探寻网络

和平

探寻网络和平

国际电信联盟秘书长

哈玛德•图埃

及

世界科学家联合会

信息安全常设监督委员会

2011年1月

法律告示

各位作者本人保留其作品的版权。酌情引用了第三方资料。国际电信联盟（ITU，国际电联）对本出版物中引用的包括外部网站在内的外部资料来源的内容不承担责任。

无论国际电联还是代表国际电联行事的任何人，对本出版物中所含信息可能受到的利用都不承担责任。

免责声明

本出版物各章内容代表作者本人的意见，不表示他们任职的组织或隶属的组织赞同这些意见，也并非要代表这些组织的意见。文中提到或引用具体的国家、公司、产品、举措或指南绝不意味着国际电联、作者或作者隶属的任何其他组织承认其优于其他未提及的同类事物或予以推荐。

致谢

国际电联秘书长和世界科学家联合会感谢Jody Westby、Henning Wegener和所有把自己对这一正在形成的全球问题的见解综合在一起的作者。秘书长还向世界科学家联合会主席Antonino Zichichi教授表示感谢，并向国际电联综合战略处主任Alexander Ntoko表示感谢，特别是向领导本出版物编写和协调工作的Jeoung Hee Kim表示真诚的感谢；向Rebekah Lewis、Deepti Venkateswar、Preetam Maloor、Marco Obiso和Elizabeth Aschenbrener表示感谢；向Claude Briand及其团队表示感谢；向国际电联和世界科学联合会的众多其他人员表示感谢，没有他们的贡献，本出版物就无法面市。

如果您有评论意见，请通过strategy@itu.int与国际电信联盟综合战略处联系。

目录

页码

缩写表

AIS	自动化信息系统
ARPA	高级研究计划署（美国国防部）
C3	命令、控制和通信
CoE	欧洲委员会
COP	保护上网儿童举措（国际电联）
CRS	美国国会研究服务处
CSCW	计算机支持的协同工作
DARPA	国防部高级研究计划署（美国国防部）
DNS	域名系统
ECOSOC	经济及社会理事会（联合国）
ESCAPE	电子安全协作专家应用平台（IMPACT）
EU	欧洲联盟
FG Smart	智能电网焦点组
FTC	联邦贸易委员会（美国）
GCA	全球网络安全议程（国际电联）
GRC	全球响应中心（IMPACT）
HRC	人权事务委员会（联合国）
ICT	信息通信技术
IGF	互联网管理论坛
IMPACT	国际打击网络威胁多边伙伴关系（马来西亚）
IP	网际协议
ISOC	互联网社会

IT	信息技术
ITR	《国际电信规则》（国际电联）
ITU	国际电信联盟（国际电联）
ITU-T	国际电联电信标准化部门
LOAC	武装冲突法
MIT	麻省理工学院
NATO	北大西洋公约组织
NEWS	网络预警系统（IMPACT）
NPT	不扩散核武器条约
NSF	美国国家科学基金
RFID	射频识别
PDA	数字个人助理
PMP	信息安全常设监督委员会（世界科学家联合会）
SCADA	数据采集与监控
SOA	面向服务体系结构
TCP	传输控制协议
UN	联合国
UNCPCJ	联合国预防犯罪和刑事司法大会（联合国）
UNESCO	联合国教育、科学及文化组织（联合国）
UNODC	联合国毒品和犯罪问题办公室（联合国）
URL	统一资源定位符
WFS	世界科学家联合会
WSIS	信息社会世界峰会

国际电信联盟和全球网络安全议程

国际电信联盟（ITU，国际电联）是联合国负责信息通信技术事务的专门机构，也是各国政府和私营部门发展网络和服务的全球协调组织。

信息社会世界峰会（WSIS）和国际电联2006年全权代表大会之后，树立使用信息通信技术（ICT）的信心并提高安全性成为国际电联的一个重要作用。参加WSIS的各国首脑、政府元首和其他全球领袖以及国际电联成员国，委托国际电联采取切实步骤以抑制信息社会面临的威胁和不安全性。为完成这一使命，国际电联秘书长哈玛德•图埃博士于2007年发起了《全球网络安全议程》（GCA）活动，将其作为国际合作的框架。

《全球网络安全议程》旨在加强信息社会的信心和安全性，促进合作，提高效能，鼓励所有相关利益攸关方开展合作，避免与现有举措重复。《全球网络安全议程》是第一个真正意义上由利益攸关多方和公私联盟组成的打击网络威胁全球联盟。2008年国际电联和国际打击网络威胁多边伙伴关系（IMPACT）正式签署了一份谅解备忘录，之后位于马来西亚赛城的IMPACT技术总部成为《全球网络安全议程》在现实中的家。IMPACT是一个国际性公私举措，旨在加强全球社会预防、保护和响应网络威胁的能力。该协作向国际电联192个成员国提供专业技能、设施和资源，以有效增强全球社会预防、保护和打击响应网络威胁的能力。成立之后，《全球网络安全议程》得到了世界上诸多领袖和网络安全专家的支持。哥斯达黎加共和国前总统及诺贝尔奖获得者奥斯卡•阿里亚斯•桑切斯博士阁下以及布基纳法索总统布莱斯•孔波雷阁下均为全球网络安全议程的形象大使。

GCA已推动相关举措，如保护上网儿童（COP），建立网络安全关口等。通过与IMPACT建立伙伴关系并在全球互联网主要参与者的支持下，目前GCA正在为世界一些国家提供网络安全解决方案。国际电联感谢哥斯达黎加总统劳拉•钦奇利亚阁下担任国际电联“保护上网儿童”举措的形象大使。

世界科学家联合会及其信息安全常设监督委员会

世界科学家联合会（WFS）于1973年在西西里岛埃里切由Isidor Isaac Rabi和Antonino Zichichi为首的一些杰出科学家创立。从那时起，许多其他科学家也加入到该联合会。其中包括T. D. Lee、Laura Fermi、Eugene Wigner、Paul Dirac和Piotr Kapitza。

世界科学家联合会是一个自由社团，目前已壮大到拥有来自110个国家的1万多名科学家。联合会所有成员分享同样的目标和理念，自发为维护联合会的原则做出贡献。联合会旨在促进世界各地 — 东西南北的科学家和研究人员间的国际科技合作。联合会及其成员力争实现信息自由交流，使科学发现和进步成果不再局限于被少数人拥有。其目标是在所有国家之间分享知识，使每一个人都能享受到科学进步带来的益处。

世界科学家联合会是由位于埃里切的一个科技文化中心促成的。该中心以物理学家埃托雷•马约拉纳的名字命名，被称做“**埃托雷•马约拉纳基金会和科学文化中心**”。该中心一直被称做“第三千年大学”，是一支全球性教育力量。自1963年成立至今，该中心已在123个学院开展教学工作，设置了1 497门课程，参与者来自140个国家的932所大学和实验室，共103 484人（其中有125名诺贝尔获奖者）。

埃托雷•马约拉纳中心系世界科学家联合会的前身，在出现全球突发事件时采取行动缓解事态。世界科学家联合会很快就确定了**全球突发**事件的15个等级，并开始组织反击这些威胁的战斗。其主要成就之一是于1982年拟订了《**埃里切声明**》，该声明由Paul Dirac、Piotr Kapitza 和Antonino Zichichi起草，明确制定了联合会的理念和一系列将理念付诸实践的建议。另一个里程碑是举办了一系列国际核战争研讨会。这些研讨会对降低全球核灾难危机产生了极大影响，最终对结束冷战做出了贡献。1986年，通过一群杰出科学家（其中大部分是WFS成员）的活动，**在日内瓦成立了科学文化国际中心（ICSC）世界实验室**，以实现《埃里切声明》所制定的目标。

世界科学家联合会在2001年成立了信息安全常设监督委员会（PMP）。其报告《迈向普遍有序的网络世界：网络犯罪到网络战的威胁管理》是2003年日内瓦召开的联合国信息社会世界峰会第一阶段由民间团体提交的最重要的文件之一。常设监督委员会出版了许多有关网络安全和网络战的文件，作为极其重要的全球突发事件议题在每年8月埃里切举行的全会上定期报告信息安全问题。2009年8月，常设监督委员会对潜在网络战将扰乱社会、导致不必要的伤害和痛苦非常担忧。于是起草了《**关于网络稳定与网络和平原则的埃里切宣言**》，并于2009年8月20日在埃里切第42届全球突发事件国际研讨会上由世界科学家联合会全会通过。该宣言已分发至联合国所有会员国。

常设监督委员会由来自柏林和马德里的Henning Wegener大使和来自华盛顿特区Global Cyber Risk LLC公司的首席执行官Jody R. Westby博士共同主持。常设监督委员会中对本书做出贡献的成员还包括：

对本书做出贡献的常设委员会成员

William Barletta

William A. Barletta是美国粒子加速学院，一个国家级研究生项目的执行主任。他是麻省理工学院和加利福尼亚大学洛杉矶分院的物理学兼职教授。他同时是斯洛文尼亚卢布尔雅那大学经济学客座教授，在那里教授战略管理。他还是意大利同步辐射光源实验室主席的高级顾问。此外，他是美国物理学会研究员，是该学会公共事务专门组成员，也是该学会国际物理学论坛副主席和该学会粒子束物理学部副主席。他是5本著作的合著人和编辑，发表了150余篇文章，内容涉及广泛的技术性主题。barletta@mit.edu

Vladimir Britkov

Vladimir B. Britkov（博士）是位于莫斯科的俄罗斯科学院系统分析学院信息建模实验室主任。他也是莫斯科物理技术学院（国立大学）系统分析和系统建模领域的特聘教授。其主要研究领域包括基于计算机的建模与

仿真，以及基于知识用于决策支撑的系统应用。他一直是国际应急管理协会（TIEMS）董事会成员。他还是建模与仿真领域各种科学期刊编辑委员会成员和各种国际工作组成员。2003年以来，他担任世界科学家联合会信息安全常设监督委员会成员。britkov@gmail.com

Jacques Bus

Jacques Bus是“欧盟数字信任”部门独立顾问，从事信息通信技术（ICT）信任与安全领域工作，也是卢森堡大学研究员。经过12年在数学领域的研究工作，他开始侧重研究管理。他为欧盟ICT研究项目工作了20多年。过去6年他是“ICT信任与安全”部门主管，现为世界科学家联合会信息安全常设监督委员会成员。他就信任、安全、隐私和身份管理等内容著书，并就这些问题发表演讲。www.digitrust.eu

Axel Lehmann

Axel Lehmann是慕尼黑联邦国防大学信息学系正教授，从事建模和仿真研究。他也是该大学智能系统（ITIS）学院院长。其主要研究领域包括基于计算机的建模和仿真、基于知识用于诊断和决策支撑的系统应用以及创新式计算机的结构设计。他曾任建模与仿真国际协会主席和德国信息社会研究员。他是建模和仿真领域各种科技杂志编辑委员会成员，也是一些国际工作组和评审委员会，如欧盟评审委员会的成员。2001年起，他是世界科学家联合会信息安全常设监督委员会成员。axel.lehmann@unibw.de

哈玛德•图埃

2007年1月以来，哈玛德•图埃博士任国际电信联盟（ITU）秘书长，2010年10月在墨西哥瓜达拉哈拉举行的国际电联全权代表大会上当选连任。1998-2006年期间，他任国际电联电信发展局（BDT）主任，在公共和私营领域均具有丰富的专业经验。他于1953年出生，拥有列宁格勒（前苏联城市名称）电子电信技术学院电气工程硕士学位和莫斯科电子、电信和信息学学院（MTUCI，俄罗斯）博士学位。他承诺把国际电联打造成具有革新精神和前瞻眼光的国际组织，适应快速变化的ICT环境带来的挑战，继续担当落实信息社会世界峰会（WSIS）决议内容和实现“千年发展目标”（MDG）的先锋。hamadoun.toure@itu.int

Vitali Tsygichko

V.N. Tsygichko博士是俄罗斯军队的一名上校，现已退休。他是俄罗斯自然科学研究院正式成员，1985年以来担任俄罗斯科学院（ISA RAS）系统分析研究所首席研究员。目前，他是俄罗斯联邦外交部信息安全问题专家。1967年以来，他一直在国防部中央研究所任职，从事军事行动数学模拟工作。1988-1991年期间，他率领一个自主研究中心开展对国家安全问题的研究。Tsygichko博士的科学兴趣包括模仿社会经济进程方法和系统问题、决策理论、分析应用系统、社会经济预测理论和方法、确保国家安全和战略稳定性、信息安全问题以及地缘政治问题。他发表了200篇论文，撰写了8本著作。他是一些杂志如《军事思想》、《军事通讯》、《独立军事评论》和许多国外出版物的固定作者。他毕业于Ryazan炮兵军事学校和Dzerzhinsky军事学院，持有理学（工程）博士学位和教授证书。vtsygichko@inbox.ru

Henning Wegener

Henning Wegener是德国前大使。1981-1986年担任驻日内瓦裁军大使，1986-1991年担任北大西洋公约组织政治事务助理秘书长，之后任驻西班牙大使。2001-2009期间，Wegener大使担任世界科学家联合会信息安全常设监督委员会副主席，现担任主席。他负责外交和安全政策领域工作，包括网络安全政策方面的出版物。Wegener拥有耶鲁法学院法律学博士学位。henningwegener@hotmail.com

Jody R. Westby

Jody R. Westby是位于华盛顿特区的全球网络风险有限公司的首席执行官，也是卡内基梅隆网络实验室特聘研究员。她在隐私、安全、网络犯罪、关键基础设施保护和经济间谍等方面为世界上的公共和私营部门客户提供咨询和法律服务。她是美国律师协会（ABA）隐私和计算机犯罪委员会（科技法律部）主席，并代表美国律师协会参加国家律师和科学家大会。Westby女士曾是国际电联秘书长的高级专家组成员，领导了国际电联

网络犯罪立法工具包的开发工作。她是世界科学家联合会信息安全常设监督委员会联合主席。她是4本有关国际网络犯罪、网络安全、隐私内容书籍的合著人和编辑，另外还发表了许多文章。她在全球就这些议题发表演说。westby@globalcyberrisk.com

序

我们处于2011年的世界，我们享受着无限的全球信息社会的福祉，但随之而来的还有网络攻击的威胁。这些网络攻击可以在任何地方发生，并在转眼间带来巨大的毁坏。随着信息通信技术（ICT）与重要的国家基础设施链接，这种潜在的毁坏正在以指数方式增长。

现在，我们必须行动起来，遏制这一日益增长的威胁。

信息社会世界峰会（WSIS）上，世界领袖们和各国政府委托国际电信联盟（ITU）创建一个协调机制，树立使用ICT的信心和提高安全性。从那时起，图埃秘书长发起了全球网络安全议程（GCA）活动。国际电联采取了一系列举措来积极完成峰会的委托。其中，国际电联对其成员国所面临的网络威胁最为关注。

世界科学家联合会（WFS）致力于促进世界各地科学家和研究人员之间开展科技国际合作。它力求促进信息的自由交换以使每个人都能享受到科学进步带来的益处。2009年，WFS信息安全常设监督委员会（PMP）起草了《关于网络稳定与网络和平原则的埃里切宣言》，呼吁国际社会共同采取行动，确保信息网络和系统保持稳定、可靠、可用和可信性。该宣言于2009年8月20日在西西里岛埃里切的第42届全球突发事件国际研讨会上通过，并已分发至国际电联所有成员国。

为实现确保网络安全的共同目标，开展国际电联与科技团体成员之间的合作至关重要。专家们拥有改变全球面貌的技术见解和专业知识。没有他们的参与，我们无法有效对抗网络战的威胁。

本书让这些科学团体发出声音，发表意见。它代表了建立国际合作应对网络挑战的一个必要步骤。我们对有这样一个机会就这一重要议题发表意见表示感谢。

国际电信联盟
秘书长
哈玛德•图埃博士

世界科学家联合会
主席
Antonino Zichichi教授（博士）

1 引言

作者：Jody R. Westby

本书旨在通过阐述以下内容推广全球网络安全的概念：

- 审查ICT 如何支撑日常生活;
- 评估目前的网络威胁和趋势；
- 分析网络犯罪和网络冲突的影响；
- 评定目前法律框架的有效性；
- 定义网络和平概念，将其作为网络空间和平行为高于一切的指导原则；以及
- 设计一条前进的道路。

互联网是社会的中枢系统。每个关键的基础设施部门都依赖于ICT。它们被数据采集与监控系统（SCADA）和其他复杂的信息技术(IT)程序控制，而这些系统和程序均与互联网相连。例如，医院和医疗中心使用ICT做每件事，从急救出诊到生命支撑系统。石油、天然气和交通部门部署的尖端处理和导航系统完全计算机化，金融公司通过电子付费系统和电子处理运作业务。政府依赖ICT提供服务、对各种地域进行管理，维护公共安全和保卫国土。商业依赖计算机系统来管理供给链、客户关系和资金流并执行生产功能。通信系统和公共电网更是所有其他行业依赖的“超级关键”的基础设施。

如今，互联网亦与每个人的工作和生活密不可分。无论工作、学习或者娱乐，ICT均渗透其中。互联网使得知识和信息以历史上前所未有的水平传播。社交网络以与政府完全分离或政府始料不及的方式将人们链接到一起，影响着他们的交往方式。它给予个人展现自我的能力，通过在很大程度上不受国界、外交和政治机制的约束，散播不同寻常的想法。今天，简

单通过其创建内容并向全球传播，某个个人就能快速影响他人的观念、价值观、想法和偏见。

然而，互联网的普及也催生了犯罪活动，开辟了情报搜集和冲突的新途径。操作系统、软件和安全设定中存在的漏洞给对平民百姓提供的基本服务造成了威胁，促进了经济间谍活动，影响了政府运作。病毒、蠕虫、分布式拒绝服务(DDoS)攻击，偷窃专有数据、垃圾邮件和诈骗，所有这些都削弱了ICT的可靠性和社会、经济的运行能力。

有效的安全软件将改善系统的恢复能力，帮助检测、防止和减轻这些行为。技术补丁和新的技术革新将有助于阻止和跟踪攻击，协调一致的网络犯罪法规将促进对网络犯罪的调查和起诉。每个领域都还有许多工作要做。但最危险和具有潜在破坏性的问题是当国家采用这种战术发动网络冲突[1]的时候。如今有很多政治和军事冲突蔓延到网络世界的例子，极大破坏了人们对ICT的信任，带来了严重的风险。本书后面几章将描述其中的一些例子。

信息社会出现之前，权力和领导权通常被那些拥有政权、军事优势和经济支配能力的人所持有。国家和国际组织规定了规范和价值观，武装冲突受基于保护领土完整和陆地、空中和海上防御能力的法律和公约管辖。然而今天，互联网彻底改变了这一权力平衡。没有什么能比互联网自身历史更好地证明这一点。

全球性事件可能是重要的诱因。第二次世界大战后不久，美国面临着一类新的敌人：冷战、共产主义和核打击威胁。苏联发射了第一颗人造地球卫星Sputnik。出于对苏联科技力量的担忧，艾森豪威尔总统成立了美国国防部高级研究项目署（ARPA），现在的DARPA，负责协调美国所有技术研究工作。[2] 麻省理工学院(MIT)聘请J.C.R. Licklider牵头开展ARPA计算机研

1 网络冲突一词旨在包含标记为“网络战”的各种情况。

2 《网络简史》，见财富杂志，2000年10月9日，第34页，

究项目。几个月前，他出版了关于讨论互联计算机“银河网络”使程序和文件能够共享的一系列备忘录。Vint Cerf、Bob Kahn和其他一些“互联网之父”随后指出，“实质上，这一概念非常类似于当今的互联网”。[3]

大约在同一时间，空军对遭受核进攻之后保持指挥和控制运作能力感到担忧，于是委托兰德公司开展一项研究，让可能幸存的军队网络能提供“最低限度的基本通信”。[4] 兰德公司提交了一份由Paul Baran撰写的报告，结束了这项工作(1962 – 1965)。报告描述了分组交换计算机网络如何能提供这种能力。[5] 与此同时（兰德小组并不知道），三位麻省理工学院的工程师正在讨论网络化计算机和分组交换的概念。[6] 1966年年底，麻省理工学院的一名工程师，Lawrence Roberts，加入了DARPA“去发展计算机网络概念”。[7]

余下的历史众所周知。1971年，ARPANET作为互联网最初的名称，拥有23个主机，将全美国的政府研究中心和大学连接到了一起。到1981年，

---

http://money.cnn.com/magazines/fortune/fortune_archive/2000/10/09/289297/index.htm（以下简称“财富”）；亦见 Dave Krisula，“互联网历史，”2001年8月（2009年修订），http://www.davesite.com/webstation/net-history1.shtml（以下简称“Krisula”）。

3 Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel，Larry G. Roberts，Stephen Wolff，“互联网简史，”互联网协会(ISOC)，http://www.isoc.org/internet/history/brief.shtml（以下简称“互联网简史”）；Licklider于1962年8月公布了他的“银河网络”系列备忘录，并于1962年10月开始效力于ARPA。

4 Krisula；亦见财富杂志，Stewart Brand，“创立者，”*Wired*杂志，2001年3月，第148页，http://www.wired.com/wired/archive/9.03/baran_pr.html（以下简称“Brand”）。

