Interdisciplinary Science Letters 交叉科学快报, 2018, 2(1), 19-25
Published Online March 2018 in Hans. http://www.hanspub.org/journal/isl
https://doi.org/10.12677/isl.2018.21004

Hans汉斯

The Fierce Cyber War

Bo Li[1], Xie Han[1,2], Wenxiang Hu[1,2,3*]

[1]Institute of Physical Organic and Medicinal Chemistry, Beijing Excalibur Space Military Academy of Medical Sciences, Beijing
[2]School of Chemical Engineering and Pharmacy, Wuhan Institute of Technology, Wuhan Hubei
[3]Space Systems Division, Strategic Support Troops, Chinese People's Liberation Army, Beijing
Email: *huwx66@163.com

Received: Dec. 15th, 2017; accepted: Jan. 1st, 2018; published: Jan. 8th, 2018

Abstract

As a new mode of war, cyber war is highly valued by governments and militaries. This article mainly collects the literature dates on the concept, characteristics, and real cases of "cyber war", as well as the construction situation of cyber war force in leading military powers across the world. And authors put forward the concept of "cyber soft atomic bomb" for the first time, aiming to provide foundations and references for future cyber war research in the 21st century.

Keywords

Information, Cyber War, Cyber Warfare Force, Cyber Attacks, Cyber Soft Atomic Bomb

风起云涌的网络战

李　博[1]，韩　谢[1,2]，胡文祥[1,2,3*]

[1]北京神剑天军医学科学院物理有机与药物化学研究所，北京
[2]武汉工程大学化工与制药学院，湖北 武汉
[3]中国人民解放军战略支援部队航天系统部，北京
Email: *huwx66@163.com

收稿日期：2017年12月15日；录用日期：2018年1月1日；发布日期：2018年1月8日

摘　要

网络战作为新的战争样式受到各国政府及军方的高度重视。本文主要是收集了文献上关于"网络战"概念及特点、网络战现实案例、世界军事强国网络战部队建设态势等方面资料，加以叙述，并首次提出"网

*通讯作者。

文章引用: 李博, 韩谢, 胡文祥. 风起云涌的网络战[J]. 交叉科学快报, 2018, 2(1): 19-25.
DOI: 10.12677/isl.2018.21004

络软原子弹”概念，为进一步研究21世纪未来网络战争提供借鉴。

关键词

信息，网络战，网络战部队，网络攻击，网络软原子弹

1. 引言

网络战也称网络信息战，或者网络空间战，是近年兴起的一种除陆、海、空、天战之外的新的第五维战争样式，是现代高技术战争的重要内容，是为干扰、破坏敌方网络信息系统，并保证己方网络信息系统的正常运行而采取的一系列网络攻防行动，正在成为现代高技术战争的一种日益重要的作战方式[1]。网络战旨在破坏敌方的指挥控制、情报信息和防空等军用网络系统，甚至可以悄无声息地破坏、瘫痪、控制敌方的商务、政务等民用计算机网络系统，达到不战而屈人之兵之目的。从某种意义上说，网络攻击可以说是穷国的“软原子弹”(第二次世界大战以后，谈原(子弹)色变，至今仍未改变，还将持续相当长的一段历史时期)，花费不大，硬件条件要求不高，经济不发达国家也可以大肆研究并占据一定的制高点，其杀伤力不亚于硬杀伤兵器，有时能让一支部队瘫痪，甚至一个国家瘫痪，在未来战争中将发挥愈来愈大的威力。

2. 各国网络战

2.1. 美军网络战

据说，美国正在秘密研发超级网络武器，地位相当于原子弹，这虽然有点夸张，但并非危言耸听。早在 2009 年 6 月，面临日益严峻的全球网络安全形势，时任美国国防部长盖茨正式下令创建网络军司令部，目的在于协调网络安全以及指挥网络战[2]。这是美军继上世纪末提出网络中心战概念以来，又一次率先提出的新作战概念。所不同的是，这一次美军不仅将这一概念停留在理论层面，而且很快将其落实到具体实施阶段。根据盖茨当天(6 月 23 日)签署的一份长达 3 页的备忘录，指出：“随着我们越来越依赖网络空间，再加上不断增加的网络威胁和漏洞，这对我们的国家安全意味着新增的风险。”

