



# 走向中美网络关系共同安全平台

## Towards a Common Security Platform for Sino-US Cyber Relations

帕纳约提斯·雅纳科乔戈斯博士, 美国空军大学空军研究所防务分析员 (Dr. Panayotis A. Yannakogeorgos, Research Professor, USAF)

### 引言

网络空间及其组成部分互联网, 已经成为二十一世纪的火药桶。这个领域, 原本代表着全球信息化社会项目的成果, 却在过去十年中充斥着竞争利益和意识形态的分歧, 各方在其中争夺着数码影响势力范围。今天, 网络罪犯、恐怖团伙和其他恶意破坏分子利用国际网络合作的不力和大国之间的紧张关系, 在这个领域中为所欲为。各国非但不去寻找加强合作的途径, 反而缠斗于意识形态, 力图推行自己认定的合作行为规范。

互联网不是奢侈品, 它是一个至关重要的工具, 在没有限制的情况下, 能使信息自由流动于全世界, 打开经济发展、知识交流和创新的大门。在互联网骨干的开发和维护上, 美国的技术创新领先是毋庸置疑的。然而在网络行为规范上, 美国以“盟主”身份主导制定全球网络安全行为规范的努力却一再走入死胡同。借用社会科学的术语来说——正如我们未能就如何保护非排他性全球公共利益达成协议一样——如果无法建立合适的全球规范, 就只会增加所有角色的不安全感。于是, 一切的努力导致了负和的结果。

网络犯罪和间谍活动将继续呈上升趋势。越来越多的人获得先进的信息和通信技术, 进入数字化信息社会, 但是, 有关各国如何主导和应对针对商业系统和关键基础设施的恶意网络攻击, 以及这些行为的后果,

都还有待澄清。消弭分歧固然重要, 澄清混淆更为迫切。本文拟就中美网络关系讨论提出一些澄清, 目的在于推动两国间实现共同网络安全。笔者虽无法提供最重要的结果即解决方案, 惟希望能说清我们面临的问题, 认识问题的性质, 提出一些供商榷的建议。

### 简述美中网络合作历史

#### “奥习”会

美中合作前景从大势而言是积极的, 与此大势直接相联, 两国的经济和金融关系也日趋紧密。中国持有上万亿美国的美国主权债务, 不仅使美国沃尔玛和塔吉特的货架更加充裕, 也解决了中国数百万人的就业。<sup>1</sup>当我们探讨两国领导人的政治声明时, 一定要牢记这个背景, 而无需深究所谓的资产负债表。

2013年6月7-8日, 奥巴马总统和习近平主席在加州会面, 讨论了包括网络冲突在内的各项议题。两位领导人表示愿意加强合作。习近平主席说:“我们需要密切关注这个问题, 研究解决这个问题的有效办法。网络安全议题实际上可以是中美相互务实合作的领域。”奥巴马承认:“有关黑客或盗窃等网络安全议题, 并非是美中关系中所特有的, 这是国际关注的问题。那些非国家的行为者也经常在从事这些非法活动。即便我们在同

\* 本文作者出席了2013年长沙国防科技大学第二届网络安全研讨会并做发言, 现对其发言稿加以整理和更新, 投寄本刊发表。

其他国家磋商建立应遵守的公共规则，我们也必须在私营和公共部门建设防御和保护系统。”<sup>2</sup>

鉴于美中两国都在研发技术，扩大用户数量并承担大国地位的领导作用，奥习两位领导人将须拉动世界马车，以身作则，开始解决 21 世纪初最大的安全困境。中美在网络合作上存在着巨大的机遇，其进展将在未来数月 and 数年中展现出来。奥巴马和习近平并同意设立高级别的工作组处理网络问题。双方加强网络合作，应表现在减少针对知识产权的入侵企图。另外，中美计算机应急响应小组加强及时分享信息，加大执法活动力度，也应作为双方提升合作的明显指标。

### 立足合作精神推进网络合作

奥习会营造出来的美中合作乐观气氛来之不易。曾担任美军参谋长联席会议副主席的美国空军退役上将约瑟夫·罗尔斯顿曾令人信服地指出通过两军交流建立与中国互信的长期效益。同理，在计算机安全和关键基础设施保护领域方面，我们也能同中国建立互信。<sup>3</sup> 美国海军退役中将迈克·麦康纳尔提议，美中合作将有助于“清理”恶意网络活动，降低黑客和网络犯罪导致的敌对入侵和破坏。<sup>4</sup>