5 Brand第145-153页；亦见Krisula。

6 互联网简史；亦见Brand第146页；Krisula。

7 互联网简史。

它被称为互联网。到1991年，Timothy Berners-Lee先生[8]在欧洲核研究机构（也被称为“CERN”）创建了万维网。互联网和万维网的合并点燃了将其商用的想法。但各公司因需通过国家科学基金会网络（NSFNET）接入骨干网而受阻。

1995年，美国国家科学基金会默许四家商业公司接入互联网骨干网，到1996年，有近千万主机联机，互联网随之遍布全球。30年时间里，互联网由“一个对破烂残余的后核社会进行控制的冷战概念成长为信息高速公路”。[9]合并后的互联网和万维网已渗透到经济和社会的各个层面，它所带来的社会变革是20年前无法想像的。今天，有近20亿在线用户，并且在互联网上没有地域界限。今天对互联网的管理既包含技术问题，也包含公共政策问题，涉及所有利益攸关方和相关政府间和国际组织。

具有讽刺意味的是，冷战时代的发明随着科学国际化的发展形成网络，如今成为对全球和平最严峻的挑战之一。尽管在分析国家安全和经济安全时地缘政治因素[10]仍必须是考虑的重点，但互联网已经改变了外交政策的传统分析。地域网络范围日益影响国家的管理方式，地缘政治障碍正被迫形成新模式。

维持“最低限度的基本通信”对于美国已不是问题。世界上所有国家如何维护地域网络稳定并确保其关键基础设施不被用做伤害无辜和手无寸铁的平民的武器、造成不必要的伤害和毁坏才是最重要的问题。

---

8 Elizabeth D. Hoover著，“万维网的发明者”*AmericanHeritage.com*，2005年11月12日，http://www.americanheritage.com/articles/web/20051112-internet-world-wide-web-tim-berners-lee-computer-geneva-cern-enquire-html-url-world-wide-web-consortium.shtml

9 “互联网上的生活：网络时间表”PBS，http://www.pbs.org/opb/nerds2.0.1/timeline/；亦见Krisula。

10 地缘政治学被定义为“（1）是对政治和地理、人口统计学和经济学关系尤其是对一个国家的外交政策的研究（2）a.运用地缘政治的政府政策b.纳粹哲学认为由于德国的地理、经济和政治需要使其有正当理由入侵和占有他国领土（3）有关或影响一个国家或地区的地理和政治因素组合”《美国传统词典》，2000年。http://www.dictionary.com/search?q=geo-political。

作者对“地域网络”的定义是，地域网络是互联网与一个国家地理学、人口学、经济和政治以及外交政策之间的关系。“地域网络的稳定性”是指所有国家通过在经济、政治、人口领域使用互联网受益，同时避免能导致不必要伤害和毁坏活动的能力。[11]

今天，整个世界面临着互联网带来的新的威胁。每个国家维护其通信、指挥、控制和计算机（C4）免受恐怖分子、犯罪集团和其他国家袭击的能力并不十分确定。ICT给各国带来了前所未有的国家安全和经济安全方面的挑战。现在，个人可以破坏管制和发动非对称攻击，使整个基础设施瘫痪，通信停止。现在最薄弱的系统也能对那些最强大国家造成威胁。

当关键信息基础设施遭到毁坏，网络冲突能导致危及生命的后果。网络冲突也会引起严重侵犯国际人权、挑起暴力和导致严重经济损失的信息操作。针对个人和国家的风险是巨大的 – 并且游离于目前法律框架的保护。目前的法律框架不能充分适应网络时代的需要。

需求非常急迫。各国必须签署协议，承认新的受冲突保护的“最低限度基本通信”水平，以平衡各国发布网络命令，扩张军事能力将网络冲突包含其中的快速步伐。该行动将阻止冲突双方遭受不必要的毁坏和痛苦，并保护其他未介入冲突的国家不受伤害。这样的地域网络稳定性水平至关重要，以免互联网带来的益处被技术的破坏力吞噬。

多国组织是合乎逻辑的起点。他们必须首先定义保护无辜平民和基本社会功能所需的基础设施和通信稳定性的最低水平，并通过外交协议和法律规则确保其实现。这需要广泛的利益攸关方包括个人、业界、民间团体、学术界、律师、政策专家、一线应急和执法机构提交输入意见。以此方式，ICT和互联网可以提供一个积极的国家间合作的国际框架，从而更好地理解和认同世界上的不同文化和社会价值观。

---

11 在ANSER学院家园安全大会上首次介绍，“家园安全 2005年：设计前进道路”，由马里兰大学的Jody Westby介绍，“地域网络稳定性和安全性的转变”，2002年5月6-7日。

本书阐述了网络和平的概念，将其作为网络空间行为的定向原则。网络和平因此应是所有国家的追求。网络和平的益处远远超出网络冲突的后果。

本书由国际电信联盟秘书长哈玛德•图埃和世界科学家联合会信息安全常设监督委员会成员共同撰写，旨在号召所有利益攸关方共同参与努力，确保互联网和基础设施稳定性的最低水平，推进全球网络和平概念。

2 网络空间和网络战威胁

哈玛德•图埃

信息通信技术（ICT）已成为世界上许多人每天生活不可或缺的组成部分。数字通信、网络和系统为全球社会提供着必不可少的资源和基础设施。没有这些资源和基础设施，很多人无法很好地生活甚至生存。这些结构和系统代表了一个新领域，他们的出现也给维护和平和稳定带来了挑战。没有确保和平的机制，世界城市和社区将很容易受到前所未有和各种没有止境的攻击。这种攻击可以没有任何预警就到来。突然之间，计算机和移动电话停止工作，提款机和银行机器屏幕一片空白地茫然瞪着顾客，空中交通管制、铁路和汽车交通系统中断，高速公路、桥梁和航道陷入混乱，易腐烂货物滞留无法运抵饥饿的人们。随着电力丧失，医院、家庭、购物中心以及整个社区将陷入黑暗。政府当局将无法对毁坏程度做出评估，无法与世界其他地方联络传递预警信息，或者无法保护其脆弱的公民免于随后的攻击。这就是因瞬间丧失数字网络而陷入瘫痪的社区的棘手困境。这就是一种新型战争 — “网络战”的潜在毁坏。

一个新领域：网络空间、网络安全和网络战

如今，网络战威胁正在日益逼近，其威胁比以往任何时候都大。今天，技术进步和不断增长的数字基础设施将整个人类绑定到复杂、交互交织的系统。对互联网和数字连接的需求要求ICT不断与以前没有ICT工作的产品进行集成，比如汽车、建筑甚至巨大的电网和运输网的控制系统。电力供应、运输系统、军事和后勤服务 — 事实上所有现代服务都依赖于ICT的使用和网络空间的稳定。“网络空间”是物理和概念范畴，是所有这些系统存在之所在。因此，“网络战”可能被广泛理解为在网络空间使用ICT

和以ICT为目标进行的战争。[12] 对智能电网和其他基于互联网的控制和检测系统依赖性的快速增长，使能源、交通和国防资源的核心处在了可以被那些试图对政府和平民百姓发泄施暴的人触及的地方。[13] 于是，加强网络安全和保护关键信息基础设施是每个国家的安全和经济保持良好状态必不可少的重要因素。

随着全球对ICT依赖的日益加大，也存在通过网络空间对关键基础设施进行攻击的漏洞。尽管仍未对“网络战”准确定义，过去十年中对信息基础设施和互联网服务的重大攻击还是提供了网络空间冲突的一些潜在形态和范围。对格鲁吉亚[14]、爱沙尼亚[15]、韩国和美国[16]的攻击与网络战相关。巴西的多次停电亦与网络攻击有关。2008年黑客侵入其政府网站，将该网站控制了一个多星期。[17] 巴西停电说明了新兴的网络攻击种类的可能

---

12 Steven Elliot著，“网络战和防御分析”，*信息安全岛杂志*，2010年7月8日，https://infosecisland.com/blogview/5160-Analysis-on-Defense-and-Cyber-Warfare.html（以下简称“Elliot”）。

13 Ellen Messmer，“网络攻击是美国电网的头等威胁”，*网络世界杂志*，2010年6月2日www.networkworld.com/news/2010/060210-nerc-cyberattack-power-grid.html（据报告，协调性网络攻击可能与物理攻击相结合，被认为是对北美电力供应最紧迫的“高冲击，低频率”威胁）（以下简称“Messmer”）。

14 Thomas Claburn著，“遭受网络攻击，格鲁吉亚与谷歌找到防弹软件”*信息周刊*，2008年8月12日，http://www.informationweek.com/news/security/attacks/showArticle.jhtml?articleID=210002702。

15 Joshua Davis著，“黑客拿下欧洲最敏感的国家，”*Wired*杂志，2007年8月21日，www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all。

16 Choe Sang-Hun和John Markoff著，“牙买加政府网站和美国及韩国商业网站遭到网络攻击，”《纽约时报》，2009年7月8日，www.nytimes.com/2009/07/09/technology/09cyber.html; Jack Date，Jason Ryan，Richard Sergay和Theresa Cook著，“黑客对联邦实验室发动攻击”ABC新闻，2007年12月7日，http://abcnews.go.com/TheLaw/Technology/story?id=3966047&page=1。

17 Michael Mylrea著，“巴西下一场战争的地点：网络空间，”外交政策杂志，2009年11月15日，http://foreignpolicyjournal.com/2009/11/15/brazils-next-battlefield-cyberspace（以下简称“Mylrea”）。

范围：报告内容类似科幻大片，地铁、交通信号灯和世界第二大水力发电站、伊泰普大坝均完全停止工作，超过6000万人受到影响。[18]

网络战也可能涉及私营部门。网络服务巨头如谷歌[19]和推特[20]在2009年已遭到攻击，早在2000年，曾发生过针对一些知名公司如CNN、eBay和亚马逊发动拒绝服务的攻击。[21]结果，这些公司数小时甚至几天都无法提供一些服务。黑客锁定机场控制系统，使诸如电话服务和跑道灯等关键设备瘫痪。[22]根据一些统计，过去三年有超过6个国家遭受了网络打击，仅在2010年年初几个月至少有34个私营公司遭到攻击。[23]尽管这些安全问题十分严重，但对于通过国际合作创造更安全的产品、做法和标准以避免潜在的灾难来说为时未晚。[24]如果我们想保护民众、确保基础设施有效运行和持续开发新业务，就必须将使互联网更安全，保护ICT免遭混乱和毁坏工作作为优先重点。

---

18 同上。

19 Andrew Jacobs和Miguel Helft，“谷歌，Citing Attack，Threatens to Exit China”，《纽约时报》，2010年1月12日，http://www.nytimes.com/2010/01/13/world/asia/13beijing.html。

20 Eliot Van Buskirk.“Denial-of-Service Attack Knocks Twitter Offline (Updated)”，Wired.com，2009年8月6日，www.wired.com/epicenter/2009/08/twitter-apparently-down/。

21 见Abraham D. Sofaer和Seymour E. Goodman著书，网络犯罪和恐怖主义的跨国规模，第14页，2001年出版，http://media.hoover.org/documents/0817999825_1.pdf。

22 关键基础设施保护：人们已经开始采取多种努力保障控制系统安全，但是挑战仍存在。美国政府问责办公室2007年9月，GAO-07-1036，www.gao.gov/new.items/d071036.pdf。In 1997（黑客攻击美国Worcester机场，造成机场指挥塔电话服务瘫痪和跑道信号灯管理控制系统关闭）。

23 Elliot。

24 Joshua Pennell著，“保证智能电网安全：前进之路，”第2页，*NetworkSecurityEdge.com*，2010年2月5日，www.networksecurityedge.com/content/securing-smart-grid-road-ahead。

网络战对国家基础设施的威胁

网络战概念包含的不仅是对军事能力和系统的打击，也包含对社会必不可少的基础设施的打击—包括智能电网和监督控制系统以及数据采集（SCADA）网络—允许其运行和保护自己。尽管使用不同介质（网络空间和运行其中的ICT），对手仍能向传统战争一样部署武器和挑起攻防冲突。网络战策略通常采取数据收集或对计算机系统渗透来破坏关键系统。[25] 潜在的网络武器包括：计算机病毒和蠕虫，网络数据收集利用，无线数据通信干扰器，缺乏抵抗力的计算机盗版软件，电磁脉冲武器，计算机和网络侦查工具以及嵌入式木马定时炸弹。

日益依赖智能电网使许多国家的电力系统尤其容易受到攻击。智能电网是数字化的系统，它将公用事业供给连接到一个中心监测网络，通常称为SCADA网络。SCADA网络收集电力使用和供给的信息，而智能电网为该信息在用户和供应商之间流动提供一条数字化通道。[26] 如今这些技术被广泛用于各种进程和系统，包括：水管理系统、煤气管道、电力传输和分配、风力发电系统、大众通信系统、制造、生产、公共交通系统、环境控制系统、空中交通管制和信号灯等。[27] 越来越多的供应商将智能电网与互联网连接，以允许远程接入和增进功能。

电网连接提供了实实在在的好处，如减少能源浪费和加快用户与提供者之间的沟通速度，还能将数据集中，在拥有多接入点的网络上控制巨大的电网。随着端点越来越多，互联网络、智能电网和SCADA网络为攻击者渗透提供了多种途径。[28] 例如，智能电表（电表与电网连接）可以被黑客入侵并被相当轻易地感染。它可被用于向其他电表传播蠕虫，最终导致电

---

25 Elliot。

26 “智能电网，”美国能源部，http://www.oe.energy.gov/smartgrid.htm；“SCADA”，*TopBits.com*，www.tech-faq.com/scada.html（以下简称“SCADA”）。

27 SCADA。

28 Katie Fehrenbacher，“关于智能电网安全必知的10件事，”2009年10月9日。Earth2Tech，Gigaom，http://gigaom.com/cleantech/10-things-to-know-about-smart-grid-security/（以下简称“Fehrenbacher”）。

浪涌或关闭。[29]虽然许多公司纷纷寻求通过将控制系统与其他网络隔离的方式（一种被称为“空气间隙”的技术）确保电网安全，这些完全封锁某些元器件的企图经常失败，往往连系统管理员都不知道。[30]逻辑炸弹是攻击者可能制造混乱或甚至毁坏智能电网的另一种方式；黑客可能渗透进电网，在其中隐藏恶意软件，等待以后激活这些炸弹发动部署好的攻击或造成供电不足。[31]这些炸弹产生了一个额外的安全问题，因为它们可以在日后被意外引爆或由其他发现这些炸弹的黑客引爆。[32]

目前，已经对智能电网投资的国家报告每天都有数以千计的攻击企图和编码探测。[33]根据一些估计，网络攻击是国家电网最大的威胁。[34]远程攻击可以准确锁定像发电机和变压器这样的物理基础设施，导致它们彻底自我毁灭。[35]这种攻击极有可能带来长期的后果。因为电力公司通常不会储存昂贵的替换部件，这会导致花费几个月的时间生产和交付替换部件。[36]对智能电网的攻击不仅会让客户没电可用，还会造成巨大的财政损失。对

---

29 同上。

30 “SCADA安全和恐怖主义：我们不是哭泣的恶狼，”BlackHat，第26页。www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf。

31 Siobhan Gorman，“间谍入侵的美国电网”，华尔街日报，2009年4月8日，http://online.wsj.com/article/NA_WSJ_PUB:SB123914805204099085.html。

32 Ellen Messmer。“网络战的作者：美国需要重大的改变以抵御攻击，”网络世界，2010年4月7日，www.networkworld.com/news/2010/040710-clarke-book-review.html（以下简称“重大改变”）。

33 同上。（报告显示，美国电网每天遭受了成百上千次被侦查）；Fehrenbacher（表示全球安装的4000万智能电表已可见大量的安全漏洞）。

34 Messmer。

35 Mylrea。

36 “网络战：第五领域战争”2010年1月7日，经济杂志，www.economist.com/node/16478792（以下简称“第五领域”）。

一些国家来说，让发电机运行需要数百万美元，对智能电网的总投资要数百亿美元。[37]

除带来潜在的大规模毁坏和瞬间的财政损失，未来网络攻击的威胁还会削弱人们对现有和未来新技术如智能电网的信心，相应地，削弱人们对电子、金融和健康资源可靠性的信心。仅仅是这种信心的损失就可能带来巨大的社会和经济动荡。[38]随着智能电网与核反应堆（核武器设施）一起使用，还会带来更大的危险和潜在破坏。超出传统的攻防战略，网络战可能会攻击某个实体或国家内部系统，以便暂时分散对方注意力或限制对方，而不是直接摧毁。[39]某个国家可能选择此类网络攻击，例如，它会尽可能长时间地锁定对手盟友的支持以达到某个特定目的。[40]

网络战的特征和影响

虽然网络战在某些方面可能类似于传统战争，网络空间的独特性仍带来了新的意料之外的特征。因为网络空间系统是由计算机和通信网链接的，基于ICT的攻击所导致的崩溃远不止是单个系统的毁坏，而经常超越了国界。许多数据传递过程中会牵涉一个以上国家，许多互联网服务均基于来自境外的服务。例如，主机提供商可以在一个国家向另一个国家提供网络空间租赁服务。即使是短暂的服务中断也会给电子商务造成巨大的经济损失。民用通信网不是唯一易受攻击的系统，对ICT的依赖对军用通信也风险巨大。不像传统的军事格斗，网络罪犯不需要在攻击现场现身，或者甚

---

37 智能电网：硬件和软件展望，Zpryme著，2009年，第2页，www.zpryme.com/SmartGridInsights/2010_Smart_Grid_Hardware_Software_Outlook_Zpryme_Smart_Grid_Insights.pdf（2009年，美国智能电网行业价值214亿美元。到2014年估计将达到428亿美元）；Jonathan Weisman 和 Rebecca Smith著，“奥巴马鼓吹能源津贴，”华尔街日报，2009年10月28日，http://online.wsj.com/article/SB125663945180609871.html（据报道，奥巴马总统宣布将投资34亿美元拨款用于激励先进的电网项目建设）。

38 第五领域。

39 比如，同上。（表示“更适合使用网络武器作为局部战争的工具”）。

40 同上。

至不需要在发动攻击的源头现身。虽然实施了攻击，罪犯仍可以使用匿名通信和加密技术来隐藏自己的身份。[41]

更有甚者，互联网上广泛使用的软件工具，正在被用来发动自动攻击。在此类软件和预装攻击的帮助下，单个罪犯可以在一天之内使用一台计算机对数千个计算机系统发动攻击。如果罪犯接入更多计算机，例如通过僵尸网络，他们还可以进一步扩大攻击范围。例如，针对攻击爱沙尼亚政府网站的分析表明，这些攻击是僵尸网络控制的数千台计算机发起的或是某一组缺乏抵抗力的计算机受外部控制运行程序。[42]由于初始痕迹只导向僵尸网络的其他成员，僵尸网络也使追踪真正的罪犯变得更加困难。目前分析表明，所有与互联网连接的计算机中，多达1/4可能被软件感染，成了僵尸软件的一部分。

软件工具还使进攻得以简化，使缺乏经验的计算机用户或不太先进的军事装备引发网络攻击。此外，基于ICT的攻击通常比传统的军事行动代价低，甚至效果也可以发动攻击。如今，即使一个历史上军力薄弱的国家也能通过网络攻击严重毁坏关键基础设施。这一潜在的不对称使网络战成为竞技场上的一种战略方式，不同于David与Goliath对决的场景。人们对网络战的恐惧因实际发生的网络攻击（尽管有限）而日益增强，这削弱了公众对使用ICT的信心。因此，网络冲突造成的潜在的心理影响可以带来广泛的连锁反应，扰乱人们有效地使用新技术，妨碍许多领域的发展。

---

41 2006年CERT年度研究报告，卡耐基梅隆大学，软件工程学院，第7页，www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf。

42 了解网络犯罪：发展中国家指导手册，第72页，国际电信联盟，2009年4月，www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf（以下简称“了解”）。

3 社会依赖性和信任

3.1 现代社会对信息通信技术和互联网的依赖

作者：Jacques Bus

自上世纪下半叶以来，计算机和信息技术一直与我们同在，而互联网的出现不过是38年以前的事，当时也只是ARPA（DARPA）的一个通信网络项目。然而，在过去的短短15年间，由于发明了万维网（为方便起见，在下文中我们将互联网和其他网统称为“互联网”），互联网以令人目眩之势渗透到经济和社会生活当中。目前，我们可以随时随地且随心所欲地使用通信和社交网络，能够获得几乎无限的信息，可以与世界各地的人们讨论和社交，坐在家里便可随时比较和订购我们想要的服务和产品。

根据国际电联的估计，2009年，全球有25.9%的人口连接到互联网（达18亿人）。人们每周花在互联网上的时间比看电视要多两倍。全球有46亿移动电话用户，占世界人口的67%。2010年7月，Facebook宣布已有5亿多名活跃用户。仅在2010年7月，Facebook、MySpace和Twitter便吸引了共计2.2亿名活跃用户。全球的一大变化是移动电话变身为网络电话，并取代个人电脑成为用户最喜欢的上网装置，而全球亦有9.5%的人口拥有移动宽带。

