第一部分 概论

第一章：国际法在网络空间里的运用

当新技术为某个国家提供了相对于其他国家的潜在军事优势时，居于劣势的国家会迅速寻求使这些技术的军事应用非法化，或努力限制将这些新技术作为新军事手段或新作战方法，也即在国家间使用武力的方法。例如，当热气球的军事潜力让国际社会感到惊恐时，有关方面进行了将空中轰炸确定为非法行为的努力。

在第一届海牙和平会议上，俄罗斯提议禁止“用气球或类似手段投掷任何物体或爆炸物①。”该提议最后成为由 25 个国家签署和批准的国际规范，要求“在 5 年内，禁止用气球或用在性质上类似的其它新方法投掷物体或爆炸物。”②

①《武装冲突法》201（迪特里奇·辛德勒与奇里·托曼编撰，1988 年第三版）。

②宣言（第 4 条第 1 款），在 5 年内禁止用气球或其它在性质上类似的方法投掷物体和爆炸物，1899 年 7 月 29 日，重印自《武装冲突法》。本书文献附录 D 提供了该宣言。

该规范在 1907 年第二届海牙和平会议上得到了重新确认,当时有 27 个国家签署了类似的宣言，这一宣言同样在时间上有限制①。虽然最初的反应是使空中军事活动非法化，但是，随着空中导航技术的发展，对空中轰炸潜在优势的预测，使国际社会对禁止空中军事行动持更为保留的态度。②

1907 年，国际社会在永久性禁止空中轰炸所做的努力只带来了一个结果，即：在关于陆地战斗的海牙规约第 25 条中插入“不得以任何手段”这些词汇，禁止对未设防的城镇或乡村进行攻击或轰炸③.

尽管在一个世纪以后看来这个历史事例很可笑，因为飞机在百年来的战争中起了关键作用④。但它却展示了两个方式，这两个方式都试图限制恐怖却低估了正在发展着的技术在军事上的潜在价值。第一，国际社会试图彻底禁止空中轰炸。尽管某些人会将禁止空中轰炸的努力归为军备控制，但它实际上却是根据武装冲突法使空中轰炸成为非法手段的努力。在无法达成关于彻底禁止空中轰炸的国际共识时，国际社会试图通过在武装冲突法的范围内，限制技术的使用来规

① 宣言（第１４条）禁止用热气球投掷物体或爆炸物，１９０７年10月1月8月日重印自武装冲突法》。后来有一个国家签署了该宣言，但只在第三次海牙合平会议召开前有效。第三次海牙和平会议一直没开成，因而，该宣言至今在形式上仍然有效。美国和英国都签署了该宣言。本书文献附录文件 E 提供了宣言（14条）。

② 参见《武装冲突法》。

③同上。

④作为一个新近的事例，可以考虑国际社会对于海湾战争中令人恐惧的环境破坏所最初出现的强烈抗议。当达成共识后，国际社会承认，在武装冲突中绝对禁止环境破坏是不可能的，这种行为已经为《武装冲突法》所禁止，没必要增加新的限制。参见沃尔特·加里·夏普，《在武装冲突期间对环境破坏的有效威慑:对海湾战争的案例分析》，1992年。

约(航空技术)的军事潜能。

尽管国际社会的最初反应是彻底禁止空中轰炸，但第一和第二次海牙和平会议却只是将已有的国际法应用于新技术。这两届海牙和平会议都试图用武装冲突法禁止或节制有关活动，将争议中的有关活动设定为使用武力。1923 年，国际法学专家完成了关于空中战争的海牙原则①。虽然这些原则从未以任何具有法律约束力的形式被采纳，但它们是习惯法和武装冲突法的总体原则在飞机在战争中的使用这一问题上的应用②。

仅当新技术的军事运用的确是在所有情况下都令人憎恶且不接受时，如化学战争和生物战争，国际社会才能达成关于禁止将其作为战争手段或方法的共识③。然而，如果新技术的效果没有达到可接受行为的公认标准，如空中轰炸，那么，战争的新手段和新方法则仅受现有法律、必要时还有国际公约及演变中的国家行为的节制。我们不应该匆忙得出结论认为，应完全禁止将新技术使用于军事目的，或现有国际法并没有隐含地规约新技术的军事使用问题。

