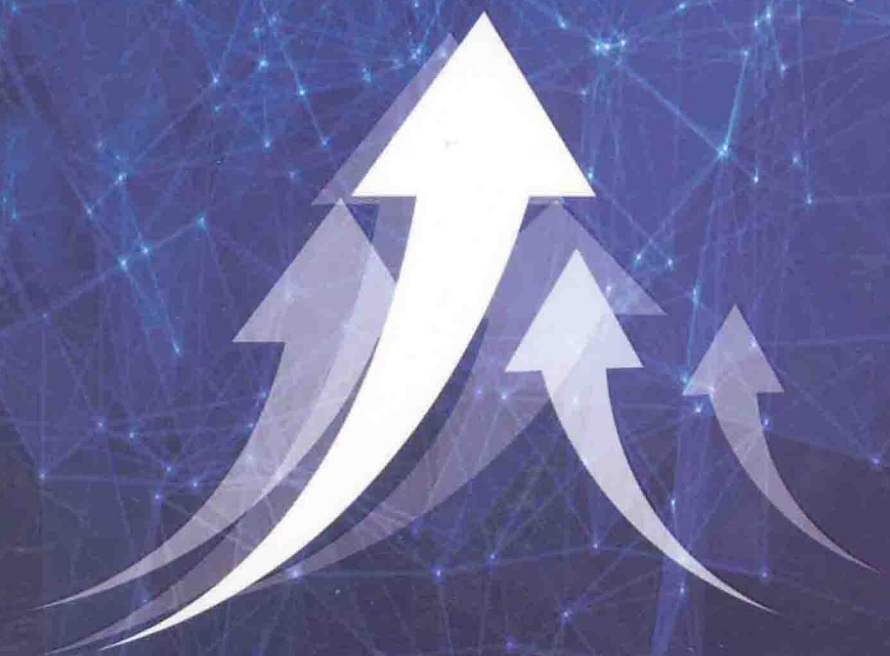
国内外互联网研究系列丛书

国外网络与信息安全战略研究

程工 / 编著



電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

国内外互联网研究系列丛书

国外网络与信息安全战略研究

程　工　编著

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

本书包含“国外网络安全战略分析”、“主要国家网络安全战略概要”和“主要国家网络安全战略译文”，通过介绍和研究除美国外的世界主要国家在制定网络空间安全战略方面的经验和做法，希望能推动我国尽早出台一部国家级的网络安全战略，从而更好地调动和协调各方力量，保护我国在数字时代的核心利益。

本书可供从事信息安全、网络安全、危机处理的工作人员参考，也可供对互联网信息安全、网络安全领域的大学、研究所等各类学术机构的工作人员、学生阅读参考。

图书在版编目（CIP）数据

国外网络与信息安全战略研究 / 程工编著. —北京：电子工业出版社，2014.11
（国内外互联网研究系列丛书）
ISBN 978-7-121-20348-0

Ⅰ. ①国… Ⅱ. ①程… Ⅲ. ①计算机网络—信息安全—研究—国外 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2014）第 250533 号

责任编辑：赵 娜 特约编辑：韩奇桅
印 刷：北京天宇星印刷厂
装 订：北京天宇星印刷厂
出版发行：电子工业出版社
北京市海淀区万寿路 173 信箱 邮编 100036
开 本：787×1092 1/16 印张：19.5 字数：487 千字
版 次：2014 年 11 月第 1 版
印 次：2014 年 11 月第 1 次印刷
定 价：58.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前　言

进入 21 世纪，网络恐怖主义、网络战争等新兴的安全威胁日益加剧，全球网络安全事件频发，对各国的关键基础设施安全、经济和社会造成严重后果，对各国政府在网络与信息安全管理方面带来了巨大挑战。保护网络空间安全正在成为各国政府的重大优先事项之一，网络空间也被视为领土、领空、领海以外另一个需要国家保护的领域。

随着网络安全问题上升到国家安全层面，各国政府纷纷将强化网络空间防御提升到战略高度。美国是最早制定网络空间安全战略的国家。1998 年，首次提出了“信息安全”概念，并优先发展网络安全防御构想。2000 年，美国通过了《信息系统保护国家计划》，2003 年出台《网络空间国家安全战略》。美国先后颁布的与网络安全有关的文件多达 40 多份。到 2014 年，已有 40 多个国家颁布了网络空间国家安全战略，欧盟及其成员国对网络安全的关注度也在不断增加。目前，已经有十余个欧盟成员国（爱沙尼亚、芬兰、斯洛伐克、捷克、法国、德国、立陶宛、卢森堡、荷兰、英国、奥地利、比利时、匈牙利、波兰、罗马尼亚和西班牙）制定和公布了本国的网络空间安全战略，其中英国政府更是在三年之内连续两次出台了国家网络安全战略。在亚太地区，日本、韩国、新加坡、澳大利亚、新西兰等信息通信技术较为发达的国家也先后出台了本国的网络安全战略。

