基于信息系统的网络作战理论研究

Constructs of Information System-Based Network Warfare

李大光博士，中国人民解放军大校，国防大学教授（Dr. Li Daguang, Senior Colonel & Professor, PLA National Defense University）

恩格斯曾经提出："一旦技术上的进步可以用于军事目的并且已经用于军事目的，它们便立刻几乎强制地，而且往往是违反指挥官的意志而引起作战方式上的改变甚至变革。"[1] 当今信息技术的发展正在推动军事领域变革，网络技术作为信息技术的重要内容，正在推进战争向信息化战争形态转变。基于信息系统的网络作战作为信息化战争中重要的作战样式，对赢得信息化战争胜利具有不可替代的重要作用。

一、基于信息系统网络作战概念阐释

正如美国著名未来学家托夫勒所预言："电脑网络的建立与普及将彻底地改变人类生存及生活的模式，而控制与掌握网络的人就是主宰。谁掌握了信息，控制了网络，谁就将拥有整个世界。"[2] 在信息时代，计算机信息网络向全球的各个角落辐射，其触角伸向了社会的各个领域，正在成为当今和未来信息社会的联系纽带。重要的信息网络系统成为维系国家和军队的命脉和战略资源，一旦这些计算机网络系统被攻陷，整个国家的安全就面临着崩溃的危险。因此在信息化战争中，谁在网络空间的角逐中占据优势，谁就能占据二十一世纪战争的战略主动权。

所谓基于信息系统的网络作战，是指高度依赖于信息、信息系统和信息化武器装备，在信息网络空间展开的、对敌方的战争体系或作战体系实施网络摧毁和破坏、同时保护己方体系的攻防作战行动。它是一种以信息主导、体系对抗、网电一体为主要特征的全新作战样式。网络作战的根本目的是通过对计算机网络信息处理层的破坏和保护，来降低敌方网络信息系统的使用效能，保护己方网络信息系统的正常运转，进而夺取和保持网络空间的控制权。网络空间的虚拟性、瞬时性和异地性等特征，赋予网络作战隐蔽无形、攻防兼备、全向渗透的优势；而网络作战简单易施、隐蔽性强等特点又使得它可以较低的成本获得非常高的军事效益。因此，网络作战所达成的作战效果是传统军事手段难以比拟的。

基于信息系统的网络作战的作战机理，是通过计算机信息网络系统对其他各相关系统进行有效控制，将计算机网络的信息优势转化为时空优势、决策优势和行动优势，从而产生和释放更大的作战效能。其内在的构成要素主要包括：计算机信息网络 — 以信息技术和计算机网络技术为主导；力量 — 网络作战部队、网络作战武器装备；战场 — 计算机网络空间；方式 — 网络化、一体化和精确化作战；目的 — 营造夺取战争胜利的军事、政治、经济、科技、外交、文化的综合优势。这种基于计算机信息系统的网络作战，向我们展示了一幅全新的战争画卷：作战空间和领域从传统的陆、海、空，向电磁领域向网络空间延伸，使未来战场空间呈现出由区域向全域、由地面向空天、由有形战场向无形战场全方位和全维域扩展的趋势。全空间和领域之间形成了网络化的相互关联、相互影响、相互渗透的体系关系，任何局部行动或对抗都可能牵一发而动全身，

触发信息主导下的整体对抗。如今，以计算机为核心的信息网络系统已经成为现代化军队的神经中枢，传感器网、指挥控制网、武器平台网等网络，将成为信息化战争的中心和重要依托。一旦计算机网络遭到攻击并被摧毁，整个军队的战斗力就会大幅度降低甚至完全丧失，国家军事机器就会处于瘫痪状态，国家安全将受到严重威胁。正因为计算机网络系统的这种重要性，决定了计算机网络系统必将成为信息战争双方攻击的重点目标，全新的以计算机网络为主要对象的计算机网络攻防战也随之出现并不断发展。在近几场局部战争中，拥有计算机网络优势的发达国家军队，以电脑病毒及黑客对其作战对手的网络及通讯系统实施攻击，完全主宰了网络空间，取得信息化战场优势，在极短的时间内瘫痪了对手的防空指挥系统，有力地支援其他战场作战。