网络司令部的成立的必要性，基于已具备的利用先进网络技术进行渗透、监控、摧毁敌网络系统的能力和“制网络权”绝对优势，不仅需要研发越来越多的网络战武器，而且还急需制订关于如何运用这些武器的策略，因此必需成立网络司令部，应对日益增长的网络威胁势在必行，同时也是美军战略转型的需要。对目前分散在美国各军种中的网络战指挥机构进行一个整合，以更大地促进美军的战略转型——由传统战争转向一种从未有过的新型的网络战。

网络攻击频发。近年来，随着互联网及网络技术的普及，美国似乎成为世界上数字敌人发动网络攻击的中心。2007 年，仅公开媒体报道的对政府和私人系统的攻击次数就达 37,000 次。此外，还有约 13,000 次直接对联邦机构发动的攻击，80,000 次试图对国防部系统的网络攻击。据美国国会研究处的统计，网络威胁对商业和政府机构以及国家安全构成的危险还在不断增加，仅对商业造成的经济影响每年就超过 2260 亿美元。

网络司令部攻防兼备，绝非仅仅为了实施防御性行动。在2009年上半年的伊朗大选中，美国就曾利用手机和互联网发出大量的信息，这实际上完全是利用网络进行的一种信息攻击行动。此外，美国还多次对其它国家进行所谓的“网络制裁”，即停止某些国家和地区的某些网络服务。这从某种意义来说，也应该属于网络进攻行动。其实，美国官方在公布网络司令部的职责时，指出其将主要负责美国军队的网络安全和网络行动。“网络行动”显然是对“进攻”和“防御”两种行动的一种概念模糊化处理。结合美军利用网络组织的事实上的进攻性行动，美国在网络上的作战已经跨出防御范畴，演变为攻防兼备的行动方式。而现在网络司令部的组建，只是对整个网络作战功能的全面强化和提升。为了淡化这一目标，实际上，美国此前在舆论上已经做了大量铺垫——新闻媒体常常长篇累牍地报道美国受到网络威胁和黑客攻击，其中不乏公开针对中国、俄罗斯黑客的例子。从而造成网络司令部只是作为一个防御性作战指挥机构，是为了应对这些网络上的攻击而成立的假象。美军网络司令部表面上以防御性为主，实际上也干了许多攻击性的事件。

在伊拉克战争开始前，美国通过第三方把一批打印机卖给了伊拉克，并且在战争中通过无线电遥控激活了事先已隐藏在打印机芯片中的计算机病毒，破坏了伊拉克国内的计算机系统。

在海湾战争沙漠盾牌行动中，美军有上千台的PC机感染了“犹太人”、“大麻”等病毒，并已开始影响作战指挥的正常进行，美国从国内迅速派出了计算机安全专家小组，及时消除了病毒，避免了灾难性的后果。

在科索沃战争中，以计算机病毒攻击为重要手段的计算机网络战则更为激烈。南联盟黑客使用“爸爸”“梅利莎”“疯牛”等病毒进攻北约的指挥通信网络，致使北约通信陷入瘫痪。美海军陆战队所有作战单元的E-mail均被“梅利莎”病毒阻塞。北约在贝尔格莱德的B-92无线电广播网，以及在布鲁塞尔北约总部的网络服务器和电子邮件服务器，均连续受到计算机病毒的破坏。南联盟计算机专家在俄罗斯黑客的帮助下，曾造成美国海军“尼米兹”航母上的计算机系统瘫痪时间长达3个多小时。据战后权威机构评析，如果说在空袭与反空袭交战中，南联盟一直处于守势的话；那么，在网络战场上，南联盟却是处于攻势。