当前，网络空间安全已成为国家安全的重要组成部分，将其放在战略高度来进行审视，是我国面临的紧迫任务。面对全球互联网领域的巨大变革，依托相关的技术与业务优势，编撰了《国内外互联网研究系列丛书》。本书共分“国外网络安全战略分析”、“主要国家网络安全战略概要”和“主要国家网络安全战略译文”三部分内容，除原文摘录外，通过分析和比较研究世界主要国家在制定网络空间安全战略方面的经验和做法，希望为推动我国尽早出台一部国家级的网络安全战略提供借鉴和参考，从而更好地调动和协调各方力量，保护我国在数字时代的核心利益。

由于本书所涉及的文献数量巨大，在此要感谢陈志伟、张百玲、孙菲阳、杜薇、陈侠、王龙飞、赵慧、刘传相、牛泽亚、褚立文、胡英、周恬、程姣、李小琴、管燕飞、卞丽娟等同事在资料翻译方面的耐心细致工作；感谢陈志伟、张百玲、孙菲阳、杜薇、陈侠、姜文华、李雄、王召伟、赵明杨、王艳磊、徐小磊、毕明珠在资料整编校对等方面的辛勤努力。感谢毕明珠小姐在本书最后统稿中的不辞辛劳，尤其要感谢孙小宁女士在本书出版全过程始终如一地支持与帮助。没有各位同事的热情鼓励和无私支持，就没有本书的最终完成。

欢迎领导和专家对本书提出批评指正意见。联系电话：（010）82990605。

作　者

2014 年 9 月

目　录

第一章　国外网络安全战略分析

第一节　全球网络空间安全国家战略概述

随着人类社会的各个方面越来越依赖网络空间和信息通信技术，多种形式的网络犯罪也正在以前所未有的规模出现，网络空间的脆弱性凸显。进入 21 世纪，网络恐怖主义、网络战争等新兴的安全威胁日益加剧，对各国的关键基础设施安全形成严峻挑战。关键信息系统的故障或中断可能会影响社会的正常运转并引起潜在的不可预见的灾难性后果。例如，一旦国家的信息基础设施遭到破坏，电力供应、食品分配、供水和污水处理、金融服务、广播、交通、卫生、急救，国防和政府服务都将受损。

保护网络空间安全正在成为各国政府的重大优先事项之一，网络空间也被视为领土、领空、领海以外另一个需要国家保护的领域。英国前首相布朗就表示："正如在 19 世纪我们为了确保英国的安全和繁荣必须保护海洋一样，20 世纪我们必须保护天空，在 21 世纪我们同样必须保护我们的网络阵地，使个人和企业有信心安全地生活和工作。"

一、重大网络安全事件催生各国家网络安全战略

近年来，重大网络信息安全事件频发，进一步刺激了各国政府加快推出网络安全战略的步伐。爱沙尼亚是历史上第一个政府和关键基础设施经历大规模网络攻击的国家。该事件发生在 2007 年 4～5 月的 3 个星期里，爱沙尼亚遭到大规模的网络袭击。黑客目标包括国会、政府部门、银行以至媒体的网站，其攻击规模广泛而且深入，该事件普遍被军事专家视为第一场国家层次的网络战争。爱沙尼亚国防部前国防次长劳里·艾尔曼说，网络攻击的成果之一就是它把网络战概念从国防、情报和网络安全专家研究的重点提升到引起国家政府决策者们关注的高度。2007 年 5 月，爱沙尼亚成立了网络安全战略委员会，并在 2008 年发布了国家网络安全战略。

韩国先后两次遭遇针对政府网站和金融系统等的大规模网络攻击。2009 年 7 月 7 日，网络黑客利用奥地利、格鲁吉亚等五国的 IP 地址对数十个韩国政府部门及商业网站发动大规模分布式拒绝服务（DDoS）攻击。韩国总统府、国防部、外交通商部等政府部门和主要银行、媒体网站同时遭到攻击，瘫痪时间长达 4 小时。攻击虽然并未造成大量中断服务，但持续了很多天，引起了媒体的极大关注。时隔两年，2011 年 3 月，韩国有 40 家网站遭到计算机病毒攻击，这些网站包括韩国总统府青瓦台、外交部、一些大银行、该国两个最大的搜

索引擎和一个主要在线拍卖行的官方网站及美国驻军和韩国军方的一些网站。痛定思痛，在韩国政府 2011 年出台的《国家网络安全总体规划》中，将每年 7 月的第二个星期三设定为“国家网络安全日”；每年的 7 月设为“信息安全月”。