随着社会形态由工业化向信息化转变，军事对抗的重心与焦点正由有形的地理空间向无形的计算机网络空间拓展，网络成为继陆、海、空、天、电之后的“第六维战场”。在这神秘的“第六维战场”里，虽然看不到刀光剑影的拼杀，听不见震耳欲聋的枪炮声，只有微弱的键盘击打声，但它却将各种作战信息即刻传输到散布于战场空间的任何作战单元，发挥出足以使敌方蒙受灭顶之灾的能量。这一点在科索沃战争中已初现端倪，巴尔干半岛的一些计算机专家有的单枪匹马，有的则联合俄罗斯等国的“黑客”，通过互联网对北约的军用计算机网络发动了进攻，对北约尤其是美国的军用计算机网络系统构成严重威胁，美国白宫的网站和“尼米兹”航母的指挥控制系统曾一度无法正常运行，迫使整个北约组织紧急采取了三项措施，局面才有所改变。[3]

二、基于信息系统网络作战指导思想与基本原则

基于信息系统网络作战作为一种作战样式，是敌对双方利用高技术手段来控制、割裂和破坏对方计算机网络系统和部件，达到摧毁和瘫痪对方战争机器的一种全新的信息作战样式，因此必须要有正确的作战指导思想和基本原则。

1. 基于信息系统网络作战指导思想

基于信息系统的网络作战不同于传统的火力杀伤作战，应对网络作战威胁必须首先从战略层面上树立积极防御的作战指导思想。与之相应，实施基于信息系统网络作战必须要树立“网络积极防御”的作战指导思想。这种“网络积极防御”的作战指导思想的基本内涵就是在战略上是防御的，在战术上是进攻的，强调在网络总体防御的态势下，寓攻于防，攻防结合，以积极的攻势作战达成防御目的，使网络作战在开局上是防御，但在具体的网络作战过程中又不局限于防御。坚持“网络积极防御”作战指导思想主要是基于如下几点考虑：

第一，防御性的国防政策，是树立“网络积极防御”作战指导思想的必然要求。在网络作战中，“进攻未必就是最好的防御”，积极防御的网络作战指导思想，体现着进攻与防御的辩证统一，体现着坚持自卫与后发制人的辩证统一，体现着打赢网络战争和遏制网络战争的辩证统一，当然也体现着我们网络技术水平较低与未来和平发展的辩证统一。

第二，在网络防御技术和能力上的差距与不足，是我们树立“网络积极防御”作战指导思想的现实要求。当今世界信息技术飞

速发展，但中国的信息网络技术还显得非常单薄，计算机及网络的核心技术仍然受制于人。最根本的平台核心，中国自己却无法把握，如 IT 技术至今仍处于“组装式生存状态”，操作系统的安全性、CPU 的安全性和加密技术的安全性无疑是最为重要的，而这些基础性的安全问题，我们均处于被动受控的情况下。由于国外电脑硬件、软件中可能隐藏着“特洛伊木马”，一旦发生重大情况，那些隐藏在电脑芯片和操作软件中的“特洛伊木马”就有可能在某种秘密指令下激活，或使民用电脑全部无法启动，或使我国政府、军事电脑网络、电信系统瘫痪，造成灾难性的经济、社会和军事后果。因此，我们必须坚持“网络积极防御”作战指导思想，防患于未然，做好防御准备，防止网络系统遭到瘫痪性的打击。