2.2. 俄罗斯网络战

与美国相比，同为网络大国的俄罗斯在网络战宣传方面则低调得多。那么俄罗斯网络战实力究竟如何？俄军网络战现状和发展趋势又是怎样的呢？

a) 起步早，理论功底深厚

受制于电子战水平和网络核心技术，俄罗斯在网络战领域实力不及美国，但事实上俄罗斯对网络战的理论研究很早就已经起步。早在上世纪90年代，俄罗斯就设立了专门负责网络信息安全的信息安全委员会，在2002年推出的《俄联邦信息安全学说》中，网络信息战更是被提升到新的高度，被俄军方称作未来的“第六代战争”。

俄军网络战理论认为，网络世界的战争将主要在以下四个层面展开：

1) 信息基础设施，也就是计算机和通信设施的物理连接，包括有线、无线通信设施、通信卫星、计算机等硬件设备；

2) 基础软件系统，包括操作系统、网络协议、域名解析等；

3) 应用软件系统，包括涉及金融、电力、交通、行政、军事等领域的软件系统；

4) 信息本身，也就是在网络中流通的所有信息。

在俄军看来，网络战是一种变相的突击手段，它能起到与传统火力突击相似的作用，可用于对敌实施直接军事打击。如今网络就像人的神经系统一样，已经延伸到世界各国的政治、经济、军事、文化等

各个领域。因此，通过网络战，俄罗斯可以在发动传统军事行动之前通过破坏敌民用网络来扰乱其正常的社会秩序，破坏敌方的指挥控制系统来降低敌军的反应能力，打击敌方军事和通信及其他关键基础设施以削弱敌作战实力从而进一步降低敌人对联合威胁的反应能力。

b) 基础牢，网络战潜力不俗

在网络信息安全领域，俄罗斯一直保持着世界领先的地位,这与其扎实的基础教育密不可分。俄罗斯在基础教育方面做得相当出色，计算机和数学等基础学科尤为突出，这为俄罗斯带来了一大批精通网络和计算机技术的精英，其中的很大一部分人已经参与到制定保护计算机系统方案的国家项目中去，为俄罗斯的国家网络安全和网络战实力的提升作出了相当大的贡献。

同时，一些大型网络安全公司和实验室也和俄罗斯政府有着广泛而且深入的合作，为政府提供了强有力的安全支持。比如著名的 Dr.web 是俄国防部指定的信息安全合作公司；而卡巴斯基实验室更是替俄政府主办了俄罗斯现代化和经济技术发展委员大会，赢得了俄高层的肯定。

此外，俄罗斯的黑客举世闻名，网络精英众多；俄也是全球重要的软件工业国，技术走在世界前列，具有雄厚的实力。已有的强大技术储备使得俄罗斯在遇到威胁或有需要时，这些人才和技术能很快地转入军事用途。

c) 实战应用，手段更加多样

俄军的网络战理论不仅仅停留在纸面上，在战争实践中已有所运用，爱沙尼亚和格鲁吉亚都曾经谴责俄罗斯对其发动网络战。2007 年 4 月，爱沙尼亚决定将位于首都塔林的苏军纪念铜像移到军人坟场，这一举动引起了居住在爱沙尼亚国内的俄罗斯人的大规模骚乱，同时也招致了俄政府的强烈抗议。2007 年 4 月 26 日晚上 10 时左右，在没有任何征兆的情况下，爱沙尼亚政府网站突然被来自世界各地电子信息淹没。尽管有防火墙、备用服务器和经验丰富的技术人员来应对这种突发性事件，但防线还是迅速遭到攻破，网络攻击次数呈指数式增长，包括政府、银行、新闻媒体在内的各大网站相继遭到攻击，无一幸免。这场大规模网络攻击一直持续到 5 月 18 日才结束，使爱沙尼亚整个国家的秩序陷入一片混乱。

另据报道，在 2008 年 8 月的俄格冲突之前，俄罗斯就控制了格鲁吉亚的网络系统，冲突爆发后，几乎所有的服务器都被完全冻结，这使得格鲁吉亚的交通、通讯、媒体和金融等互联网服务陷入一片瘫痪，格军接收不到上级的指令，上级也无法获悉战况，从而为俄军军事行动的顺利开展开辟了道路。