与历史上国际社会对热气球战争的反应相类似，在网络空间里出现敌对的国家行为和军事行动这一前景，已经引起国际社会的关注。当国际法学界开始考虑规约主权国家在网

① 海牙空中战争原则，1923 年 2 月。重印自《武装冲突法》。

②《武装冲突法》。参见 W·海斯·帕克斯《空中战争与战争法》，1990 年。该书详细而深入地探讨了在武装冲突期间国际法在空中战争中的应用，在考虑空中战争法问题时为美国国防部所广泛引用。

③参见《禁止研制、生产、存贮和使用化学武器及消毁化学武器的公约》(即《化学武器公约》)，1993 年 1 月 13 日；《禁止在战争中使用窒息、有毒和其他气体，及细菌战方法的日内瓦协议》，1925 年 6 月 17 日。

络空间里的活动和军事行动时，某些美国政府律师相当大胆地声称现代信息系统技术的军事应用是全新的事物，没有任何法律可以对此起作用。然而，目前几乎已为普遍接受的观点是，现有国际法中有相当可观的内容的确适用于主权国家在网络空间里使用武力。

与国际社会对热气球的军事潜能的最初反应相类似，本书的书名反映了国际社会对信息技术的军事潜能的关注，针对由因特网联接起来的信息系统所展开的军事行动，或通过信息系统发起的军事行动，有可能造成损失和破坏。本书开头引用了根据俄罗斯联邦的提议而形成的联合国大会决议。该决议呼吁联合国成员国增进对“在信息安全领域的现有和潜在威胁”的多边考虑，并提请这些国家将它们对于与信息安全有关的几个问题的看法告知联合国秘书长①。尽管该决议使用了犯罪和恐怖主义威胁（也即非国家行为主体使用武力）等术语，但这一问题却是由裁军委员会提出的②。其进一步发展趋向必将是试图禁止通过因特网进行某些军事行动，也

① 联合国大会决议第 53/70 号。联合国大会决议对成员国无约束力。参见联合国宪章。

② 该观点也隐含在“美国对投票的解释”里。在美国对联大 53/70 号决议投赞成票后，进行了如下解释：

联合国大会一致通过该决议，这将国际社会开始一个包括众多相关因素的复杂努力。它将使第一委员会面临许多不在通常职能范围之内的问题。例如，有关与全球通信相关的技术问题；与经济合作和贸易相关的非技术性问题；知识产权保护、执法，反恐怖主义合作，以及其他应该在第二和第六委员会考虑的问题。

本书文献附录文件 C 提供了美国的“对投票的解释”。联合国大会设立了七个主要委员会，分别处理有关问题。特别政治委员会，处理第一委员会所不涉及的政治问题；第一委员会，裁军及有关安全问题；第二委员会，经济和金融事务；第三委员会、社会、人道主义和文化问题；第四委员会，负责非殖民化问题；第五委员会、管理和预算问题；第六委员会，法律问题。联合国公众信息部，《每个人的联合国、联合工作手册》，15－16，1986。

即主权国家在网络空间里使用武力。当然，这一努力不太可能带来新的国际法规范，使主权国家在网络空间里的（军事）活动非法化，但它可以引发争论，这些争论也许会就国际法对主权国家在网络空间里的军事行动的适用性问题达成某种程度的共识。

三类相关的国际法可以用来分析何者构成使用武力或武装进攻。第一，《国际法和平时期机制》规约主权国家在和平时期的行为，只要不与敌对状态相背离，在武装冲突时期该机制仍然适用。例如，当两个国家处于交战状态时，有关条约要求两国在某个水平上中止双边贸易，但武装冲突时期在进行海上封锁时，和平时期环境条约仍然对海军指挥官对是否击沉对方油轮的决定有影响。第二，《武装冲突管理法》是和平时期国际法机制的一个组成部分，该法界定和管制主权国家在和平时期相互使用武力。它是在武装冲突时期仍然生效的和平时期国际法机制的一部分。在武装冲突爆发之前，冲突管理法管制主权国家间使用武力；在武装冲突期间，冲突管理法主要使主权国家承担如下义务，在与自身自卫要求相符的情况下尽早结束敌对状态。根据冲突管理法，使用武力达到一定的范围、持续时间和强度即构成武装冲突的法律事实。第三，武装冲突法管制实际发生的敌对行为。该法特别授权在武装冲突期间使用范围广泛的军事手段，这些军事手段的使用在和平时期是非法的。