第三，网络攻击特点决定我们应该树立“网络积极防御”作战指导思想。当前网络战中普遍存在的“重攻轻防”思想，可能也主要是基于网络进攻易于防御的特点而产生的，但其偏颇之处也在于过分夸大了主动网络攻击的可操作性。传统作战中的经典论断是“进攻是最好的防御”，然而此论断可能不完全适用网络作战，例如，当己方第一波次网络攻击完毕或在己方发起第一波次网络攻击的同时，对方可以凭借稍强的防御能力启动应急方案施以精确反击；此时，如果己方自身的网络防御能力跟不上，则必会遭受对方的网络反击而遭到毁灭性的打击。因此，任何时候都不能因为网络防御太难就忽视防御，更不能因为网络防御的建设成本较高就将网络作战主要寄望于进攻。只有积极防御下的进攻才可能真正握有主动。因此，越是在网络防御很难的情况下，越要加大对网络防御的研究，建设和保持一支符合足够原则的网络战反击力量，保证在遭受对方首波网络攻击时仍能实时进行网络反击，这正是积极防御网络作战指导思想的内在要求。

2. 基于信息系统网络作战的基本原则

在争夺激烈的计算机网络战场上，计算机每比特的字节的作用往往比弹药更大，工业时代“打钢铁”的传统战法将被“打硅片”的方式取代。这种新的战争方式与传统的战争方式有很大的不同，因此其作战的基本原则也与传统的有所不同。

一是全域部署、整体对抗。计算机网络作战包括陆、海、空、天、电所有领域，贯穿于战役战斗的全过程，涉及军队、国家和地方的各种参战力量，涵盖信息获取、传递、处理等多个环节。因此，实施计算机网络作战必须全域部署，即在计算机网络作战中，要充分发挥信息网络系统的监控、监测和监视功能，在所有作战领域的空间进行全面部署，并对配置在各领域的计算机网络作战力量实施有效的协调和控制，并根据计算机网络作战不同阶段情况的变化，有重点地组织信息防护，集中使用建制和配属的计算机网络战武器于主要方向和重要时节，重点打击敌计算机网络系统的要害部位。

整体对抗就是将计算机网络作战纳入战略、战役和战斗的整体作战计划之中，围绕战略、战役和战斗的总体目标，统一计划和协调各种作战活动，综合使用各种力量，形成整体合力与敌在计算机网络系统开展对抗。因此，各级指挥员及其指挥机关，要从作战全局上统一筹划计算机网络作战行动；将各种计算机网络作战要素和力量有机组合，使之形成合力；把各种计算机网络作战的战法和手段有机组合，使之互相作用；把不同领域的计算机网络作战行动有机组合，使之

互相协调，从而形成对敌计算机网络作战的整体合力，才有可能夺取和保持计算机网络作战的主动权。为此，一要建立统一的计算机作战指挥协调机构；二要制订统一的计算机作战计划;三要周密组织计算机作战协同。

二是软硬一体、技战并重。“软杀伤”手段是指以干扰、压制、致盲、欺骗、削弱敌计算机网络系统功能为直接目的的作战手段，主要包括电子干扰、计算机病毒攻击、网络渗透、碳纤维弹攻击、虚拟作战、心理攻击等手段。“硬毁伤”手段是指以摧毁、破坏敌计算机网络系统、信息化武器装备，杀伤敌计算机网络作战人员等为直接打击目的的作战手段。主要包括常规火力打击、兵力破袭、电磁脉冲攻击、定向能武器攻击等。虽然运用“软杀伤”手段具有较为广泛的适用性、较强的欺骗性和较大的干扰破坏力，并且既可以是一种单独的计算机网络作战行动，也是实施“硬毁伤”的重要保障，但“软杀伤”手段不能对敌计算机网络系统、信息化武器装备等硬件设施及网络作战人员直接造成杀伤破坏效果，只能暂时使敌计算机网络系统和信息化武器丧失或降低能力。运用“硬毁伤”手段可长久地影响对方的信息作战能力，削弱敌整体作战能力，有利于组织“软杀伤”作战行动。同时,“硬毁伤”手段也只有在“软杀伤”手段的配合下才能更好地发挥作用。因此，将“软杀伤”手段与“硬毁伤”手段综合、协调运用，方能从根本上削弱以至摧毁敌网络综合作战能力。