在全力提高自身网络战水平的同时，俄罗斯表示不主动发起但也绝不畏惧网络战。此外，俄罗斯也积极推动国际社会建立一个互信的国际信息安全系统，避免信息安全领域的威胁，限制和预防网络安全冲突，反对网络军备竞赛。

俄罗斯主张在联合国、欧洲安全组织、上海合作组织等国际组织框架内拟定一份具有普遍性的国际法律文书来规范和限制网络空间的战争和制定网络战条约。比如俄罗斯曾经向联合国提交了一份名为“国际电信和信息领域发展安全”的议案，希望能把未来的信息安全和网络战等问题条约化，此举得到了除美国外大多数国家的支持。

此外，加强国际合作，共同应对挑战，与其他国家联合将网络战技术用于打击网络犯罪和恐怖主义也是俄罗斯关注的重点。在将来，俄罗斯仍将是网络战中一支不可小觑的劲旅。

2.3. 韩朝网络战

近年来，韩军正在悄悄发展应对未来信息作战的网络战部队。韩国国防部在 1999 年 3 月的总统业务报告中提出，从 1999 年起到 2015 年为止，分 3 个阶段确立国防信息化的目标，首先要对信息组织进行统一调配，并建立信息通信网，以应对网络战，1999 年年底前组建一支网络战特殊部队——反黑客部队。从 2000 年开始，韩国每年的国防预算都有 5%专门用于“提高应对信息战的核心技术”。与此同时，韩

国军方也开始加大力度培养和招收计算机专业人才。目前韩军已经培养了数万名信息战专业人员。韩国执行网络作战的主要机构是 2003 年 11 月成立的国防信息战中心。国防信息战中心目前由数十名业务精干的人员组成。他们对韩国国防计算机网和互联网进行 24 小时实时监控，以发现和阻止黑客的网络侵袭行为以及在遭到侵袭后，迅速进行修复和调查。据了解，每次韩军进行应对紧急情况的演习时，该中心都要参与。韩国国防部有关人士表示：“21 世纪战争的胜败取决于对计算机等尖端装备的运用程度，要想为国家信息网构建可靠的防护墙，就要拥有比入侵者实力更突出的黑客。”韩国国防部认为，提升韩军网络作战能力的关键取决于能够选拔多少优秀的黑客。为此，韩国国防部计划从韩国国防科学研究院所和各军兵种部队，甚至包括普通民众当中选拔计算机能力出众的精英组成网络作战团队。韩国军方呼吁政府、民间、军方共同努力，建立应对网络战的多边合作体系。

2014 年 3 月，韩国国防部高调宣布正在对朝鲜实施网络战，他们以此前成功攻击伊朗核设施的“超级工厂病毒”(Stuxnet)为蓝本，正在研发一种类似的网络病毒，旨在对朝鲜核设施造成物理性破坏，而且，这种病毒攻击只是韩国对朝鲜的大型网络战的第二阶段，战役的第一阶段，即对朝网络宣传战，则早在 2010 年就已经打响。韩国时间 2013 年 3 月 20 日，一位匿名的韩国政府公务员在首都首尔向极光透露，韩国国内的三家电视媒体和两家银行的计算机网络遭遇大规模网络攻击，导致网络服务暂时中断。一名新韩银行的员工在接受极光采访时说，大约在当地时间下午两点，她的工作计算机突然黑屏，随后屏幕上出现骷髅标志。新韩银行是韩国的第四大金融机构，该银行的自动柜员机、柜台服务及企业服务中断了将近十个小时。朝鲜为了实施网络战，在人民武力部总政治局下设了 121 部队，履行扰乱韩国指挥通信网、破坏网站等网络系统的实质性的网络战。朝鲜黑客部队直接由朝鲜人民军总参谋部指挥自动化局和人民武力部侦察局领导，负责收集韩国、美国、日本等国的军事情报，并执行干扰军事指挥、通讯网络及发起网络战的任务。