伊朗工业控制系统遭到蠕虫攻击。2010 年，伊朗境内的诸多工业企业遭遇了一种极为特殊的代号为“震网”（Stuxnet）的“电脑蠕虫”攻击，它侵入了工厂企业的控制系统，并有可能取得对一系列核心生产设备，尤其是发电企业的关键控制权。广受西方关注的布舍尔核电站也是其攻击的重点对象。计算机安全专家在对“震网”蠕虫进行了深入分析后发现，这可能是全球第一种投入实战的“网络武器”。新病毒采取了多种先进技术，具有极强的隐身和破坏力。只要计算机操作员将被病毒感染的 U 盘插入 USB 接口，这种病毒就会在不需要任何操作的情况下，取得工业用计算机系统控制权。“震网”是世界上首个针对工业控制系统编写的计算机病毒。这种病毒结构异常复杂、隐蔽性超强，专家认为个人无法制造出这种病毒，只能由国家层面研发。而美国《纽约时报》于数月后爆料，美国和以色列政府可能正是研制“震网”蠕虫的幕后黑手，旨在破坏伊朗的核计划。

二、世界主要国家相继推出国家级网络安全战略

近年来，随着网络安全问题上升到国家安全层面，各国政府纷纷将强化网络空间防御提升到战略高度。到 2014 年，已有 40 多个国家颁布了网络空间国家安全战略，而美国先后颁布的与网络安全有关的文件多达 40 多份。欧盟及其成员国对网络安全的关注度也在不断增加。德国在 2005 年制定了《国家信息设施保护计划》（NPSI），瑞典于 2006 年通过了《瑞典改善互联网络安全全战略》。2007 年爱沙尼亚遭到大规模网络攻击之后，欧盟国家开始将网络空间安全纳入国家安全议程。目前，已经有十几个欧盟成员国（爱沙尼亚、芬兰、斯洛伐克、捷克、法国、德国、立陶宛、卢森堡、荷兰、英国、奥地利、比利时、匈牙利、波兰、罗马尼亚和西班牙）制定和公布了本国的网络空间安全战略，其中英国政府更是在三年之内连续两次出台了国家网络安全战略。在亚太地区，日本、韩国、新加坡、澳大利亚、新西兰等信息通信技术较为发达国家也先后出台了本国的网络安全战略，具体见表 1。

表 1　部分主要国家网络安全战略出台时间表

国家（地区/组织）	战略名称	发布时间
美国	《确保网络空间安全的国家战略》	2003 年
	《网络空间可信身份标志国家战略》	2011 年 4 月
	《网络空间国际战略》	2011 年 5 月
	《网络空间行动战略》	2011 年 7 月
加拿大	《网络安全战略》	2010 年 10 月
俄罗斯	《俄罗斯联邦信息安全学说》	2000 年 6 月
欧盟	《欧盟网络安全战略：公开、安全、可靠的网络空间》	2013 年 2 月
英国	《网络安全战略》	2009 年 6 月
	《网络安全战略》	2011 年 11 月
法国	《信息系统防御与安全战略》	2011 年
德国	《网络安全战略》	2011 年

续表

国家（地区/组织）	战略名称	发布时间
瑞士	《瑞士防范网络威胁国家战略》	2012 年 6 月
西班牙	《国家网络安全战略》	2013 年
澳大利亚	《网络安全战略》	2011 年
日本	《日本保护国民信息安全战略（2010—2013）》	2010 年 5 月
	《保护国家信息安全战略》	2013 年 6 月
韩国	《国家网络安全总体规划》	2011 年 8 月
印度	《国家网络安全战略》	2013 年 7 月
新加坡	《国家网络安全总体规划（2005—2007）》	2005 年
	《国家网络安全总体规划（2008—2012）》	2008 年 4 月
	《国家网络安全总体规划（2013—2018）》	2013 年 7 月

三、各国网络安全战略的特点

（一）主要网络安全威胁分析

网络安全威胁多种多样，纵观各国网络安全战略，主要将安全威胁分为以下四类（基于动机和实施者）：①网络犯罪（犯罪分子实施）；②网络窃密（国家间谍机构或有组织犯罪团伙实施）；③网络恐怖主义（恐怖分子实施）；④网络战（国家支持）。

加拿大战略的分类：网络犯罪、恐怖分子使用互联网、国家支持的网络间谍和军事活动。

爱沙尼亚战略的分类：网络犯罪、网络恐怖主义和网络战。

新西兰战略的分类：网络犯罪、网络窃密、黑客活动、恐怖分子利用网络。

意大利战略的分类：①网络犯罪：在网络空间中实施的带有犯罪意图的所有恶意活动，如欺诈或互联网诈骗、身份盗窃、数据或知识产权的窃取。②网络间谍活动：不正当地获取不一定具有经济价值或商业价值的机密或保密数据。③网络恐怖主义：以意识形态为驱动的利用系统漏洞来发动影响国家或国际组织的活动。④网络战争：以实现具有军事意义的行动优势为目的的在网络空间上实施的活动和行动。

（二）战略目标分析

总体来看，在推动数字经济发展的同时确保国家关键信息系统安全，打造本国在网络空间安全领域的领先地位是各国政府制定网络安全战略所追求的主要目标，并在此基础上明确政府、企业和个人所应扮演的角色和承担的职责。