技术与战术并重是由基于信息系统网络作战的规律决定的。关于技术对作战的重要影响，恩格斯曾说：“技术每天都无情地把一切东西、甚至是刚刚开始使用的东西当作无用的东西加以抛弃。……我们在作战的技术基础这样不断革命化的条件下，将不得不愈来愈多地考虑这种无法估计的因素。”[4] 在网络对抗领域中，将技术转变成战法，以技术推动战术同样更加重要，可以说整个网络对抗都是建立在一定技术基础之上的。但在注重技术的同时，也不能忽视战术，巧妙的战术不仅可以弥补技术差距，还能降低敌方的技术优势。所以，指挥者在指挥计算机网络对抗时，要二者并举，即在强调技术的同时也要充分发挥战术的作用。

三是攻防结合、以防为主。计算机网络进攻和防御是基于信息系统网络作战行动中不可分割的两个部分，单纯的进攻或防御都不能达成网络作战的目的。有效的进攻可以从根本上削弱甚至摧毁敌方的计算机网络作战能力，制止敌方计算机网络技术手段、装备和系统效能的发挥，从而相对增强我方计算机网络系统和信息系统的防护能力。通过防御，可以最大限度地降低敌对我方计算机网络系统的毁伤程度，使我方计算机网络进攻能力得以保持。因此，计算机网络作战必须贯彻攻防结合的原则。

以防为主是基于“网络积极防御”作战指导思想的作战原则。这是因为我们的主要战略对手具有较高的网络作战技术和手段。记得在 2001 年 4 月的中美撞机事件发生后，美国黑客也对中国发起了一场网络大战。尽管中国黑客高手奋起还击，但是由于中美在技术等方面的差距，我们在这次网络大战中损失惨重。中国青少年发展基金会网、西安信息港、中国科学院理化技术研究所等众多网站遭到攻击，一些大型门户网站也相继被“黑”，数据或被盗窃或被删除，引发了泄密、数据错误等问题，有的甚至是整个系统陷于瘫痪。因此，我们必须清醒地认识到，与美国等强大作战对手相比，我军的计算机网络技术及其武器装备还比较落后，而且这种状

况在短期内还得不到根本改善，因而还不具备在全时域、全空域与对手较量的能力。网络进攻作战只能在重点方向、重要时节，选择关键性的目标进行。这些都从客观上要求我们必须确立“攻防结合,以防为主”的思想。为此，一要同时做好网络进攻和防御两手准备；二要严密组织网络信息防御；三要选择技术精、作风硬的专业骨干，集中性能好的网络战武器，在主要方向和关键时节对敌实施突发性网络攻击。

四是分散部署，协调使用。自古以来，集中兵力一直被兵家视为取胜的法宝。从集中兵力的实质来看，集中兵力就是为了集中火力。因为过去的火力不够准确,威力不够大，才使得通过集中兵力的方式集中火力。由于网络把分散在世界各地、部署于陆、海、空、天的所有武器系统和指挥体系都联接在一起，便具备了将所有分系统综合集成为大系统的能力。无论坦克、飞机、舰艇和卫星怎样分散部署，无论这些武器身在何处，只要想用它来打仗,随时调用都能够做到“指哪打哪”，实施精确打击。因此，在网络作战条件下，各种力量特别是计算机网络系统的节点可以分散部署。这是计算机网络技术和网络化战场发展的必然结果。