朝鲜虽然经济不发达，但网络战的水平接近经济发达国家水平，现在拥有建造和部署网络武器和蓄电池 EMP(电磁脉冲)装置的技术能力，它们能在有限的范围内摧毁电子设备和计算机。2007 年春，朝鲜实施了一次网络武器试验。10 月朝鲜试验了首个逻辑炸弹。逻辑炸弹是一种含有恶意代码的计算机程序，一旦发生某些事件或在某个预设的时间点就会自动执行或被触发。一旦触发，逻辑炸弹就能使计算机宕机，数据被删除。

进入 21 世纪以来，发生在国际互联网上的几起重大网络对抗事件表明，随着各国军队对网络战的重视程度不断增强、各国军队的网络战能力也将不同程度地得到增强。一旦战争爆发，大规模的网络战进入实战将不可避免。从海湾战争和科索沃战争中的网络战实践可以看出，网络战将贯穿战争活动的始终，其地位作用更加显著。而且，发生在国际互联网和战场两条战线上的网络战不会分开，而是相互配合，相互支援。

2.4. 欧亚网络战

除了美俄之外，欧亚等很多国家也争相提高网络战水平。

中国的“网军”成立于 1999 年，当时还不是正式的部队编制。但到 2001 年就形成了正式的部队建制。在 2001 年发生美中军机碰撞事件后，中国的“红客联盟”网络组织开始向美国发动大规模网络进攻，甚至把中国国旗都插到了美军的网上。此事被称为中国“网军”大发展的契机。据认为，中国“网军”主要负责破解暗号、解读情报等工作。台防卫当局认为大陆“网军”有 40 万人。但无论如何，中国拥有当今世界最大的网络部队，这一点是确定无疑的。中国参与网络战的并不仅仅是军队。一些政府部门除了审查、监视等功能之外，也能进行网络进攻。不仅能在一定程度上遮蔽来自敌国的网络进攻，在发生紧急情况时还可成为强有力的网络战工具。

英国早在2001年就秘密组建了一支隶属军情六处、由数百名计算机精英组成的黑客部队。2009年6月25日出台首个国家网络安全战略，并宣布成立两个网络安全新部门，即网络安全办公室和网络安全行动中心，分别负责协调政府各部门网络安全和协调政府与民间机构主要计算机系统安全保护工作。英国认为，网络安全在21世纪的重要性相称于19世纪的海上安全和20世纪的空中安全。

北约正采取进一步措施抵御来自网络攻击的潜在威胁，其中一项关键的举措是建立网络防御快速响应部队。2008年5月，爱沙尼亚、拉脱维亚、立陶宛、德国、意大利、西班牙和斯洛伐克签署协议，将共同出资建立一个反网络攻击研究中心，以提高防御网络攻击的能力。由此可见，“网络军事化”已经渐渐走向战争舞台的最前沿。2009年7月，北约计划未来18个月内，通过强化北约所有通信与信息系统，使北约计算机事件响应能力达到全面作战能力。

以色列在1998年就将成功入侵美国防部网络的青年招入部队，并开始加大对网络作战的研究力度。在巴以冲突、黎以冲突中，以色列利用网络进攻的方式篡改网页、攻击电视台，以达到影响舆论导向的目的；侵入军方电脑窃取机密，以确定火力打击的重点目标和精确坐标；阻断敌人通信指挥系统，以掌握最佳的作战时机，这一切都是以军进行网络战真实写照。

2009年1月中旬，德国内阁就批准了一项旨在“加强联邦政府信息安全”的法案。德国联邦国防军正在训练自己的网络战部队，这不仅仅是为防御某些国家的黑客袭击。德国政府同样对未来世界范围内的网络战做好了准备。德国国防部长命令德国国防军在未来三年内组建一支网络黑客部队。陆军准将克里塞尔的新任务就是为未来网络战做好准备。克里塞尔将率领总数为6000人的部队——“信息和网络技术管理部”，该部队主要应对网络突发情况，主要针对有关外部服务器和网络的攻击。克里塞尔的76名部下正忙于测试最新的网络渗透、扫描、操纵或攻击技术。克里塞尔的76名网络战士大部分毕业于联邦国防军大学计算机专业。该部队已经在阿富汗执行了网络监控行动。他们会在网络渗透实验中，进行模拟网络攻击。

