网络军备竞赛

兵不血刃，不战而屈人之兵。——《孙子兵法》

孙子是中国古代著名的军事家和政治家，《孙子兵法》集中反映了他的战争思想和攻防理念，被誉为“兵学圣典”。在孙子看来，兵学的最高境界，就是“不战而屈人之兵”。在现代国际关系中，这种思想有时会被异化为一种“遏制”战略，即保持远胜于对手的军事实力，使对方甘愿放弃对抗念头。而一旦对手不愿甘拜下风，或束手待毙，则会竭尽全力，利用一切机会和手段，发展各种进攻和防御能力，而刺激本方进一步发展军备实力以继续保持优势，这就会引发不断螺旋上升的军备竞赛。

1.“青铜战士”

爱沙尼亚共和国，波罗的海三国之一，自 1940 年 8 月到 1991 年 8 月，是原苏联的一个加盟共和国。二战结束后，原苏联政府在爱沙尼亚首都塔林市中心一块三角形的小山坡上竖起了一尊青铜所铸的战士像，也被称为“青铜战士”碑。碑的下方两边分别用俄文和爱沙尼亚文写着“纪念 1941 年至 1945 年战争的牺牲者”字样。纪念碑基座之下是一座苏联红军烈士墓，安葬着 1944 年秋天苏联红军解放德国控制的塔林时牺牲的 13 名红军战士。纪念碑和烈士墓于 1947 年 7 月 22 日落成，此后，这里成为原苏联和现爱沙尼亚纪念反法西斯战争胜利的重要活动场所。人们在此敬献花圈，吟唱革命歌曲，缅怀先烈。

谁也不曾料到，60 年后围绕这座纪念碑的去留问题引发了爱沙尼亚和俄罗斯之间的争议，进而导致了一场具有划时代意义的网络战争。当时，爱沙尼亚已经是世界上信息化程度最高的国家之一，互联网普及率超过三分之二，绝大部分金融交易以电子和在线方式进行。爱沙尼亚拥有多项网络应用水平的世界第一，比如第一个通过网络进行总统选举，第一个将“上网是公民的基本权利”写进宪法，第一个推出“电子身份证”等等。而在另一方面，爱沙尼亚经济社会运行高度依赖互联网的同时，这个网络应用发达的国家抵御网络攻击的能力却很脆弱。

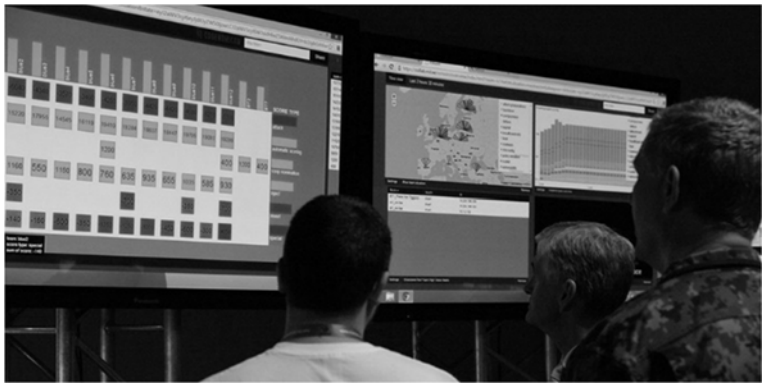
2007 年 1 月 10 日，爱沙尼亚议会通过一部《军人葬地保护法》，规定国家

在建设新的公共设施需要用地或是出于安全考虑时，可以将军人墓地、纪念碑等迁移，这一法律为拆除塔林纪念碑提供了法律依据。4 月 27 日，爱沙尼亚政府下令拆除塔林纪念碑，并将择时将烈士墓搬迁至郊区。这一决定和行动激起了反对者的极度不满，进而引发街头暴力冲突，致使 1300 多人被捕，100 受伤，1 人死亡。俄罗斯人把移走纪念碑视为对原苏联将士在二战期间浴血奋战历史的否定，俄罗斯外交部指责爱沙尼亚政府一手促成了紧张局面。

街头骚乱和外交指责的同时，爱沙尼亚的整个网络开始经历当时最严重的分布式拒绝服务攻击，持续时间长达三个星期，多达 8.5 万台分布在世界各地的计算机被劫持用于实施攻击，网络袭击的目标包括爱沙尼亚国会、政府部门、银行以及媒体网站，很多重要网站不堪重负陷于严重瘫痪，爱沙尼亚最大的银行汉莎银行的在线服务也一度中断。这次攻击规模广泛而且深纵，造成了巨大损失。

