网络空间安全威胁与对策思考

Recommended Citation

Senior Colonel Fan Gaoyue 作者：樊高月大校, "网络空间安全威胁与对策思考", NAPSNet Special Reports, June 13, 2013, https://nautilus.org/napsnet/napsnet-specia-reports/%e7%bd%91%e7%bb%9c%e7%a9%ba%e9%97%b4%e5%ae%89%e5%85%a8%e5%a8%81%e8%83%81%e4%b8%8e%e5%af%b9%e7%ad%96%e6%80%9d%e8%80%83/

by Senior Colonel Fan Gaoyue 作者：樊高月大校

13 June 2013 / 13日6 月 2013

I. Introduction

For the English language version of this report please click here. In this Special Report Senior Colonel (Retired) Fan Gaoyue argues that the internet and cyberspace in broad terms have an openness and ability to transcend geopolitical borders that makes it vulnerable. Therefore there are several practical measures for international cooperation that can promote cyberspace security.

This work was originally presented at a Swedish-sponsored conference and is being published as a Special Report with the author's permission.

Fan Gaoyue recently retired from the Chinese People's Liberation Army. His most recent assignment was at the Chinese Academy of Military Sciences. He was also a WSD-Handa Fellow at PACFORUM CSIS (Center for Strategic and International Studies) in 2011.

The views expressed in this report do not necessarily reflect the official policy or position of the Nautilus Institute. Readers should note that Nautilus seeks a diversity of views and opinions on significant topics in order to identify common ground.

II. SPECIAL REPORT

网络空间安全威胁与对策思考

内容提要：随着信息时代的到来，互联网络越来越普及，全球互联网用户急剧增加，目前已达20多亿。人们在网上发送和接收信息，控制交通运输，调配能源电力，购物付款，欣赏音乐，交流感情，感知世界……
互联网已经成为打破各国边界、沟通全球信息、对国际国内事务施加影响的有效工具。然而，由于具有遍布全球、超越地缘政治边界、任何人都可不同程度地轻易进入、受制于电磁频谱的可用性等特点和固有的薄弱环节，网络空间正面临黑客入侵、网络犯罪、网络病毒、网络攻击等严重威胁。要应对这些威胁，就必须提高网络安全意识，加强网络安全防护；加强网络技术创新，降低网络系统脆弱性；建立国家网络安全监测预警系统，及时发现和有效防止网络攻击；完善网络空间安全法规，加强网络空间管理；加强国际合作，共同促进网络空间安全。

随着计算机网络技术的飞速发展，互联网时代正在到来。当前，已有数百万人靠网络技术谋生，20多亿人通过网络进行日常社会交流。人们在网上发送和接收信息，控制交通运输，调配能源电力，购物付款，欣赏音乐，交流感情，感知世界……
网络已成为人类新的生存空间。然而，在人们享受网络带来的种种好处的同时，网络间谍、网络诈骗、网络色情、网络病毒在网上的活动也越来越猖獗，个人隐私、知识产权、国家机密等面临巨大威胁。这种现实迫使我们不得不认真思考和应对网络空间的安全问题。

一、网络空间的作用与特点

网络由成百上千相互连接的计算机、服务器、路由器、转换器和光纤电缆等组成，是交通运输、能源电力、通信服务、医疗卫生、金融服务等关键基础设施的神经系统。随着信息时代的到来，互联网络越来越普及，互联网用户急剧增加。从2000到2010年，全球互联网用户从3.6亿增加到20亿以上。[i]
截至2012年6月底，中国网民数量达到5□38亿，互联网普及率达39□9%；手机网民达到3□88亿，较2011年底增加了约3270万人；网络购物用户达到2□1亿，较2011年底增长8□2%；网上银行用户达1□91亿，较2011年底增长14□8%；中国域名总数为873万个（其中□CN域名数为398万个），网站总数升至250万个。[ii]
每日每时全世界都有不计其数的网民在互联网上获取或发送信息，互联网已经成为打破各国边界、沟通全