尽管有相当可观的国际法适用于主权国家在网络空间里使用武力这一问题，但其适用性并非总是很明晰，在确切界定

国际法与在网络空间使用武力的关系方面，尚存在诸多问题。例如，何者构成在网络空间里使用武力？何时允许主权国家在网络空间里相互使用武力？国际法如何禁止或管制主权国家在网络空间里使用武力及其他活动？国际法对主权国家在网络空间里所进行的非使用武力活动是否有约束力？何者构成在网络空间里的武装进攻？何时可以认定在两个或更多国家之间存在武装冲突？主权国家在网络空间里的活动会导致武装冲突吗？何时主权国家有权为自卫使用武力？计算机间谍活动合法吗？计算机网络攻击合法吗？计算机网络攻击构成使用武力吗？何时主权国家可以为自卫目的使用武力对付计算机网络攻击？本书第 6、第 7 章将回答这些以及其他一些重要问题。

然而，本书并非涉及另外一些重大问题，因为本书仅对在冲突管理国际法背景下的主权国家相互使用武力进行分析。例如，本书未涉及主权国家使用武力对付娱乐性的黑客、恐怖主义、有组织犯罪和其他非国家行为主体这些问题。主权国家使用武力对付非国家行为主体是个执法问题，这一问题主要通过合作性双边和多边引渡及相互司法援助条约解决。这些条约是和平时期国际法规范的一部分，但不是冲突管理法的组成部分。

本书也未讨论除了冲突管理法之外的国际法规范可能对主权国家在网络空间里的活动的约束这一更广泛的问题。在不同的情况下，许多条约和国际规范在约束和制止网络空间

里的某些国家行为上具有法律效力。① 例如，这些条约包括管制卫星使用、电信、外层空间和海洋的国际法。

与此类似，本书也未讨论一旦敌对行动已经开始后，武装冲突法对主权国家在网络空间里使用武力行为的适用性问题。在可称为交战状态的国家间活动中，某一时刻一个主权国家使用武力的行为构成法律意义上和受武装冲突法管制的国际武装冲突。尽管在武装冲突期间冲突管理法仍然适用，武装冲突法却特别授权主权国家为在最短时间内、以最小的人力和物资资源使敌国部分或完全屈服使用所有必要和相称的武力，只要这些武力不为武装冲突法的有关条款所禁止。

此外，本书也未讨论美国国内法和对外法对网络空间里的主权国家行为的影响。网络空间里的许多国家行为在国际

① 尽管非国家行为主体可以像一个主权国家一样，对主权国家的信息基础设施造成危害，由非国家行为主体在网络空间里所采取的敌对的跨国行动仍然属于执法问题。然而，在某些情况下，如国有商业公司和代理行为主体的行为，以及技术所提供的隐蔽性，使区分主权国家与非国家主体的行为变得非常复杂。尽管如此，法学分析家的态度还是很明确的。例如，确定国有商业公司作为商业企业在活动还是在国家当局的指使下活动，需要根据有关事实进行判断，如谁控制公司，谁对有关行动负责，以及行动本身的性质等。这不是个法律问题。

因此，从法律视角来看，网络空间里所有的敌对性跨国行动或者是由非国家行为主体进行的，因而，是根据国内法和和平时期公约法解决的犯罪问题；或是由主权国家进行的，因而，是根据冲突管理法和武装冲突法管制的使用武力问题。值得注意的是，尽管由娱乐性入侵者、恐怖主义分子、有组织犯罪和其他非国家行为主体所进行的敌对性跨国行动可能造成极大的破坏，但这些行为在冲突管理法的范畴内并不构成使用武力的行为。即使某个敌对的破坏性行动是由军人或其他政府工作人员进行的，只要这一行动不是由国家当局所指使，并完全依靠个人的能力，那么，它也仍然是执法问题。与此类似，在解决非国家行为主体在网络空间的敌对性跨国行为方面，合作性国家之间执法安排的失效，不能改变这一法律问题的基本性质，不会使犯罪问题变成使用武力问题。