事后调查显示对爱沙尼亚发动网络攻击的来源分布在一百多个国家，尽管有一些线索显示攻击指令的源头位于俄罗斯境内，但是没有确凿证据证明攻击发起者是俄罗斯境内的组织或机构。俄罗斯政府也极力否认参与或策划了这次网络攻击。由于攻击规模大，持续时间长，网络瘫痪严重，一些媒体将之称为有史以来第一次国家之间的网络战争。

大规模网络攻击事件之后，爱沙尼亚共和国发布了世界上第一个《网络安全战略》，建立了国家网络防御分工协作系统，2014 年又出台了第二个《网络安全战略》，进一步增强打击网络犯罪和网络防御能力，提高网络教育水平和意识，促进关键网络基础设施的保护。



“锁盾”网络战演习（2014）

图片来源：北约网络合作防御卓越中心网站 http://www.ccdcoe.org

2008 年 5 月，爱沙尼亚和德国、意大利、西班牙、斯洛伐克、立陶宛和拉脱维亚等七个北约国家在首都塔林签署协议，建立一个北约网络合作防御卓越中心。这也第一个以网络战为主要研究对象、由多个国家政府共同发起成立的国际合作机构。卓越中心的核心宗旨是通过理论研究和政策建议，提高北约网络防御备战和协作能力，研究和撰写服务于北约的网络战国际法手册。卓越中心举办的“锁盾”和“十字剑”等一系列网络战演习，是世界上规模最大和最先进的国际网络防御演习。

2．网络武器

网络战是国家之间网络攻防力量的对抗，网络武器就是网络对抗的工具。网络战争没有硝烟，不会造成人员伤亡，网络武器的杀伤对象是关键基础设施、网络系统和数据。与常规战争使用战机军舰、枪炮导弹进行战场对抗不同，网络战攻防双方运用的武器是代码和程序，系统和基础设施中的漏洞也被制作成网络武器。

以攻防方式和作战对象区分，网络武器主要有以下三类：

第一类是病毒和木马。计算机病毒本质是一个程序或一段代码，它通过修改代码的方式，将自身代码植入其它软件、程序和文件之中，并隐藏起来。病毒发送者通过预先设定的条件，激活预设任务或继续将病毒代码植入更多软件、程序和文件，从而形成单机或网络系统的病毒感染。计算机病毒具有传染性、隐蔽性和破坏性等特点。攻击者使用病毒武器可以执行多种作战任务，包括瘫痪敌方计算机网络系统，阻隔敌方信息传递通道，以及修改或摧毁敌方数据等等。

木马是一个软件或程序包，它通过隐藏在目标计算机系统内，在设定条件下激活自身，将目标计算机编程可，执行远程控制目标计算机、获取计算机控制权或发送数据信息等任务。木马进入目标系统通常有两种方式，一种是线下或线上进入目标系统进行安装，另一种是诱使目标计算机系统的操作者在不知情的情况下点击链接，执行安装程序。

相比较而言，木马的功能更复杂，可执行操作更加全面，攻击能力更强，但隐蔽性和传染性不如病毒，侵入目标系统的难度也更高。病毒强调其传染性和破

坏性，而木马强调其受控接受指令和执行远程任务。从网络武器的角度来看，病毒和木马的共性是都具有很强的隐蔽性，隐藏性越好，应用就更广泛，攻击成功率就越高。

第二类武器是系统漏洞。网络攻防部队的首要任务是熟悉计算机和网络系统，寻找其中的安全短板和漏洞，并加以利用。因此，掌握可实施网络攻击的系统漏洞的多寡，就成为一个网络部队攻击力的重要指标。同样，发现自身军事指挥和控制系统、国家关键基础设施、重要网络系统的漏洞并及时加固，是网络部队提升防御能力的重要内容。

网络部队的技术专家不断地扫描和探测敌方和己方的网络，发现敌方网络系统中的漏洞，尽快开发出攻击软件，在需要时发动攻击，这种攻击不论成功与否，往往都是一次性的，因为敌方会很快发现自身系统的漏洞，并加以封堵，所以一次性使用是漏洞型网络武器最重要的特点。另外，由于通过漏洞发动攻击意味着可以直接绕过网络系统的防御措施，故可以实施更大的破坏。故漏洞型网络武器是“杀手锏”，网络战攻防双方都不会轻易使用，往往被开发成可以定时发射的攻击武器。