球信息、对国际国内事务施加影响的有效工具。各种网络的广泛应用，极大地提高了社会劳动效率和生产率，降低了成本，改变了企业、政府和各种社会团体的活动方式和决策方式。各种广域网、局域网、城域网上高速流动的公用和专用信息，已成为推动世界政治、经济、军事、外交等各行各业快速发展的原动力。

目前，网络发展很快，普及率越来越高。清楚地认识网络空间的基本特征，对我们管好网络、用好网络意义重大。从网络发展和使用的情况看，网络空间主要具有以下特征：由公众、私人和政府创造、维持、拥有和运作，遍及全球；随着技术、构造、程序和专门技术的共同发展而变化，产生新的能力和运作结构；受制于电磁频谱的可用性；利用高质量的决策信息，可实施接近光速的作战机动；使空中、地面、海上和太空的作战行动成为可能；超越通常定义的地缘政治边界；由支持性关键设施、储存、处理与传输数据设备、硬件软件应用系统等构成；包括静止的和运动的数据、声音和视频；其他国家、组织、伙伴、私人部门和对手都可不同程度地轻易进入等。[iii]
此外，网络空间还在构造、技术、物理保护、公开来源信息、训练、政策等方面存在薄弱环节。

二、网络空间面临的巨大威胁

由于具有上述基本特点和薄弱环节，网络空间面临多种复杂而危险的威胁。有的威胁来自国外，有的威胁来自国内，有的威胁来自国家政府，有的威胁来自非国家行为体，还有一些威胁来自计算机系统本身的脆弱性。小技术可以造成大影响，不能建造复杂昂贵武器系统的潜在对手，可以通过网络对大国安全造成显著影响。在美国计算机安全学会2003年进行的一次调查中，90%的参与者称他们在自己的网络系统中安装了反病毒软件，然而85%的系统还是遭受过计算机病毒的侵害。在同样一次调查中，89%的参与者安装了防火墙，60%的人拥有非法闯入探测系统，然而90%的人称发生过安全破坏事故，40%的系统遭受过侵入。[iv]网络空间面临的这些威胁，大致可以分为以下几类：

1、网络入侵。网络入侵是指潜入网络刺探或搜集信息，但并不增加或修改数据，也不破坏或干扰网络设备。鉴于从网络获取情报比人工情报容易，代价也小得多，各国情报部门和非国家行为体都特别重视从网络获取各种情报。因此，网络入侵行为急剧增加。2005年8月，IBM
发布计算机安全报告称，在当年上半年，全球报告的入侵总数达2□
37亿次。其中，政府机构受到的攻击最多，达5400万次；生产业第二，为3600万次；金融业和卫生行业分别为3400万次和1700万次。按照国别划分，美国政府与各行业受到的攻击最多，为1200万次；新西兰第二，为120万次，中国第三，为100万次。[v]《2011年中国互联网网络安全态势报告》显示，2011年境外有近4□7万个IP地址（位于日本22□8%、美国20□4%、韩国7□1%）参与控制中国境内近890万台主机；境外11851个IP通过植入后门对境内10593个网站实施远程控制。[vi]2012年1月至3月，根据IP
地址显示，中国国防部网站和中国军网每月平均遭受来自境外的入侵多达8万余次。[vii]
无论是为了金钱、获取知识产权还是破坏重要的国防系统，这些网络入侵都对一个国家的政治、经济、军事、外交等构成复杂而严峻的挑战。

2、网络犯罪。网络犯罪是指利用网络进行犯罪活动，如开设色情网站、进行网络诈骗、利用网络贩卖非法物品等。据统计，1998年美国FBI
调查的犯罪案件共547件，结案399件；1999年调查了1154件，结案912件。一年之间，翻了一番。2006年以来，中国网络上的犯罪总量也持续高位运行，年平均在470万起左右。而网络犯罪的发案率，根据业内人士最保守的估计，应当是这个数字的两倍。网络犯罪中最突出的问题是色情泛滥成灾，严重危害未成年人的身心健康；软件、影视、唱片的著作权受到盗版行为的严重侵犯，商家损失之大无可估量；网络商务备受诈骗的困扰，有的信用卡被盗刷，有的购买的商品如石沉大海，有的发出商品却收不回货款。根据台湾和日本的统计，两地网络色情案件均占网络犯罪总数的30~
35%；其他所占比例较大的，依次为网络诈骗、贩卖非法物品、恐吓与勒索、非法侵入、侮辱与诽谤等。