在美国对台湾售武、联合国制裁伊朗、谷歌被迫撤出中国大陆，以及美国的互联网自由议程等问题导致美中两国出现一系列不断加剧的分歧后，2013 年 4 月，美国国务卿克里赴华访问，企望重新改善双方关系。<sup>5</sup> 克里的访问没有取得预期的成功，对减少中国网络间谍活动效果不大。布拉德·德隆据此认为：在中美关系中，由于基本的经济因素出现变动，影响力的消长已发生巨大的变化。显然，这种双边关系会经常出现起伏——

最近的“低潮”涉及美方曝光中国持续支持解放军发起大规模工业间谍活动，以及中国在南中国海问题上日益强硬。<sup>6</sup>

此外，一些民间组织以建立互信为己任，例如东西方研究所（East-West Institute）发起了第二轨道外交计划，最近在去年 6 月启动了第五轨道。第五轨道会晤是美国国务卿克里 2013 年 4 月访问北京的结果，克里在北京宣布，要推出一个正式的计划，开始为美中合作建立基础。克里国务卿在声明中说：

由于网络安全影响每个人，我们将立即设立一个工作组。网络安全不仅影响天空中的飞机和轨道上的火车，还关系到大坝泄洪、交通运输网络、发电站、金融、银行和证券交易。使用网络的现代国家在方方面面都受到影响。很明显，我们所有国家都必须保护人民，保护其权益，保护其基础设施。因此，我们将立即行动起来，加速展开网络合作。<sup>7</sup>

如果美国和中国领导人的公开声明是真挚的，那么这是美中在网络空间关系中的一个积极步骤。

### 超越空谈

不仅政治家释放出善言，我们也看到美中两国执法当局加强了打击网络犯罪的实际合作。中国当局将恶意黑客行为入罪，一旦行为者通过侵入电脑系统和网络的非法行动造成损害的罪名成立，将被判刑入狱。中国的执法部门还与美国同行开展合作。<sup>8</sup> 在最近的一起案例中，美国联邦调查局和中国公安部合作，相互提供帮助，打击提供儿童色情中文网站。<sup>9</sup> 该案延续了双方近年来在刑事案中有限的合作精神。美中经济与安全审议委员会成员拉里·沃茨尔 2010 年在国会的作证也清楚地表明网络合作是可能的，并

列举了具体的执法互相支持的例子：“……在某些打击网络犯罪领域，如打击信用卡偷盗集团以及银行信息盗窃，中国执法部门与美国进行了合作。”<sup>10</sup> 对付网络犯罪的共同历史，可能有助于增加战略信任，为两国之间开展认真讨论（并导致正式的双边会谈）铺设道路，使双方能就打击犯罪、国家安全、网络军事行动等事宜协商制定出坚实行为准则的方式方法。双方之间已经存在一些共识基础，能够支撑美中在网络安全合作上的双边讨论及最终正式会谈。

整体而言，美中两国在网络安全方面的合作需要涵盖军事和非军事网络领域。对军事领域的知情关注和对非军事领域的知情关注，同等重要。在这种合作的基础上，双方可以走向共同网络安全。

## 谋求共同网络安全

为有助于双方建立信任，让两个大国走向相互保证安全的网络空间关系，本文提出四项建议，相信这四项建议应成为两个大国领导世界建立正式国际条约的长征的第一步。

### 建议一：规定网络空间恶意行为的通用词汇

参与陆、海、空、天力量辩论的人对武装攻击的含义有一致的理解，就是说，通用词汇及其定义是一切理性辩论的基础。美国及其盟国和世界上其他国家在网络空间投入巨额资金。网络空间不仅是重要的然而漏洞重重的国家基础设施，也是空军和其他军种开展作战和能力建设愈益不可离开的作战领域。本文的目的是鼓励正式的辩论，因此需要我们制定出大家认同的网络空间术语和定义，并最终产生出连贯的国内和国际网空政策、战略和理论。这不只是一个纯粹的学术语义题目。1911年，英国航海理论家朱利

