630.

(32) Robert Mackey, "'Operation Payback' Attacks Target MasterCard and PayPal Sites to Avenge WikiLeaks," *New York Times*, December 8, 2010, http://thelede.blogs.nytimes.com/2010/12/08/operation-payback-targets-mastercard-and-paypal-sites-to-avenge-wikileaks/.

(33) John Markoff, "Before the Gunfire, Cyberattacks," *New York Times*, August 12, 2008, http://www.nytimes.com/2008/08/13/technology/13cyber.html.

(34) Christopher Drew, " Stolen Data Is Tracked to Hacking at Lockheed," *New York Times*, June 3, 2011. http://www.nytimes.com/2011/06/04/technology/04security.html.

(35) Christopher R. Hughes and Gudrun Wacker, *China and the Internet: Politics of the Digital Leap Forward* (London: Routledge, 2003), 145.

(36) Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (New York: HarperCollins, 2010), 198.

(37) William J. Broad, John Markoff and David E. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *New York Times*, January 15, 2011, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all.

(38) George R. Lucas, Jr. "Permissible Preventive Cyberwar: Restricting Cyber Conflict to Justified Military Targets." Presentation at Society of Philosophy and Technology conference, University of North Texas, May 28, 2011.

(39) Jerry Brito and Tate Watkins, "Loving the Cyber Bomb: The Dangers of Threat Inflation in Cyber Policy," *MercatusCenter Working Paper*, April 2011, http://mercatus.org/sites/default/files/publication/WP1124_Loving_cyber_bomb.pdf

(40) Peter R. Teachout, "Making Holocaust Denial a Crime: Reflections on European Anti-Negationist Laws from the Perspective of U.S. Constitutional Experience," *Vermont Law Review* 30 (2006): 655-692.

(41) 甚至连美国政府2011年的防谍报告虽然指向中国，但也反复强调完全确认攻击归属目前很不能达到。Office of the National Counterintelligence Executive, "Foreign Spies Stealing US Economic Secrets in Cyberspace," October 2011, available at http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf

(42) Teresa Larraz, "Spanish "Botnet" Potent Enough to Attack Country: Police," *Reuters*, March 3, 2010, accessed September 26, 2011, http://www.reuters.com/article/2010/03/03/us-crime-hackers-idUSTRE6214ST20100303.

(43) Singer and Schachtman, 2011.

(44) Carr, J. (2008, October 17). Project Grey Goose Phase I Report. Retrieved from http://www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report; Krekel, Bryan. "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," Northrop Grumman Corporation, 9 October 2009.

(45) "War in the fifth domain. Are the mouse and keyboard the new weapons of conflict?" *The Economist*. July 1, 2010. http://www.economist.com/node/16478792.

(46) 更多的内容请参考 Mark Bowden, Worm: The First Digital World War, (Atlantic Monthly Press, 2011).

(47) Larry Magid, "Many Ways to Activate Webcam sans Spy Software", cnet News, February 22, 2010, accessed September 27, 2011, http://news.cnet.com/8301-19518_3-10457737-238.html; Lech Janczewski and Andrew M. Colarik edited, *Cyber Warfare and Cyber Terrorism*, (London: IGI Global, 2008), 311.

(48) Noah Shachtman, "Exclusive: Computer Virus hits US Drone Fleet," *Wired Danger Room*, Oct. 10, 2011. http://www.wired.com/dangerroom/2011/10/virus-hits-drone-fleet/

(49) John W. Rittinghouse and Bill Hancock, *Cybersecurity Operations Handbook: The Definitive Reference on Operation Cybersecurity* (Digital Press, 2003), 42-45.

(50) 对于高级持续性威胁的一个例子，可参考 Mark Clayton, "US Oil Endustry Hit by Cyberattacks: Was China Involved?" *Christian Science Monitor*, January 25, 2010. http://www.csmonitor.com/USA/2010/0125/US-oil-industry-hit-by-cyberattacks-Was-China-involved

(51) "The Stuxnet Outbreak: A Worm in the Centrifuge," *The Economist*, September 30,2010, http://www.economist.com/node/17147818.

(52) William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs*, September/October 2010.

(53) 美国国家安全局信息保障理事Debora Plunkett 讲到："没有什么所谓的安全了。最老练的敌人在我们不知不觉中行动。我们应当把系统建立在敌方将侵入系统的前提下。在强调一边，我们必须假设系统的任何部分都是不安全的，并且能够在这个基础上做调整。" Jason Mick, "NSA Switches to Assuming Security Has Always Been Compromised," *Daily Tech*, Dec 17, 2010.

(54) Michael Brown et al, *Offense, Defense and War* (Cambridge, MA, MIT Press, 2004).

(55) Mark Clayton, "How Stuxnet cyber weapon targeted Iran nuclear plant," *Christian Science Monitor*, November 16, 2010, http://www.csmonitor.com/USA/2010/1116/How-Stuxnet-cyber-weapon-targeted-Iran-nuclear-plant.

(56) Ibid.