印度军方基于对网络技术的精通和利用网络能够达到何种战争效果的认识，坚持自主研发、军民合作的原则，投入大量人力物力，力求在网络技术、密码技术、芯片技术以及操作系统方面自成体系。“闪光信使”高速宽带网络以及被称为“第三只眼”的海军保密数据信息传输网络的建成使用，将进一步增强印度军方应对未来网络战争的不对称优势。除完善防御体系外，印军一方面将网络进攻写入作战条令，明确指出要建立能够瘫痪敌方指挥与控制系统以及武器系统的网络体系，在陆军总部、各军区以及重要军事部门分别设立网络安全机构；另一方面通过吸纳民间高手入伍和对军校学员进行“黑客”技术培训等方式，逐步完成未来网络战的人才储备。目前，印军组建了陆海空三军联合计算机应急分队，并计划征召“黑客”入伍。同时，印军也在位于新德里的陆军总部建立了专门负责网络中心战的网络安全部门，他们还将在所有军区和重要军事部门的总部建立网络安全分部。这些部门将负责审查印军现有网络的安全状况。为应对不断增长的网络威胁，2009年印陆军决定将网络安全能力延伸到印陆军师一级，还将通过陆军网络安全机构(ACSE)对有关单位进行“定期网络安全审核”。2010年4月，印度国防部高级官员宣称，印度已经决定成立网络防御司令部，以保护政府和军用网络的安全。

日本防卫厅根据其2005~2009年《中期防卫力量发展计划》，正在组建一支由陆海空自卫队参加、人数多达5000人的“网络部队”。日本众议院已通过《自卫队法》修正案，“以应对未来弹道导弹、网络战等多种威胁”。日本“网络部队”专门负责进行反黑客、反病毒入侵任务，其重要作战指导思想是通过掌握“制网权”达到瘫痪敌人作战系统的目的。日本在构建网络作战系统中强调“攻守兼备”，拨付大笔经费投入网络硬件及“网战部队”建设，分别建立了“防卫信息通信平台”和“计算机系统通用平台”，实现了自卫队各机关、部队网络系统的相互交流和资源共享；研制开发的网络作战“进攻武器”和网络防御系统，目前已经具备了较强的网络进攻作战实力。同时，日本注重与美国联合发展，在引进

先进技术的基础上不断完善自身建设，不断提升“网战”能力。

3. 结语

随着计算机网络在战争中的地位与作用日益突现，计算机网络战部队将不断出现、并向专业化方向发展。专门的计算机网络攻击武器平台将会爆发式涌现，这种攻击武器将不仅仅是一种普通计算机，而是一种由计算机软、硬件紧密结合的武器系统。它会根据不同需要，可以包括大、中、小型、或固定式、台式、便携式等许多种。利用这种网络攻击系统，可以对敌方网络进行侦察、入侵等活动。同时，计算机病毒、特洛伊木马、后门程序等计算机恶性软件也会不断发展更新，逐渐成为实用的计算机网络战武器。而且这种软件武器会随着计算机技术的发展，而不断升级换代，以便对抗不断提高的计算机网络防护能力[3]。因此，可以预见，随着信息技术的进一步发展和广泛地运用，世界军事强国在信息网络战领域的竞争必将更趋于激烈,“网络软原子弹”将像物理原子弹一样，在未来高技术战争中发挥愈来愈重要的作用。

参考文献

[1] 网络战－百度百科[EB/OL]. https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E6%88%98/995931?fr=aladdin

[2] 美军网络战主要干什么？－中国军网[EB/OL]. http://www.81.cn/jmywyl/2016-11/18/content_7365326.htm

[3] 千桥飞梦编写组. 千桥飞梦—胡文祥学习研究成果实录[M]. 北京: 知识产权出版社, 2014: 155-161.