不过，如果在制止或预防公认的由非国家主体在某个主权国家里，在网络空间发起的敌对性跨国行动上，某个主权国家采取完全拒绝或否认的立场，那么，这会使这一敌对行为变成事实上的使用武力行为。因而，使冲突管理法适用于这一情况，可能会使其他国家有权为自卫目的而对这个国家或在这个国家内的非国家行为主体使用武力。对于没有主权国家支持的恐怖主义活动或犯罪活动，在未经有关国家同意的情况下，一个主权国家对在这个国家境内的非国家行为主体使用武力，可能会达到对这个国家非法使用武力的程度。

法意义上是合法的，但却为某个主权国家或多个主权国家的国内法所禁止或严格限制。例如，如果某个国家的军队在网络空间里采取行动，在己方境内采取行动，打击目标在另一个国家境内，中间要经过 5 个国家的信息基础设施，那么除了有关国际法之外，共有 7 个国家的国内法适用于这种国家行为。在美国，涉及情报搜集、间谍、在未经同意的情况下侵入计算机以确定袭击者的身份、通过不属黑客所有的服务器和计算机网络系统对黑客采取反制措施的活动，是被严格限制、在某些情况下则是非法的。因特网是全球性的，对于执法机构和情报界来说，当美国公民在网上时，如何根据美国国内法来确定可否进行合法监视和截收非常具有挑战性。

最后，本书未讨论根据联合国宪章第七条强制授权规定由安理会授权采取的国家行为这些特殊的情况。联合国宪章第 39 条赋予安理会采取武力行动以维持国际和平与安全的权力，根据国际法进行这种授权，其标准低于允许主权国家为自卫而使用武力的条件。例如，在国际法意义上，一个主权国家所进行的非法封锁，如获得安理会根据联合国宪章第七条所授予的权力，那么，它就是合法的。与此类似，在未经有关国家同意的情况下，一个主权国家在另一个国家境内所进行的大多数活动都是非法行为；然而，如果得到安理会授权，即使未经有关国家同意，在联合国维持和平行动中某主权国家在这些国家境内的活动仍然是合法的。此外，联合国宪章第 103 条会自动要求主权国家承担大多数国际义务，如果这些义务与主权国家根据该宪章所承担的其他国际义务相冲突。

因此，如果获得安理会根据联合国宪章第七条强制授权规定的授权，在国际法意义上某个非法的国家行为可能会变得合法。

因此，本书的主要目的是考察下列两个条件：

(1)根据冲突管理国际法，哪些网络空间里的和平时期国家间活动，构成使用或威胁使用武力的行为。

(2)根据冲突管理国际法，何时这种使用或威胁使用武力的行为构成武装进攻，主权国家可以据此为自卫目的使用武力？

这两个条件是信息冲突法中最重要的两个问题。信息冲突法是国际法、冲突管理法和武装冲突法的和平时期规范的一个构成要素，它管制网络空间里的所有国家行为。对信息冲突法的全面研究需要对五个领域进行探讨。本书未进行这种探讨，目的是使本书能够集中分析冲突管理法对在网络空间里主权国家相互使用武力的影响问题。

不过，还有其他许多功能性问题，需要在分析这两个条件之前先予探讨。例如，什么是网络空间？为什么网络空间使主权国家成为易受攻击的目标？为什么主权国家企图在网络空间里使用武力？主权国家何时有权使用武力？在使用武力方面联合国安全理事会承担什么样的责任？什么是交战姿态？武装冲突法包括哪些内容，如何根据武装冲突法界定何者构成使用武力和武装攻击行为？本书第 2 至第 5 章回答这些以及其他一些问题。

第 2 章分析事实基础。我们将网络空间界定为由协作性

的计算机网络、信息系统、电信基础设施的相互影响所创建的环境，一般通称因特网和万维网。本章阐明为什么网络空间使主权国家易受攻击；提供了网络空间的弱点可被利用的事例；这些事例表明网络空间不过是主权国家使用武力或对使用武力的行为进行支援的另外一种媒质或环境。最后，本章的结论是主权国家很可能对网络空间作军事上的应用。

第二部提供法律基础。这一法律基础是理解根据国际法何者构成在网络空间里使用或威胁使用武力之所必需。在对武装冲突法的演变进行简要历史评述后，第 3 章详细讨论联合国宪章确立的那些管制和平时期国家间使用武力问题的国际规范。本章阐明何时主权国家可获得授权依据国际法对其他主权国家使用武力；为维持国际和平和安全，何时联合国安理会有责任授权对某个主权国家使用武力。本章还详细讨论了必要性原则、相称性原则、非必要的对平民的附带损伤与危害原则以及预期自卫原则。