澳大利亚的战略目标：旨在充分维护一个安全、复原能力强和可信的电子运营环境，从而促进澳大利亚的国家安全并从数字经济中最大限度地获取收益。其战略目标是：①让澳大利亚所有公民都意识到网络风险，确保其计算机安全，并采取行动确保其身份信息、隐私和网上金融的安全。②让澳大利亚企业能利用安全、灵活的信息和通信技术，确保自身操作和客户身份信息与隐私的完整性。③让澳大利亚政府能确保其信息与通信技术的安全性且对风险有抵抗力。

英国的战略目标：①应对网络犯罪，使英国成为世界上商业环境最安全的网络空间之一。

②使英国面对网络攻击的恢复力更强，并保护其在网络空间中的利益。③帮助塑造一个可供英国大众安全使用的、开放的、稳定的、充满活力的网络空间，同时支持社会开放。④构建英国跨层面的知识和技能体系，以便对所有的网络安全目标提供基础支持。

法国的战略目标：旨在确保法国同胞、企业和国家在网络空间中的安全。该战略主要有四个目标：①成为网络防御的世界级强国；②通过保护主权信息，确保法国决策自由；③加强国家关键基础设施的网络安全；④确保网络空间安全。

西班牙的战略总目标：通过加强面对网络攻击时的预防、防卫、侦测和响应能力，保证西班牙能够安全地使用信息与通信系统。

新西兰的战略目标：提高网络安全感知能力及个人与企业对此的理解；提升政府内部网络安全水平；在有关方面之间建立战略联系，以促进关键国家基础设施及其他企业的网络安全。

加拿大的战略目标：保障政府系统安全；与联邦政府外的伙伴合作，确保关键网络系统安全；帮助加拿大人提高网络安全。

荷兰的战略目标：强化数字化社会的安全，提升民众、企业界及政府使用 ICT 技术的信心。

新加坡的战略目标：到 2018 年使新加坡成为“可信且强健”的信息通信中心，具体目标是建成安全、可恢复的信息通信环境和有活力的网络安全生态系统。

俄罗斯制定《国家信息安全学说》的主要目标：①确保遵守宪法规定的公民的各项权利和自由；②发展信息通信工具，保证本国产品打入国际市场；③为信息和电视网络系统提供安全保障；④ 为国家的活动提供信息保障。

（三）各国战略重点比较

从战略重点来看，各国的关注点主要集中在以下一些方面：①注重防御能力建设，包括检测、预警、响应、恢复等方面的能力；②注重重要信息通信系统的安全防护；③注重制度建设，如完善相关的政策法规；④注重公私营领域合作和国际合作；⑤注重人才培养。具体来看：

欧盟提出五大战略重点：①提升网络复原能力；②大幅减少网络犯罪；③制定与《共同安全与防务政策》（CSDP）有关的网络防御政策，发展防御能力；④发展网络安全方面的工业和技术；⑤为欧盟制定一致的国际网络空间政策，宣传欧盟的核心价值观。

法国提出了七项主要工作：①跟踪与分析；②检测、预警、响应；③提升并保持科研、技术、工业和公众的安全能力；④保护国家信息系统和关键基础设施运营商；⑤修订法律；⑥拓展国际合作；⑦沟通、告知和说服。

澳大利亚确定了七个战略重点：①发展威胁感知和反应能力；②改变公民的安全文化；③促进公共部门和私营部门的合作关系；④确保政府系统的安全；⑤与国际社会的合作；⑥建立有效的法律框架；⑦建立一个熟练的网络人才队伍。

新西兰列出三个优先领域：①增加感知能力与网上安全；②保护政府系统和信息；③对突发事件的反应与计划。

韩国提出推进五大方面（预防、检测、应对、制度、基础）的重点战略课题。其中，在检测方面，为了应对整个国家的网络攻击，韩国政府将指导本国的国际通信网关部门、互联网服务提供商、企业及个人共同构筑能探测和防范网络袭击的“三线防御体系”以探测和提

前防范网络袭击，并切断攻击流量。

新加坡提出三个关键方面：①提高关键性信息通信基础设施（CII）的安全性和恢复能力；②宣传促进个人和企业采用信息通信安全措施；③培养信息通信安全专业人才。

瑞士国家战略关注七大领域：研究与发展；网络风险及漏洞分析；网络威胁状况分析；能力建设；国际关系与主动权；连续性及危机公关；有法可依。

当前，网络空间安全已成为国家安全的重要组成部分，将其放在战略高度来进行审视，是我国面临的紧迫任务。他山之石，可以攻玉。本书通过介绍和研究世界主要国家（除美国外）在制定网络空间安全战略方面的经验和做法，希望可以推动我国尽早出台一部国家级的网络安全战略，从而更好地调动和协调各方力量，保护我国在数字时代的核心利益。