安·科贝特爵士论述了定义的重要性：“如果缺少这样一个工具，没有两个人甚至能顺着同样的思路思考，更难指望他们理出导致分歧的真正所在，找到心平气和的解决办法。”<sup>11</sup>

### 关键基础设施

在一些流行的演说、政策辩论和作战准则中，人们常常混淆“网络空间”和“互联网”、“网络攻击”和“网络利用”或“拒绝服务中断”等术语。部分原因是信息和通信技术的融合，经由各种工业控制系统被全球民众使用，支撑着各国的国家关键基础设施的运作，社会依靠这些系统提供二十一世纪生活所依赖的公共事业和其他服务。奥巴马总统最近颁布的一项行政命令朝着区分信息通信技术和工业控制系统迈出了必要的一步，但混淆依然存在。本文将对此做些进一步的澄清。<sup>12</sup>

网络空间包括公开的多功能网络（如互联网）和封闭的固定功能网络（如工业或建筑控制系统）。这两种网络有根本的区别。公开网络的效用取决于网络的用户数量，随着用户数量的增加，网络的效用也随之放大。网络效用最大化的原则是：用户如果信任一个公开网络，相信自己的隐私能受到保护，就倾向于加入。相较而言，封闭的固定功能网络必须确保信息能安全、可靠、经过认证地从传感器传给操作者。工业控制系统的重点放在确保可获得性，即能向重要基础设施和关键资源机器处理过程操作员或操作器提供所需的控制。

工业控制系统因其系统使命特征，在设计上很少考虑安全因素。“震网”攻击和最近其他一些事件表明，它们可能成为军事目标。如果工业控制系统发生故障或遭到破坏，将引发设备受损，资产毁坏，乃至危及生命。

这些系统因设计上的某些欠缺已经导致一些事件发生，造成大规模的损毁。一个例子是2009年萨扬-舒申斯克水电站大坝的爆炸，有分析认为这场造成大规模爆炸和环境损失的灾难是由计算机配置错误引起。如果属实，那么这次事件显示，对计算机实施网络攻击也可能造成如此程度的破坏。<sup>13</sup> 如果粗心的系统管理员未能适当地实施系统隔离的话，攻击者可以利用互联网发动针对此类系统的网络攻击。现在，随着专门的通信协议、软件、设备配置，以及这些系统操作的标准都在不断改进，也要求攻击者具备更高超的技术才能实施成功的攻击。“极光”（Aurora）漏洞的出现，对电力发电机构成了完全真实的威胁。在美国国土安全部主持的一次演练中，黑客通过远程遥控成功地进入了一台发电机的SCADA控制系统，并能导致物理性摧毁发电机——这次演练支持了把网络犯罪及间谍与网络战争加以区分的必要性。工业控制系统中的很多漏洞是被硬编程到可编程序逻辑控制器和远程终端装置及其它系统部件中，因此，修补起来比商业系统更加困难。

#### 定义网络武装攻击和网络武器

现有的国际法框架对如何对待网络战争事件做出了明确的法律和政策规定。《网络战争适用国际法塔林手册》或许是当今对此议题做出最详尽解释的文件，它给出网络攻击的定义是“网络行动，无论进攻或防御，合理预期会造成人员受伤或死亡，或损害或摧毁目标。”<sup>14</sup>

如果网络事件中使用了网络武器，就意味着突破了网络武装攻击的门槛，这同使用诸如“火焰”、“宙斯”、“高斯”或其他恶意代码等间谍或一犯罪工具有本质的区别。网络武器可以是指专门攻击工业控制系统的软

件代码，也可以是指嵌入关键系统的硬件缺陷。鉴于工业控制系统的复杂性，要想发现漏洞（所谓零日漏洞），以及找到可攻击目标，获得进入并实施攻击，这一切需要高超技术水平及大量的物力和人力投入。根据国际法，今天只有“震网”事件上升到被视为网络武装攻击的程度，因为它造成了被攻击目标的物理性摧毁。也有人认为，用“沙蒙”（Shamoon）病毒对石油能源设施实施攻击的网络事件是仅次于的第二个事件，这场攻击毁坏了虚拟记录，但后来纪录获得恢复，没有造成大规模财产毁坏或人身伤害。但是，“沙蒙”针对的是网络空间的商业应用，而不是针对可能引发国家安全关切的工业控制系统。