尽管互联网已从根本上以真正意义上的全球规模改变了现代社会，但未来还会有更多未知成为现实。我们在许多刊物上[43]获悉未来世界在25年后的可能情景。身份识别令牌将广泛应用于公交、健康记录、政府服务和网络服务。社交网络的规模将进一步扩大，而新的、更有效且更令人振奋的应用将不断涌现。数据链接将带来全新的信息服务，这将有助于研究人

---

43 信息社会中的信任：RISEPTIS顾问委员会的报告，http://www.think-trust.eu/; David-Olivier Jaquet-Chiffelle等，身份革命：多学科观点，FIDIS，2009年5月，http://www.fidis.net/resources/identity-revolution/。

员开展更为有效的研究，游客将可更惬意地享受旅程，市民将可更好地了解主管部门的规定和政治家的动机等。代理和基于策略的程序将令我们从行政负担中解脱出来，诸如安排会面、筹备会议及遵守司法辖区的规定将易如反掌。

基于信息通信技术的社会革命将在权力平衡方面带来至关重要的变化。在国家层面上，公民将可获得关于政治进程的丰富信息，而这将有助于民主进程，在国际层面亦然。互联网的使用将可令公民更好地融入经济和政治生活，与此同时亦可了解到其他文化的情形和生活方式。我们都知道社交网络已被用于美国总统奥巴马的竞选，可以预期未来在支持政府决策方面还会出现类似的活动。

信息通信技术还允许国际公司在内部组织中最优地利用自己在世界各地的机会。这将大大促进全球的经济发展，在低成本国家更是如此。我们看到：发展中的大国已利用这一点发挥了重要的经济和政治作用。

然而，和历史上的每次革命一样，机会和利益永远都会有负面因素相伴。

信息通信基础设施和服务已成为我们经济的要素，但它们极其脆弱，关于这一点几乎每天都会有许多关于攻击的报道见诸报端。大多数的其他关键基础设施（如能源、水利、交通、金融系统）都极其依赖于信息通信技术来实现通信和控制。因此，意外或蓄意攻击这些关键基础设施的风险非常之大，这可能导致混乱和巨大的经济损失，其中包括对国家安全机构的数据库系统的入侵和攻击。

我们所处社会的信息通信基础设施的脆弱性使之极易成为“网络战”或“网络恐怖主义”的靶子，这对地缘政治的稳定构成了威胁。由一国首肯、支持或控制某组织蓄意发起针对他国的社会关键系统的攻击有时也被称为“网络战”。需要指出，这里所说的“战争”可能会带来混淆，原因是它与大多数人在讨论战争时脑海里浮现的事物不可同日而语，通常人们以为的“战争”多指对物理基础设施的长期破坏和大量的生命损失。

在过去几年里，在发生几次攻击时使用了“网络战”一词，例如在爱沙尼亚[44]、格鲁吉亚、韩国、美国发生的攻击。此类战争有时始于业余的心理“战”，且具有宣传目标，在第二阶段则包括了网络攻击活动专家（罪犯或其他方式）通过僵尸网络全面展开的针对社会和经济基础设施的DDoS攻击。在其他情况下，网络攻击的执行时间为动力学战争行动之前或期间。截至目前，由网络攻击造成的破坏有限，被破坏的能力在几天后便可修复，且尚无资料提及因网络攻击导致的直接生命损失。

国家在这些冲突中所扮演的角色大多是未经证实的，但这也证明亟需国际协定来限制和防范网络攻击，并为此进行国际合作来对其加以控制。显然，冷战时期旧有的威慑学说不适用于网络空间。在此很难详解这种威慑应包括什么，更重要的是，很难发现敌人（属性的缺乏和代理服务器的使用）。

让我们暂且搁置就“网络战”术语的政治辩论。毫无疑问，网络犯罪已成为一个非常令人忧虑的问题。恶意代码的威胁和犯罪的数量在成倍增长。仅在2008年，赛门铁克公司就检测到160万项威胁，占2008年之前各年所检测到威胁总数的60%。800多万名美国公民成为身份盗用的受害者。在美国，一项数据破坏的平均成本约为670万美元。众所周知，2010年2月，全球有75万个公司计算机系统被僵尸网络感染和控制。前美国官员Amit Yoran认为，多数公司根本没有为相关防卫做好准备，但此后这一看法却被美国安全部门的人士刻意淡化。

在认识到互联网恶意使用问题日趋严重的同时，Howard Schmidt（美国总统特别助理和网络安全协调员）明确指出了其中的轻重缓急所在。他反对将所谓“网络战”列为“一个可怕的概念”。他认为在这种环境中没有赢家，并建议把重点放在网络犯罪和间谍活动上。

---

44 亦见Kertu Ruus，“网络战I：爱沙尼亚遭遇到来自俄罗斯的攻击”，欧洲时事，2008年第9卷第1-2册，http://findarticles.com/p/articles/mi_7054/is_1-2_9/ai_n28550773/。

尽管存在不同意见，但各界普遍认为，有必要就互联网安全和信任问题敲响警钟。当前的趋势使公民担心乃至拒绝新的数字世界的风险在增加。如果政治和技术无法化解这些消极的社会发展趋势，这可能会产生巨大的经济后果。

美国国务卿希拉里•克林顿在其2010年1月21日的讲话中强调了全球合作及发展开放和自由互联网的重要性。她提到了罗斯福所述的“四项基本自由”— 言论自由、信仰自由、不虞匮乏自由和免于恐惧自由 — 以及互联网对这些自由尤其是言论自由的重要影响。互联网已在信息交流和社交方面衍生了革命。它具有为每个人创造更多财富的巨大潜力，当全面实现了“连接自由”时更是如此。但它也导致了全球犯罪的日益增加和恐惧的滋生，因此需要对互联网加以控制。

政治家们清楚地认识到互联网在全球地缘政治舞台上所发挥的重要作用。他们明白公民期待政府为其给予安全和保护，而国家的辖区和边界已不再像以前那样可以给予公民上述庇护。目前在许多国家适用的消费者权益保护法以及产品和服务责任尚不能在网络世界中适用，原因是这个世界里的客户和供应商来自不同的、非合作的管辖区，且服务是通过临时子服务链以数据形式从遍布全球的云计算网络交付的。

各国领导人正面临着巨大而空前的挑战。譬如，气候变化、全球经济力量的遽变和能源的安全性等问题均需政治上的关注，全球数字连接亦带来风险。我们需要强有力且有远见的全球领导者，只有他们方可解决上述问题。

在所有这一切中，最重要的一点是要充分利用我们业已取得的教训，这些教训来自过往有关社会结构、价值观念、安全、信任和国际关系的历史。我们必须在全球进行变革，改变我们的文化、社会价值观和优势所在，并进行国际合作，以便在一个承认数字网络现实的世界中发挥用武之地。

信任的必要性

信任的概念及其在社会中的作用

“信任渗透在我们的日常生活中。如果我们从信任发挥着作用的、令人目眩的各种场合中撷取一个小样本，我们便可看到，在所有社会现象中，信任肯定是最重要的现象之一。但是，这一核心现象却为信任研究带来了问题 — 我们如何才能真正理解这一千变万化的社会力量呢”？[45]

信任和诚信的概念是人类生存的基础。我们直观地使用着它们，对它们的评估总是依赖于具体情境。但当我们将这些概念转至数字环境时，却很容易碰到麻烦。

Luhmann [46] 将信任解释为一种机制，它可以减少复杂性，使人们能够应付（当代）生活的高度不确定性和复杂性。因此，信任令人们得以更成功地与现实世界建立关联，而这一世界的复杂性和不可预测性远远超出我们所能承受的范围。因此，信任是一个必要的机制，它让人们得以过上自己的生活：进行沟通、合作和开展经济交易等。它丰富了个人的生活，鼓励着人们进行活动、有勇气、富于冒险和创造力，并丰富了人际关系的范畴。

站在另一角度，有人或许可以说，信任是产生信任的一方在一定情况下对良性行为的预期。正如Hardin所说 [47]：“信任是知识和信仰的认知类别，说我相信你是说我知道或相信关于你的某些东西，这让我相信你对我是值得信赖的，且在不可预知的情况下你也会采取“无害”的行动。”

---

45 Kieron O’Hara，信任：从苏格拉底到炒作，剑桥图标图书，2004年，第10页，http://eprints.ecs.soton.ac.uk/9361/。

46 Niklas Luhmann，“信任：一种用于减少社会复杂性的机制”，信任和权力，纽约：Wiley，1979年，第4-103页。

47 Russell Hardin，信任和诚信；Russell Sage基金会关于信任的丛书第4卷，2002年。

信任是一种三方关系（A信任B会做X事）。对A信任B做X事的评价在A做出参与和B之间的任何交易、交换或沟通的决定过程中起着重要作用。通过减少与B沟通的复杂性和感知风险，信任有效地促进了经济活动、创造力和创新。信任是高度依赖具体情境的，它取决于：时间（一个人很容易失去对某人的信任，但这一概念也随着时间而变化）；历史与记忆；场所与境遇；文化；角色（私人或专业）；情绪；和其他变数（如信誉、重复发生和建议等社会学方面的考虑）。

可见，信任是一种在特定情况下在特定双方之间可以逐步增强的概念。通过其他传感器或关系，更多的信息有助于增进信任，并促成历时较长的一种成功合作关系。

在本次讨论中，我们可认为A方和B方是人类，但这并不排除以下可能性，即这些人以组织或团体的名义行事。然而，在实践中，很多人也会谈到对其他实体的信任，如政府、企业、系统或服务、数据库或信息服务（如一篇论文、技术博客），或甚至某一软件代理虚拟实体。哈丁将其称为“对实体的行动、行为和完整性的信心”。这种信任的建立可以通过问责制、透明度、保证和责任、审计和声誉或对实体意图的了解等来实现。

信任作为社会资本的概念或者“社会信任”已为Fukuyama[48]、Putnam[49]和其他专家讨论并发展过。这是一个统计概念，表达着人们对其所处社会的各方面的可信性意见，或换言之：人们对政府、机构、法律、制度、社会等的信心。较高的社会信任和经济高速增长与繁荣之间似有某种密切相关性。

我们这里所说的“信任”也是Hardin称之为“信心”的东西。不过，为进一步讨论，需要对在交互时利用网络化数字系统和服务的人与人之间的信任以及人对某一非人类实体或机构的信任或信心做出区分。

---

48 Francis Fukuyama，信任：社会美德和繁荣的造就，自由出版社，1995年。

49 Robert D. Putnam，Robert Leonardi，and Raffaella Y. Nanetti，让民主奏效：现代意大利的民事传统，普林斯顿大学出版社，1993年。

数字技术的引入实现了人际交往与合作的革命，因为它引入了一种全新媒介，此媒介由基于技术的一系列复杂“机构”组成（包括网络、数字服务、数据库、社交网络）。因此，在处理人际关系中的信任时，我们必须考虑对这种技术基础设施的信任（或信心）问题。

Nissenbaum [50] 仅讨论了利用网络化数字系统进行沟通的人与人之间的信任问题，并列出了导致产生系统化信任（或不信任）反应倾向的各个因素：

1. 历史和声誉。
2. 基于个人特征的推论，例如：美德、谨慎、忠诚、对他人好感的渴望、行为、服装。
3. 关系：相互性和互惠性、家庭、同舟共济、有共同目标。
4. 角色实现（飞行员、巴士司机）。
5. 情境因素（群体和社区—宣传；奖罚；规范；信托保险或社会保障网，如责任或消费者权益保护法）。

上述若干因素（特别是1和3）存在着哈丁所定义的“信任的封装利益”方面的问题，详见Hardin的定义[48]。对被信任的人而言，以良性方式行事符合其本人的利益，可使其不致失去声誉，而这可能导致被信任的人失去某种关系（如失信的飞行员可能会失业）。她还列出了在网上形成信任的障碍所在：

1. 缺失的身份（但要注意到匿名权）
2. 缺失的个人特征（但要注意到隐私权）
3. 神秘背景（未知和混乱造成模糊，也释放人性）

---

50 Helen Nissenbaum，“确保网上信任：智慧抑或矛盾？”波士顿大学法律评述，2001年6月第81卷第3册第635-664页，http://www.nyu.edu/projects/nissenbaum/main_cv.html。

第三点可以仅仅被看做网络的复杂性更高。网络允许更多的自由，当然，在同一时间，为正确进行交易或通信，人们需要建立更多的信任，因此也更加依赖彼此。Nissenbaum还指出，安全不会带来信任。倘若有了安全，便不再有形成信任的必要。然而，信任令人们生活在一个极其复杂且不安全的世界中，而更多的安全则减少了不安全的多样性和复杂性。其他作者则认为，安全位于信任天平的一端，而无来由的信任（天真）则位于天平的另一端。

事实上，利用全球信息基础设施，（对陌生人的）信任随着（对他们的）了解的增多而增加，经济学家们因此指出："如此多的人有这样的愿望，只要有机会[...]生活在不同的其他国家，便会令一个长期以来建立的、在政治和哲学方面的共识成为空谈，即：人这种动物关在家里才是最好的。"[51] 还有："哲学的错误在于假设人是一种社会动物，因此人应属于某种特定的社会。"[52] 不过，这可能过于鲁莽地概括了一种少数行为，原因是那些有机会参加由高端旅行社组织且提供优质保险的假日旅行的人虽然走得更多和更远，但他们毕竟仍是极少数人。

然而，在信息通信新技术和互联网的推动下，全球化增进了人与人之间的理解，也因此创造了更多的信任。在这方面，对社会历史和信誉、社会特征及某些社会中人之生活状态的信息的传播功不可没，这也令全球沟通变得轻而易举。这确实也可能导致进一步冲击"人这种动物关在家里才是最好的"这一概念。为此，可能需要对社会及其凝聚力以及信任必须发挥的作用形成一种全新的观点。

数字社会的信任

综上所述，我们必须区分：

---

51 "其他人"，《经济学家》，2009年12月17日，http://www.economist.com/node/15108690。

52 同上。

- 在一个广泛使用数字技术进行通信和交易的社会的人与人之间的信任；
- 人们对用来实现服务、通信、数据存储、计算等的数字网络和系统基础设施的信任或信心。

先谈第一点。

数字社会与“旧有社会”中（人与人之间的）信任的问题要特别涉及到以下问题：[53]

- 数据收集、存储、处理、提供和保护方式的转型变化。数据的收集和存储不仅源于人需要收集和存储数据本身，而且源于需要通过监测来收集有关人类行为的数据（从街头走访到访问网站或打开网络广告）。
- 身份、信誉、认证和问责制在互联网上有不同的含义。一个人需要证明其属性，提供密钥或生物特征信息来说服别人相信其身份。传播令人不适或虚假的信息可以很容易地毁掉其声誉，且其恶果很难纠正。如果没有任何关于执法和引渡的国际协议，那么藏身于其他司法管辖区的可能性会大大削弱问责制和透明度的作用。
- 复杂性的增加、缺乏认证和标准化的深奥技术以及数据收集和使用流程和方法方面的透明度不足已衍生出一个玄奥的背景，这破坏了数字环境中需要在人与人之间建立的信任。人们可能会对周围发生的一切感到困惑，且其往往对就其自身所收集的资料及其使用方法一无所知。

当身份和/或关于第三方的其他身份认证信息（凭证、属性或要求）（可能为受信任的第三方）获悉或确认时，信任将更易于建立。从网络或社交网络的朋友处获得的声誉和其他知识可能带来额外的信任。此外，公民在与第三方进行交易时将会获得更多的信任，前提是其能够控制与第三

53 见Nissenbaum。

方交流和交换数据的风险。数据收集器和处理器的透明运作以及上述实体的声誉也将会增进信任。

现在我们来谈第二点，如果一个人能在用于通信、交换数据、确认身份和包含名誉或凭证等其他信息的系统中获得信任，那么人与人之间的这种信任便只能在技术世界中获得。要使用互联网，公民必须对其用于交易和通信的工具、系统和基础设施拥有信心。如果一个人能拥有某种合理的信任，即该系统或服务将按照它的描述和承诺来运作，且在不同情况下不会执行没有描述的行动，那么我们便说这种系统或服务值得信赖到一定程度。合理的信任可以通过问责制（产品责任）、数据处理和存储的透明度、技术体系认证以及事后审计能力获得，也可以通过提供易于理解的有用工具和机制进而实现对凭证、信誉或身份要求等的确认得以加强。人们需要可以帮助其建立和加强服务质量、安全性、弹性、数据保护和隐私方面的服务和工具，为此须遵守预先规定且易于理解的政策，这可以通过第三方服务供应商以及政府主管机构来获得。

正如Vitali Tsygichko [54]所指出的，现代社会中的一个重要作用是由特殊的自动化信息系统（AIS）发挥的，它在国民经济所有部门的公共管理制度中变得日益一体化。AIS在几乎所有社会经济组织中均构成了决策支持系统的核心。它不仅是公共主管机构、经济和自发性组织的效率所在，而且也关乎到在很大程度上依赖于AIS性能的可靠性的国家安全。

显然，很重要的一点是要考虑这些系统的可信性。这主要涉及其基本模型的有效性、其软硬件设施的可靠性、系统维护人员的专业资质以及为防范外部威胁所采取的保护措施的有效性。

根据Tsygichko的观点，要保证AIS的可信度，需要开发一套用于安全性、可靠性（包括作为现实代表的一个底层模型）和数据完整性的要求和指标。一个安全漏洞风险指标可被用做一个评估标准。**风险管理**被定义为涉及风险识别、分析和决策的一系列过程，其中包括风险事件发生的正面影响的最大化和负面影响的最小化。

54 Vitali Tsygichko是PMP InfoSecur的准成员，并参加了上述讨论。

除了为建立信任所需要的技术手段之外，我们还需要规章制度和社会的接纳。要使公民信任社会对其个人资料所做的处理，必须做到：隐私和个人数据保护条例得到遵守和执行；相关机构应遵守公民感知的问责制文化，为此须借助于适当的消费者权益保护和纠正法规；关于审计和透明度的法规；以及在交易环节的各方中实现明确的责任分配。

在宏观政策层面上，只有在整个价值链中实行适当和公平的激励分配措施，才能建立起并维护好一个值得信赖的信息通信技术基础设施。

透明度和问责制的实行需要确保公平和可执行性。为此，需要解决系统责任的问题，特别是软件和数据完整性方面的问题。这可能需要开发一个安全漏洞风险的保险体系，这反过来将推动为实现风险评估的测量和相应工具的开发。这些都可能促成可基本上实现自我监管的可持续制度。

在利用互联网的人们之间建立信任的一个基本要求是开发一种可在全球互操作的可信系统来实现**识别和认证**。各国政府根据全球统一标准开发的可靠的电子身份证和护照便是多国共同发展的一个明证。但对全球电子交易而言，我们需要在互联网上实现可互操作的要求和凭据管理，为此须确保遵守隐私权。问责制对互联网经济而言乃首要要求，要实现问责制，只能通过个人和机构对其公共与合同行动履行有效责任来实现。后者通常要通过证明凭据、证明属性或使用仅此人知道的密钥的方式来实现。人们在不同情况下可使用不同密钥、凭证或属性，从而导致不同的“身份”。用于身份确认管理的元级标准已由Cameron、Posh和Rannenberg等人提出。[55]

互联网及其众多不同社交网络也为个人和机构提供了建立各自资料、交际圈和在不同社区中树立声誉的机会。在FIDIS项目[56]的术语中，这将导

---

55 Kim Cameron，Reinard Posch和Kai Rannenberg，*关于共同身份框架的建议：一个以用户A为中心的身份元系统*，联合‘ICT安全性’—关于“未来数字社会中的身份管理”的用于政府和公共服务的ICT讲习班，2008年10月14日，http://www.identityblog.com/?p=1048。

56 “关于FIDIS人才网络”http://www.fidis.net/about/。

致出现一个人的“部分身份”。在需要问责的情况下，这可能要涉及隐私保护方面的身份鉴别、认证和数字签名。作为一种社会和经济活动机制，它也有助于在互联网中提供更多的信任。

概要

我们讨论了信任在社会中的重要性和关于信任的不同意见，当我们的社会变得日益依赖于经由互联网的数字通信和交易时，当中也逐渐出现了一些变化和问题，对此我们也做了特别的讨论。足够的识别手段的缺乏、在某些情况下对匿名性的尊重、个人特征方面经验的欠缺、隐私保护需求以及在我们的通信中使用的技术基础设施产生的玄奥的具体情境（这一点也非常重要）剥夺了人类创造信任的重要机制，而这对他们在全球化的社会中生活和发挥创造力至关重要。

因此，我们必须在数字环境中开发全新的信任机制，使人们在相互之间建立信任，并使信任与其所在地或会面方式无关。

我们必须确保安全和可靠的通信网络；确保遵守数据保护和隐私法的信息系统；一个用于识别和认证/要求管理的、值得信赖的全球互操作框架；和可满足适当的责任和消费者保护法要求的服务。在设计和开发这种技术的过程中必须充分考虑到信任、安全和隐私要求，并确保可执法性和透明度的实现，而法律和法规的制定亦须充分考虑到技术发展趋势和潜力。

公共和私营部门必须在国际层面共同构筑极为均衡的技术和法律/监管基础设施，以便授信于民，令公民充分利用全新数字世界所带来的机会。

在这样做的过程中，迄今为止，人类已可利用不可预见的机会进行沟通与合作，并在信任机制的基础上建立起全球性的经济交易机制，这类似于我们耳熟能详的那种小型社区机制，即通过直接的人与人之间的互动进行的经济交易。这将成为我们迈向全球稳定的坚实一步。