第二节　当前全球网络与信息安全形势

进入 21 世纪，随着信息技术的广泛应用和互联网迅速普及，信息浪潮对人类社会的冲击体现出前所未有的渗透力，以互联网为主体的网络空间成为陆海空天电实体空间之外的“第二类”生存空间，人们的生产方式、生活模式、文化生态和冲突形态悄然发生了变化。而当前的全球网络安全事件频发，引发的网络与信息安全问题给经济和社会带来了严重后果，给各国政府在网络与信息安全管理方面带来了巨大挑战。

一、信息泄露引发巨额经济损失和个人隐私担忧

近年来，信息泄露事件频发不止，涉及的范围和造成的影响不断升级。

美国数据隐私研究公司波耐蒙研究所的一项研究显示，2011 年，美国企业处理数据泄露的花费超过 1300 亿美元，每家企业数据泄露的平均代价为 450 万美元。而《美国新闻与世界报道》周刊报道，黑客每年给消费者和企业造成 3750 亿～5750 亿美元的损失。随着互联网使用率的提高，在线信息窃取行为还会增加，损失数字肯定也会增加。美国战略与国际问题研究中心研究报告称，据估计，在线犯罪造成的损失达到世界国内生产总值的 0.8%，北美和欧洲等地区的发达国家所蒙受的损失大于拉美或非洲国家。

信息泄露带来的并不限于经济损失，部分事件因涉及个人隐私，还可能影响社会稳定。例如，2013 年发生在我国的如家等快捷酒店开房记录泄露，以及中国人寿 80 万份保单信息泄密事件等。

二、网络安全威胁日益严峻

（一）政府机关等关键部门仍然是网络攻击的主要对象

数据显示，当前全球网络攻击事件的数量不断上升，网络攻击的频次和强度均呈增长态势。而 Lulz Security 、“匿名者”等国际黑客组织通常以全球的政府机构、金融、卫生等关键部门为攻击对象。仅在 2011 年 5～6 月期间的 50 天内，Lulz Security、“匿名者”这两个黑客组织就攻破国际货币基金组织、美国参议院、中央情报局和英国有组织犯罪重案局的网站，领导了针对美国银行、北约的攻击。世界经济论坛公布的《2012 年全球风险》报告显示，针对政府以及商业机构的网络攻击已经成为危及全球稳定的五大威胁之一。

尽管多国政府积极采取行动，抓捕涉嫌对政府网络及商业系统进行攻击的黑客，但这些黑客组织依然活跃，频频做出网络攻击的动作。如，2013 年 11 月，国际黑客组织“匿名者”成员通过网络视频发出威胁，声称如果新加坡政府不重新考虑有关新闻网站运营的新规定，将会攻击新加坡的一些网络设施。与新加坡有类似遭遇的还有很多国家。

而日本政府 2014 年 7 月公布消息称，2013 年度该国政府机构网络受到 508 万次非法访问，其中包括网络攻击等行为。这一数字是上一年度的约 5 倍，且攻击手法的多样化和巧妙化日渐突出。

（二）关键基础设施成为网络威胁的目标

进入 21 世纪，互联网已经成为国家关键基础设施的重要组成部分，与能源供应和供水系统一样不可或缺。人类社会的各个方面依赖互联网的正常运转，网络一旦瘫痪，对于国防安全、经济安全的影响将是不可估量的。而英国 BAE 系统公司的最新研究显示，网络威胁的目标正从数据泄露转向全球关键基础设施。

虽然网络攻击不像炸弹袭击那样能够对目标进行物理摧毁，但仍然会给平民百姓及其财产带来灾难性的后果。国际红十字会的法律顾问基瑟尔说，许多专家都发出警告，网络攻击可以打开水坝导致洪水泛滥，或者使化学工厂和核电站发生环境灾难，给数以千计的平民百姓的生命和健康造成不堪设想的损害。

三、网络战成为战争重要组成部分

从国家层面看，各国备战“网络战”的意图更加明显，网络安全厂商 McAfee 2009 年 11 月发布发表的一份题为《网络战时代已在眼前》的研究报告称，全球一些主要国家已投身于一场网络空间里的“冷战”。这些国家正在努力扩充自己的“网络武器库”，开展相关的间谍活动，并进行网络测试，为开展网络战积极做准备，报告引用美国国家安全局副局长威廉姆·克罗威尔的话，“未来 20～30 年，数字化攻击将逐渐成为战争的一个重要组成部分”。据外媒 2014 年 4 月报道，英国最大保险组织劳合社的成员公司 Aegis London 研究了能源领域网络威胁的演进及其对包括英国在内的欧洲各国、美国和加拿大的关键基础设施的影响。研究结果显示，对于电力公司和公用事业机构来说，由国家发起的网络攻击带来的威胁非常严重且在不断演变。