3、恶意软件。通常包括病毒与蠕虫、特洛伊木马与逻辑炸弹、信息垃圾与捕获程序。病毒与蠕虫是指利用非法渠道在网络上传播、对计算机及其系统加以破坏的程序。80年代开始兴起并广泛传播，引起较多关注的主要包括：“莫里斯”蠕虫，导致6000多个系统被感染，占当时互联网的1/10；“梅利莎”
病毒，在4天内感染10多万台主机；“红色代码”病毒，在14个小时内影响了15万台计算机系统；“尼姆达”
将计算机蠕虫和计算机病毒结合到一起，从出现到传遍全国，前后只花了1小时，在持续数天的攻击中，8□6万台计算机受到攻击；“震网”

病毒，被用于攻击伊朗核设施，因其技术复杂、针对性强而被认为掀开了利用网络空间的新篇章。[viii]
特洛伊木马与逻辑炸弹是依附在程序或系统中的破坏性代码，在特定条件下进行破坏。信息垃圾是指商家为推销产品而向用户发送的大量电子邮件，只能带来一些小麻烦。捕获程序是当前最为普遍的在线诈骗方式之一，用以捕获用户的个人信息，诱骗用户进入看似合法的网页，从而骗取用户的账户名和密码。这些恶意软件通常通过漏洞侵入、后门植入、硬件注入、接收路径传入等方式，对计算机系统进行破坏。

4、网络攻击。迄今为止，真正意义上的“网络战争”并未发生，但网络攻击却多次出现，并且战果卓著。2003年3月，美军在开始常规攻击之前，侵入伊军专用军事保密网络，向数以千计的伊军军官发送电子邮件，劝其将坦克和其他装甲车辆整齐地停放在基地外面并远离它们，获得成功，致使伊军部队未经交战就消失得无影无踪。2007年9月6日深夜，以色列战机通过发动网络攻击骗过叙利亚防空网，毫发无损地摧毁了叙利亚境内的“核设施”
。在2008年8月7日爆发的俄格冲突中，俄对格实施了持续、复杂和高强度的网络攻击，致使格鲁吉亚丧失对本国“.ge”
域名的控制权，被迫将许多政府网站转移到国外的服务器上，但俄随即改变攻击路径，假装是来自格鲁吉亚的网络攻击，结果触发了多数国外银行的自动保护机制，关闭了它们与格鲁吉亚银行的连接，致使格银行因无法访问欧洲的结算系统而业务瘫痪，不但信用卡系统停止工作，移动电话系统也随即崩溃。[ix]
尽管网络战争至今尚未发生，但网络战争的威胁确实存在。有的国家从上世纪90年代开始培养网络战士，至今已建成较大规模的网络空间作战部队、军种网络司令部和联合网络司令部，并经常进行网络空间作战演习，一旦需要，即可打响网络战争。

5、网络漏洞。计算机系统的安全脆弱性——
软件和硬件中存在的允许未经授权的网络进入能力，在2000年到2002年出现了显著的增长，弱点的数量由1090个增加到4129个。即使软件和硬件被整合进一套运行系统，他们仍然处于恶意篡改的风险之中。一些国家使用的信息技术产品大多数是在海外制造和组装的，这些产品是否带有不可预知的风险，值得怀疑。[x]
中国缺乏拥有自主产权的计算机核心技术（芯片），绝大部分计算机采用外国核心技术，这也为中国网络安全埋下了隐患。因此，计算机安全的新脆弱性总是会不断出现，要确保网络和系统的安全，就必须持续不断地升级防护措施，而不能仅靠现有的安全防护手段。