有人会争辩，目的在于获取非法进入某个系统的软件或硬件，只需轻按开关就能导致损毁，网络战争的“不同”正在于此。但这种常常被引用的说法却没有根据。诸如“火焰”、“毒酷”等访问软件也许像一束瞄准激光那样，起到导引武器攻向目标的相同作用。然而，瞄准激光只是武器系统的一部分，导弹的载荷才是武器系统中造成摧毁性效果的实际物体。同理，具体到网络武器，攻击者可能使用先前的进入，导引武器攻击特定目标，但是攻击者还必须研制出另外一套单独的软件，利用漏洞，造成伤亡或毁灭的物理效果。

有人会进一步争辩说，这套软件可以包含在进行网络侦察的工具内，由此产生“按动按钮就能发动网络攻击”的论点。但是，鉴于工业控制系统独有的特征，没有专门针对特定目标的数字和物理环境而制作的网络武器，就不能产生效果。简言之，这需要攻击者勾画出工业控制系统结构图和网络地图，配备程序员团队和密码专家，复制目标的虚拟环境，通过预演测试武器对目标的攻击效

果，然后投入部署和实战。以上的争辩就像是在说，身负击毙本拉登使命的海豹突击队指挥官可以把其对阿伯特塔德的本拉登住宅的第一次侦察和后来的突击行动合并起来同时进行，指望一气呵成获得成功。事实上，这两种攻击都需要在实施前做大量的准备。

#### 对和平的威胁与侵略行为

低于网络武装攻击门槛的事件，虽然可能带有恶意和具有破坏性，也具有挑衅性，但没有上升到武装攻击的程度。人们常说的分布式拒绝服务（DDOS）属于网络犯罪的范畴，而不是网络战争。中国黑客窃取美国知识产权是网络间谍或盗窃的事例。<sup>15</sup> 虽然网络间谍事件可能对国家安全构成长期的负面后果，但窃取数据本身的行为并非网络武装攻击。

尽管私营界的观点与上面相左，工业间谍不可视为战争行为，不需要政府依据美国法典第 10 卷做出反应，而应以更好的信息安全手段来防范此类犯罪的发生。联邦政府对诸如《计算机欺诈和滥用法》等法律进行修改，将允许私营企业有效保护自己，对数据盗窃行为做出积极的回应——包括销毁被窃数据。

《国防部军语词典》给非致命性武器下的定义是：“专门设计的、主要用于使人员或装备丧失能力，同时尽量减少死亡、人身永久伤害、财产和环境连带损失的武器。”分布式拒绝服务、操纵物流网络中的数据，以及其他软件和硬件事件，都可归于这一类。

由此推论，2012 年末对爱沙尼亚和格鲁吉亚，以及对美国金融行业开展的各种网络攻击，当然达不到网络武装攻击的门槛。这些破坏针对的是互联网的网络层面。但并非所有拒绝服务的事件都是如此。所谓的“简

单网络管理协议过载”（SNMP）就是非网络过载拒绝服务攻击的事例。例如，如果运行陈旧“视窗 2000”的电脑在一个工业控制系统网络上的电脑上为逻辑控制器编制程序，这些电脑就可能成为利用其未修补漏洞的恶意代码的攻击对象，造成“SNMP 过载”。在这个案例中，电脑的内存，而不是网络连接，将会失效。恶意者可利用这个漏洞，造成系统的停顿，使目标机器上的任何新程序无法起动，于是机器必须关闭，然后重新起动，才能恢复运行。但是许多关键的基础设施必须保持连续运行，否则就会发生事关国家安全的事件。在这种情况下，拒绝服务攻击就不只是针对网络层面的攻击让网站无法访问，而且是针对特定目标电脑的应用层面，有可能导致整个电厂停工。

结论似乎已一目了然——我们必须把关于网络犯罪/网络间谍行为的讨论与关于网络战争行为的讨论截然分开。如果继续交互使用这些术语和概念，目前的讨论就可能从如何保护信息系统，偏移向可能需要做出军事反应的国家安全威胁上去。应对网络犯罪和网络间谍的手段和方式，与打赢网络战争所需的手段和方式，也各不相同。随着美中两国就保护各自重要信息和关键基础设施的网空合作关系逐渐走向成熟，我们必须对各种恶意网络活动做出明确的区分，这一点至关重要。不加区别囊括一切的概括和断言已经不适时宜。