3.2 网络犯罪的社会-经济影响

作者：Jacques Bus [57]

数字业务的提供，以及总体上讲正在我们的社会中形成的数字基础设施，具有巨大的积极作用。同时，它们像所有技术一样，可以用于恶意的活动。我们也许可以把与社会 – 经济发展有关的问题分成以下四个领域：

1. **数字空间的全球性特征**：互联网上跨境业务和通信的出现带来了诸多经济和社会信任问题以及国家安全问题，直到现在，国家安全问题要么是在民族国家边界线上处理（进出口控制，护照控制，海关，国家间的侵略等），要么是在国境内当地或国家的警察对登记在册的市民采取行动。无论是在国家层面，还是在国际层面，都很难解决数字空间中缺少边界控制所造成的负面结果。但毫无疑问的是，这一状况给犯罪分子创造了一种豁免的机会，因而促进了犯罪的发生，因为一方面网络上行动的参与者是很难追踪的，另一方面这些参与者处在一国之内，使他们可以不受国际法执法的控制。

2. **业务的复杂性**：网络上的交易和业务越来越多地采用专门的一系列子业务形式，它们触及各国管辖领域，使用云中遍布的数据。这些子业务或数据可能涉及不同的，甚至相互抵触的管辖制度。消费者很难意识到这一点，也很难搞清其后果。各国无法继续通过现有的方式来确保产品的可靠性和保护其消费者。它们需要通过国际协议和执法合作解决这一问题。此外，各种业务需要在业务链上确保透明性，并对消费者就此提出的条件（自动地）做出反应。这一现状和第一点给那些无法追踪的欺诈行为有了更多的可乘之机。

3. **社交网络和聊天室**：它们常常用来进行具有恶意动机的联络活动，主要针对儿童和老年人。这并不是什么新问题。各种欺诈行为一直就存

---

57 本文作者在此感谢Udo Helmbrecht和及其在ENISA（欧洲网络与信息安全署）的团队所做的工作。

在。但是，由于验证技术不高，在个人证明信息方面（例如姓名，生日信息，年龄，性别，就业信息，密码）缺乏安全的隐私保护机制，欺诈变得十分容易，且有利可图。另外，病毒也已经进入社交网站，因为在这可以把信任作为一种遗传媒介来使用。利用社交网络进行攻击的成功率很高。对银行来说，网络钓鱼成为第一大威胁，但银行尚未向客户提供用来认证银行自身的业务。

4. **国际犯罪组织**：根据过去几年许多地方的报道，国际犯罪不仅开始利用网络来实施其犯罪意图，而且存在一个国际性的黑市，正在出售犯罪工具（僵尸网络，网络钓鱼工具，病毒等）和被偷盗数据（个人信息，信用卡数据，公司机密信息）。网上犯罪和利用网络实施的犯罪的组织更加严密和国际化，并广泛延伸到各管辖领域，包括那些司法制度薄弱的地方，而且重点是为了谋取钱财。这种情况可以举出很多例子。FTC在三月份取缔了一家年收入达1.8亿美元的、半合法的威吓软件公司。用于犯罪活动的病毒、技术支持和“自助”工具还可以得到无效退款保证。黑市上宙斯（Zeus）银行木马软件（Zeus用来干扰验证系统，例如二因式系统和万事达安全码系统）售价700美元（最新版本为4000美元）。多个层级的合法和半合法供应商通过地下经济活动谋利。

有关这些非法活动造成的社会和经济损失的研究和统计数字有时候让人十分震惊。从全球看，这些损失可以高达上万亿美元[58]，相当于全球GDP的近2%。据波士顿计算网络估测，1999年头六个月，美国企业因病毒造成的损失超过76亿美元。德国因网络钓鱼造成的财政损失估计每年为1500万欧元，信用卡损失为1.55亿欧元。

总的来说，有关经济损失的大部分数字是基于有争议的估测，是对已知情况进行的必要推断，而且很多问题没有公开报道。但结论可能是，网

---

58 “McAfee公司研究表明全球经济萧条增加了知识产权风险”，McAfee 新闻公告，2010年2月，见 http://www.mcafee.com/us/about/press/corporate/2009/20090129_063500_j.html；亦见保护重要信息的不安全经济，McAfee，2009年，http://resources.mcafee.com/content/NAUnsecuredEconomiesReport。

络犯罪的社会-经济成本非常之高，它们常常被那些不得不就安全措施投资做出决策的人低估了。安全投资的收益问题应予以更加认真的考虑。

打击网络犯罪需要明确在数字环境下各种行动的责任，其中包括对全球不断产生的扩展业务采取配套行动。在更高的国际政治层面上，需要开展法律合作和外交行动，以便制定共同的政策和程序，确保各种业务及公共和经济行动的可靠性和责任。

需要通过开展技术研究寻求各种解决方案，一方面可以保持全球性的和不可分离的网络，使企业和消费者可以在家中和在旅行时通过接入网络工作、通信和交换信息，但所使用的方式应确保遵守适用于各种活动的法律；另一方面，人们有权把自己的私生活搬到网上，因此在某些情况下，他们应能够在自己选择的、有限的安全信任范围内进行网络活动，服务提供商应确保不把他们的数据用于其他目的。

遗憾的是，目前我们看到一种个人数据经济正朝着相反的方向发展。数据采集和处理公司现在采用的完全是利用客户的私人数据来盈利的商业模式。消费者可能认为自己是这些服务提供商的客户，因此所用的业务可能要对他们承担责任。但事实上，由于这些消费者无须为所用的业务付一分钱，因此他们实际上只是产品。营销公司、数据分析师、系统分析师、广告商和其他公司是社交网站和各种门户网站等出售消费者数据的**真正**客户。

实际上，私生活似乎成为了社会-经济空间数字化和网络化发展的真正受害者。数据存储价格正在迅速下降，数据的存储最终将没有数量和时间的限制。这将对我们的沟通方式产生深刻的影响，也会给将来带来新的犯罪（侵犯隐私、非授权数据整理和非授权数据挖掘）和新的政治控制方式。其中很多做法可能违反现有的宪法权利，它们对社会的、经济的和政治的稳定性的影响几乎没有得到研究。

除了以上谈到的数字环境给犯罪和人权可能带来影响之外，对于社会和经济来说，一种完全不同的威胁就是未来数字社会基础设施的极度脆弱性。在犯罪分子为了敲诈，恐怖分子为了制造恐惧和不稳定，或是其他国家为了战争或威慑目的攻击和破坏通信网络或其他关键基础设施时，整个社会可能遭受严重的经济和社会损失。各国对此类攻击采取的反制措施实际上仅限于防御行动。像威慑或反击等更具攻击性的战略很难得以实施，这是因为这些攻击常常不可溯源，而且是在未知的地方或流氓国家发起的。技术研究如果不充分重视网络和系统的安全和信任问题，将会加剧这些问题的产生，并可能导致未来的国家和国际冲突变得无法控制。

最后一点，必须考虑的另外一个重要因素就是给社会造成的长期风险。攻击的时间可能只是持续几秒钟，但会产生非常广泛的影响。要重建这几秒钟造成的社会信任损失可能需要若干年的时间。人与人之间、人们与企业之间、公民与国家之间以及国与国之间的信任缺失，从长远角度看，将会给社会和全球稳定性带来灾难性的后果。它将成为未来经济实现有效增长的一大障碍，而目前后经济危机时代的经济十分依靠加强信息通信技术的应用。在这方面，我们承担不起因信任损失造成经济的停滞。

数字环境下包括认证在内的网络和信息安全必须确保公民的安全（身体的、经济的和隐私的）。可靠的ICT系统、基础设施和机构将确保我们社会具有一定程度的社会信任，正如许多研究结果所表明的那样，这对于经济的繁荣是至关重要的。

社会的不稳定和经济上的损害（就经济增长而言）是很难计算的，但可能非常巨大。这迫切需要做好准备，加强保护以及具备系统快速的恢复和自愈能力。

总之，可以说：

数字空间的全球性特征，加上用户难于识别、行为难于溯源、复杂的国际扩展业务、社交网站的全球发展以及正在出现的国际犯罪网络和市场，引起了人们对网络犯罪上升和作为个人发展和经济繁荣基础的稳定社会的可持续性的严重担心。

我们社会中ICT基础设施的脆弱性和数据搜集和存储的无限制性构成了个人自由和国际稳定的威胁。

公民对社会和政府在保护其和平、安全和繁荣方面的信任因技术发展带来的危险和不确定性而受到侵蚀，且会产生潜在的和沉重的经济损失。

因此，我们迫切需要在全球范围内采取新的政治行动，通过深入分析技术、社会、经济和政治趋势及后果来解决这些问题。

4 技术的趋势和威胁

4.1 目前的潜力、趋势和威胁

作者：**Axel Lehmann，Vladimir Britkov，Jacques Bus**

技术创新的驱动力是技术“推动”和市场“拉动”。在这方面，在分析ICT创新的未来方向和潜力时，必须考虑当前的和预测的技术进步以及未来消费者或市场需求的趋势。因此，本章的前三个部分谈的是这些趋势和需求，然后分析了主要的威胁，最后提出了一些结论性意见。

在本章开始，先对后面的分析和评估加以概括。我们认为，预测的技术创新不仅可以促进新的微型和奈米技术的快速进步，而且还能够推动新网络和通信技术以及创新业务和应用中大规模集成传感器和计算设备的发展。另外，这些创新还可以促进两个主要的演进方向：

- 现有的单一计算机和用户移动电话的融合向单一便携式和移动多用途技术和通信设施发展；而且
- 现行互联网、网络技术和业务向未来互联网演进。以个人之间和各种设备和物体（“东西”）之间实现大规模通信和移动性为特征的“物联网”将是我们朝着一个有效的、可靠的和可信的未来互联网目标走出的一大步。

市场和消费者对新的ICT产品、业务和技术发展的需求将进一步促进这些技术的进步。根据福布斯公布的一项研究结果，娱乐和通信、能源和医疗保健行业尤其会成为ICT创新产品[59]的驱动力和主要应用领域。

---

59 Robert Krysiak，“2010年半导体大趋势2010”，*Forbes*，2010年1月，见 http://www.forbes.com/2010/01/04/stmicroelectronics-healthcare-entertainment-technology-cio-network-semiconductors.html。

在这方面，以下三个部分将总结影响未来ICT发展的主要因素及其结果：技术趋势，市场和消费者需求和“物联网”，最后两个部分则概述了这些ICT创新给我们个人和公众生活带来的基本机遇、威胁和挑战。

技术趋势

毫无疑问，在这个十年中，微型化和数字化对于我们大步迈向各种数据、信息和知识以数字方式进行存储、传送和处理的“数字化世界”发挥了重要作用。通过对半导体这一目前的基片技术的发展进行趋势分析可以看出，“每两年将平方英寸的晶体管数量增加一倍”的摩尔定律至少在今后十年依然是有效的。目前的设计和制造技术可允许在单个芯片上集成约十亿个晶体管。即使从长远看，现有的半导体技术将会逐步被诸如生物技术或量子计算等新技术所取代，这些增强小型化和数字化并扩大功能和应用的一般趋势将继续下去，并将进一步促进ICT和基于ICT的产品和应用的发展。

在这方面，必须从硬件、固件和软件发展的角度考虑四个主要领域未来数字系统的发展和组织原则：

- 单计算机和多计算机系统。
- 通信网络、协议和业务。
- 纳米技术、材料科学、传感器、作用物和嵌入式系统。
- 数字系统的分散式操作和组织机制。

由于每个芯片区晶体管的超大规模集成和不断增加的时钟频率造成了过热问题，目前的**微处理器**是按照多芯处理器设计的，以降低的时钟频率工作，但性能因芯片具备并行处理功能而得以提高。处理器进一步的创新可以通过多层半导体技术、增加核心处理器的数量和降低每个芯片的功耗来实现。由此将通过多芯处理器、多处理器系统、进一步增加缓存和主储存容量以及芯片系统开发大大地改进性能。这些趋势将会改善从单芯片计算机和嵌入式计算器件到超级计算机等各种计算机的性能。由于通信和交换网络也会发展，将来可以提供各种结构和体系的互连计算机。

另外，通过经改进的微型化技术，还可以提供存储容量更高、存取时间更短的快速外部存储设备。随着结构方式和软件技术的改进，大量地同步运行复杂的软件应用技术将是可行的。与此同时，通过开发新的低功耗技术和电池，计算机和各种计算设备的移动性将会得到大大改进或促进。

在**通信网络、协议和业务领域**，重大的创新将来自于无线和卫星通信技术的不断改进，可以提供更多的连接和更宽的带宽。其中一个主要趋势是动态地形成虚拟网络，例如虚拟专用网[60]。这种技术已经得到应用，可以迅速形成和使用由特定网络成分和业务组成的应用和面向用户的网络。

另外一个趋势是使现有的计算和通信基础设施具有更高的灵活性和使用率，涉及网络的重叠。作为目前的一个重要研究课题，这种技术被看做解决现行IP/TCP协议目前的限制和IPv4向IPv6演进的有效手段，这是提高互联网和“物联网”使用的重要步骤。这两个方向技术的进步是进一步创新互联网技术和应用的先决条件。当前互联网的巨大发展，特别是就与互联网相连物体的类别和数量而言，一方面需要大大扩展面向IPv6的互联网物体的现有地址空间（IPv4）[61]。因此，必须开发一种允许这两种标准之间实现升级过渡的特殊转换技术。另一方面，在IPv4向IPv6演进的同时，必须制定未来IP/TCP协议的标准，以便通过“未来互联网”实现各种物体之间的通信。虽然这两个方向的研究仍需要具体的解决方案，但可以推断的是，未来互联网所需的技术将在今后几年内得到应用，它们将为诸如“物联网”等互联网应用提供高级的和新的能力。

---

60 James Henry Carmouche，*IPsec虚拟专用网的基本要素*，Cisco简讯，2006年7月19日，见http://www.ciscopress.com/bookstore/product.asp?isbn=1587052075。

61 S. Deering 和R. Hinden，“网际协议，IPv6的技术规范”，互联网协会，1998年12月，见http://www.ietf.org/rfc/rfc2460.txt；Walter Goralski，“图解网络：TCP/IP 如何在现代网络中工作”，Morgan Kaufmann 网络系列丛书，2008年，见 http://www.freshwap.net/forums/e-books-tutorials/120250-illustrated-network-how-tcp-ip-works-modern-network.html。

除了上述ICT系统的发展趋势外，在分析ICT的未来趋势和威胁时，还必须考虑在奈米技术、材料科学以及专用数字器件领域（例如基于半导体的传感器、作用物或嵌入式系统）技术和制造的快速发展。这些发展将会导致产生某些ICT器件，例如：

- 可见的用户接口。[62]
- 聚合物显示器。
- 数字化服装（可穿戴式计算机）。[63]
- 无源和有源感应器（RFID 技术[64]）。
- “环境智能”[65]或“智能”系统。

随着这些技术的发展，改进的和新的**固件/软件产品、服务**以及组织机制将为改善和增加功能和业务带来机遇。这些技术发展包括各种创新的软件技术（例如代理式软件开发），面向业务的结构（SOA），新的网络业务或管理系统（例如有效的存储或检索数据以及有效的负载平衡），还有有效地使用由分布式计算机和通信资源组成的庞大网络形成的网格式基

---

62 Hiroshi Ishii，“有形的用户结构及其革命”ACM通信，第51卷，第6期，2008年6月6日，http://portal.acm.org/citation.cfm?id=1349026.1349034。

63 Steve Mann with Hal Niedzviecki，电子人：可穿戴式计算机时代的数字化命运和人类可能性，加拿大双日出版公司，2001年11月。

64 RFID的应用和影响，欧盟（企业和工业总局，ICT用于竞争和创新），企业和工业总局，行业电子商务观察，Impact Study No. 07/2008，最后报告，2008年9月，http://www.ebusiness-watch.org/studies/special_topics/2007/rfid.htm；Arun N. Nambiar，“RFID 技术：对其应用的分析”，2009年世界工程和计算机科学大会文件，第2卷，WCECS 2009，20–22 October 2009年10月20-22，美国旧金山，http://www.iaeng.org/publication/WCECS2009/WCECS2009_pp1253-1259.pdf。

65 E. Aarts，R. Harwig，M. Schuurmans，“环境智能”一节，in Peter J. Denning，ed.，不可见的未来：技术无缝进入日常生活，McGraw-Hill 公司，2001年，电话235-250；D. Wright，S. Gutwirth，M. Friedewald et al.，环境智能世界的保护，施普林格出版集团，2008年，http://www.springer.com/computer/database+management+&+information+retrieval/book/978-1-4020-6661-0。

础设施。最有现实意义和深远影响的应用是网格计算或云计算[66]，它们从经济、性能，可提供性和可靠性等方面开辟了一个新的ICT时代。

除了上述所有的技术发展外，在分析ICT创新的主要趋势和威胁时，尤其要考虑涉及**组织和运行原则**的两个根本性的重要趋势：**虚拟化和分散化**。一方面，异质性数字器件功能和互连程度不断增加，另一方面，对其有效使用的需求不断增加，促生了虚拟系统的形成和运行，例如虚拟处理器，虚拟存储器，甚至是虚拟计算机。此外，连网计算机和通信系统不断增加的复杂性和上述虚拟网络的使用常常会阻碍集中控制的有效运行。但是，越来越多用于分散式系统控制的运行机制正在得到应用，它们相对集中控制来说具有更高的灵活性和有效性。代理式软件应用或生物模拟系统控制就是分散式系统控制的例子。

同时实现并应用虚拟化和分散化这两种原则已经为有效利用网络化数字资源带来了新的机遇。这种网络可以形成“网格”：[67]由连网计算机节点组成的计算机网格，由互连的分布式存储系统组成的数据网格，或是由可以远端接入的专用设施组成的设备网格。就云计算而言，这些网络化和互连的资源可以通过服务提供商远程接入和使用。除了这些经济上和性能上的优势外，其风险也是需要考虑的。一般性的挑战（也是目前一种主要风险）就是要把握好这些系统的复杂性，尤其是在安全和可靠性方面。从目前的科学进展来看，这些已经运行的网络系统既不能全面检验其适当与否，也无法完全确认其具体的应用，而且由于它们巨大的状态空间，更不能进行充分的测试。这种情况尽管已经给ICT创新[68]带来根本性问题，但目前尚未得到充分的重视。除了这些挑战之外，其他风险来自于出现故障和失效以及潜在的使用不当和操控行为。在全面评估这些ICT创新技术时必须考虑这些风险，而且迫切需要就应对方案进行更多的研究。

---

66 Vladimir Britkov，“网格和云计算”，向世界科学家联合会信息安全常设监督委员会提交的文稿，2010年5月，（以下称“Britkov”）。

67 Britkov.

68 Vladimir Britkov 和Axel Lehmann，“信息和通信技术（ICT）创新产生的安全挑战”，*核战争和全球突发之间国际研讨会*，第38次会议。E. Majorana科学文化中心，意大利埃里切，2007年8月19日至24日，电话503-515。

消费者和市场需求趋势

目前市场和消费者的一种主要需求是泛在计算、通信和信息接入，这意味着在“任何地方和任何时间”都能使用数字设备和网络能力。消费者较高的移动性以及信息和知识的全球分布和提供增长了对改善ICT产品、增加功能及其有效使用的需求。这些需求将会不断地和大幅地增长，并在不同的市场上出现。例如，业界和经济领域对本地分布的和时间独立的合作越来越有需求。

所有这些需求都完全基于这样一种假设，即我们将要在一个完全数字化的世界里生活和工作，可以在任何时候从任何地方找到和使用任何一个物体或一种信息。这些由消费者和市场驱动的需求大大地“拉动”了技术的创新，例如有效地使用多媒体或视频应用，泛在网络接入，计算机支持的合作活动（CSCW），或使用大量的（基于网络）的业务和应用。除了新的和有用的ICT器件和产品外，“物联网”的发展可能带来新的社会和管理问题，并且给安全带来潜在的威胁。因此，必须从一开始（就是现在）就认真分析这些创新及其影响（见下一部分）。

如上所述，现在和将来硬件/固件/软件的发展将沿着这一思路促进开发基于ICT的新产品和创新的应用，并用于各种应用领域。这种应用领域包括：

- 环境辅助生活（例如用于老年人）。[69]
- 智能控制系统（例如交通，物流，导航航空，节能等）。
- “智能”家庭。[70]

---

69 Kizito Ssamula Mukasa，Andreas Holzinger，Arthur I. Karshmer，“环境辅助生活的智能用户接口”，第13次国际智能用户接口大会文件，ISBN：978-1-59593-987-6，2008年，http://portal.acm.org/citation.cfm?id=1378856；Fraunhofer IRB Verlag，ISBN 978-3-8167-7521-8，http://verlag.fraunhofer.de/PDF/English_Publications_2010.pdf。

- 医疗保健。

娱乐和通信行业的需求主要集中于ICT的性能和经济方面，而能源或医疗保健行业诸如控制或监测系统等其他应用领域主要必须满足安全性和可靠性需求。正如前一部分所述，在这些应用中，所使用数字设备数量和性能的不断增加及其无限的互联性导致产生了“状态空间爆炸”的问题。为确保这些质量要求，迫切需要加大基础研究和应用研究的力度，找出适当的设计、检验和确认方法以及测试战略。