有关国家间使用武力的任何有意义的法律基础，必须包括对冲突管理法与武装冲突法的讨论。尽管武装冲突法仅对敌对期间武力行为构成约束，第 4 章还是详尽讨论了武装冲突法的一个规定，该规定为广泛接受为界定国家间存在武装冲突的标准。在根据冲突管理法确定何者构成使用武力或武装进攻时，主权国家对该规定的使用是关键性的。“敌对”这个术语一般仅指国家间的敌对状态，在国际法范围内并无特别的法律意义。一般情况下，该术语泛指武装冲突或战争。如第 4 章更为详细地讨论的那样，“武装冲突”和“战争”这两

个术语实际上也是指同样的国家间敌对状态。不过，“战争”根据法律确定，“武装冲突”根据事实确定。第 5 章对第 3 章和第 4 章的内容进行归纳，总结出支持后续分析的基本原则，从而结束对第二部分关于法律基础的讨论。

第三部分的两章是本书的核心。这两章详细讨论了根据国际法何者构成使用武力和武装进攻。第 6 章分析管制国家间使用武力的现有国际规范，并将其运用于在网络空间里的国家行为。本章剖析主权国家通过和平方式解决争端的义务，并分析何时政治、经济和非军事行为可能构成非常使用武力和武装进攻。本章还界定何时威胁使用武力是非法行为，何时对国际法的违背或间接使用武力可以构成非法使用武力。威胁使用武力这个问题很有趣，因为它将基于客观事实的对法律问题的分析引入到对敌对意图的讨论，也即使分析进入采取攻势行为的国家的意图及潜在受害国家对此的认知的领域。在第 6 章的最后，对何者构成国际法意义上的武装进攻进行详细讨论，并提供第 3 章至第 6 章内容要点的图表。

接下来的第 7 章将第 6 章讨论过的原则，应用于战斗员、决策者和国际律师当前所面临的两个最紧迫的问题：计算机间谍和计算机网络攻击。最后，第四部分对本书讨论过的核心原则进行总结，这些原则可以作为分析所有使用武力问题的基础。

第二章　网络空间的军事应用

网络空间不是一个实体性的空间——它不能用任何实体性的指标和时空连续性来衡量。它是一个缩略语，用来指代由协作性的计算机网络、信息系统和电信基础设施的相互影响所创建的环境，一般指因特网和万维网。信息是网络空间里有价值的商品，但没什么东西在网络空间里实际存在。当说起某个东西在网络空间里时，它实际是在计算机里或信息系统里，或在通过电信基础设施进行传输。

现代电信系统演变从 1837 年出现电报到 1866 年铺设跨大西洋电缆，1876 年出现电话 1895 年出现无线电报， 1946 年出现第一个商用公共无线电话服务①，1958 年由美国发射第一颗通信卫星②，直到 1943 年才发明出电子计算机， 1946 年制造第一电子真空管计算机 ENIAC 埃尼亚克）。20 世纪 50

①史第芬·利维，《计算机》新闻周刊１９９７－９８冬季特刊，第 28、30 页。
②纽约公共图书馆索引，同注１６第１３８页。

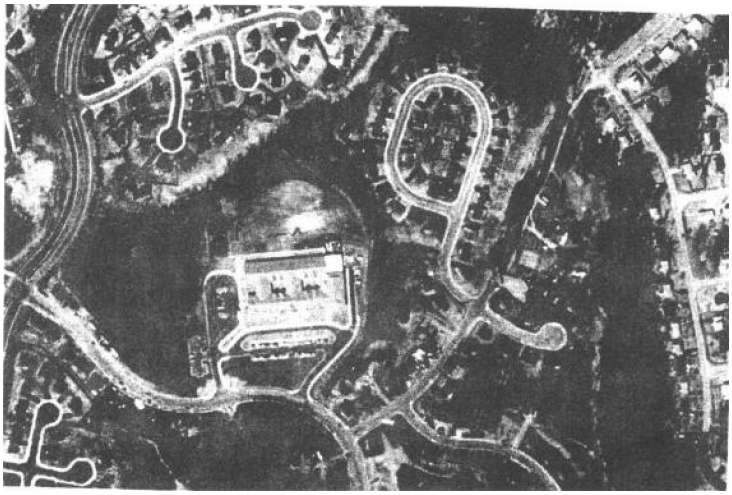
年代，IBM 公司构想出计算机的世界市场，并开始推销商用计算机。最后在 1975 年，世界上第一台个人计算机问世。最初的电子管计算机是个庞然大物，它有 80 英尺长、30 吨重，共有 17,000 个电子管，当今的计算机的存贮容量，是第一台计算机的一百万倍，运算速度则提高 5 万倍。

