

网络战：看不见硝烟的"第五战场"

你每天用手机刷视频、用电脑上网课，可能已经习惯了"网"的存在。可你大概没想过：军队也离不开网。现代的军舰、战机、导弹，甚至一颗卫星，背后都有成百上千台计算机在调度；前线的命令、后方的补给、雷达传回的图像，全都在看不见的光缆和电波里跑。网络，早就是现代军队的"神经"。而正因为这根神经太重要，有人就想方设法去掐断它、扰乱它、窃取它——这，就是网络战。

网络战，通俗地说，就是利用计算机网络进行的攻击与防御。它和我们在电影里看到的爆炸、枪炮很不一样：没有火光，没有轰鸣，攻击者可能坐在几千公里外的房间里，敲着键盘就能让对方的一座城市停电、让一家银行瘫痪、让一套防空系统变成"瞎子"。它的核心目的，往往不是夺人性命，而是让对手"看不见、听不到、指挥不灵、打不准"。

这场看不见的战争，是什么时候开始变得这么重要的呢？从上世纪九十年代起，世界各国的军队陆续把指挥、通信、侦察、后勤都搬进了数字系统。这带来巨大便利，也带来巨大风险：一旦这些系统被人攻破，整支部队就可能瞬间"失聪失明"。于是，网络从"工具"变成了"战场"。今天，人们常把作战空间分成五个领域——陆地、海洋、天空、太空，以及"网络空间"。网络，被称为继陆海空天之后的"第五战场"。

网络战的手段很多，但最常见、也最容易被普通人理解的有几种。第一种叫"拒绝服务攻击"，英文缩写 DDoS。打个比方：一家小店本来一次只能接待十个客人，突然涌来一万名捣乱的人堵在门口，真正的顾客就进不去了。攻击者用成千上万台被控制的电脑，同时向一个网站或服务器发送海量垃圾请求，把它彻底淹没，让正常服务瘫痪。2007 年，欧洲小国爱沙尼亚因为搬迁一座历史雕像，遭到了持续数周的大规模网络攻击，政府网站、银行系统、新闻媒体接连瘫痪，全国上下几乎"断网"，这是网络战走进大众视野的标志性事件之一。

第二种手段更隐蔽、也更危险，叫做"恶意软件"，也就是我们常说的电脑病毒、蠕虫。它悄悄钻进敌方电脑，潜伏、复制、搞破坏。这里面最有名的一个，名字叫"震网"（Stuxnet）。大约在 2010 年前后，这种特殊的程序出现在伊朗的纳坦兹铀浓缩工厂。它不走寻常路，而是通过 U 盘和内部局域网悄悄传播，专门寻找工厂里控制离心机的工业计算机。它让离心机在操作员看不见的情况下超速旋转、失控损毁，据公开资料，大批离心机因此报废。很多人把它称作历史上第一个真正用来破坏实体设备的"网络武器"——它不用一颗子弹，就重创了一座工厂。

第三种是"钓鱼"与窃密。攻击者伪装成可信的人或单位，发来一封看起来正常的邮件，诱使对方点开链接、输入账号密码，从而溜进内部网络偷走机密。第四种则是勒索软件：它把电脑里的文件加密锁死，逼对方交"赎金"才肯解开。2017 年，一种叫"NotPetya"的勒索程序从乌克兰蔓延到全世界，工厂、港口、医院接连中招，造成的损失极其惊人，后来被多国认定为一次国家背景的网络攻击。

网络战为什么让各国都这么紧张？一个重要原因是它"难找、难认、难防"。你被偷了、被黑了，往往要过很久才发现；而究竟是谁干的——是黑客个人、犯罪团伙，还是某个国家的军队——常常很难立刻说清。这种"灰色地带"的特性，让网络战常常在和平与战争之间游走，不宣而战，却又真实存在。正因如此，世界主要国家都开始组建专门的网络部队：美国早在 2010 年就成立了网络司令部；此后，越来越多的国家把网络能力写进了国防规划，把"懂网络"的军人当作和飞行员、舰长一样重要的角色来培养。

网络战也不是纸上谈兵，它已经多次出现在真实的战争里。2008 年，在高加索地区的一场武装冲突中，针对政府网站和新闻机构的网络攻击，几乎和地面的坦克推进同时打响，让对方在开战之初就陷入了"信息黑洞"。到了 2022 年的乌克兰战争，网络行动更是和导弹、火炮几乎同一时刻展开，多个部门的重要系统遭到能彻底擦除数据的恶意软件打击。这些例子说明，今天的战争，常常是从屏幕里先打响的。

当然，有攻就有守。保护网络，靠的是一套组合拳：把最关键的系统"物理隔离"，也就是不让它直接连上公共互联网，行内叫"气隙"；给数据加密，让即使被截获也读不懂；建立"态势感知"，像雷达一样随时发现异常流量；还有专门的"网络靶场"，让防御人员在虚拟环境里反复演练怎么应对攻击。可以说，今天守护一个国家，光有城墙和军队还不够，还得有人 24 小时盯着屏幕上那些跳动的曲线，守住那张看不见的"网"。

需要说清楚的是，网络战虽然厉害，但并不是"万能钥匙"。它能瘫痪系统、制造混乱，却很难单靠键盘就决定一场大规模战争的胜负；在真实的战场上，它几乎总是和常规的陆军、海军、空军行动配合着用。也正因为它太新，关于"网络攻击算不算战争行为""什么时候可以还手"这些规则，全世界到现在还在慢慢摸索、争论。

回过头看，网络战给普通人最大的提醒也许是：我们每天依赖的网络，既方便又脆弱。保护好密码、不随便点陌生链接、留意自己的信息安全，这些小事，其实也是在守护那片看不见、却无比重要的战场。

冷知识 - 人们把作战空间分成"陆、海、空、天、网"五个领域，网络是最后一个被公认的"战场"，直到本世纪才真正写进各国军队的条令。 - "震网"之所以特别，是因为它是少数被公开确认、专门用来破坏真实工厂设备的恶意程序，它攻击的不是电脑屏幕上的

文件，而是地下的工业机器。 - 有一类最坚固的防护叫"气隙隔离"——让重要电脑彻底不联网。可就连这种方式，也曾被一种会"听"电脑风扇嗡鸣声、或靠键盘指示灯闪烁来偷偷传数据的奇招绕过，让人不得不佩服攻防双方的脑洞。