“物联网”

“物联网”是一种愿景，即除人类以外，各种物体、设备或我们日常生活的物品（“物”）都可以通过未来互联网连接起来。这些“物”通过连接其他“物”、个人或业务，可以接收、存储、处理或发送数据和信息。这要求更多的“物”必须具有同一个可在IPv6环境下实现的互联网地址，并且自身可提供服务，或在子网上作为物理源、目的地或接入点进行通信、合作和计算[71]。

逐步实施这一愿景可以实现Mark Weiser在20年前提出的“泛在计算和通信”的理念。[72] 这种愿景的一个主要特征是开发面向“智能物体”的技

---

70 P. Rashidi，D. J. Cook，“把居民留在圈子里：让智能家庭服务于用户”，*系统，人类和控制，A部分：系统和人类，IEEE Transactions*，2009年9月，39卷，Issue:5 at 949–959，http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?reload=true&punumber=3468；CASAS智能家庭项目华盛顿州立大学，美国，http://ailab.eecs.wsu.edu/casas/。

71 *互联网 — 欧洲的行动计划*，欧共体委员会提交欧洲议会、欧洲理事会、欧洲经社理事会及地区委员会的报告，http://ec.europa.eu/information_society/policy/rfid/documents/commiot2009.pdf；附录F：物联网（背景），破坏性技术：2025年的全球趋势，SRI Consulting Business Intelligence，http://www.dni.gov/nic/PDF_GIF_confreports/disruptivetech/appendix_F.pdf.。

72 Mark Weiser，“二十一世纪的计算机”，*美国科学*，Sept.1991年9月，电话 94-110，http://www.cim.mcgill.ca/~jer/courses/hci/ref/weiser_reprint.pdf。

术物体，它们具有有限的计算和辨别能力，而且通过互联网与网络空间连接起来。例如，这种“智能物体”可以是一种有源感应器，它可以接收来自于其他物体的信息，处理这一信息，并且可以根据自己当时的状态通过向其他物体发出应答信息做出反应。它不仅能够实现个人与“物”之间的通信，而且可以实现“物”之间的通信，为各种应用带来了全新的机遇，但也会带来安全性和IT安全方面的风险（隐私，认证，数据安全）。

目前的威胁

如上所述，数字网络世界的规模、复杂性和开放性已经达到了相当程度，出现滥用网络行的快速增长一点也不奇怪，如果不认真对待的话，ICT未来的发展趋势甚至会增加威胁的数量和潜力。

这方面有很多报告，有些报告是来自那些希望出售ICT安全解决方案的公司，例如MacAfee,[73] Symantec,[74] Kaspersky,[75] 或者是那些研究一般性安全问题或出于自身IT系统和产品安全考虑对此感兴趣的公司[76] 。这些报告涉及最多的网络犯罪类别是：

1. **恶意代码或恶意软件**：基于发明者知觉到的个人意图，而非具体功能的软件。恶意软件包括计算机病毒，蠕虫，特洛伊木马，间谍软件，欺诈性广告软件，犯罪软件，大部分根工具包及其他恶意和不需要的软件。[77] 根据Symantec的报告，新的恶意威胁从2007年的62.4万个增至2008年的165.6万个。
2. **垃圾信息**是滥用电子信息系统（包括大部分广播媒体、数字传输系统），任意地发送大量对方不需要的垃圾信息。最常见的垃圾信息

---

73 McAfee 安全顾问中心，见http://home.mcafee.com/advicecenter/。

74 “互联网安全威胁报告”，Symantec，见 http://www.symantec.com/business/theme.jsp?themeid=threatreport。

75 Kaspersky，http://www.kaspersky.co.uk/index.html。

76 “安全技术中心”，见 http://technet.microsoft.com/en-us/security/default.aspx；SANS，http://www.sans.org/。

77 要了解该定义和更多解释，见：http://en.wikipedia.org/wiki/Malware

形式是垃圾邮件，或是大量发送的、具有商业内容的不需要的垃圾信息。发送成本低产生了很高的价值回报。但是，越来越多的垃圾信息具有犯罪性质，包括恶意软件或意在欺骗人们支付和提供信息等（网络钓鱼）。

为了隐藏发送者的地址和增加发送量，犯罪分子常常使用僵尸或机器人（利用外部控制把其他人的计算机作为一个远程奴隶，而计算机所有者却不知晓）或僵尸网络 （也称为botnets）。2008年发送的垃圾信息数量估计达到3500亿条，其中90%是通过僵尸网络发送的。这一数字占全球总信息量的85%。

3. **网络钓鱼**网站和服务器是伪装有信誉的机构（例如银行）的网站或电子邮件地址，具有获取诸如用户名、密码或信用卡资料等敏感信息的犯罪目的。恶意软件可以装在一台计算机上，把使用这台计算机的用户带到一个网络钓鱼网站，而非用户需要的有信誉的网站，或者发送带有欺骗性地址的垃圾信息，诱骗用户点击一个与网络钓鱼网站相连的链接。有报道显示，2008年发现的网络钓鱼主机达到5.5万个，比2007年增加了66%。

4. **机器人和僵尸网络**是通过使用许多用户的计算机并在其不知晓的情况下建立的。它们或是直接地使用，或是在黑市上以“租赁”方式用于犯罪目的。Symantec发现，每天有7.5万台计算机受到机器人病毒的感染，还有1.5197万台新的机器人命令和控制服务器。地下经济服务器成为被盗信息（涉及信用卡和身份证等）或出售/租赁恶意软件或僵尸网络的黑市。

虽然报道一般都认为，大部分攻击的源头是美国，其次是巴西和中国，但攻击可以由任何人在任何时候，甚至是在远端发起。尽管利用零日脆弱性发起的Conficker蠕虫攻击对我们仍然记忆犹新，但我们可以谨慎地认为，由于大的软件公司日益重视操作系统和应用的安全问题，严重的零日漏洞数量正在减少。

犯罪行为主要针对金融行业，该行业吸引了70%的网上钓鱼活动，互联网服务提供商居其次，只占11%。

FORWARD [78] 集团发布的《白皮书：正在出现的ICT威胁》试图系统地研究当前和未来的威胁问题。它们提出了预测未来发展或目前正在出现的四个轴：新技术，新应用，新商业模式和新的社会动态。它们把28种威胁分为8大类：

1. 网络：使用和部署新的网络技术和互联网基础设施业务（路由，DNS）面临的威胁。
2. 硬件和可视化：新的硬件和软件开发在可视化和云方面的威胁。
3. 设备的脆弱性：新的计算设施因计算能力和容量有限带来的威胁。
4. 复杂性：因未来系统的复杂性和规模水平带来的威胁，导致产生了意料之外的依赖作用和安全后果。
5. 数据操纵：因人们（和系统）在网上存储过多数据产生的威胁，而且这种数据变得越来越有价值和敏感。
6. 攻击基础设施：这种威胁指的是，对手积极开发和部署攻击性平台（例如僵尸网络）。它们不再进行打了就跑的攻击，而是在互联网上建立进行恶意活动的操作基地。
7. 人类因素：因内部攻击，特别是外包产生的威胁；与新的社会工程攻击相关的威胁。
8. 安全要求不充分：这种威胁指的是传统的和即装即用式商业系统没有足够的保护，目前使用和部署方式缺乏相应的保护机制。

这种分类法在考虑到威胁的严重性、可能造成的后果和目前工作的同时，可确定用以减少威胁的其他（研究）活动的先后次序。它们最后提出了威胁最高优先范围：并行性，规模，地下经济支持结构，移动设备恶意软件和社交网络。

78 “FORWARD发布的正在出现的ICT威胁白皮书”。见http://www.ict-forward.eu/whitebook/。

目前的威胁状况已足以引起我们的警惕，需要各行业专家以及政治家和外交家在全球层面上就各种原则问题采取紧急协调行动。有些威胁的应对主要需要调整或改进安全规则、标准、技术或手段，其他威胁则迫切需要基础科学研究和切实可行的解决方案。

结论

有关ICT的未来研究的产品开发将会在全球范围内极大地影响私人和公众生活中的个人、社会和文化行为。数字系统、互联网及其业务和应用的不断发展正在成为日常生活的基本资源。这种数字化世界为人类和技术发展带来了许多益处和机会，也为解决诸如能源或医疗保健等一些全球性问题提供了新的途径。本章讨论的是未来ICT技术和应用产生的基本机遇和益处。

虽然有这些积极的方面，但要解决新的和更大的问题则需要更深入的基础研究和适当的解决方案：根本的问题是缺乏设计和分析方法，以便科学地控制未来互连数字系统的巨大复杂性，特别是那些涉及安全性、可靠性、功能性和保障性（隐私，真实性和数据安全）的问题。研究这一根本性问题的解决方案是计算机科学和网络科学研究领域面临的一个最重要的挑战。就像世界科学家联合会所做的那样，全球发布一个开放的“难题清单”，再加上有效的应对措施（如果有的话），可能是这方面应采取的一个有益的行动。

然后，这种“控制差距”不仅体现在目前的设计和生产技术方面。必须考虑因人类错误、技术故障、失效或滥用和操纵造成的后果，而且还需要研究和实施应对措施，尤其是要充分考虑后者面临的某些限制。

此外，由于缺乏适当的措施，用户、消费者和公共机构无法了解使用ICT资源带来的主要问题、风险，甚至是威胁。媒体专业人员应参与编制有关IT安全问题的信息材料，以满足不同使用者的需要。正如第二章所述，现代社会依赖于ICT和不断发展的互联网。因此，为了建立信任，必须认真分析和宣传面向数字化世界的未来技术发展所产生的影响。

4.2 政府互联网审查：网络压制

作者：Henning Wegener

自由表达言论和自由获取信息是信息社会运转的核心所在，也是网络稳定和网络和平的基本组成部分，正如同一个作者在第四章“网络和平的概念”所述的那样。对行使这种权利的威胁剥夺或否定了互联网的主要益处，因此被列为目前网络空间的主要威胁。[79]

言论自由和自由获取信息长久以来一直是建立文明社会的关键要素。它们是人权和公民自由权不可缺少的一个部分，因此成为几乎所有现代宪法的主要特征。实际上，个人获取信息、发表和交流意见的自由可以看做人类进步的标志。另一方面，从公共安全、正当性和公共秩序等方面考虑，如何定义这一主要自由权的限制一直是内部政治辩论的一个固有部分，这种努力对于协调和优化个人自由与公共利益之间的关系是经常的和必要的。

政府审查系统地越过了这些限制，并对公众意见和思想交流加以紧密控制针对的主要是印刷材料，这是人类历史的一个痛苦但却时常出现的部分，已经不断地引发了有关思想自由的斗争。

在互联网时代，这一基本现象没有改变，但其影响和形式的确发生了变化。数字技术使接入信息和沟通的机会一下子进入到一种新的境界；这

---

79 世界科学家联合会在提交2005年突尼斯阶段“信息社会世界峰会（WSIS）”的文稿中提出了这一问题，“数字鸿沟环境下的信息安全”，第5项建议具体提到“利用互联网过滤阻止信息接入”，第12页和第24-30页中的解释性意见，见 http://www.itu.int/wsis/docs.2/tunis/contributions/co1.pdf，和 www.unbiw.de/infosecur. 同时见与本章类似的观点，Henning Wegener“网络压制：锁定这个问题。分析应对战略的辩论情况和思想”，网络空间的权利和责任。平衡2010年安全和自由的需求，东西方研究所和世界科学家联合会，见 http://www.ewi.info/rights-and-responsiblities-cyberspace-balancing-need-security-and-liberty。

正是今天我们面临的信息社会的实质。像其他每个方面一样，互联网扩大了思想的广度，模糊了数量和质量的衡量标准，否定了距离和时间概念，并带来了互为矛盾的新的现象。

这是因为互联网不仅使信息及其接入水平呈指数增加，而且也扩大了干预基础技术进程和操纵数字内容的潜力。数字技术可以让过滤软件阻止整个互联网上或某个服务器上的各类信息，而且它可以使政府引入政府审查手段，包括大范围的审查。因此，必须重新考虑言论和信息自由这一人权问题：在争取人权和言论自由权方面，互联网正在迅速成为一个新的战场。

政府审查时采用的主要技术是IP拦截、DNS过滤和转向、通过扫描目标关键词进行URL过滤，或进行分组过滤，就是一旦检测到争议性关键词，就终止TCP分组传输。其中一个特征是，现有的过滤软件只能机械地对重复出现的某些词或词组做出反应，因此常常超出目标范围 （“过渡拦截”）。

使用上述技术或其他技术的过滤软件工业提供商有很多。它们既包括大部分信息技术知名公司，也有专门的公司。有几个网页专门就其效率水平进行比较分析和软件排名，由主张互联网言论绝对自由的人士运营的几个网页对这种技术大加批评。

过滤技术必须与规避技术一并考虑。开发过滤器的复杂性在于它同时也带来了用来防止、规避或破坏过滤器的技术。由于网络的基础技术是分布式的，彻底审查互联网上的信息非常困难，甚至不可能实现。因此，有一些资源和解决方案可允许用户避开互联网审查。其中大部分依靠接入不受过滤的互联网链接，它们通常处在不受相同审查法律控制的不同管辖范围。政府互联网审查的实施者面临的直接挑战是，只要世界上还存在一个不受审查的公共接入系统，接入受审查的材料仍然是可能的。用于这种偷偷接入的技术包括使用代理服务器，建立虚拟专用网和下载那种允许匿名搜索、聊天和发送文件的开源软件（例如Psiphon，I2P，Tor）。

确切地说，内容过滤也具有一种重要的社会保护功能。一般来说，拦截那些涉及儿童色情，煽动暴力、种族仇恨和犯罪的网页对任何人似乎都是合法的，同样，针对国家和国际恐怖主义越来越多地利用互联网采取相同措施也是如此。那些无法在互联网之外合法传送的内容需要在法律上取缔，同时也需要在网络之内禁止。在这方面，过滤软件行业满足了法律的需求。

但这里有一个重要的区别。

无论过滤器及审查的效率和效果如何，也不管涉及何种商业利益，最为重要的是，在“自由”社会中 — 主要是（但绝对不单是）具有高度价值认同的所谓西方民主，有关言论和信息获取自由的限制在法律上有明确的规定，其范围受制于适度和对称规则，并且可以通过公开的法律审议程序进行评估。明确的法律框架和独立的法律控制的确是将合法的内容控制与非法审查区别开来的决定性尺度；另外，它们还为接受文化价值和隐私定义的不同提供了手段。攻击某些国家的文化、宗教、道德和其他根深蒂固的共同信仰的内容不应打着互联网绝对自由的旗号免受控制，而那些合法地谴责政府政治审查制度的人们在这些问题上应谨慎表态。

就政府互联网过滤而言，限制言论自由应遵守的限度，应取得的平衡，IT行业在为互联网控制提供技术基础方面应发挥的作用，均涉及国家主权等敏感问题，本文无意指责任何一个政府或追究其责任；实际上没有提到任何一个国家的名字。同样也没有提及任何一家IT硬件、软件或服务提供商的名字。实际上，本文目的在于指出这一问题和分析各方意见，而非草率做出结论。按照同样的克制精神，引用网页或文章只是为了参考起见，并不说明本文认同或支持其内容。

考虑到互联网的无国界特征，国家规则不足以管理互联网自由。因此，自1999年以来，欧盟实施了一个早期欧盟国家机制，管理互联网内容侵犯和相关程序（“更安全的互联网计划”）。它主要依赖于互联网行业自治原则，并利用搜索工具排除非法或有害内容，确保符合国家法律。在有些地方，这种自制做法运行良好，虽然有时候还需要制定补充性法律。

从全球角度看，国际法律标准是联合国成立初期由两个了不起的人权条约特别确定的，即《世界人权宣言》（1948年）和1966年《政治权利和公民权利国际公约》。实际上，所有国家都签署和批准了这两个被视为国际习惯法的条约，因此他们对非签字国也具有约束力。巧合的是，这两个文件的第19条都承认主张和发表意见的自由，这包括任何人通过任何媒介不论国界接受和传递各种信息的权利。它毫无疑问也包括通过互联网接收信息和接入信息的权利（就如同不接入信息的权利一样），因此，信息社会世界峰会（WSIS，2003年和2005年）已经郑重地将这些原则确定为信息社会的核心和不可缺少的支柱，它具体反映在《日内瓦原则宣言》（第4、第5和第55条原则）中。值得一提的是，WSIS文件强调了自由这一点，未强调国际公约中的告诫。

“自由”社会中的内容审查问题最终归结为在明确的法律标准下自由与国家干预之间的永久政治平衡问题，不可否认，这是个难题，因此在其他许多国家，这个问题变成了人权问题和全球信息秩序的质量问题。政府在没有法律限制并严重地和深刻地影响个人寻求和传递信息的情况下进行互联网审查，构成了一种高度违反人权的行为。这方面存在的一个实际问题是，西方技术公司不仅向主张审查的政府提供过滤技术，而且在使用上还参与合作，由此产生了有效的审查系统。这一现象是本文分析的主要内容，因为本文目的也是就如何在国际层面上反对这些做法提出建议。正如“审查制度索引”[80]机构的编辑Jo Glanville所说的：“目前的审查制度有史以来第一次变成了商业经营”。[81]

在这本书问世的时候，无论是实行损害政治权利和自由的互联网审查制度的政府的数量，还是过滤技术的成熟度，都出现了根本性的增长或发展。

---

80 审查制度索引是英国一家提倡言论自由的知名机构，见 http://www.indexoncensorship.org

81 Jo Glanville，“网络审查的大买卖”卫报，2008年11月17日，见 http://www.guardian.co.uk/commentisfree/2008/nov/17/censorship-internet。

政府互联网审查制度的发展情况受到许多私人机构的跟踪，包括创始机构“开放网络促进会”（ONI）、“记者无国界”以及经常使用相同或相似数据和分类的“互联网审查制度报告”。[82]

这些组织都发现审查制度的数量出现了惊人的增长。它们根据国家名单和数字提出，目前至少有17.2亿人受到互联网审查的影响。这相当于目前世界人口的25.3%。

采取这种做法的国家名单很长，至少有25个或30个以上的政府严重剥夺了其公民接入网上所有信息的可能性。互联网上提供了一些由监测这些国家的机构提供的清单。开放网络促进会把它们分为普遍的，实质性的，形式上的和间接的等几大类，同时还有一个“观察名单”类别。记者无国界罗列了前13个“互联网的敌人”名单。大部分被监测的国家干预的重点是禁止政治内容 — 自由，民主，自由选举，法律救济方法和涉及敏感政治事件的报道，这些是它们政府自身的制度所不允许的，但很多政府超出了这个范围。有些政府重点是限制道德内容，涉及传统的道德和文化秩序。控制的程度和范围各不相同。一些国家的审查部门拦截网页，但又把它转到说明性网页，如果能证明对信息具有“合法的”兴趣，就可以提供接入，因此至少提供了一定程度的透明性。其他国家的审查零零散散，也没有效率，在封锁被破坏的情况下，禁令就无法奏效了。

但是，一般来说，政府审查制度的实施是没有限制的，涉及广泛的人类知识，没有任何解释或合理的依据，甚至在一些非常体面的国家也是如此：一个国家离西方民主越远，利用互联网过滤实施审查的概率就越高。有些国家把通过互联网审查教育国民的做法发挥到极点：互联网用户在接入受禁止的网页时如果被发现将受到惩罚，有些国家是由放肆的网络警察来为难用户。据了解，用户被投入监狱的数量无论从哪个角度看都是令人

82 全球网络倡议，见www.opennet.net。该项目利用一个国际调查者网络了解政府互联网过滤计划的范围和性质。参与的学术机构包括多伦多大学Munk国际事务学院的国际研究中心，哈佛法学院的Berkman互联网和社会中心，牛津大学的牛津互联网学院以及接管剑桥大学剑桥安全计划高级网络研究集团的SecDev集团。亦见www.chillingeffects.org，它是一个更大的组织，专门支持“跟踪互联网活动的法律环境”的学术机构。

吃惊的。一些提供这种软件的国际性IT公司不得不容忍这样的怀疑，也就是它们积极帮助和怂恿这种告发方式，因此造成了人类的痛苦。

全面审查造成的后果非常严重，是不能低估的。不仅是公民按照国际法应享受的权利受到限制，而且他们无法获得信息时代的重大益处，看到的是扭曲的世界，参与丰富全球思想交流的机会减少了。大量地过滤互联网可能改变一个国家的集体心态。另外我们还必须考虑这种审查制度产生的双重负面效果：公民被剥夺了获取信息和无限制地了解世界的机会，而且审查同时也是一种进行政治压制、限制行动自由的手段。

这种状况和不断恶化的互联网审查记录迫切要求采取行动。其中欧盟就意识到了这一点，并采取了行动。它不接受压制的政府借助IT技术公司来巩固其精神独裁。同时，我感谢欧盟用“网络压制”这一十分贴切的用语给这些做法命名。