因特网最初是 20 世纪 70 年代由美国国防部管理，用于军事和政府目的、由电信基础设施联接起来的计算机网络。美国各大学及其他研究机构分别建立了各自的内部计算机网络。这些内部计算机网络逐渐相互融合，形成协作性运行的计算机网络集合，这些协作性运行的全球网络采取通用编址，因特网就这样诞生了。万维网指由 1989 年创建的超文本联接起来的文件和数据库的集合，它是因特网的主要平台，可以将各种各样的计算机协议转换成标准形式。

对因特网的依赖带来利益，也会产生新的弱点。美国国防部前常务副部长约翰·J·海默把万维网比作“防务改革计划的中心，重组和优化国防管理与支援体系的关键①。”然而，海默同时指出：

万维网也为我们的对手提供了潜在的工具，可以用来获取、比较及评估有关美国国防部的能力、基础设施、人员和行动的程序等大量的信息，特别是当这些信息与其他来源的信息结合在一起的时候，会增大美国国防部系统的弱点，可能还会危及国防部人员和家属的安全。

①美国国防部前常务副部长约翰 J·海默备忘录，《信息弱点和万维网 1》（1998 年 7 月 24 日）。



例如，刚才引用的这个备忘录可以在美国国防部（DoD）的网站上找到①。还可以在美国国防部网站上找到碳疽病免疫计划②和‘沙漠之狐’行动的详细情况③。

为进一步展示万维网上的信息，请看下图。这是我在 10 分钟内在万维网上找到的我所在的弗吉尼亚州北部的部分航空照片④。

① 参见 http://www.defenselink.mil/other - info/depsecweb.pdf.

② 参见 http://www.defenselink.mil/specials/Anthrax/.

③ 参见 http://www.defenselink.mil/specials/desert - fox/. ‘沙漠之狐’行动是美军对伊拉克境内军事和安全目标进行的军事打击，伊拉克境内的这些设施可以用来生产、存贮、维护和发射大规模毁伤性武器。

④ 参见 http://www.terraserver.com, Microsoft@ 地形服务器使用，根据美国地质测绘及高精度卫星照片制造的地形校正数字化航空照片。这些地质照片由俄美合资公司出售，是根据俄罗斯制造的先进测绘卫星照片制作的非保密产品。

这个照片是 1994 年美国地质测绘飞机，在 2 万英尺高空拍摄的，在网上可以找到有关世界各地的高质量航空地貌照片。访问这种公共信息可以为穷国的侦察情报机构提供初步能力。

除了信息公开化所带来的弱点之外，主权国家或商业企业还必须要考虑对内部计算机网络和计算机系统的非法渗透和黑客入侵问题。因特网和万维网采取开放式的体系结构，特别容易为不对称战争和有组织的间谍所利用。主权国家和非国家行为主体可以隐蔽地通过因特网与万维网窥探某他国家的公开、敏感和保密的计算机系统；搜集范围广泛的政府和商业信息 操纵数据 欺骗决策者 影响公共舆论 甚至在境外对某国进行实体性破坏。一个善于使用计算机和信息系统技术的国家，在发起进攻行动破坏另一个国家时，无需大规模地面部队，无需将海军机动至敌国沿海，也无需出动空军来夺取空中优势。只要在个人计算机上投入几千美元，一个意志坚决、坚韧的敌人可以对世界上任何一个其信息基础设施与因特网相联的国家造成不良影响。网络空间技术增加了超视距战争的新手段。只要敲击一下计算机键盘，命令就可能以光速发向全球，于是，便可隐蔽地实施有组织的大规模进攻。

例如，在 1997 年 7 月进行的“合格接受者”军事演习中，美国国防部国家保密局展示，一个敌对国家对美国采取信息进攻行动，可以破坏主要军事指挥机构的计算机运行，导致大范围停电，可以干扰华盛顿特区及美国其他几个城市的电话服务。接下来，1998 年 2 月，两位加利福尼亚少年在一个以