(57) Jon Russel, "Importance of Microblogs in China Shown as Weibo Pass 550 Million Users," *The Next Web*, Nov. 11, 2011. http://thenextweb.com/asia/2011/11/11/importance-of-microblogs-in-china-shown-as-weibos-pass-550-million-users/

(58) Kim Zetter, "Fearing Industrial Destruction, Researcher Delays Disclosure of New Siemens SCADA Holes," *Wired*, May 18, 2011, accessed September 27, 2011, http://www.wired.com/threatlevel/2011/05/siemens-scada-vulnerabilities/.

(59) David Hoffman, *The Dead Hand: The Untold Story of the Cold War Arms Race and its Dangerous Legacy* (New York: Doubleday, 2009).

(60) Ralph Langner. Transcript of "Deterrence in Cyberspace: Debating the Right Strategy with Ralph Langner and Dmitri Alperovitch." Washington, DC, September 20, 2011.

(61) Ibid.

(62) Tom Espiner, "McAfee: Why Duqu is a big deal, ZDNet UK, 26 October, 2011. http://www.zdnet.co.uk/news/security-threats/2011/10/26/mcafee-why-duqu-is-a-big-deal-40094263/

(63) "Security in Embedded Devices", McAfee presentation, June 22, 2011.

(64) 见 Carolyn Bartholomew, *2009 Report to Congress of the U. S. -China Economic and Security Review Commission*, (DIANE Publishing, 2010), 170.

(65) 一些第二轨道对话有意为隐蔽的，但可以参考报道 Joseph Menn, "Agreement on Cybersecurity "Badly Needed,"" *Financial Times*, Oct. 12, 2011.

(66) Louis Kriesberg, *Constructive Conflicts: From Escalation to Resolution,* 3rd ed. (Lanham, MD: Rowman & Littlefield, 2007), 239

(67) Department of Homeland Security, "Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action," March 23, 2011, http://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf.

(68) United States House Financial Services Subcommittee on Oversight and Investigations, testimony by Stuart Levey, Under Secretary for Terrorism and Financial Intelligence, U.S. Department of the Treasury, 109th Congress, 2nd Session, July 11,2006, http://financialservices.house.gov/media/pdf/071106sl.pdf (accessed Oct. 7, 2011); Sue E. Eckert, "The US Regulatory Approach to Terrorist Financing," in *Countering the Financing of Terrorism*, ed. Thomas J. Biersteker and Sue E. Eckert (New York: Routledge, 2008); Phil Williams, "Warning Indicators and Terrorist Finances," in Jeanne K. Giraldo and Harold A. Trinkunas, *Terrorism Financing and State Responses: A Comparative Perspective* (Stanford, CA: Stanford University Press, 2007).

(69) Robert Radvanovsky and Allan McDougall, *Critical Infrastructure: Homeland Security and Emergency Preparedness*, 2nd ed. (Boca Raton, FL: Taylor & Francis, 2010), 3; 张成福、唐钧, "信息化风险管理：基本战略与政策选择," 《中国行政管理》 260, no. 2 (2007): 52-54.

(70) Stanford Arms Control Group, *International Arms Control: Issues and Agreements*, 2nd ed. edited by Coit D. Blacker and Gloria Duffy (Stanford: Stanford University Press, 1976), 237.

(71) 这里领域需要更多的研究和相互讨论。因为有反对的观点指出：当无法认明攻击来源的情况下，这种宣誓性政策可能产生负面作用，比如怀疑对方违反誓言时。但反过来说，这也把违反誓言的内部和外部代价都提高了。

(72) Karl Rauscher and Zhou Yonglin, "Fighting Spam to Build Trust," EastWest Institute and Internet Society of China joint paper, May 2011. Available at http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?ots591=0c54e3b3-1e9c-be1e-2c24-a6a8c7060233&lng=en&id=130065

(73) Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*, July 2011, accessed Oct. 7, 2011, http://www.defense.gov/news/d20110714cyber.pdf

(74) Amy F. Wool, "U.S. Nuclear Weapons: Changes in Policy and Force Structure," *CRS Report for Congress*, Jan. 23, 2008, accessed Oct. 7, 2011, http://fpc.state.gov/documents/organization/101742.pdf.

(75) Mendez, *The Master of Disguise: My Secret Life in the CIA* (New York: William Morrow Paperbacks, 2000), 348.

(76) 被引用在Andrea Shalal-Esa, "Ex-U.S. general urges frank talk on cyber weapons," *Reuters*, Nov. 6, 2011.

作者简介

李侃如博士是布鲁金斯学会约翰•桑顿中国中心主任，以及外交政策项目和全球经济与发展项目资深研究员。1983~2009年，他曾任密歇根大学教授。著有十七本书和专题论文，以及七十余篇文章，大部分与中国有关。1998年8月至2000年10月，他曾任国家安全事务总统特别助理兼国家安全委员会亚洲局资深主任。他的政府职责包括制定美国的东北亚和东亚政策。

彼得•辛格博士是布鲁金斯学会21世纪防御计划的主任、外交政策项目资深研究员。辛格博士的研究集中在三个核心领域，即战争的未来、美国国防的当前需求及未来的优先次序，和美国国防体系的未来。辛格博士经常向美国军方讲话并发表过包括《遥控战争：机器人革命与21 世纪》在内的多本书籍和文章。

BROOKINGS
The Brookings Institution
1775 Massachusetts Ave., NW
Washington, D.C. 20036
brookings.edu