虽然美国在网络空间一直是技术的开拓者，中国正在证明自己是战略思维的先锋。一名中国军事理论家说：“在未来战场的对峙中，比技术弱势更可怕的是思维弱势。”<sup>16</sup> 另一方面，美国一直着重如何使用技术手段解决问题，却不以战略角度来思考如何走出困境，也不知道其技术手段是否有方枘圆凿之

嫌。<sup>17</sup> 于是，中国在网络间谍活动中采取的方式，证明非常有效。

## 建议二：美国应停止推动互联网自由进程

迄今为止，美国的政策一直侧重于保障互联网的言论自由，以此作为国际接触的主要政策优先。鉴于美国在该问题上的前后不一，以及它在全球网络安全对话中产生的摩擦，继续侧重于国际互联网的自由，只会妨碍美国在国际社会中建立信任。美国领导“互联网自由进程”的努力，致使各方的状况都今不如昔。实际上，创建互联网和监管互联网，是非常不同的两种使命。

固然，言论自由是美国的一项核心价值，但在震撼从欧盟到中国政府的“阿拉伯之春”的背景下，言论自由成了为其背书的辩说理由。世界应该知道，其之需要互联网的言论自由，不在于为了言论自由本身，而在于认识到自由、公开和稳定的互联网能生成强大的经济效益。以促进互联网的繁荣为重，可能比目前强调言论自由更有说服力。立足于这种思路，我们就会更加重视经济效益的得失，而不是在辩论中一味地强调个人的网络自由表达权利。

此外，美国以争取信息自由流通作为一个人权问题而参与公开鼓动和组织“网络活动人士”，导致了国际上的摩擦，对促进国际间网络安全合作适得其反。“互联网自由进程”计划就是这样一个例子。美国国务院公开发“活动人士”软件即翻墙软件，企图帮助这些活动人士避开专制政权设置的网络安全措施。这种技术还能帮助公民活动人士绕过政府的数字哨兵，传播被禁的信息。对俄罗斯、中国，以及其他非民主国家的政府而言，这些活动被认为等同于挑动数字化政权更迭。从他们的角度来说，美国是在帮助和煽动犯

罪活动。这无助于美国在网络安全方面所做的努力。

由于我们把重点落在强调互联网自由的说辞上，就难以在那些肆意滥用信息技术——窃取我们数据，瘫痪我们电脑，甚至引发更恶劣后果——的国家找到愿意与我们合作的伙伴。对很多国家来说，美国国务院推动传播的内容在他们眼中的危害性，决不亚于美国认为的恶意代码或窃取知识产权对美国的危害。

世界各国政府应理解，如果互联网能够发挥其今天的作用，自由流通的信息对其国家的繁荣将产生直接积极的影响。这项美国的发明已经与世界共享，今天互联网作为包容性信息社会的基础，能促进全球社会和经济的发展。如果互联网能允许信息在主权国家所设的合理安全限制内自由流通，这些效益才能得以持续。

## 建议三：中国国营公司应增加透明度来减少美国的疑虑

在计算机科学和工程方面，中国取得长足的发展。正如美中经济与安全审议委员会的报告说：“如果目前的趋势持续，根据消费、生产和创新，中国（以及其代理利益）将有效地成为包括通信在内的很多行业的主要市场动力。<sup>18</sup> 美国的决策者担心，依赖中国作为电脑芯片和其他信息和通信技术硬件的制造方，会让病毒和后门程序埋伏在美国部门——包括美国军方——使用的设备中。中国制造的电脑硬件价格极为便宜，在亚洲和发展中国家非常畅销。<sup>19</sup> 此外，中国企业，如华为公司，在发展下一代移动4G LTE网络标准方面处于领先优势地位。<sup>20</sup> 长沙是世界最快超级计算机“天河-2”的所在地，也是中国设计的开放源代码软件“中标麒麟

麟”Linux操作系统的研发基地。<sup>21</sup>虽然设在美国的企业传统上建立了互联网技术的标准，但来自中国的企业，如中兴通信公司，正在国际电讯联盟领头起草的、将影响全球下一代网络的重要国际标准中，发挥越来越重要的作用。

