# 21世纪 超级战争杀手
# ——网络战

宋秀昆

网络战，是敌对双方针对战争可资利用的信息网络环境，围绕“制信息权”的争夺，为达到赢得战争的最终目的而展开的对抗活动。作为世纪之交的一种全新的作战模式，网络战在1999年的科索沃战争中已显示出神奇的软战魅力，受到各国军事家们的广泛青睐。根据近期局部战争中外军网络战的实践经验及未来战争的发展趋势，新世纪网络战将具有以下4个主要特点：

## 依赖性

随着计算机技术的飞速发展以及在军事领域的广泛运用，敌对双方将依赖绵密的各种信息网络运转它们的战争机器。未来战争的胜负已不再取决于谁在战场上投入的资源、人力和物力的多少，而取决于谁对战场上的“制信息权”掌握得好或差。对信息权控制的程度，将直接影响到对有限的人力、物力资源运用的效能。而在网络空间，对信息的收集、传递和加工处理等哪一个环节也离不开计算机。因此，网络战中敌对双方攻击和保护的重点目标都是军队的神经中枢——计算机网络系统。敌对双方交战最初将在网络上展开，并在网络上一决高低。双方都通过破坏敌方计算机系统的软、硬件支持系统，力图扰乱、削弱、瘫痪敌方的武器系统、控制系统、决策系统，造成敌方信息控制系统的紊乱、通信联络中断、指挥失灵、武器失控、秩序混乱，使敌方军队指挥官成为“聋子”、“瞎子”，使敌方成为“瘫子”、“呆子”，丧失战头能力，并且想方设法确保己方信息系统的畅通和对“制信息权”的可靠控制与掌握，以便为夺取战争的最终胜利创造最有利的条件。网络战是尖端技术作战，是技术、知识密集型作战。网络战技术涉及到网络软件侦察与反侦察技术、网络软件攻击与反攻击技术、网络软件冒充与反冒充技术、网络软件控制权易位与反易位技术等。没有网络技术就无法作战，网络技术不精就不能胜敌一筹。谁掌握了最先进的网络技术，就有可能成为最后的赢家。当然，网络系统对技术过分依赖的结果也具有任何事物所有的二重性，即必然造成网络系统面对敌方进攻而难以察觉的脆弱性。敌我双方不仅要挖空心思研究攻击对付网络系统的措施，而且也要千方百计地寻找和利用保护自己网络系统的防御技术，比如电子盾牌、电子闸门、电子宪兵、自我修复等日新月异的计算机网络防御技术。

## 越限性

现代通信技术与手段的飞速发展，使网络覆盖面

---

扰机，由美国陆军信号战实验室研制。该干扰机由天线、干扰机和电池组成，具有体积小、重量轻(2.3kg)、容易携带、操作简便、隐蔽坚固、防水性能好等特点。可由人工摆放在预定目标附近自动实施干扰，用来阻塞敌甚高频和特高频通信。其工作频率范围为20~30MHz，输出功率为10W。干扰机的尺寸较小，机内装有电子自爆装置。

## 六、炮射通信干扰机

这是美国陆军信号战实验室研制的一次性使用的阻塞式通信干扰机。该机由155mm榴弹炮发射，每颗炮弹内装有6台干扰机，发射后炮弹在飞行过程中弹底板分离，干扰机根据预先调整好的定时一个接一个地弹出。脱离弹体后，在旋转离心力作用下，张开4个稳定翼片制止干扰机旋转，同时放出一条长约1m的尾伞，使干扰机以4m/s的速度着陆而插入地下，几秒钟后自动发射无线电并接上地线，开始对敌通信网实施干扰。这些遍于战场的小型干扰机可连续工作几个小时，几乎可使敌各种通信方式的战术通信都受到干扰。该干扰机的特点是成本低、使用隐蔽、干扰数量大、范围广。