（一）美国在网络战中处于优势地位

美国智库兰德公司早在 2009 年就指出，“网络战是信息时代的核武器”。2010 年 9 月，伊朗布舍尔核电站遭到“震网”（Stuxnet）蠕虫攻击，导致核电设施推迟启用。业界普遍认为，这是第一次从虚拟世界对现实物理世界的网络攻击。2012 年 6 月，美国《纽约时报》曾透露，美国总统奥巴马秘密下令进行“震网”攻击。旨在破坏伊朗的核浓缩设施。2011 年、2012 年伊朗先后破获了“繁星”（Stars）、“火焰”（Flame）、“高斯”（Gauss）等一系列超复杂恶意软件，这些恶意软件被认为是来自某个敌对国家。正是由于这些受到国家资助的恶意软件不断涌现，一个网络冷战的新时代正在形成。

美国在网络战敢于先下手，并且动作频频，依靠的是其雄厚的软硬件实力。首先，美国控制了全球互联网的大部分设施。例如，全球互联网 13 台根域名服务器中，有 10 台在美国；微软操作系统在个人计算机操作系统领域的市场占有率在 85%以上；思科核心交换机、路由器遍布全球网络节点；英特尔的 CPU 占据全球计算机 90%以上的市场份额；谷歌在全球搜索市场份额高达 68%；高通和苹果的芯片占据了 60%的智能手机市场。如果美国愿意，它可以让世界上任何一个国家的网络和信息系统立刻瘫痪。除硬件之外，美国网络科技公司所存储的数据也完全在美国国安局控制之下，美国政府想要哪个用户的个人资料，这些科技公司都会积极提供。例如，谷歌提供的《透明度报告》可以看出，美国政府 2012 年下半年共向谷歌提出了 8438 次数据要求，涉及账户 14 791 个，88%的要求被执行了。

（二）网络战在国际冲突中的作用显著

在乌克兰局势动荡、伊拉克内战等国际冲突中，网络对抗已经成为各界关注的焦点之一，出现了利用网络战来破坏敌方关键基础设施和部队 C4ISR（指挥、控制、通信及计算机系统）的战略。可以预见，未来，网络战将更频繁地出现战争中。

据美国防务新闻网站报道，多份报告表明乌克兰已经遭受了俄罗斯发起的具有高度针对性的网络攻击，这些攻击的目标是电信基础设施以及新闻媒体机构。

伊拉克反政府武装“伊拉克和黎凡特伊斯兰国”（ISIS）被外界认为最擅长使用网络的组织之一。在 6 月份第一周，伊拉克经历了全国性的网络中断，6 月 5 日一次 3 小时的中断导致了该国 80%的交通系统失去联系。有媒体称，这种大范围的中断是 ISIS 行动导致的。

网络在朝鲜半岛局势中发挥着越来越突出的作用。韩国于 2010 年即成立了网络司令部，来防范朝鲜精英黑客的威胁。据韩国国防部消息，韩国正在研发一款进攻性网络武器，针对朝鲜的核武器计划。这一战略计划的第二阶段要求开发一款网络工具，就像破坏了伊朗铀浓缩设施的“震网”病毒一样，以此来削弱朝鲜的导弹和核设施。

朝鲜也积极培养自己的网络攻击力量。有报道称，朝鲜培养的黑客部队规模甚至超过美国。朝鲜侦查总局下设有黑客部队，该部队的黑客达 1200 多人。而且近两年还在扩编网络战部队，规模约达 5900 人。

四、网络恐怖主义成蔓延之势

1997 年，美国加州情报与安全研究所资深研究员柏利·科林第一次提出了“网络恐怖主义”一词，认为它是网络与恐怖主义相结合的产物。国际社会认为，与传统意义上的恐怖主义一样，恐怖组织一切与网络有关的活动都可列入网络恐怖的范畴，包括恐怖宣传、招募人员、传授暴恐技术、筹措资金、组织和策划恐怖袭击、实施网络攻击和破坏等。现实与虚拟世界的结合处成为恐怖分子最好的突破口和进攻点，与恐怖分子相关的网站数量增长迅速，遍布全球。

互联网是恐怖分子发动心理战和宣传战的“天然战场”。美国参议院国土安全和政府事务委员会 2008 年报告称，“基地”组织已逐步建立起一个遍及全球的多层面网络宣传网，从制作到传播都有严格程序。以色列海法大学传播学教授加布里埃尔·威曼统计，1998 年与恐怖分子相关的网站有 12 个，如今已增至近 1 万个。2011 年俄罗斯境内极端主义网站达 7500 家；东南亚地区以印尼、马来语为主宣扬极端思想的网站和论坛增长快速，“印尼解放党”、“天堂圣战”等网站声势浩大。数据显示，近年来，“东伊运”制作的恐怖音视频数量呈明显增长态势，尤其是在 2013 年出现爆发式增长。网络成了这些恐怖音视频播、散播的最佳渠道，是“疆独”组织传播极端主义思想的重要手段。