除这些人为威胁外，网络空间还面临某些自然威胁和意外威胁。自然威胁是能够损害和破坏网络空间的威胁，包括洪水、飓风、太阳耀斑、闪电、龙卷风等。意外威胁是以多种形式出现的、难以预测的威胁，包括无意传播病毒、锄耕机挖断光纤电缆等。

三、对策思考

在信息时代，网络空间已经成为各种社会活动的基础，为国家政治、经济、军事、外交、民用基础设施和国家安全提供重要支撑。如果网络空间遭受重大攻击，就会对电力能源、交通运输、金融行业等造成大量的物理损伤和经济破坏，严重影响社会稳定和国家安全。因此，必须采取切实有效的措施，确保国家网络空间安全。

首先，应开展全民网络安全教育，提高网络安全防护的自觉性。网络威胁看不见，摸不着，来无影，去无踪，很难感觉到它的存在，致使广大网民网络安全意识淡薄。当前，多数国家急于大规模、高速度地建设网络，却忽视了相应的安全保障措施，许多应用系统实际处于不设防状态，给网络安全留下了重大隐患。各国政府和相关部门，应投入一定经费，通过广播、电视、网络、报刊等，开展全民网络安全教育，使广大网民了解网络安全面临的重大威胁和可能造成的严重损害，增强广大网民的网络安全意识，自觉加强对网络系统的防护。

其次，加强网络技术创新，降低网络系统脆弱性。对国家网络系统的攻击能够在很少或根本没有预警的情况下发生，而且其速度极快，许多受害者根本没有时间接收警报。即便收到预警，通常也没有必需的时间、知识和工具来保护自己。因此，依赖计算机网络系统的机构必须采取主动行动，对自身的脆弱性进行识别和修补，而不是等着攻击者出现时再去制止或直到获得关于攻击行动的警报时才采取行动。一是持续评估网络系统的脆弱性，并及时采取补救措施。二是制造一个多层而灵活的防御网络，用来修补和防护脆弱性。三是投入必要的经费，研制新型网络防护产品，降低系统本身的脆弱性。四是经常开展网络安全防护演练，

确保网络免遭攻击或在遭受攻击后能在短时间内恢复功能，降低网络攻击的破坏程度。

第三，建立国家网络安全监测预警系统，及时发现和有效防止网络攻击。一个国家的大部分网络空间通常不是由一个公共或私营机构所占有，所以没有一个全景制高点来看清正在来临或不断扩散的攻击。为了减轻网络攻击的影响，政府必须广泛而迅速地发布有关威胁的信息，必须协调许多组织对突发事件的分析和快速反应能力，以决定如何最好地防御攻击、减轻危害并恢复服务。因此，应由政府和非政府实体共同组建网络安全监测预警系统，担负分析、预警和管理具有国家级重大意义的事故、提高政府系统和私营部门基础设施运行的连续性、增加机构组织之间的信息共享等任务。该系统应设信息共享与分析中心、事故处理中心、事故管理中心、应急反应计划中心等机构，并与国家通信系统、国家基础设施保护中心、国家能源保障办公室等机构协作，全面开展国家网络安全监测预警工作。这样，就能及时发现网络空间潜在的破坏行动、分析危害、警告潜在的受害者、协调事故反应行动，并恢复那些遭到破坏的重要的服务。