欧盟不是孤立的。为倡导信息自由和全球互联网一体化而游说的互联网机构非常活跃和警觉，甚至超过上述那些监测网络压制情况并对此公开谴责的许多知名机构。

考虑到有经验的互联网用户有能力避免或绕过过滤器，许多捍卫互联网自由的国际组织已经开始为住在受谴责国家的公民提供上文提到的反审查软件。这些反过滤技术也已经发展成为一个名副其实的产业，它有助于减少政府审查的有效性，但不能彻底消除审查。开放网络促进会和其他组织一样积极从事这方面的活动，通过提供特别有效的系统（例如Psiphon）允许一般家庭计算机作为个人加密代理服务器，然后在跳过政府施加的强制性“防火墙”后可以自由地在全球网络上搜索。但是，这种设备和其他相似设备的应用正受到某些过滤器提供商的积极抵抗。这再一次证明了跨国企业商业活动的这种成问题的本性，也就是有意或无意的连带损害，实际上促进或帮助了网络压制行为。此外，显而易见的是，数字技术发达的国家能够在国内开发过滤器，许多国家已经这样做了，这将使外国软件提供商摆脱困境。

前面已经强调，本文目的不是就各国情况进行详细的分析，同时也考虑到互联网在这方面已经提供了充分的信息。但是，即使是本文的简要介绍和刚出现的公众讨论，都提出了一个如何采取实际行动和国际社会如何抵制网络压制继续违背国际法的问题。

确定国际认可的互联网过滤和禁止的界限所涉及的法律和政治问题是显而易见的，也是非常多的。国家管辖和主权问题，公民自由权与压倒一切的公共利益之间要形成广泛有效的界限几乎不可能，法律选择和执法方式的问题，还有互联网治理这个更大的问题，所有这些使制定国际法则的努力变得不可行，可能也是徒劳的。另外还有文化多样性和其他人对它的尊重问题。文化和宗教的*公共秩序*定义不可能对所有国家都千篇一律，尽管我们可以合理地假定存在一个具有一致基本信念的国际组织，也尽管国际人权宣言和权利公约必须看做具有国际约束力。正像大部分国际法一样，不存在简单的定义，也很难迅速得到核准。

因此，必须从*程序*和*长远战略*角度看待改革全球互联网过滤问题。人们应该从程序上进行思考，因为程序会提高世界的认知，唤起公众的意识和压力，而对相关政府而言，则会形成公众舆论的挑战和提供详细依据的压力。

国家政府、行业和善于提出意见的民间机构负有重要的责任。政府可以促进反过滤技术的研究和提供，可以对过滤技术出口进行适当的控制，并从维护透明性角度利用国家外交手段对那些实施审查的政府施加压力，迫使它们公开限制性政策并证明其合理性。

IT行业，即软件制造商和提供ISP业务的公司及其协会，显然负有责任，它们应遵守行为准则，避免将其技术用于政治审查。虽然事实上人们不能要求这些公司完全放弃追求利润，虽然把政府审查的主要责任转嫁到行业身上是十分愚蠢的，但公司自愿地采取集体行动还是涉及声誉，将会加强正面形象。具有明确共同标准的自律政策已经在欧美取得了很好的效果，而且还可以加强单个公司的抵抗力量，更好地应对那些急于与它们做生意、主张审查的政府施加的压力。例如，由美国技术公司自愿发起的

“全球网络倡议”就制定了这种标准（“治理宪章”），对政府审查要求做出反应，促进互联网自由。[83]

那些不遗余力地谴责网络压制的学术机构和人权组织（有些上面已经提到）正不断得到支持其事业的政府的鼓励和支持。但是，考虑到互联网的跨界和国际性特点以及网络压制涉及的国际人权问题，最重要的任务是通过完全不同的方式把这个问题纳入国际组织的议程。

第一步可以就目前互联网过滤的发展和技术基础达成比较广泛的国际共识并建立国际性监测机制。

第二步可以考虑引入一种国际申诉程序，广泛面向所有相关方，并采用一些简要报告标准。

哪个国际组织或机构可以服务于这种斗争呢？

首先，人们可能会想到按照WSIS的决定（“突尼斯议程”）于2006年成立的互联网管理论坛（IGF）。互联网政治审查对网络运行和管理施加的限制显然涉及该论坛的任务，而且很容易纳入其职能（突尼斯议程第72 a）、b）、e）和k）条），虽然网络压制问题没有从文字上体现在这些条款中。遗憾的是，互联网管理论坛成立五年以来局限于一些丰富且有意义的议题，包括互联网的自由问题，但没有启动具体的活动。如果建立一种对过滤器行为进行跟踪、分析和认真评估的监测程序，按照该论坛的职能（似乎很可能延续下去）将是可能的和适宜的[84]（相比而言，每年一次的WSIS论坛是一种没有具体任务的开放式讨论论坛，不太适合承担这项任务）。

联合国教科文组织（UNESCO）宣称，根据其基本法，它是保护信息自由的一个独特国际组织，并且根据WSIS明确的任务负责其中有关“获得

---

83 全球网络倡议，见http://www.globalnetworkinitiative.org。

84 IGF至少已经说明审查问题与其工作职责并不抵触。在目前讨论该论坛工作的延续和扩大其职责问题上，已有建议提出就议论自由议题进行更多对话，更多地关注国际治理的发展和人权问题。见2010年5月7日联合国大会文件A/65/78（E/2010/68）。

信息和知识”以及“互联网的道德问题”的内容。联合国教科文组织在所通过的宣言和建议中要求各成员国和国际组织在自由和不受限制地接入互联网方面做出努力[85]，该组织总干事不断地公开谴责违反信息和新闻自由的行为。因此，为了完成这些任务，启动对话，接着定期对审查做法进行审议是再合理不过的了。

既然我们谈到的是人权和涉及各国义务的两个基本国际公约，那么开展国际行动的主要场所应该是联合国的专门人权组织，也就是2006年成立的人权理事会，它是讨论违反《政治权利和公民权利国际公约》情况的专门机构。具有广泛职能的人权理事会有权制定针对所有联合国会员国政府的正式申诉程序。另外一种可能是将互联网自由和审查内容强制性地纳入国际定期审议机制之中，据此对各国人权记录进行对等审议。无论选择何种程序方式，共同强调这一领域违法人权的问题可能会给那些被怀疑有不合法行为的政府带来积极的压力和必要的辩论。另外，在申诉程序中，还可以充分地了解国际性IT行业在为网络压制提供手段过程中发挥的令人可疑的作用。和人权理事会一样，联合国人权委员会定期的国别审议也可以包括互联网自由的内容。

不管这种纯粹程序上的手段是多么不足，一种可见度很高的要么遵守要么解释的机制最终会带来公众的压力和谴责，它的确可以为国际上提高对这一问题的认识和最终规范数字世界的行为铺平道路。

---

85 “关于大众媒体有利于加强和平和国际共识、促进人权和打击种族主义、种族歧视和煽动战争的基本原则的宣言”，联合国教科文组织，1978年11月28日，见 http://portal.unesco.org/en/ev.php-URL_ID=13176&URL_DO=DO_PRINTPAGE&URL_SECTION=201.html；“有关促进多语言使用和普遍接入网络空间的建议”，联合国教科文组织，2003年10月15日，见 http://portal.unesco.org/ci/en/ev.php-URL_ID=13475&URL_DO=DO_TOPIC&URL_SECTION=201.html（提倡“普遍接入互联网是促进实现世界人权宣言第19条和第27条所确定的人权的工具”）。

5 网络冲突与地缘网络的稳定

5.1 网络冲突

作者：Giancarlo A. Barletta, [86] William A. Barletta, [87]
Vitali N. Tsygichko[88]

引言：挑战的性质

信息战与人类冲突同样古老。其动机几乎没有改变，包括破坏对手的信心，损坏和混淆对手的通信线路，制造有关冲突性质与状况的假象。这些动机都依然存在。在当前21世纪，这个高带宽数字链路不断扩张、电子信息基础设施日益普及的新时期所出现的新情况是：a）能够破坏目标国家的社会结构的信息攻击的破坏性和频率；b）造成广泛的物理性破坏的巨大潜力；c）向非政府组织甚至个人敞开大门的发动持续性信息攻击的扩散能力，让他们现在能够参加不对称战争；和d）一个广泛存在的、长期的低层次冲突的基本状态的发展 — 可称之为网络冷战。新的信息技术的密集出现，大大增强了常规武器和其他军事技术的作战能力。出于这个原因，军方现在认为信息通信技术（ICT）既是武器也是目标，并将网络空间视为类似空中、太空、陆地和海洋的战争空间。[89]

---

86 全球网络风险有限责任公司，华盛顿特区，美国。

87 麻省理工学院，剑桥，马萨诸塞州，美国。

88 俄罗斯科学院系统分析研究所，莫斯科，俄罗斯。

89 例如，“美国空军的使命是为美国的国防及其全球利益提供主权手段，在空中、太空和网络空间中飞行、战斗并赢得胜利”，“空军战略：确保全球稳定和繁荣的主权手段”，2008年3月26日，空军司令办公室。信息作战，电子战和网络战：能力和有关政策问题，美国国会研究服务（CRS）报告，RL31787，2006年9月14日，http://www.stormingmedia.us/98/9868/A986884.html（以下简称“CRS报告”）进一步阐述了美国的观点。

在过去的二十年间，工业化国家已经部署了通过ICT连接的广泛存在的经济、物质和社会等主要资产的网络，以促进其生活水准、经济繁荣、国际影响和实力。同样地，发展中国家将信息技术视作全面参与全球经济的一个经济快车道。工业智能设备（包括传感器和微处理器）比比皆是，带微处理器与无线（或蜂窝）功能的消费设备，如手机、掌上计算机（PDA）和电子记事本也是如此。广泛的通信网络使信息资源得以充分利用，以促进商业，提供服务，监测环境和解决复杂社会问题。所有这些设备都在迅速发展，并具备了与地球上任何地方的其他设备进行沟通的能力。

正如美国一位前军事将领指出的，同样是这些连接主要经济、物质和社会资产的ICT已被军方和准军事行动所采用和改动，带来了军事领域的一场革命，改变了战争的计划、组织和操作方式。这场“革命”包括开展情报、监视和侦察；指挥和控制部队及其活动；优化后勤行动；使用精确导航和采用“智能”武器等方面的能力的发展。很明显，还可以利用“网络”作为媒介，基于网络、通过网络和在网络内部开展军事行动。[90]

信息技术在提高经济增长、促进人权和揭露政府镇压方面所具有的自然潜力为整个社会催生和推动了新的因果关系。在国家统治当局充分享受便利的自上而下的沟通同时，更重要的是，在扩大人权和经济福祉方面，自下而上的和横向的信息细流已扩大成为巨大的河流。现代信息社会中，信息节点（产生和消费信息的地方）的数量与品质和链接的数量与带宽都在不断增加。此外，带有运行状态自主传感器的节点与链接的比例在不断上升。

这种高度非线性的连接同时增加了信息网络的灵活性，骨干节点和链接遭到恶意攻击的风险与后果，以及预测网络故障的后果的难度。ICT的快速发展和随之而来的全球信息社会的发展有可能带来各种消极的地缘政治影响：富裕国家与贫穷国家之间更加迅速的全球两极分化，高度工业化国家与发展中国家之间日益扩大的技术差距，越来越多的经济上被边缘化的

90 John Casciano将军，“威胁因素和武装冲突法”2005年8月（WFS信息安全PMP的文件）。

国家被抛离文明进步的道路——成为滋生政治不稳定和冲突的主要温床。因此，随着信息网络的复杂性的有机演变，信息化战争的潜力也朝着危及越来越大的社会价值的方向发展。

公共取缔的网络攻击与由政府主导的网络战

针对计算机网络、系统和电子数据的攻击促使许多国家颁布了有关网络犯罪的法律。虽然许多工业化国家已有各种网络犯罪的法律，但在定义何种行为构成网络犯罪、侦查和识别网络空间中的犯罪行为以及适用的具体程序规则方面的重大差异严重阻碍了为网络犯罪调查提供协助的国际合作。欧洲委员会（CoE）《网络犯罪公约》是旨在发起全球网络犯罪法律协调的一个多边协议。然而，现实没有达到人们的期望，到2010年中期，自公约开放签署近九年时间里，只有26个国家批准了该公约。国际电联制定了网络犯罪立法工具包，作为一种更灵活的替代途径；它提供了与欧洲委员会公约和工业化国家的网络犯罪法律相协调的示范性的立法语言，可供全球各国用于起草或修订各自的网络犯罪法律。

其他与某些类型的网络活动相关的法律包括那些保护物理系统和通信供应商的设备的法律、禁止经济间谍行为的法规，知识产权法等。总体而言，这些法律的目的在于为取缔针对各种类型的基础设施、系统和数据的各种攻击提供法律依据。

随着更为强大、更具渗透性的信息技术的普及，各种可能性每天都在增长。难怪不管一个国家对其他国家采取何种态度，它自身都有强烈的动机去规范网络空间行为。由于信息技术可以很容易跨越国际边界，犯罪分子再也不用实际进入受害人所在的国家。因此，国家之间的合作需求很大，尤其那些信息资源成为对犯罪行为具有吸引力的目标的国家。事实上，无论是在通过信息网络来推动富有成果的协作方面，还是在防止或至少阻止网络空间中的不当行为方面的合作已成为国际电联之类的国际组织本身的关注。

由于各国政府越来越多地依赖互联网来促进向本国公民提供信息和服务，信息社会成为罪犯、次国家恐怖组织或敌对国家之类的恶意分子的一个诱人的目标。2007年4月爱沙尼亚国家信息基础设施所遭受的攻击[91]既清楚地证实了电子政府存在的可以预知的隐患，也清楚地表明了震慑攻击者因素的缺失。许多专家表示，攻击的技术复杂度超过了以往已知事故。虽然有些专家甚至表示这种攻击需要国家级机构的知识和配合，但一些美国专家否认了这种猜测。不过要注意的是，爱沙尼亚事件既没有提什么政治要求或索要金钱，也没有假定袭击领导者的自认声明，[92]使得该事件不像是没有政治动机的犯罪行为。

另一个更为持久和广泛的网络攻击例子是由GhostNet[93]和Aurora提供的2009年攻击。这些攻击其中的一个目标集中于谷歌服务器，明显是经协

---

91 这次袭击已被国际媒体广泛报道。例如，见Traynor，“俄罗斯被指发动网络战来瘫痪爱沙尼亚”，卫报，2007年5月17日。http://www.guardian.co.uk/world/2007/may/17/topstories3.russia。

92 6月初，一个亲普京的俄罗斯青年团体Nashi声称此次攻击是他们干的。http://www.rferl.org/content/Russian_Groups_Claims_Reopen_Debate_On_Estonian_Cyberattacks_/1564694.html 。该声明真实性尚未得到证实。

93 追踪GhostNet：数字间谍网络调查，信息战跟踪，2009年9月1日，http://www.infowar-monitor.net/2009/09/tracking-ghostnet-investigating-a-cyber-espionage-network/ “调查最终发现了103个国家的超过1 295台感染主机的网络。高达30％的受感染主机被认为是高价值目标，其中包括位于外交部、使馆、国际组织、新闻媒体和非政府组织的计算机。我们对西藏计算机系统进行人工调查，这也是我们调查开始的地方，该系统因多重感染完全中毒，为攻击者提供了前所未有的访问潜在敏感信息的机会…但是，把所有来自中国的恶意软件归为中国政府采取的故意或有针对性的情报搜集行动是错误和误导的。数字可以做出不同的说明。中国目前拥有世界上最大的互联网用户数。年轻网民的绝对数量足以解释中国恶意软件增加的现象。随着越来越多的富有创意的人士接触计算机，预计中国（包括中国公民）将在网络犯罪中占较大比例。”

调的政治与商业间谍行动的一部分，“企图利用电子邮件附件的安全漏洞来偷袭美国主要金融、国防、技术公司和研究机构的网络”。[94]

正如爱沙尼亚事件所表明的，激烈和持久的网络攻击事实上可能会对民间和国家实体构成比单纯犯罪水平更高的直接的实质性破化。这种攻击的特点可能包括：a）对关键设施造成严重的物理损害；b）大范围的伤亡和生命损失；c）金融机构的混乱；和d）关键基础设施的功能中断。这种攻击若经过协调或长时间持续，可能会使其后果更为严重。在这种情况下，无论是否了解攻击者的身份或动机，名族国家可能会将大规模网络攻击视为[95]一种恐怖主义或其作用等于武装袭击的行为，理应予以特殊考虑或采取特殊应对措施。

至少，信息社会大规模破坏所表现出的潜在后果要求建立跨国界相互合作的文化。在爱沙尼亚的例子中，第一波的政府网站破坏启动了响应预案，预计到如网上银行之类的金融服务将遭受一波袭击。事实上，就在几天之内，“私营部门银行和网上媒体也受到大量有针对性的袭击，并影响到了爱沙尼亚网络基础设施的其余部分的功能。”[96] 与此同时，全球互联网服务供应商合作采取应对措施，加大对从特定IP地址群发出的流量的拦截，以阻断到爱沙尼亚银行系统的国际流量。值得注意的是，处理网络攻击造成的后果所需的网络资源要大大超过发动攻击所用的资源。

网络空间中攻防之间显著的不对称关系并没有被忽视。虽然不存在如此大规模的攻击，美国和其他一些民族国家（俄罗斯、中国、印度、巴基斯坦、伊朗）的军方和情报机构已开展“侦察和探测，以确定潜在对手的

---

94 Ariana Eunjung Cha 和Ellen Nakashima，专家表示“谷歌中国网络攻击是大规模间谍网络攻击的一部分”，华盛顿邮报，2010年1月14日 http://www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html。

95 例如，2009年，美国前国家情报总监Mike McConnell将网络武器归类为大规模杀伤性武器（或潜在的大规模杀伤性武器），CRS报告第3页。

96 “ENISA对爱沙尼亚大规模网络攻击的评论”，ENISA新闻发布，2007年5月24日，http://www.enisa.europa.eu/act/cert/contact/press-releases/enisa-commenting-on-massive-cyber-attacks-in-estonia。

数字网络中的可利用的弱点。”这些国家的决策者的行为就好像当前已处在网络战时代。事实上，正是美国这样的国家才具有这样的不对称力量和能力，来对没有这种能力的国家发起或支持网络攻击（特别是隐蔽的行动）。此外，这些国家和其他一些国家的当局清楚地知道，攻防之间的明显不对称与几乎是匿名的坚决攻击者相结合，提高了直接或间接地利用小规模的网络雇佣军“部队”或“非法作战部队”的可能性，从而为国家当局提供了绝佳的推诿否认的借口。

在实践中，一次特定的攻击的可能引起的伤害差别很大，这取决于社会的预警程度和受攻击基础设施内置的安全性能。从政治或军事决策者的角度来看，“打击任何形式的网络攻击的关键所在是迅速判断出攻击类型和敌人，然后做出适当反应。目前，追踪计算机入侵是一项执法职能……传统上负责作战的军方被禁止在国内执行该项任务……因此国内执法部门在国家安全和国防方面要起到关键作用。”[97] 民族国家军事和执法机构均需要强大的数字取证工具，使用这些工具的合理的法律结构，保护证据完整的可信手段，和对违法者具有真正威慑价值的处罚措施。由于这些工具有着强烈的“双重用途”的潜力，那些具有最强大最灵活的防御和侦查能力的国家就更有理由拥有相当强的进攻和网络间谍活动能力。虽然双重用途的潜力和攻防的不对称性在物理武器装备领域也同样存在，但由于威慑作用和攻击来源归属相对容易确定，动力攻击的可能性受到了抑制（虽然没有被消除）。

信息与动力冲突的相互作用

新的信息技术的密集出现加强和提高了常规军备和军事技术的作战能力。信息技术给军事侦察和通信带来质的变化。他们大大提高了处理海量

97 Bonnie N. Adkins，“网络冲突：从黑客到信息战：什么是执法部门的职责？”空军指挥和参谋学院，Maxwell空军基地，AU/ACSC/003/2001-04，2001年4月，http://stinet.dtic.mil/oai/oai?&verb=getRecord&metadataPrefix=html&identifier=ADA406949。

数据矩阵和进行复杂操作决策的速度，从而有可能实现向从战略到战术各个层面上用全新方式来控制部队与装备的转变。

新的信息技术大幅增加了电子战设施的作战能力，创造了新型武器，特别是以切断其计算机网络的方式破坏敌方军事和民用信息基础设施的信息武器。

对于军队，信息和技术革命大幅增加了部队的作战能力，不仅改变了不同规模的战争的形式和方法，而且还改变了军事斗争和冲突升级的传统模式。据美国专家指出，有选择地将信息武器对准敌方关键军事和民用信息基础设施可以在当事方开始动力作战行动之前终止冲突，因为信息攻击的升级将导致灾难。拥有信息武器提供了相对于缺乏这种武器国家的压倒性的优势。如果不是今天那么就在不久的将来，信息和权力对抗的政治变数的重要性将超过核武器。相反地，所有国家，特别是高度发达国家，很容易受信息武器攻击。信息武器，就同核武器一样，既可以作为一种政治施压因素，同时也可用于威慑。

信息战不是计算机游戏的虚拟现实，而是实实在在的争取军事或政治冲突胜利的工具。毫无疑问，信息武器正成为一个国家军事潜力的重要组成部分，许多国家，特别是美国和中国，一直在积极地为发动信息战做准备。