恐怖组织利用网络大量收集各国政府信息，网络敛财向智能化发展。网上内容包罗万象，恐怖分子既能获取有关国家的政治、经济和军事信息，也可掌握武器制造、黑客技术等。在阿富汗发现的“基地”组织电脑中，就存有如何利用美国通信、电力、水力分布网的指示和计划信息，以及一些水坝的详细构造图。此外，恐怖组织的网络敛财已摆脱原始的汇兑募捐方式，朝智能方向发展。恐怖组织还打着“慈善”幌子骗取钱财，如利用与“基地”及塔利班联系密切的“全球救援基金会”、打着人道救援旗号的非政府组织网站等。

恐怖组织的网上活动有了新的手法，呈现新的特点。首先，脸谱网等新媒体的普及掀起新一轮网络恐怖潮。其次，催生大量“本土恐怖”。“基地”等恐怖组织的“网上轰炸”开始把年轻人，尤其是西方的年轻人作为新鲜对象。“伊拉克和黎凡特伊斯兰国”的宣传视频亦针对英国等欧洲国家。美国华盛顿智库两党政策中心担心，“美国面临的最大恐怖威胁不再来自阿富汗和巴基斯坦的边境山区，而是来自美国国内滋生的本土恐怖分子”。再次，“独狼”式恐怖分子激增，网络技术已成“独狼”赖以生存的血液。“独狼”无须现身就可通过网站和社交媒体等工具获取各地信息，甚至直接实施网络恐袭。“基地”组织阿拉伯半岛分支就专门制作、出版英文网络杂志《激励》，煽动西方极端分子发动“独狼”式恐怖袭击。最后，恐怖分子开始从利用网络转向攻击网络，激进分子、黑客、恐怖分子之间的界线趋于模糊。

五、从“棱镜门”事件看网络霸权主义

2013 年 6 月，前美国中央情报局雇员爱德华·斯诺登将美国国家安全局的“棱镜”等一系列秘密项目披露出来，导致全球舆论震荡，此事件被称为“棱镜门”。“棱镜”计划之所以引起全球恐慌，重要原因是其反映出全球信息流向长期不平衡，全球各国的信息都大量流向美国，如果美国对这些信息进行关注整理，将有能力控制全球各国的互联网。

美国在网络信息安全领域积极布局，有效把握了信息控制权。一是基于美国 IT 企业所提供的先进便捷的互联网服务，全球用户个人信息都向美国单方聚合；二是依托成熟价值观和法律机制打造出的优势地位和输出能力，美国持续而主动地深刻影响全球的政治与文化。

棱镜门事件爆发后，美国对包括中国在内的各国互联网目标的监控行为被公之于众，促使世界各国更加重视网络安全问题，同时引起网络安全界对国内 IT 基础设施的思考和担忧。

综上所述，网络与信息安全已演化为全球性和战略性问题，激发了社会形态和国际竞争的演化。国际关系学院战略与安全研究中心编写的《中国国家安全研究报告（2014）》指出，从国际看，为争夺网络空间的制信息权，大国围绕保持网络空间发展权，保护互联网用户隐私，打击网络犯罪，防止、威慑和劝阻网络空间破坏行为等问题展开了一系列角逐。世界主要国家已深刻认识到网络空间安全的重要意义，纷纷出台相关安全战略，增设相应机构，加强网络安全建设。

第三节　主要国家网络信息安全战略及措施

随着全球信息化步伐的加快和互联网渗透的日益加深，美日俄欧等主要国家及地区对网络信息安全的重视程度日益提高，并纷纷制定了相关战略规划，出台了多种网络信息安全举措。如将网络信息安全战略列为国家安全战略的主要组成部分，并从国家层面进行顶层设计，以政府、行业、民众“三位一体”为管理和监督主体，以政策法规为后盾，以保护关键网络信息资源为核心，以网络管理系统为手段，对网络信息进行多管齐下、进退有度、封堵结合的管理。

一、将网络信息安全纳入国家安全战略，加强顶层设计

网络信息安全挑战的规模和复杂性对强有力的国家领导提出了要求，美俄等网络强国也纷纷将网络信息安全上升到国家层面，确立以国家主导的网络信息管控体制机制。

美国将网络信息安全纳入国家长期发展战略。2000 年，美国总统克林顿在任职期间颁布的《国家安全战略》将信息安全列为国家战略的重要组成部分。“9·11”恐怖事件发生后，布什政府将网络信息安全战略提升至国家战略的核心地位。奥巴马上任伊始就开始推进网络安全评估，并先后发布相关战略文件，确立网络信息安全在国家战略中的地位，给予总统“宣布网络安全的紧急状态”的权力，允许“关闭或限制事关国家安全的重要信息网络”，同时还成立了网络战司令部，可见其对互联网络安全全的重视达到了空前的高度。美国三届政府在网络信息安全战略方面呈现出“全面防御—攻防结合—攻击为主、网络震慑”的进化链条，不尽相同却一脉相承。