在网络化战场中，作战平台远程化使得协调使用火力更容易，这种火力协调使用更有突然性。在网络系统内的各种作战平台，既包括陆、海、空、天、电的武器系统，也包括远、中、近的武器系统，所有这些都可对目标实施协调使用，集中打击。这样，依靠网络力量无形中就增加了火力的打击威力。一方面是由于武器的射程日益增大,比如，战斧式巡航导弹射程达 1300 公里，使得它可以打击 1300 公里远的目标；另一方面，由于计算机网络系统与武器以及武器系统之间互相联结构成“系统集成”，使得火力协同变得容易，这使得当敌人遭打击时，很难辨别攻击是来自陆上、海上还是空中。而由于网络的四通八达，利用网络使指挥官可以根据战况变化更容易实施超越指挥。同时，由于在网络中的信息共享，不同兵种、不同级别的部队相互间的协同作战也更加容易。此外，在网络化战场中，由于火力协调作用替代了传统的兵力集中，打击对象不再是通过消灭敌有生力量来消灭火力，而是通过破坏其“系统集成”和破坏其网络结构来削弱对方的火力。“协调使用”增强了单兵对战场全方位实时情报资源和火力资源的占有程度和利用程度，使单兵战场控制能力有了大幅度提高。

五是军民结合、平战一致。由于网络对抗大量涉及信息技术，而信息技术最具有军民通用的特性。因此,在组织信息网络作战时，要充分发挥人民战争优势，以国家信息基础设施为依托，充分利用和协调一切可以利用的网络作战资源，将军用网络系统和民用网络系统有机融合，高度集成，土洋结合，多种手段并用，力争夺取和保持网络作战的主动权。贯彻“军民结合”的原则，首先，要把国家的网络基础设施，特别是作战地区的民用通信、邮电、能源等网络信息设施和已开发的民用网络技术成果直接用于网络作战，并动员和利用地方雄厚的信息技术和网络技术人才参战，以弥补部队信息技术和网络技术人才之不足。其次，要充分利用许多国家和地区的军事网络系统都与因特网互联的特点，使我国相当数量的网上用户成为我军网络作战的“网络战士”，对敌发动一场网络上“人民战争”。此外，还要广泛利用国家的各种网络传播媒体和社会舆论，大量散布有利于我而不利于敌的信息，牵制和离间敌人的

行动。总之，要运用各种力量，采取多种简便易行、军民通用的战法，通过多种途径，多方位、多领域、全时空对敌展开网络人民战争,使敌陷入“人民战争的信息海洋之中”。

基于信息系统的网络作战，主要的作战都是在战时，但大量的准备工作是在平时，因此实施网络作战必须坚持平战一致。在网络作战中，平时敌方实施的计算机病毒及其它侵入，可能潜伏数年不被发现。因此敌方往往在战前就预先侵入，故防御一方必须不间断地开展网络防御建设，认真检查和评估所依靠网络设施的漏洞和易受攻击之处，预测潜在敌人可能采取的破坏行动，有针对性地预先采取必要的防御行动。而作为进攻者，侵入一个网络往往仅是时间问题，所以平时就提前研制侵入方法，进入网络并潜伏其中，那么战时就能从容对敌实施攻击。因此，必须坚持平战一致原则。

三、基于信息系统的网络作战攻防理论

基于信息系统网络作战与传统作战方式一样，也包含进攻和防御两个基本方面。但无论是网络进攻方面的理论还是网络防御方面的理论，都与传统的作战理论有所不同。

1．基于信息系统网络进攻作战理论

网络进攻是指通过侵入敌方计算机网络系统，窃取、修改或破坏敌方信息，散布对敌方不利的信息，或破坏敌方网络系统的硬件和软件，从而降低或破坏敌方网络系统的作战效能。它是利用敌方网络系统自身存在的漏洞或薄弱环节，通过网络的指令或者是专用的软件进入敌方的网络系统进行破坏，或者是使用强电磁武器摧毁它的硬件设备，通俗的说法叫“破网”。实施破网攻击的前提是破解敌方网络系统的“安全阀门”，并发现网络系统存在的安全漏洞，然后采取相应的方法进行攻击。在网络时代，军用网络系统已经成为高技术战争的神经中枢，一旦网络系统遭到攻击，整个军队的战斗力就会降低甚至丧失。因此，是否具有网络战能力，尤其是网络进攻能力，将成为衡量一个国家军事实力的重要标志。