中国当然有权在全球市场上竞争其信息技术领域的份额。但是那些不幸的事件降低了外界的信任，例如发生在2010年4月8日的流量路由误导影响了美国政府和美军的网络，当时“中国电信公司服务器错误地开始在广告上标榜自己是互联网大流量的最佳路径。过去也因简单的配置错误发生过类似的路由变更事件，但这一次无疑是蓄意行为所致。”<sup>22</sup>这类事件发生后，却缺乏公开的惩罚，让美国的一些人对中国公司介入美国和盟国境内的通信行业表示担忧。中国的这些通信公司因此被认为不负责任，缺乏透明性，对技术事件不承担责任，因而被拒于美国国内市场大门之外。因此，对中国来说，在这个领域增加一些透明度，将有助于中国通信公司发展壮大，也减少美国公司的担忧。

#### 建议四：明确界定和理解国家间谍的含义

阻碍美中网络安全合作的一个最关键的领域，可能是两国对间谍活动的不同解读。有人认为，美国最近对中国五名军人的起诉，以及美国私营网络安全公司CrowdStrike（众击）对中国间谍活动的更多曝光，将严重打击美中两国在网空领域的合作努力。<sup>23</sup>就在此前一个星期，中国人民解放军总参谋长房峰辉将军应美军参联会主席邓普西将军邀请访问了五角大楼。在访问中，中方表示：“目前，中美双方正在依据两国领导人取得的重要共识积极构建新型大国关系模式，两国关系一步一步走到今天来之不易。双方的军事

关系发展表现出积极势头，这对中美两国人民都有益，有助于保证地区和全世界的和平、稳定和繁荣。”<sup>24</sup>一周之后，美国司法部却根据美国国内法，以中国盗窃美国公司知识产权为由宣布起诉中国军官。美国司法部长霍尔德在新闻发布会上表示：“当一个外部国家动用军事或情报资源和工具来以美国企业主管或公司为目标，图谋窃取商业机密或敏感业务信息，提供给其本国的国有企业以获益，我们必须说：‘够了。’要让他们知道，美国政府将不容忍任何国家以非法手段破坏美国公司，侵蚀自由市场的公平竞争原则。这项诉讼应被视为一声棒喝，宣告美国开始对日益猖獗的网络窃密采取行动。对他们的犯罪指控代表着美国跨出具有划时代意义的第一步，今后将加大努力解决这种威胁。”<sup>25</sup>虽然这项指控的对象是中国政府和中国人民解放军，起诉书的内容列举了有关犯罪手段和范围的大量细节，可以被解释为美国对外国政府的网空领域行为划出红线。

在美国发出对中国政府支持工业间谍活动的指责之后，中国组织互联网媒体研究中心立刻反击，发表《美国全球监听行动纪录》，但其中对国家间谍行为问题有明显误读。文件中重复列举美国前情报合同官员斯诺登已经曝光的美国机密项目内容。从分析角度看，这份文件没有认真解读美国起诉中国军官的原则立场，这就是，为了国家安全目的开展网络间谍活动和一国政府为帮助本国企业在国际竞争而进行网络窃密的行为有本质区别。当然，文件中确认了美国对这两种活动的区分，也提出了数码时代侵犯个人隐私的合理忧虑。<sup>26</sup>

起诉事件发生之后，有人可能觉得美中网络安全合作从此走入死胡同。这种观点其实是短视的。大国之间面对战略性挑战，需

要时间、冷静和理性应对。美中网络对话目前（截至本文完稿时）停摆，但未来一定会恢复，两国间的合作努力从过去到现在一直就是这样，在网空领域及其它场合有许多迹象可为印证。首先，今年6月5-6日，中国外交部在北京主办“信息与网络安全问题国际研讨会”，美国派代表团与会。在另一个非网空领域，中国受邀参加了世界最大规模的环太平洋国际海上演习。早先，在中国和俄罗斯等国向联合国大会共同提交“信息安全国际行为准则”后，美国没有给予支持，当时因为国际上对网络空间行为规范并没有取得共识。这本身就表明美中两个大国需要通过对话和交往加深理解，才能领导世界建设起一个有利商业发展与繁荣而非充斥着冲突与猜疑的网络环境。美国反对这份联合国大会议案的主要理由是，这份议案将允许政府对互联网实施更严格控制。眼下，中国激烈反对美国对中国盗窃知识产权的起诉，美国也不支持中俄的议案。但是，美国和中国之