第四，完善网络空间安全法规，加强网络空间管理。目前，全球有40多亿件无线数字设备，有约1/3的人使用互联网，还有无数人在日常生活中接触互联网。为加强网络管理，维护网络安全，不少国家都制定了网络空间安全法规。例如，中国就先后制定了《中华人民共和国计算机信息系统安全保护条例》、《中华人民共和国计算机信息网络国际联网管理暂行规定》、《计算机信息网络国际互联网安全保护管理办法》等法规。此外，欧洲理事会的26个欧盟成员国和美国、加拿大、日本、南非等30个国家还于2001年11月在布达佩斯共同签署了《网络犯罪公约》，希望共同致力于促进网络空间安全。这些国际国内法规，对于加强网络管理和维护网络安全发挥了重要作用。但这些法规已不能完全满足各种网络快速发展的需要，一方面它们需要进一步完善，另一方面也需要制定新的法规，这样才能更有效地对网络实施管理，确保网络空间安全。一是修订部分过时的网络空间安全法规，使其内容更加充实、实用。二是制定新的网络空间安全法规，覆盖那些未能涉及到的领域，如建立身份管理制度等（身份管理不只是用于人员认证，还可以帮助确保在线交易）。三是加强执法力度，提高网络安全管理水平。

第五，加强国际合作，共同促进网络空间安全。由于一国的网络空间与国际网络空间紧密相连，不同于传统的领土、领海、领空有明确的国际边界，要维护本国网络空间安全，仅凭自身的努力是远远不够的，应该加强国际合作，共同促进网络空间安全。一是扩大《网络犯罪公约》签约国数量，共同应对非法进入、非法截取、资料干扰、系统干扰、设备滥用、伪造电脑资料、电脑诈骗、儿童色情犯罪、侵犯著作权等网络犯罪行为。二是推动建立国际“观察和警报”
网络系统，及早侦测和阻止正在发起的网络攻击。三是建立共同打击网络犯罪的国际司法合作机制，加大打击跨国网络犯罪力度。四是定期或不定期举行网络安全国际会议，共同商讨应对网络空间安全挑战与威胁的大计。五是尽早制定维护网络空间安全的国际行为准则，并共同遵守这些准则，为实现国际网络空间安全贡献力量。六是尽早制定防止网络战争的协定或条约，禁止攻击供电、供水、金融、医疗、教育等国计民生网络系统，明确网络战争界线，防止将一般的网络攻击行动升级为网络战争，确保人类赖以生存的信息环境不会遭受毁灭性打击。

本文只是作者自己的观点，不代表中国人民解放军军事科学院。.

III. NAUTILUS INVITES YOUR RESPONSES

The Nautilus Peace and Security Network invites your responses to this report. Please leave a comment below or send your response to: nautilus@nautilus.org. Comments will only be posted if they include the author’s name and affiliation.

IV. REFERENCES:

[ii] 中国互联网络信息中心，中国互联网络发展状况统计报告，2012年7月。

[iii] C JC S, THE NATIONAL MILITARY STRATEGY FOR CYBERSPACE OPERATIONS, p.3, December 2006.

[iv] The White House, THE NATIONAL STRATEGY TO SECURE CYBERSPACE, P. 8, February 2003.

[v] IBM Global Services, IBM SECURITY REPORT: GOVERNMENT, FINANCIAL SERVICES AND MANUFACTURING SECTORS TOP TARGETS OF SECURITY ATTACKS IN FIRST HALF OF 2005, August 2, 2005.

[vi] 杨婷婷、伍铎克，中国遭网络攻击数量大增，《环球时报》，2012年3月21日。

[vii] 刘扬，国防部：中国军网月遭8万次境外网攻，《环球时报》，2012年3月30日。

[viii] Paul Cornish, David Livingstone, Dave Clemente and Claire Yorke, On Cyber warfare, A Chatham House Report, 2010, P.7.

[ix] Richard A. Clarke and Robert K. Knake, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT, Harper Collins Publishers, 2010.

[x] The White House, THE NATIONAL STRATEGY TO SECURE CYBERSPACE, P. 8, February 2003.

View this online at: https://nautilus.org/napsnet/napsnet-specia-
-
reports/%e7%bd%91%e7%bb%9c%e7%a9%ba%e9%97%b4%e5%ae%89%e5%85%a8%e5%a8%81%e8%83%81%e4%b8%8e%e5%af%b9%e7%ad%96%e6%80%9d%e8%80%83/

Nautilus Institute
2342 Shattuck Ave. #300, Berkeley, CA 94704 | Phone: (510) 423-0372 | Email: nautilus@nautilus.org