网络攻击模式。基于信息系统的网络作战攻击模式主要有三种：一是体系结构破坏模式，即通过发送电脑病毒、逻辑炸弹等方法破坏敌方网络系统的体系结构，造成敌方指挥控制系统的结构性瘫痪。二是信息误导模式，即向敌方网络系统传输假情报，改变敌方军事网络系统功能，可对敌方决策与指挥控制产生信息误导和流程误导。三是综合破坏模式，即综合利用体系破坏和信息误导，并与其他信息作战样式紧密结合，对敌方军事网络系统特别是指挥控制网络系统造成多重杀伤功效。

网络进攻战法。网络作战具有与传统作战不同的作战方法，具体主要包括以下一些内容：一是网络虚拟战。网络虚拟战是运用计算机成像、电子显示、语音识别和合成、传感等技术为基础的新兴综合应用技术，在网络战场以虚拟现实的形式实施的网络作战。二是网络破袭战。网络破袭战主要是通过摧毁敌方网络系统的物理设备达到瘫痪敌方军事网络系统的目的，一般它是采取突然袭击的方式，用以摧毁、破坏敌方电子网络系统，可分为火力破击和电子破击。三是网络病毒战。网络病毒战是把具有大规模破坏作用的计算机恶性病毒，利用一定的传播途径，传入敌方雷达、导弹、卫星和自动化指挥控制中心的计算机信息情报搜集系统中，在关键时刻使病毒发作,并不断地传播、感染、扩散，侵害敌系统软件，使其整个系统瘫痪。

网络攻击方式。网络作战攻击方式是指利用敌方网络系统的安全缺陷，窃取、修改、伪造或破坏信息，以及降低和破坏敌方网络使用效能而采取的各种攻击方式。由于计算机硬件和软件、网络协议和结构以及网络管理等方面不可避免地存在安全漏洞，使得网络攻击方式有多种多样。一般常见的网络攻击方式主要包括：节点破坏、拒绝服务攻击、入侵攻击、物理实体攻击、网络欺骗攻击、邮件攻击和信道干扰等。

2．基于信息系统网络防御作战理论

基于信息系统网络防御作战是以积极防御的作战思想为指导，为保护和增强己方实时、准确、可靠的收集、处理及利用信息的能力，而采取的一系列连续性的军事行动。它是通过对已方的网络系统采用各种防护措施，防止敌方的网络入侵和其它形式的破坏活动,保护已方网络系统的正常工作和使用。网络攻击的隐蔽性、破坏性和攻击方式的多样性,使网络防御成为网络用户的头等大事。特别是随着国家对计算机网络的依赖越来越大而导致计算机大面积联网，网络遭到攻击的危险也随之增大。因此，在“无网不在”的信息社会，只有扎实地搞好积极防御，才能确保在网络作战中赢得主动。

网络防御模式。网络作战防御是在联合作战的信息防御作战中，为保护己方计算机网络系统免遭干扰和破坏而采取的所有网络防护行动。通常以防止敌方网络渗透、病毒侵害、预置陷阱为主要内容，采取技术与战术相结合的措施，运用电磁遮蔽、物理隔离和综合防护等模式进行防范，以确保己方网络系统安全。具体的防御模式有三种：一是电磁遮蔽，就是通过各种有效的技术和战术手段，减小己方电磁辐射的强度，改变辐射的规律，使敌人无法侦测己方计算机设备辐射的电磁信号，从而保护己方计算机信息系统的信息安全。二是物理隔离，就是采取各种技术手段，防止计算机病毒侵入己方网络系统。三是综合防护，就是指采取各种措施，加强对黑客攻击和新概念武器等的防护，尽量减少己方网络系统在敌方攻击中的损失。