间在网络安全问题上将继续进行政府间对话，双方需要对共同关注的问题协商出共同的立场。只要这些问题存在，双方就必须珍惜过去十多年来建成的合作基础，坚持对话，找到解决方案。

## 结语

网络冲突，从非法进入到破坏到武装攻击，构成一种新的力量形式。防止网络战争符合所有人的共同利益，它应比任何纯粹的国家福祉利益和国家安全更重要。真正的网络安全不仅应存在于中美两国的合作中，而且应存在于世界各国的集体努力中。中美关系的合作发展是积极的一步。这将要求双方——今天的形势也迫切需要双方——切实放弃过去寻求网络安全的做法。很清楚，从真正意义上来讲，过去的国家安全模式与我们希望实现的网络空间安全目标并不契合——毕竟，网络空间包含着很多的相互依存关系。♣

## 注释：

1. Stephen Cohen and J. Bradford DeLong, *The End of Influence: What Happens When Other Countries Have the Money* [影响力的终结：其他国家的富有对美国的影响], (New York: Basic Books, 2010); 另参看 Niall Ferguson, "Complexity and Collapse: Empires on the Edge of Chaos" [从复杂到崩溃：面临混乱悬崖的帝国], *Foreign Affairs*, March 2010.
2. 有关两位领导人的引述见 Remarks by President Obama and President Xi Jinping of the People's Republic of China After Bilateral Meeting [奥巴马总统和中国国家主席习近平双边会谈后发表的评论], <http://www.whitehouse.gov/the-press-office/2013/06/08/remarks-president-obama-and-president-xi-jinping-peoples-republic-china->.
3. Joseph W. Ralston, "Why the Pentagon Needs Friends in Beijing" [为什么五角大楼在北京需要朋友], *Wall Street Journal*, 5 March 2010.
4. James Fallows, "Cyber Warriors" [网络武士], *Atlantic*, March 2010, 58-63; 另参看 "Mike McConnell on How to Win the Cyber-War We're Losing" [麦康奈尔评说如何打赢我们正在输的网络战争], *Washington Post*, 28 February 2010, B01.
5. Hillary Rodham Clinton, "Internet Freedom" [互联网自由], (Prepared Remarks, Newseum, Washington, DC, 21 January 2010); 另参看 John Pomfret, "China Suspends U.S. Military Exchanges in Wake of Taiwan Arms Deal" [美对台军售后，中国中断与美军事交流], *Washington Post* (29 January 2010), [http://articles.washingtonpost.com/2010-01-29/world/36893526\\_1\\_china-s-defense-ministry-chinese-energy-companies-china-over-internet-censorship](http://articles.washingtonpost.com/2010-01-29/world/36893526_1_china-s-defense-ministry-chinese-energy-companies-china-over-internet-censorship).
6. Richard Rosecrance and Gu Guoliang, *Power and Restraint: A Shared Vision for the U.S.-China Relationship* [权力与自律：对中美关系的共同设想], (New York: Public Affairs, 2009).
7. John Kerry, Solo Press Availability in Beijing, China [约翰·克里在中国北京举行的单独记者会], <http://www.state.gov/secretary/remarks/2013/04/207469.htm>