第三类是电磁脉冲武器。电磁脉冲武器是通过从物理上破坏网络基础设施和终端的正常运行，从而达到破坏终端、瘫痪网络、阻断系统运行和信息传播的目的。电磁脉冲武器是针对网络空间对电磁环境的依赖性和敏感性而研发出来的，大自然中的雷电可以实现短时间和大功率的电磁释放，对电子设备和网络环境的信号传输形成巨大干扰，甚至造成设备损毁。电磁脉冲武器也是通过大功率电磁脉冲的定向和集中释放，干扰电磁环境和破坏信息终端，使敌方的眼睛和耳朵失能，从而形成战场上的信息优势。

电磁脉冲武器主要针对作战指挥和控制系统，最大化地削弱敌方作战能力，因而常常用于信息化战争条件下的协同作战。而随着世界各国武装力量和作战部队加速信息化和网络化，干扰和破坏敌方电磁环境，同时增强己方网络基础设施和作战终端免受电磁破坏的损伤，成为制胜信息化战争和网络战争的关键。

3．网络军备竞赛

网络战是一种新型战争形态和作战方式，为了打赢网络战，毫无疑问必须

先建立一支网络部队。各国发展网络部队的时间和目标各不相同，一些国家将发展网络作战能力当作综合军事能力不可或缺的组成部分，一些国家看到网络战作为小国、弱国对抗大国、强国的非对称优势，还有一些国家为了避免遭受其他国家网络攻击，侧重建立防御性网络作战能力。

美国是世界头号军事强国和网络发源地，有最庞大的计算机网络系统和最发达的网络技术，其军事系统对计算机网络的依赖也最强。美国武装部队拥有 200 多万台计算机和 1 万多个局域网。美国国防部绝大部分数据通信是通过互联网信道进行传输的。美国军方和联邦决策层都非常重视网络战，尤其是网络空间的防御作战，从 20 世纪 90 年代就开始投入巨资，筹划和发展网络防御部队。美国国防部认为，网络战场对于传统军事实力无法与美国抗衡的敌对国家具有吸引力。他们不需要花上数十亿美元打造先进战机，只要培养一批高水平的黑客，就可能瘫痪美国金融体系、通讯及基础设施。很多国家都很清楚这一点，因此加紧研发网络攻击能力。一些国家和非国家组织网络攻击水平已经很高，能够威胁美国国家关键基础设施和重要网络系统的正常运行。因此美国首先把发展网络防御能力作为优先考虑。当然，五角大楼也在积极开发网络攻击能力，并且已经应用于现实作战。美国军方和情报部门已经建立了世界上最庞大的网络武器库，拥有一举摧毁很多国家计算机网络系统的能力。

“三位一体”的美国网络司令部、国家安全局、中央安全局

图片来源：美国网络司令部网站 http://www.cybercommand.mil

俄罗斯军方认为，网络战是仅次于核战争的军事威胁，因此把防止和对抗网络攻击提升到保卫俄罗斯国家利益和国家安全的高度。早在 2000 年，俄罗斯《国家信息安全条令》就明确了国家在信息和网络对抗上的立场，制定了一些确保国家安全和网络安全的具体措施，如加强关键信息基础建设和重要信息的保护，建立网络监控系统，加强网络安全防范等。该条令为俄罗斯加强网络战研究与发展网络战力量定下了基调，强调网络战要主动出击，占据先机，一招制敌。限于经济实力，俄罗斯重点开发可破坏或降低敌方电子和信息系统效能的网络武器，如能够远距离无线植入敌方系统的病毒，以对直接打击敌方军事指挥和控制系统。

日本防卫厅认为，随着军事指挥和控制系统的计算机网络化程度提高，自卫队遭受网络攻击的可能性增大，而一旦遭到系统感染病毒或黑客入侵，指挥和控制系统可能会陷入全面瘫痪。2000 年 10 月，日本防卫厅决定在防卫力量整备计划中加入网络战研究，研究如何侵入敌方电脑、破坏其指挥的通信系统、以造成敌方混乱。此后日本自卫队抓紧组建信息战部队，专门从事网络攻防，并将网络战武器的研究开发作为自卫队防卫计划的重点，并出现了在国家正常化的口号下，建立网络自卫队的声音。

韩国国防部将网络战的重点放在与朝鲜方面的网络攻防上。2010 年，韩国国防部宣布正在研发一种复杂的网络战病毒，目的是破坏朝鲜的核军备项目，并称这是韩军大型网络战计划的一部分。同时，韩国政府、军方和社会都对来自朝鲜方面的网络攻击非常警惕。因此，韩国网络部队建设有两大任务，一是保护国家关键基础设施，应对外部网络攻击，二是服务于朝鲜半岛无核化，如通过网络途径获取朝鲜核进程的情报，以及发展网络武器等。