迅猛扩大，将全球亿万计算机拥有者网罗进了网络世界。四通八达、纵横交织的全球互联网络，不断将更多的军用与民用计算机系统联为一体。军用信息资源已经开始融入社会网络系统；同时，民用信息资源也不断地向军用网络渗透。军、民网络之间通过各种电话、电报、图像、数据网络（系统）建立了千丝万缕的联系，从而正在形成一个没有国界之隔、没有网民身份之分的网络世界和“网民皆兵”的网络空间。可以预料，今后军事领域的抗衡，一定会波及这个网络空间，并扩展成为整个社会大系统的全面抗衡和较量。任何掌握网络传输技术、精通计算机知识和先进的解码技术的机构或个人，都可能成为一名“网络勇士”，去网络战场“冲浪”。作战双方通过发动网民，群策群力，依靠“网络勇士”，可能在全球任何一个角落、于任何时间通过各种接入网和计算机，进入敌方多层加密的网络系统，对敌方关系其国计民生和战略资源生长的各种领域内的计算机系统、入网设备或数据库进行渗透，修改、窃取其网络系统内部及数据库的关键资料，截取或扰乱敌方对重大国计民生系统和军事指挥系统的指挥控制权，或集中“网军”兵力阻塞、控制、改变网络中关键输出（输入）接口的信息传输，破坏其指挥中枢和武器系统，实施隐蔽或公开、跨国界、超越传统战争理念的崭新的网络战。敌方为了抗衡对方对其信息网络的打击，也许能用软、硬手段破坏对方建立在作战区域内的网络干线，以阻击对方战区内的电子攻击信息流进入“敌占区”的网络发挥作用，但是却难以破坏散布于战区之外各个角落，甚至就在敌方领土网络上为对方正义之战而对敌电子系统攻击的“网络勇士”们所利用的它自己的“网络通道”。正是网络战所具有的这种超越一般战争理念界限的特点，可能使“网络战”最大限度地容纳各种人员在各种环境下对敌作战，达到一般作战方式不可能达到或不能迅速达到的预期作战目的。

## 潜隐性

网络战中，由于“网军”可以在全球任意有网络互联的位置上于任意时间部署自己的“网络勇士”，因此，敌方很难发现对方网兵部署的位置及时间并予以消灭或控制，一旦发现之时，可能已对其网络空间造成了很大破坏。同时，由于军民网络兼容一体化，在任何一个节点都可以展开对敌方网络系统的攻势行动。这使以各种控制措施对付网络攻击难以奏效，战争的突然性增大。利用民用网络对敌方展开攻击，还能提高己方军事行动的隐蔽性，做到悄无声息地开战，行动方式包括：网络侵入，窃取情报；修改、转移数据，阻塞、改变信息流，制造混乱；截取指挥控制权，误导敌人；传播计算机病毒，瘫痪系统节点；预设“逻辑炸弹”，伺机破坏等等。网络战既可以在公开敌对的时期进行，还可以在战前、战中秘密进行；可以间断或按规定的时间进行，也可以每天每时不间断地进行；可以进行信息威慑战，也可以进行实体破坏战。因此，网络战在实施上具有很强的隐蔽性、灵活性，最能够使敌方难以预料，防不胜防，疲于应付，被动挨“打”。

## 广泛性

网络战具有实施范围、实施时间、实施人员、攻击目标的广泛性。这主要因为：一是作为连接军事与民用各行业与各领域的计算机网络，有着广阔的覆盖空间，同时由于网络信息交流和网络资源相互利用的需要，使很难对其加以限制或约束；二是每一个体，在世界任一角落，都可以极其隐蔽地利用因特网站进行破坏活动，而攻击手段并不复杂；三是参与网络战可有多种途径，且花样繁多，包括利用公众电话网、各种专用数据网、贸易手段、派遣敌特攻击等，而接入网络的媒质却可以是有线、无线或光通信系统等常用通信手段；四是实施网络攻击的时间可以在战时，也可以在平时任意时间，极其灵活。组织良好的网络先机攻击，或许可以促成“不战而屈人之兵”的最佳效果，使军事实力相对弱小的国家避免失败；五是网络攻击发起的地点可以在战区内，也可以在战区外，；可以在本国国土上，也可以在敌国国土上，或世界任何一个有网络连接的地方。参战人员可以是军事员或非军事人员、网络专家或一般网络爱好者；六是网络攻击与防护的的目标不仅仅是军事网络本身，它还覆盖今日之金融网络、商贸网络、交通网络、电信网络、科研网络等各种信息应用领域，任何国家尤其是发达国家在这些“网域”内存在着巨大的经济、政治、军事利益。近些年来发生的网络病毒泛滥和网络黑客破坏计算机系统的许多实例已经证明，这些网域是最易遭受信息攻击的领域，并越来越引起军事家、科学家的高度重视。他们甚至断言，未来战争破坏力最大的已不再是核武器，用计算机进行网络战争比用核武器进行热核战争更加有效。要摧毁美国，或许只要用高级科学技术扰乱其计算机系统 1s 就能达到目的。由此可见，网络战实施的广泛性必将使网络对抗成为新世纪的一种最突然、最难对付、破坏性最大的崭新作战形式，成为军事实力和综合国力相对较弱的国家战胜强敌的法宝。