8. James Areddy, "People's Republic of Hacking" [黑客“人民”共和国], Wall Street Journal, 20 February 2010, p. A1. 文中提到一名被判入狱三年的中国黑客。
9. 请见相关网站: <http://www.justice.gov/usao/nys/pressreleases/May13/WangYongPleaPR/Wang.%20Yong%20Indictment.pdf>.
10. Larry M. Wortzel, "China's Approach to Cyber Operations: Implications for the United States" [中国的网络作战方法: 这对美国意味着什么], Testimony to the Committee on Foreign Affairs, U.S. House of Representatives, 10 March 2010.
11. Julian S. Corbett, Some Principles of Maritime Strategy, [海上战略若干原则], (Annapolis, MD: Naval Institute Press, 1988; first published in 1911), p. 7.
12. Executive Order -- Improving Critical Infrastructure Cybersecurity [行政命令 — 改善关键基础设施网络安全], <http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>.
13. "Insulating oil spreads along Siberian River after Hydro Disaster" [水电站灾难后阻隔石油沿西伯利亚河扩散], RIA Novosti. 18 August 2009. <http://en.rian.ru/russia/20090818/155846126.html>.
14. The Tallinn Manual on the International Law Applicable to Cyber Warfare [网络战争适用国际法塔林手册], <http://www.ccdcoe.org/249.html>.
15. Mandiant Report [曼迪昂特报告], <http://intelreport.mandiant.com/>
16. Timothy Thomas, The Dragons Quantum Leap [龙的量子腾跃], (Fort Leavenworth, KS: Foreign Military Studies Office, 2009), 238.
17. 美国历史上的例子很多。第二次世界大战依靠的是技术优势,并非策略技高一筹。战争初期,美德两军力量相当时,德国人通常会获胜。最近的例子是美国入侵伊拉克。美国以错误的战略走入战争,地面的局势一直到战略赶上技术发展、“增兵”计划实施后才扭转。同上,第13-33页。
18. The National Security Implication of Investments and Products from the People's Republic of China in the Telecommunications Sector, U.S.-China Economic and Security Review Commission Staff Report [中华人民共和国对我国通信行业的投资和产品带来的国家安全考量], January 2011, 7, [http://www.uscc.gov/RFP/2011/FINALREPORT\\_TheNationalSecurityImplicationsofInvestmentsandProductsfromThePRCintheTelecommunicationsSector.pdf](http://www.uscc.gov/RFP/2011/FINALREPORT_TheNationalSecurityImplicationsofInvestmentsandProductsfromThePRCintheTelecommunicationsSector.pdf).
19. LCDR A. Anand, "Threats to India's Information Environment" in Information Technology: The Future Warfare Weapon [印度信息技术环境面临的威胁: 未来的网络武器], (New Delhi: Ocean Books Pvt. Ltd., 2000), 56-62.
20. "Huawei Conducts World's First Commercial Network LTE Category 4 Trial [华为进行世界第一个商业网络LTE四级测试], Cellular News, 9 May 2012, <http://www.cellular-news.com/story/54329.php>.
21. China to create home-grown operating system [中国将研发本土操作系统], <http://www.bbc.co.uk/news/technology-21895723>
22. 请见相关网站: [http://www.computerworld.com/s/article/9197019/Update\\_Report\\_sounds\\_alarm\\_on\\_China\\_s\\_rerouting\\_of\\_U.S.\\_Internet\\_traffic](http://www.computerworld.com/s/article/9197019/Update_Report_sounds_alarm_on_China_s_rerouting_of_U.S._Internet_traffic).
23. 请见相关网站: <http://www.justice.gov/opa/pr/2014/May/14-ag-528.html>; 以及 <http://www.wtae.com/blob/view/-/26051954/data/1/-/mbff4iz/-/Indictment--PDF.pdf>
24. 请见相关网站: <http://www.defense.gov/Transcripts/Transcript.aspx?TranscriptID=5432>
25. 请见相关网站: <http://www.justice.gov/iso/opa/ag/speeches/2014/ag-speech-140519.html>
26. China Internet Media Research Center, "America's Global Surveillance Record" [美国全球监听行动纪录], [http://www.chinadaily.com.cn/America's\\_Global\\_Surveillance\\_Recordworld/2014-05/26/content\\_17539247\\_5.htm](http://www.chinadaily.com.cn/America's_Global_Surveillance_Recordworld/2014-05/26/content_17539247_5.htm) (26 May 2014).



帕诺·雅纳科乔戈斯博士 (Dr. Pano Yannakogeorgos) 是美国空军大学空军研究所的网空政策与全球事务研究员, 其研究领域包括网空与全球安全交汇、网空规范、网空武器控制、非国家暴力行为体, 以及东地中海研究。他曾是罗格斯大学 (Rutgers University) 全球事务中心资深项目协调员, 并曾担任联合国安理会安全理事会顾问。他拥有罗格斯大学全球事务硕士和博士学位, 以及哈佛大学文科学士学位。