信息武器的性质

制定信息安全模式的概念性问题是“信息武器”的界定和识别。信息武器的特点是什么？何种水平（如果有的话）的网络冲突应作为武装冲突来对待？针对这些问题尚无任何国际共识，这阻碍了就全球信息安全开展建设性的谈判。对“信息武器”的概念进行定义的一个方法是基于它们影

响军事和民用信息基础设施的能力。[98] 这种方法的缺点是，任何类型的武器，包括常规武器，如果具有损害信息基础设施组成部分的能力，就可以被称为信息武器。例如，哪个设备导致城市经济控制系统无法运行是否重要——是程序代码、强烈电子脉冲还是常规爆炸物的直接冲击？第二种方法可能是把信息武器定义为利用ICT的所有破坏手段。

处理网络冲突问题要避免采取会将和平时期经常发生的活动也纳入网络冲突的定义，从而降低战争的门槛。信息武器的特点是什么？何种水平的网络冲突应作为武装冲突来对待？把对人类生命或社会自由没有明确威胁的冲突作为“武装冲突”来对待对于国际稳定是不明智和危险的。此外，实际上由于几乎所有复杂的武器系统都使用ICT，将信息武器从全部的武器装备中单列出来，即便不是不可能，也是非常困难的。由于信息战争是人类冲突历史上的长期现象，存在几个层面的概念复杂性，要给出清晰的定义尤其困难。例如，故意提供错误信息应该如何归类？间谍活动，或拦截信息流动呢？如果此类活动在动力战争期间进行，人们对它们的观点会受到严重影响。

信息武器的重要操作特点是：1）它们的成本相对较低，容易获取；2）隐蔽开发、积累和引进的可能性，以及3）其天生的跨界性和影响的匿名性。这些特点导致了信息武器的失控扩散，使其被有侵略野心的政权获取成为一个全球性问题。由此产生的对国际和平与稳定的威胁要求国际社会采取实际步骤消除网络威胁，以控制对国家和全球信息基础设施的威胁。作为现代社会基础设施的一部分，ICT是一个国家打击敌人的多种手段的一部分。

许多国家正在采取措施来对抗信息安全的威胁；但更加强硬措施的效率却因威胁的跨国性质和违法者匿名而降低。在这种情况下，如果各国试

98 例如，“任何如按其既定用途来使用，可能会损害到位于计算机或信息处理系统信息中的数据、程序或信息的完整性或可用性的能力、设备或能力与技术的结合。” Graham H. Todd，“网络空间的武装攻击：非对称定义的威慑性不对称作战，”空军法律评论，第64卷，第65 – 102页，2009年，http://lawlib.wlu.edu/CLJC/index.aspx?mainid=418&issuedate=2010-03-23&homepage=no.。

图凭借一己之力反击威胁，那没有哪个国家是安全的。只有靠建立一个国际信息安全制度和参与者的共同努力，才能阻止信息武器扩散和减少信息战、信息恐怖主义和网络犯罪的威胁。

至少专门为破坏信息基础设施而设计的软件（各种病毒、书签等）可以毫无疑问地归类为信息武器。许多使用ICT的复杂的武装斗争手段是多功能的，例如，不仅设计用于破坏信息基础设施，还用于其他作战任务。拥有这种基于大规模ICT应用的尖端武器系统、侦察手段、通信、导航和控制的国家具有决定性的军事优势；因此，他们是否会加入将限制其战略优势的协议是值得怀疑的。

因此，禁止或限制生产、扩散和应用信息武器的问题很可能只限于专为打击信息基础设施组成部分而设计的单一用途武器，例如，基于程序代码的武器，即各种病毒及其传播工具。不幸的是，绝大多数可用于军事、恐怖和犯罪目的的现代ICT是民用工业制造的，因此很难控制其发展和扩散。

网络冲突和信息战手段所构成的威胁对所有人来说都是真实存在的，特别是在所有重要活动均由复杂信息基础设施决定的发达国家。[99] 只有国际社会为保护重要国家信息基础设施而共同努力，才很可能缓解恶意使用信息技术的威胁。就此类信息系统达成共识能够使得更有效的威慑和更有效的保护措施发挥作用，包括只有当针对他们的信息操作会产生严重的、不可接受的直接影响时，才有权采取报复行动。即便这种情况下也必须极为谨慎。并不是任何侵略性的信息行为都可以成为发动动力战争的理由；赋予各国政府自行决定采取行动的理由将是不明智的。

---

99 信息战和网络战：能力和有关政策问题一文就美国军方决定不对伊拉克金融系统网络发动攻击进行了讨论，国会研究服务，RL31787，2004年7月19日，第5-6页，http://www.fas.org/irp/crs/RL31787.pdf。这CRS报告还列举了美国军方处理网络战的框架，并解释了网络战在军方长期运行战略中地位和信息战项目。

限制网络冲突

信息技术进攻与防守间潜在的严重不对称性导致了最终用户能够对社会重要信息基础设施发动强度几乎与国家相当的个人“网络战”的情况。因此，防止和限制国家之间的网络冲突的法律和政治制度事实上将会与为防止和处理网络恐怖主义和网络犯罪的法律和程序框架联系起来。

在信息社会的范畴内，如果可以建立一个合理的国际统一刑事法则网络，那么通过民事和刑事处罚进行威慑的概念在犯罪或“黑客行为”[100]的层面上是可操作的。可惜在国家发动网络攻击的层面，冷战时期建立的威慑的概念并无多大价值，因为类似的反击对国际社会和物理连接造成的损害可能会达到令第三方和反击者同样无法接受的水平。从计算机病毒之类的恶意软件的迅速蔓延可以看出网络空间中的这种连带损害会是世界性的。对于界于两者之间的网络恐怖主义的情况，美国最近在其“反恐战争”中对“非法作战人员”的行动表明，威慑模式在民事和刑事处罚层面同样是失败的。

虽然威慑的困难可能会鼓励对抵御网络攻击的完美防御技术的追求，每一种其他武器装备的历史告诫我们，归根结底，社会政治问题最终必须同样在社会政治层面上解决。在政治方面，国际网络冲突的严重潜在后果需要立即引起重视。该技术的双重用途性质排除了核技术使用的那种国际控制机制。目前可以期盼的（和努力的方向）是建立跨国法律框架，通过国际谈判达成的具有约束力的系列架构协议来规定网络冲突的规则和处罚。这些规则必须明确签字国在控制在其境内实际运营的非政府组织或网络方面的义务。

虽然网络恐怖或网络间谍攻击的司法管辖一般可归入一般民法和刑法以及相关司法考虑，但是它们某些特征可能要求有专门的法律，由此导致特别的司法考虑。这些特征可能包括：1）带有政治色彩的大范围伤害；

---

100 黑客行为是指编写或使用计算机代码（黑客）来攻击目标的ICT网络，以实现推动政治意识形态或社会目标的目的。黑客行为经常抗议和捍卫公民权利来为他们的行为做辩护。有关示例，见http://thehacktivist.com/hacktivism.php。

2）识别、拘捕和起诉罪犯的困难加大，以及3）存在违反普遍接受的刑法和武装冲突法的，以制造社会动乱为目的的强烈政治动机。网络恐怖主义需要特别对待还有另外一个理由。“当恐怖主义在一个能够长期集体组织行动，参与策划复杂的行动，游离于正常的生活之外，或有能力胁迫正常社会容忍其存在的团体中出现时，做出特殊的反应通常是合理的。”[101] 无论出于恐怖主义还是军事目的，旷日持久的网络冲突可能需要或刺激国际协调行动来限制或控制武力的使用。

一个有效的管制制度还必须纳入对非国家攻击者采取的行动，如果这些攻击者确实能够确认的话。在恐怖主义行动来自于受攻击国家内部的情况下，对攻击者的行动可以在包括反恐怖主义法规在内的现有国家刑法框架下处理。如果攻击是来自合作或中立国家，有多种选择：1）引渡到被攻击的国家；2）在攻击发起的中立国家内起诉，或3）引渡到具备通用司法制度和普遍接受的正当程序标准的第三方。采用哪种方案是在发起国家的参与、正义的体现和全球打击恐怖主义手段之间进行平衡的问题。

发起攻击的无赖国家或不合作国家不太可能为合作调查攻击、拘捕和起诉违法者，或酌情引渡提供正常渠道。问题的底线是，攻击者是否会在遭受袭击国家、中立的第三方国家或国际刑事法院被起诉。然后这些情况自然地转变成武力干预或国际制裁的问题。这些问题与采取动力手段的恐怖主义的情况类似。遭受攻击的国家可以选择的方案有：

1. 针对该国采取报复性措施；
2. 非法进入和逮捕犯罪嫌疑人[102]；
3. 通过第三方的中间国家的参与，适当尊重主权。

如果设想通过类似于有关动力战争的《日内瓦公约》的机制来禁止网络空间中的某些行动，人们可能会想到由国际团体参与的通用司法制度的

---

101 Clive Walker，“网络恐怖主义：法律原则和英国法律”，宾夕法尼亚州立大学法律评论，第110卷，2006年，第625-65页，http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1109113#%23。

102 根据美国法律将嫌犯带入司法管辖领土不构成对司法起诉的辩护。

情况。这种可能性提出了有关互联网一般法律（及其废止）问题的滑坡论证。请注意，欧洲委员会《网络犯罪公约》没有确定，因此也没有授权任何跨境计算机网络证据搜索的依据，即便对此有强烈的诉求。

结束语

既定的事实是：（1）多数国家的企业、政府和公用事业高度依赖于计算机和互联网；（2）虽然互联网在连接方面本身是较强健的，但连接到互联网的计算机更容易受到攻击；（3）获得一定强度的攻击能力目前仅需要相对较低水平的投资；（4）很难最终确定攻击的来源。

关于战争法律，大多数国家可能会同意一些基本原则，以作为和谐的网络空间秩序的基础。

1. 针对重要基础设施的网络攻击不是合法的攻击武器，即使是在动力战争期间。（类似于生化武器。）
2. 普遍的受政府资助的互联网间谍活动使得确定有组织犯罪、次国家组织和黑客的侵入与权利侵犯更加困难，干扰了根据计算机犯罪法律对这些组织提起刑事检控。
3. 政府开展低层次的计算机间谍活动可以被容忍，但不允许进行破坏。低层次的国家“竞争”可以刺激技术进步。此外，每个国家都有兴趣了解外国军事系统的安全性是否能够抵御潜在的恶意分子。
4. 政府对外国私人公司从事间谍活动对现实世界的影响尚不清楚，但可能很小。然而，它会在公众内部引起不良的民族主义热情，对业界发出坏的信号，如果这是代表本国的私营企业而进行的，容易构成非竞争性的经济势力。
5. 由于确定攻击源和是否为政府资助的是非常困难的，破坏性的非政府组织可能能够挑起国家冲突。

由于正式协议可能无法核查，国际对话的初步目标可能是建立执行公平游戏规则所需的证据规则。鉴此，有关经济利益或根本政治动态的断言

似乎意味着冷战式互动，将削弱国际协议[103]力求达到的目标。更重要的是，如果这是事实，没有联合国协议能够阻止这一进程。

在推进缓解网络冲突目标时，对以下领域进一步深入调查可为国际场合进行的政策讨论提供信息：

1. 理论上的计算机安全进攻/防守动态，
2. 作为投资回报的计算机安全进攻/防守动态发展，
3. 强健的安全系统上对操作（计算机处理，数据存储，系统管理，人机互动时间）的拖累，
4. 刑事措施和对跨境犯罪的威慑力，
5. 计算机间谍对公共和私营部门的影响。

103 见本书中Henning Wegener 所著的“网络和平的概念”一文。

5.2 呼吁地缘网络的稳定

作者：Jody R. Westby

不能让网络犯罪的增长速度再继续下去了。不法分子利用僵尸网络经常性地窃取机密和专有信息，对政府和商业系统进行分布式的拒绝服务攻击。据McAfee的《2009年不安全的经济：保护关键信息报告》估计，2008年受访者损失了总价值达46亿美元的知识产权，花费了约6亿美元用于弥补数据泄露造成的损失。基于这些数据，McAfee预测，2008年全世界的公司的损失超过1万亿美元。个人用户需要不断更新操作软件和病毒防护程序，即便如此，他们的许多系统还是在攻击中被感染或被利用。

各国都认识到他们的政府系统和商业系统是宝贵的，他们的国家和经济安全正受到威胁。因此，他们已开始制定网络战战略，建立具有网络攻击和防御能力的司令部。虽然这些行动是适当和可以预料的，但在有关网络和平对话方面存在明显真空，比起有关维持可接受水平的地缘网络稳定性的对话来少很多。如引言所述，笔者将“地缘网络”定义为互联网与一个国家的地理、人口、经济和政治及其外交政策之间的关系。“地缘网络稳定性”是指所有国家利用互联网来使其经济、政治和人口受益，同时避免可能会造成不必要的痛苦和破坏的活动的能力。[104]

在某种程度上，国家不愿参与有关什么是保护核心社会功能和防止网络攻击造成不必要的痛苦与破坏所需的“最低限度的通信”的讨论，可能是考虑到在当前国际法律框架下如何处理这样的议题存在普遍的不确定性。

---

104 在ANSER国土安全研究所会议上首次提出，“国土安全2005年：规划未来的道路”，马里兰大学，Jody Westby的演讲，“地缘网络的稳定和安全的转移”，5月6-7日，2002年。

武装冲突法

纵观近代历史，武装冲突国际法（LOAC）曾根据战争暴行和战争作战的新方法进行修订。目前迫切需要再次这样做使之与网络能力相适应，因为网络战行为很可能要么违反现有武装冲突法的许多规定，要么超出了所有这些法律的范围。

关于武装冲突的基本法律框架是广泛的，大部分是在上世纪的进程中制定的。有关武装冲突的主要文件包括：

- 《联合国宪章》[105]
- 《北约条约》[106]
- 1949年《日内瓦公约》[107]
- 1949年8月12日《日内瓦公约》的日内瓦附加议定书，有关国际性武装冲突受难者的保护（第一议定书）[108]
- 《海牙公约》（1899年和1907年）[109]
- 《禁止或限制使用某些可被认为具有过分伤害力或滥杀滥伤作用的常规武器的公约》。[110]

---

105 联合国宪章，http://www.un.org/en/documents/charter/index.shtml。

106 北约条约，http://www.nato.int/cps/en/natolive/official_texts_17120.htm。

107 1949年日内瓦公约，http://www.icrc.org/web/eng/siteeng0.nsf/html/genevaconventions。

108 1949年8月12日日内瓦公约的有关保护国际武装冲突受害者的附加议定书（第一议定书），1977年6月8日，http://www.icrc.org/ihl.nsf/7c4d08d9b287a42141256739003e636b/f6c8b9fee14a77fdc125641e0052b079（“下简称第一议定书”）。

109 关于陆地战争的法规与惯例的公约（海牙第二公约），1899年7月29日，http://avalon.law.yale.edu/19th_century/hague02.asp；陆地战争的法规与惯例（海牙第四公约）10月18日，1907年http://avalon.law.yale.edu/20th_century/hague04.asp。

这些文件的基本前提可以简化。武装冲突法对武装敌对行为进行了规范，军队必须在这些法律下计划和执行其运作。它们适用于军事行动和相关活动，旨在防止战争期间的不必要痛苦和破坏。一些特别条款旨在保护平民、战俘、伤病员和失事船舶的船员。

如何开展军事行动

管理如何开展军事行动有三个基本原则：必要性、区分和相称性。

必要性：必要性原则限制作战部队只能开展实现其正当军事目标的必要行动。军事设施、装备和部队可以作为目标，以使敌人的部分或全部屈服。

区分：区分的原则要求军队要区分合法目标与如平民、平民财产和伤员之类的非法目标。平民目标必须在最大可能程度上与军事目标进行区分。对军事和民用目标/平民同时进行打击被认为是不加区分的攻击。

相称性：相称性原则禁止过度地使用完成军事目标所需的力量。该原则对攻击取得的军事优势与造成的危害进行比较，要求在预期的直接军事优势和预期的平民伤亡或破坏之间进行平衡。

谁能够从事武装冲突

只有**合法的战斗人员**可以从事武装冲突。合法的战斗人员是由政府部门授权从事敌对行动的人。他们可以是非常规部队，但必须由对其下属负责的人进行指挥，具有鲜明的标志使他们能够从远距离辨认（如制服或彩色），公开携带武器，并根据武装冲突法开展行动。

非法战斗人员是指那些未经政府当局或国际法授权直接参加敌对行动的人。攻击部队的平民、海盗和恐怖分子是非法战斗人员的例子。

---

110 关于禁止或限制使用某些可被认为具有过分伤害力或滥杀滥伤作用的常规武器的公约，2003年11月28日，http://www.icrc.org/web/eng/siteeng0.nsf/html/p0811（以下简称“过分伤害力武器公约”）。

非战斗人员是指政府机构未授权从事敌对行动但参与其中的人。这组人员包括牧师、军队随行文职人员和医务人员。非战斗人员可能不是直接攻击的对象，但他们可能会因直接攻击而丧生。

如果一个战斗人员身份不明，《日内瓦公约》在该名人员的身份得到确定起适用。

何为军事目标

军事目标是指通过其性质、地点、目的或用途为敌方的军事能力做出有效贡献的目标，其全部或部分破坏或使其无效可改善攻击时的合法军事目的。

受保护目标是指受《日内瓦公约》保护的目标，如医院、伤病员的运输、宗教或文化场所和安全区。任何这些目标如果被用于军事目的，则可能受到攻击。例如，如果军方利用一个教堂作为地基的运作基地，它就成为一个合法的军事目标。[111]

在网络情况下，由这些原则形成了一些悬而未决的问题：

- 什么构成网络武装冲突行为？
- 关键基础设施能否作为目标？
- 如果关键基础设施支撑着《日内瓦公约》所保护的目标，那这些网络还可以成为目标么？
- 要达到军事目的是否需要攻击关键基础设施？
- 敌对行动参与者如何能够区分军事目标和受保护目标？
- 对关键基础设施的破坏是否与军事目的成比例？

---

111 见Thomas C. Wingfield，信息冲突法：网络空间中的国家安全法，神盾研究公司，Falls Church，弗吉尼亚州，2002年；武装冲突法：基本知识，国际红十字委员会，2002年6月，http://www.icrc.org。

- 网络空间的过度力量是什么？
- 网络战士如何分辨？
- 如何判定第三方是否为某个国家效力？

按照现有法律，这些问题的答案都不明确。比如，是否因为美国政府90%的通信需要利用商业网络，包括互联网、电话、蜂窝和卫星，美国私营部门的通信网络就成为合法的军事目标和军用必需品？[112] 拥有这些网络的公司和股东一定会反驳这样的推理。那么完全依赖于这些网络运营的医院呢？他们可能会认为这样的攻击属于攻击受保护目标。

如果武装冲突法允许使用非常规部队，政府能否雇用僵尸网络专家作为合法的战斗人员，在网络冲突中利用他们的僵尸网络？非常规部队可以被授权参加敌对行动，但僵尸网络无法被识别，他们的危害也是不可见的。

当然，僵尸网络中的僵尸不带任何标志或区分的记号。甚至可能无法追查到僵尸，因为他们通过网页、点对点网络、恶意链接、社交网站和垃圾邮件来传播他们的恶意软件。在某个国家的命令下发起的网络攻击中充当僵尸的个人计算机可能属于一个无辜的平民，他本人并不知道自己的计算机已经被感染。如果被发现，这些僵尸网络专家能否作为战犯被审判？那些计算机的所有者呢？

海牙第五和第十三公约规定了关于陆地和海上战争的中立国家的权利和义务，但那些条款在网络空间中就失效了。一个国家可能无法跨越一个中立国家的领土来移动部队或车队，或在一个中立国家的领海进行任何敌对行为，那么透过中立国家的网络呢？一个国家是否需要得到中立国家的允许来通过其网络传送网络攻击？在分组交换情况下，一个国家如何知道将使用什么网络？一个国家能否使用僵尸网络作为非常规部队，如果这涉及位于其他中立国家的计算机？

---

112 美国政府信息系统的内部威胁，国家安全通信与信息系统安全委员会，NSTISSAM INFOSEC/1-99，www.cnss.gov/Assets/pdf/nstissam_infosec_1-99.pdf。

《联合国宪章》、《日内瓦公约》、《海牙公约》和《北约条约》无法处理网络冲突。《联合国宪章》和《北约条约》均使用“领土完整”、“武力的使用”、“空中、陆地或海上部队的行动”和“武装攻击”等术语，不适用于网络的情况，似乎将其排除在国际法的范围之外。爱沙尼亚和格鲁吉亚的冲突形象地说明了网络冲突的后果和由法治的不确定性造成的应对工作的混乱。[113]

稳定地缘网络的情况

上文只讨论了关于网络冲突法律不确定性的几个方面。重新审议武装冲突法揭示了对这些文件进行更新以使其适应如海军武器和飞机之类的新技术的历史性意愿。[114] 因此，这些法律文件也可以为适应网络冲突而修正。

然而，第一个关键问题是何种水平的活动应该被允许？笔者认为，在网络冲突的情况下，应采用四个原则：

1. 一定量的关键基础设施必须得到保护，以防止不必要的破坏、损害和痛苦，并确保最低限度的基本通信。

   受保护的关键基础设施将包括那些支撑诸如医院和医疗设施、康复中心、金融系统、生命支持系统和关键医疗设备、供应链、运输、新闻报道、教育设施、教堂和宗教中心、紧急响应和执法机构的基