网络防御战法。在实施网络对抗过程中，除了要综合采取各种攻击技术与战法对敌实施有效网络攻击之外，也必须要采取有效的技术与战法对己方的网络实施防护，达到攻守平衡，这样才能确保国家和军队的网络系统安全。目前，网络防御的基本战法主要有如下内容：一是隐真示假，就是采取藏匿规避等方法，避敌侦察干扰。二是疏散配置，就是分散、不规则地配置网络各要素，削弱敌火力毁伤能力，从而达到以局部损失换取整体网络安全的目的。三是管理防护，就是通过加大对计算机网络系统的管理，达到保护计算机实体及其网络系统安全的目的。四是硬件保安，即严把硬件安全关，防止“病从口入”，如尽可能利用本国生产研制的计算机“软”、“硬”件，严把网络设备进口关。

网络防御方式。网络在拥有先进性的同时，也伴随着可侵入、可破坏、可干扰和可击穿等脆弱性。必须积极防御，努力寻求计算机网络安全防护措施。一是组成电磁频谱屏蔽层。由于无线电波所具有的特性，决定了它作为网络重要信息传输媒介时，具有易截获、易暴露、易泄漏等不利的方面。所以，网络防护必须要设法对电磁频谱进行有效保护。二是形成计算机网络安全保护网。计算机网络安全保护网是为网络建立和采取的技术和管理的安全保护，保护计算机硬件、软件和数据不因偶然和敌方攻击等原因而遭到

破坏、更改和泄露，从而保证网络连续正常运行。三是构建计算机网络“防火墙”。即为确保计算机网络安全而采取的保护措施、网络安全体系设计、安全软件开发与应用等行动。

四: 结语

制网权已成为信息化战争对抗双方争夺的新焦点。在信息时代，计算机信息网络已开始向全球的各个角落辐射，其触角伸向了社会的各个领域，正在成为当今和未来信息社会的联系纽带。重要的信息网络系统成为维系国家的命脉和战略资源，一旦这些网络系统被攻陷，整个国家的安全就面临着崩溃的危险。在军事领域，未来信息化战争将是建立在信息网格基础上的网络化战争，以计算机为核心的信息网络已经成为现代军队的神经中枢，传感器网、指挥控制网、武器平台网等网络，将成为信息化战争的中心和重要依托。未来战争，谁在网络空间的角逐中占据优势，谁就能占据二十一世纪战争的战略主动权。一个备受关注的作战新概念 —“制网权”，便伴随着一个旨在谋求对整个信息领域最高控制权的宏伟军事蓝图登上人类战争的舞台。♣

注释:

1. 马克思恩格斯军事文集，第 1 卷，第 17 页，北京，战士出版社，1981。
2. 常名：网络化战场与制网络权，解放军报，1996 年 9 月 24 日。
3. 李大光：制网权成为信息时代战争的新焦点，解放军报，2010 年 5 月 27 日。
4. 马克思恩格斯军事文集，第 2 卷，第 488 页，北京，战士出版社，1981。

参考文献:

[1] 李大光著：《基于信息系统的网络作战》，解放军出版社，2010 年 7 月版。
[2] 王力等编著：《病毒武器与网络战争》，军事谊文出版社，2001 年 1 月版。
[3]《解放军报》，2000—2010 年相关文章。

李大光 (Dr. Li，Daguang)，国防大学军事后勤与军事科技装备教研部教授，博士，大校军衔，从事军事科技装备与国家安全的教学科研工作。孙子兵法研究会理事，中国科普作家协会会员。著有《太空战》、《论制天权》、《21 世纪军事发展大趋势》、《国际机制与区域安全》《基于信息系统的网络作战》等专著，发表学术论文千余篇，数百万字。