与此同时，美国等国制定的网络安全国家战略从多个方面入手，力图统筹规划、全面覆盖。例如在规划网络安全战略时，美国对包括部门职责划分、基础设施建设与保护、网络战能力培养等多方面进行了顶层设计。在美国发布的《网络空间安全国家战略》中，明确要对国家信息基础设施进行安全保障，任命白宫网络安全协调官协调美国的网络安全事务，并成立网络战司令部加强网络攻防能力等。而欧盟则根据自身特点，将网络信息安全上升到社会形态的高度，力图统领各成员国的网络信息安全工作。欧盟于 2007 年正式通过了关于建立欧洲信息安全社会战略的决议，要求在全社会实现网络和信息系统的可用性、保密性与完整性，以原则性战略规划统领各成员国的网络信息安全战略。

日本、俄罗斯等国也制定了较为具体、细致的网络信息安全国家战略。例如日本较为关注信息安全保密，其发布的《信息安全总体战略》将信息安全置于国家安全的层面。另外，日本还出台了“e-Japan 重点计划”，首项措施就是确保 IT 社会安全的保密政策。俄罗斯则在信息安全机制建设方面发力。2013 年 1 月，俄总统普京签署总统令，责成俄联邦安全总局建立国家计算机信息安全机制，用来监测、防范和消除信息安全隐患，有效保护国家层面的网络信息安全。

二、加强网络信息安全立法，营造较为成熟的法律环境

构建网络信息安全与治理的法律法规体系，以法律对网络信息进行约束与管理，同时为网络信息治理提供坚实的后盾，是美法等国在制定网络信息安全战略时考虑的重点工作。

美韩等国构建的网络信息安全法律体系或依据其法系，采取多层立法；或依据互联网特性，多法结合。例如美国互联网相关法律法规分为联邦和州两个层次。前者是最高原则，其涉及面相对来说较为全面和广泛，既有针对因特网的宏观的整体规范，也有微观的具体规定。后者则根据各州实际情况，更加具有针对性，能因地制宜。当发生分歧时，联邦政府享有管理优先权。韩国政府针对互联网内容管理采用了普法和专法相结合的方法，加强专法管理的针对性，避免了普法在网络管理权限方面的分散，形成了比较完善的互联网法律管理体系。其普法主要是以《电子通信商务法》等为管理框架，专法则如《不当互联网站点鉴定标准》、《互联网内容过滤法令》等，对具体的互联网事务做出规定。韩国近年来陆续出台和修订了《促进信息化基本法》、《信息通信基本保护法》和《电信事业法》等多部法律，对包括对博客在内的各种新兴网络行为和现象加强管理，为打击利用新兴网络手段进行犯罪的行为提供了法律依据。

法美等积极探索，及时预防，以法律手段防患于未然。法国在互联网治理方面的立法在欧洲处于领先水平，早在 20 世纪 70 年代末，法国就成立了“信息与自由国家委员会”，针对网络引起的社会适应与变革问题做过许多探索，在电视台等各种媒体上组织过大规模的讨论。而美国则在 1996—2001 年互联网发展高速期中，通过了《禁止电子盗窃法》、《反域名抢注消费者保护法》、《数位千年版权法》、《互联网税务自由法》、《儿童互联网保护法》等一大批法律法规，为应对互联网快速发展带来的种种问题奠定了较为坚实的基础。

英德在网络立法方面态度较为积极，其网络信息安全法律法规布局全面，且“出手强硬”。英国十分重视依法监管网络信息，既有明确赋予相关机构监听权力的《规范调查权法案》，也有打击互联网犯罪的《防止滥用电脑法》，还有保护个人隐私的《数据保护权法》和《隐私和电子通信条例》，网络立法可谓面面俱到。2012 年以来，英国政府对互联网的管理“出手强硬”，推动议会通过立法对互联网采取更为严格的管理办法，例如警察和情报部门能够在特定情况下获取通信数据；允许互联网服务供应商及电信公司安装硬件，储存通信数据长达一年。新立法还要求社交网站保留用户相关信息记录，以备查询。对于政府推动出台新的网络管理法案，尽管有公众提出质疑，但卡梅伦政府的态度十分坚决。德国于 1997 年制定了世界上第一部规范互联网管理的法律《多媒体法》，后又相继出台了《电信服务法》、《数据保护法》、《数字签名法》与之相配套。此后又根据网络发展的需要，对《刑法法典》、《治安条例法》、《危害青少年传播出版法》和《著作权法》等进行修改完善，进一步加强了对互联网的管理和控制，逐步建立了一整套较为完备的互联网管理法律体系。

三、建立较为完备的网络信息安全管理机构，完善互联网管理体系

建立专门的管理机构，构建权责明确、协同联动的互联网管理体系，为网络信息安全工作提供体系保障，是俄日等国在网络信息安全管理方面较为重视的工作之一。

俄罗斯建立了以政府为主导，层级严密、分工明确的互联网管理体系。俄罗斯曾设置联邦政府通信与信息局，集情报搜集和信息安全两项职责于一身。2004 年该机构被撤销后，