上述几个国家网络部队启动较早，目标明确，走在了前列。世界此外，法国、德国、印度等国也都在加强网络战研究与网络部队军力建设，均已基本形成了各自的网络战指导思想，推出网络攻防力量发展规划，并开始招兵买马，培养高水平网络战指挥官和战士。可以预见，随着网络技术的进一步发展和广泛运用，世界主要军事强国在网络战领域的竞争将更加激烈。

4．网络军备控制

网络军备竞赛给网络空间的和平与稳定，以至人类社会的发展和未来形成了

重要威胁。一些有识之士提出应当在国际间进行网络军备控制，防止网络武器的扩散，以免人类遭遇数字领域的杀戮和灾祸。

中国政府在2017年《网络空间国际合作战略》中明确指出，“网络空间加强军备、强化威慑的倾向不利于国际安全与战略互信。中国致力于推动各方切实遵守和平解决争端、不使用或威胁使用武力等国际关系基本准则，建立磋商与调停机制，预防和避免冲突，防止网络空间成为新的战场。”中国一贯反对网络空间军事化，反对网络军备竞赛，在联合国等国际场合提出限制网络武器的研制和使用。

军备控制是国际社会对各国军事装备的发展、试验、部署和使用的限制。其对象是军事装备的发展，包括研制、试验、生产、装备、部署、使用等环节的活动，是对军备整个生命周期的关键环节的技术指标、数量等级的限制。二战结束以来，国际社会在常规军备和和核军备方面形成了多边国际条约、双边协定、单边承诺等多层次的军备控制体系，如《禁止核武器条约》,《美苏削减战略武器条约》，蒙古无核区、中东、东北亚、北欧等无核区承诺等等，国际军备竞赛一定程度上得到了有效控制。

以此对照网络军备控制议题，网络能力可以理解为研发、制造、部署和使用网络武器的综合能力。网络军备控制即是相关国家在这些环节上共同约定，限定网络军备的数量、性能和使用等。具体而言，研发阶段：需要资金、技术、人员的准备和投入，技术和人员方面需要配备数学、通信、软件、语言等方面的专家。生产阶段，需要获取相应的设备、芯片、代码、算法等，并确定杀伤范围和等级，以及针对目标系统的环境和加密体系进行优化。部署阶段，网络武器包括前沿部署和分布式部署，这是一个网络武器实现功能化的过程，钓鱼软件使用就需要获取目标对象的个人背景、社会关系，以诱使对象落入圈套，即基于社会工程的攻击。使用阶段，网络武器的使用需要获取信息、外交协调、法律评估、公众舆论等全方位准备，对攻击对象、攻击范围和破坏量级等进行选择。

网络威慑也是建立网络军备控制的途径之一。和常规作战中选择打击对象一样，网络战也是把敌方的战略目标作为首要攻击对象，如军队指挥和控制系统，国家关键基础设施如交通枢纽和通信主干道等等。通过对这些战略目标的攻击，直接地影响敌方的战略决策和战略全局，以便迅速地达成战略企图。随着网络的

发展和军队情报信息的一体化，网络战的战略作用会越来越突出，这种战略地位的提升，使战略、战役、战术的界限进一步模糊，对抗将在各个作战层次上同时进行，并且对战略全局产生重大影响。

网络威慑的目标是使发展网络作战能力和开发网络武器无利可图，或没有获胜的希望，从而放弃发展网络军备的企图，或自觉限制网络军备的规模和数量。一方面，当己方网络作战能力形成压倒性的绝对优势，或能够给对方造成空前巨大的破坏时，网络战预期就成为对方面临的网络威胁。若在网络领域确实具有较强的攻击能力和优势，并且让作战对手相信这种能力和优势，就可以在政治、外交、经济和军事斗争中取得主动权。另一方面，遵循核威慑类似的形成路径，网络均势也可以带来双向网络遏制和网络威慑。正如核威慑的产生和演变遵循的规律，当敌对双方都具有确保侵入、瓦解、破坏对方网络的能力时，就可以带来双向的网络遏制，使得双方不得不在一定条件下遵守互不攻击对方网络的游戏规则，形成一个无形的安全阀，从而在国际上形成互不攻击对方网络的惯例、协议或公约。