---

113 有关爱沙尼亚和格鲁吉亚的冲突和响应及法律问题的更为全面的讨论，见Jody R. Westby，“通往网络稳定的道路”，网络空间的权利和义务：平衡对安全和自由的需求，东西方研究所和世界科学家联合会2010年第1页，http://www.ewi.info/rights-and-responsiblities-cyberspace-balancing-need-security-and-liberty。

114 例如见“战争时期的平民和人口保护”，摘自“日内瓦公约及其附加议定书的基本原则”，国际红十字委员会，1988年12月31日，http://www.icrc.org/web/eng/siteeng0.nsf/html/57JMJV （以下简称“保护平民”）（“空中作战的迅猛发展已使我们有必要进一步发展现行武装冲突法，使之更为具体化。这是日内瓦第四公约或第一附加议定书的主题”）；增加了日内瓦第二公约，以适应海军在战争中的使用和有关对海上武装部队的伤员、病人和遇难船员的处理。

础设施。上述清单并不全面，而是为了给出这种支撑系统的一些例子，包括为儿童、体弱者与伤员、老人在内的无辜平民提供支撑的系统。利益攸关方的参与可以帮助外交官确定关键基础设施的神圣界限。

理由：现行武装冲突法支持这一概念。正如《日内瓦公约》及其附加议定书的基本条款所说明的：

> 在任何冲突中，冲突各方选择作战方法或手段的权利并非是无限制的。要遵循两个基本原则。第一是禁止使用任何具有造成不必要伤害的性质的武器、射弹、装备和作战方法。第二，为确保对平民和平民财产的尊重和保护，冲突各方有义务时刻区分平民和战斗人员，以及区分平民财产和军事目标，并将他们的行动只对准军事目标。[115]

关键基础设施系统的破坏和功能丧失所带来的危害和损失是不必要的，会导致武装冲突法意图防止的极端痛苦和苦难。此外，由于这些网络为大量人口提供服务，此类攻击造成的危害将是广泛的、与军事优势不成比例的。

日内瓦第四公约的许多款项支持该建议原则。该公约专门处理平民保护，特别是对伤病员、体弱者和孕妇的保护（第16条）。在敌对行动期间，任何一方均可提出在冲突地区设立中立区，以保护伤病战斗人员和非战斗人员，和居住在该区域的但即不参与敌对行动也不从事军事性质的工作的平民（第15条）。负责照顾伤病员、体弱者和孕妇的平民医院在任何情况下都不能成为攻击对象（第18条）。应为15岁以下的孤儿或与父母分离儿童的生活保证、宗教和教育提供便利（第24条）。禁止对任何属于个人或集体私人、国家或公共部门、社会或合作组织的不动产或个人财产进行破坏（第53条）。

---

115 “战争时期的平民和人口保护”，摘自“日内瓦公约及其附加议定书的基本原则”，国际红十字委员会，1988年12月31日，http://www.icrc.org/web/eng/siteeng0.nsf/html/57JMJV。

《日内瓦公约》第一议定书对第四公约进行了补充，将平民保护扩展在到战时。第一议定书第48-第59条尤为适用。平民是指不是武装部队成员的任何人（第50条）。平民应享受免于军事行动所产生的危险的一般保护，不得成为攻击对象或遭受旨在散布恐怖或滥杀滥伤，不针对特定军事目标的攻击（预计会造成 平民附带伤亡或破坏民用物品，超过其相关军事目的的攻击行为属于滥杀滥伤）（第51条）。民用目标不应成为攻击或报复的对象，在有疑问时，应先被假定为民用目标（第52条）。敌对行为不得侵犯历史古迹、艺术作品或礼拜场所（第53条）。禁止对平民人口赖以生存的目标（如食物、农业区、农作物、牲畜、饮水装置及供水和灌溉工程）进行攻击（第54条）。大坝、堤防和核设施之类含有危险因素的工程或设施不得受到攻击，即便它们是合法的军事目标，如果它会导致“危险的力量的释放，由此造成平民人口中的严重损失”（第56条）。必须时刻注意避免损害平民（第57条）。攻击的计划者应采取一切预防措施，以验证攻击的对象不是平民或民用物品或受到特殊保护，并应采取一切可行的预防措施以避免和尽量减少平民生命附带损失（第57条）。禁止攻击不设防的地点（在该地区没有任何军事行动或人员）（第59条）。

此外，武装冲突法含有很多多年以来陆续增加的以禁止使用具有过分伤害力或滥杀滥伤作用的技术的条款。早在1899年，《海牙公约》通过了禁止使用气球“或其他新的类似方法”投掷投射物和爆炸物的宣言[116]，禁止使用专用于散布窒息性或有毒气体的投射物[117]，以及使用膨胀或变形子弹。[118] 2001年，通过了《禁止或限制使用某些可被认为具有过分伤害力或滥杀滥伤作用的常规武器公约》，禁止了一大批特别危险和有害的武器，包括上面提到的早在

116 禁止从气球上或其他新的类似方法投掷投射物和爆炸物的宣言（海牙第四公约），1899年7月29日，http://avalon.law.yale.edu/19th_century/hague994.asp。

117 禁止使用散发窒息气体或有毒气体的投射物的宣言，1899年海牙会议，1899年7月29日，http://avalon.law.yale.edu/19th_century/dec99-03.asp。

118 禁止使用易于在人体中扩张或扁平化的子弹的宣言，海牙会议，1899年7月29日，http://avalon.law.yale.edu/19th_century/dec99-03.asp。

1899年间的武器，以及地雷、诱杀装置、燃烧武器、激光致盲武器和战争遗留爆炸物。[119]或许可以修正该公约，将针对关键基础设施的网络攻击也纳入其中。

2. 法律应禁止使用僵尸网络和其他非常规网络部队。

理由：对于受害者，在攻击开始时，这些战斗人员与其他任何攻击者难以区分；受害者不知道攻击他们系统的人是一名内部人员、一名孤独的黑客或恶意分子、一个复杂的有组织犯罪团体、一名恐怖分子，或一个国家。即便对于经验丰富的调查人员和研究人员，对网络犯罪活动进行跟踪和追踪也是困难的，有时无法确定其源头。此外，根本无法区分第三方网络士兵，因为他们不可能身穿特殊标志，他们肯定无法从远处进行识别。因此，非常规网络部队违反了武装冲突的基本原则之一。

3. 各国必须尊重其他国家的中立，不得通过其关键基础设施来传播任何类型的攻击。（海牙第五和第十三公约）。

这与《海牙公约》限制通过中立领土或水域运送部队或运输物资或军需品。许多关键基础设施如电网，可以通过使系统过载而被摧毁。因此，允许各国在许多其他国家不知情的情况下通过其传输网络进行网络攻击，与武装冲突法的历史和意图是不一致的。这项建议原则要求国家在发动网络攻击前获得其他国家的许可，从而也对发动网络冲突起到威慑的作用。

4. 各国必须为他国对网络犯罪活动的调查提供协助。

互联网服务提供商（ISP）和其他各国政府在网络犯罪活动调查中的合作，对于确保一些地缘网络稳定性措施至关重要。虽然要求中立国家来协助调查似乎违反规定，即使在战争时期也如此，所有的网络攻击在初期看起来都是类似的。只有通过调查，受害人才能进一步了解谁可能是攻击者。作为一项基本原则，希望连接到互联网

119 关于禁止使用具有过分伤害力武器的公约。

的各国应当有义务确保他们及其境内的供应商，为网络犯罪调查提供协助。如果允许国家在保持中立的外衣下拒绝提供此类援助，所有的网络犯罪分子将可以尽情地对相关敌对国家进行破坏。从反向意义上说，通过拒绝提供协助，中立国家实际上不是在帮助犯罪分子，就是在怂恿发起攻击的国家。在网络攻击的情况下，只有通过协助，一个国家才能真正保持中立。

实现地缘网络的稳定

互联网已经创造了一个不认可传统边界，基本上不在政府的操控之下的网络星球。它构成了一种新形式的武器，给平民，特别是那些年幼、年老、患病、体弱或身残的人，带来了前所未有的危险。它也触犯武装冲突法，因为网络冲突的目标更有可能是民用的而军用的，更有可能影响平民人口而非军事部队。在大多数国家中，关键基础设施是由私营部门拥有和经营。因此，对关键基础设施的攻击将等同于对平民及其维持生活和生计的那个网络的攻击。对武装冲突法进行修订，以适应这一新的威胁的迫切需求不容忽视，因为这个法律框架的缺失很容易被理解成是对攻击的法律认可。

一些法律和安全专家呼吁为网络空间制定一部庄严的法律或条约。这完全是无稽之谈。在海军、空军和其他技术的发展进程中，武装冲突法已经不断调整并始终是一个具有一致性而又不断演进的法律体系。此外，也有务实的考虑。条约是有问题的，它们在起草阶段需要冗长的多边讨论，之后是开放签署阶段。然后签署国必须批准和执行该条约，将其纳入国内法律。通常，有些签署国在条约生效之前必须先批准条约，即便如此，它也只对那些已批准和执行的国家有效。所有这一切都需要时间，将使得无赖分子和网络犯罪分子有机可乘。

然而，如《联合国宪章》、《北约条约》、《日内瓦公约》和《海牙公约》之类的现有法律文件均能够被修正，而且它们还拥有已被批准并纳入各国国内法律实施的优势。

在网络空间中，刻不容缓，解决方案明显应是那个最为便捷的方案。各国必须团结起来，在各利益攸关方的参与下，提出对现有的国际武装法的以下修正：

1. 《联合国宪章》应予修正，以适应网络冲突，澄清“领土完整”包括关键基础设施和网络的可用性、完整性和保密性。具体来说，第42条应予修正，让安全理事会能够通过网络手段采取行动。
2. 北约宪章应予修正，允许按第5条进行集体防御。第6条第（1）段中“武装袭击”的定义应扩大，应超越“领土”和“军队、船只和飞机”，以涵盖网络攻击。
3. 《海牙公约》应予修正，禁止使用非常规部队在网络作战，并禁止通过中立国家的网络传递网络攻击。
4. 《日内瓦公约》应予修正，禁止对关键基础设施进行攻击，损害最低限度的基本通信和危及平民。

有一个领域需要新的协议。各国必须分别同意合作，协助对被认为是通过其网络传递的网络犯罪行为进行调查。按照国际法，该协议的非签署国将没有追索权，如果来自其国家的通信被其他国家所阻断的话。

上述内容将使各民族国家和人民信任信息通信技术，并继续将其融入他们的生活和社会，而不必担心他们会成为网络冲突的目标。它也将开启各国之间的建设性对话，他们第一次带着共同的立场会聚到谈判桌前。

6 网络和平

网络和平的概念

作者：**Henning Wegener**

本书主题是网络和平，其内涵不同于网络战、网络恐怖和网络犯罪等负面现象。在战争与和平这对孪生兄弟中，选择正面结果意味着关注重点的深度和广度的重要变化，这有助于引导向受益于信息社会并发挥其积极作用的方向发展，并起到树立标杆的作用，通过这一标杆可以更深地理解网络战和相关术语及祸患的负面含义，同时进一步促进全球网络安全文化运动的积极开展。

这种旨在通过观念转变推动网络战非法化的尝试，首先已充分认识到了当前数字基础设施具有的无处不在特性以及不可避免用于仇恨、非和平用途的特点。那么，我们压倒一切的目标是要控制这类使用，并对ICT的任何恶意使用施以最严格的限制。由于“网络战”一词很容易让人用战争思维模式思考问题并先入为主地考虑以战争的行动和技术（“反击”）进行网络防卫，本章将尝试挑战这一机械性思维模式，并实质性地呼吁网络空间的和平行动。当然，最重要的还是要对网络和平这一词汇进行与时俱进、不断丰富的定义。本书其他各章已在这方面开展了相关工作。

多年以来，世界科学家联合会在公开会议和出版物等多种场合将网络和平这一概念置于其工作的中心，[120] 国际电联特别是通过其秘书长近年来不懈努力，已逐渐使这一概念更为具体化，[121] 虽然该词以前用过，但从没有如此的广泛。在使用这一词汇方面最值一提的是2007年埃及“苏珊·穆

120 见www.unibw.de/infosecur的“出版物”和“活动”相关参考资料，其中后者有2008年12月“全球互联网危机：探索网络和平”会议记录。

121 “联合国负责人提议国际合作，防止网络战”，2010年1月21日，http://www.thepoc.net/breaking-news/world/3930-un-chief-proposes-intl-a。

巴拉克妇女国际和平运动”（SMWIPM）[122]框架（该框架与“联合国和平文化行动宣言和项目”直接相关）发起的有关促进网络和平的倡议项目，当然这里的应用是有针对性和有限制范围，特别是从儿童角度出发的。该倡议旨在通过加强各国年轻人的ICT能力建设，促进互联网的安全并实现对创新的鼓励。网络和平一词亦散见于和平研究团体的活动中，只不过不是非常系统，也未进行明确的定义。

就本书而言，网络和平的内涵指的是在制定一种“网络空间普适秩序”时要考虑的根本性原则，这要比 SMWIPM所理解的宽泛得多。如果该词的应用涉及更多政治内容和内涵且需用以引导正确抉择的话，那么就必须保持一定程度的开放性。其定义不能是封闭的，而且要更直观，其组成元素也应不断与时俱进。

当然，首先做一个基本定义是有必要的。要做此类尝试性定义，出发点是一般理解的和平概念，即一种安静的有益健康的境界，没有动乱、侵犯和暴力，没有“直接”暴力或武力，也没有间接压力。和平意味着占主导地位的是法律和通用道德准则，冲突化解具备可能和程序，持久以及稳定。

我们要感谢联合国大会在定义和平以及和平文化概念方面开展的内容丰富的全面的尝试性工作。1999年10月“和平文化行动宣言和项目”[123]给出了和平的内容清单和必备要素，并提出通过建立和平文化方式实现并维持和平。考虑到联合国教科文组织《组织法》有“因为战争发起于人的大脑，所以必须在人的大脑内构建保护和平的意识”的描述，该决议广泛列举了其组成要素，并为至2010年这十年时间确立了行动计划。

维护和平的重点不在仅仅不使用武力和倡导、实践非暴力理念，而是要建立一整套的价值观和行为模式、国际秩序和法制、正面的动态的参与

---

122 苏珊·穆巴拉克妇女国际和平运动，网络和平倡议，http://smwipm.cyberpeaceinitiative.org/。

123 “和平文化宣言”，UNESCO，A/Res/53/243，http://www.unesco.org/cpp/uk/declarations/2000.htm

进程以及人权（主要包括坚持以下原则：自由，正义，民主，容忍，团结，合作，多边，文化多样性，对话和理解，促进冲突的解决）。除了大家都很重视的伦理道德这一和平的组成要素外，对于网络和平，还要特别重视尊重和促进每个人发表言论、意见和信息以及获得信息的自由权利。当然，这些文献资料都是表面的陈述；真正重要的是要对决议进行认真的研究。国际电联近期提出了网络和平的五项原则，其中也设定了具体的行动和义务，以确保网络空间的和平与稳定。读者有必要研读这些具有开创性的资料。

2009年8月，世界科学家联合会将以上述及的以及其他一般性的、经联合国批准的适用于网络环境中的类似原则以更为具体的方式在《关于网络稳定与网络和平原则的埃里切宣言》中阐明。[124] 该宣言指出，网络稳定与网络和平是相互密切关联的。宣言简明扼要并集中阐述了网络和平的重要组成要素。这些要素包括：

1. 各国政府都应认识到国际法保障个人信息和思想的自由流动；这也适用于网络空间。如果要加以限制，也应仅仅限于必要范围内，且应伴有法律审议程序。
2. 各国都应协同工作，制定网络行为共同准则和协调一致的全球法律框架，包括有关在尊重隐私和人权前提下提供调查协助和合作的程序条款。各国政府、服务提供商和用户都应支持针对网络犯罪的国际法执法努力。
3. 所有用户、服务提供商和政府都应致力于确保网络空间在任何情况下都不被用来对用户特别是对年轻人和无防卫能力者施以暴力或降低质量方式的剥削。
4. 政府、组织和私营部门，包括个人，都应根据国际共识的最佳做法和标准，利用隐私保护和安全技术，实施和维持全面的安全项目。
5. 软件和硬件开发者应致力于开发促进可恢复和抵御薄弱环节的安全技术。

---

124 “关于网络稳定与网络和平原则的埃里切宣言”，世界科学家联合会，2009年8月，www.ewi.info/system/files/**Erice**.pdf。

6. 政府应积极参加联合国有关促进全球网络安全和网络和平的努力，避免将网络空间用于冲突。

这些原则特别是其中第六条，深刻传达了驾驭网络空间潜在冲突的坚强信念。的确，在攻击性“网络战”力量日渐增长情况下，维护网络和平的重点应放在遏制政府和非政府犯罪分子开展的网络空间好战活动方面。

本书其他部分将详细研究这些问题。不过，这里有必要先讨论几个原则问题，以便更清楚地解释网络和平问题。网络空间是一个无比庞大以至于无法测量的、没有法律约束的空间，所有人享有不受约束和惩罚的自由，而且似乎可以开展任何法律不禁止的活动。因此在数字世界各个领域，都有希望制定通用网络行为准则的呼声。世界科学家联合会自2001年以来一直在呼吁优先考虑在联合国框架之下建立网络和平通用法则[125]。显然，最需要这一法则的便是网络空间被用做攻击和军事用途问题。

完成这一任务的复杂性，以及走这条道路面临的法律和可能最为重要的政治障碍是很明显的。正如本书其他部分所指出的，有关战争和武装冲突的传统法律在此问题上语焉不详，有的几乎没有参考价值，而且也缺乏定义。在国际法主要文本如《联合国宪章》和北大西洋公约组织的《条约》中引述这些行动的传统制约性也大多是起不到什么效果。《日内瓦公约》和联合国大会在诸如跨国有组织犯罪、外层空间恐怖主义和行为等方面所做的一些决议和公约至多也就是提供空泛的不完全对比[126]。“军控”、合法与“非法”使用ICT之间的界限、侵犯与防卫之间的界限，这些问题都没有解释清楚，因为技术都是一样的，而且缠绕军控的“双重使

---

125 见“迈向普适网络和平秩序：管理网络犯罪与网络战的威胁”，报告和建议，世界科学家联合会信息安全常设监测委员会，2003年11月19日，提交信息社会世界峰会的文稿，www.itu.int/dms_pub/itu-s/md/.../S03-WSIS-C-0006!!PDF-E.pdf。

126 内容较空，但并非没有任何意义。见Sergei Komov，Sergei Korotkov，Igor Dylewski，“制定普遍接受的确保国际信息安全的国际法的军事方面问题”，ICT和国际安全，联合国裁军研究协会，2007年，http://www.isn.ethz.ch/isn/Current-Affairs/Security-Watch/Detail/?fecvnodeid=128420&dom=1&groupot593=0c54e3b3-1e9c-be1e-2c24-a6a8c7060233&fecvid=21&ots591=0c54e3b3-1e9c-be1e-2c24-a6a8c7060233&v21=128420&lng=en&id=47166。

用”难题在这里以更多形式出现，成为这里独有的问题。此外，跟踪与追溯两难问题 — 以可靠的及时的方式确认肇事者身份 — 已经使“简单”网络犯罪执法很麻烦了，而在军事领域更为复杂，这是因为好战攻击分子将尽一切可能采用更为复杂的逃避和伪装技术。作为军控重要组成部分的验证缓解，在这里变得实际上是几乎不可能做到的。传统意义上的遏制措施也变得不再可行，因为其基本要件是缺失的（溯源定人，确定始发地点，反应的级别）。因此，大量文献都支持将赌注押在网络防卫（包括向同盟方提供“扩展的”网络防护）而不是网络遏制上，这从逻辑上说也是最为可行的选项。[127]

尽管如此，如果我们要严肃认真研究网络和平问题的话，就有必要有一个法律框架，用以定义什么是对和平的破坏，而且政府应特别注意不应因噎废食，不应因此类法律框架的固有的不如人意之处就放弃制定此类框架。国际电联秘书长从国际电联五项原则出发，进一步建议各国应在此类文件中承诺不首先对其他国家发起网络攻击（“不首先使用”原则），且不应在其国内为网络恐怖分子和攻击者提供不受惩罚的庇护。[128] 同时，鼓励各国缔结双边或多边的不进行网络攻击的协定。这些协定可以是相互承诺不攻击对方的国家关键基础设施（特别是那些已受当前国际法保护的具有人道主义用途或提供基本生活需求的基础设施），也可以是确认跨边境数据网络的不可侵犯特性。一个意义重大且具有鼓舞性质的步骤将是在一个国际法文件中将攻击性网络武器和使用这些武器的攻击性战略确定为违法。

现实一点考虑，这类旨在促进网络和平的战略或原则无论如何也不能指望那些已经利用目前网络空间法律真空而投入巨大资源和继续投入资源以应对潜在网络战的国家的主动支持。的确，目前有关有计划有步骤地促使网络空间“武器化”、创建网络司令部、发展攻击性网络战略等的报告丝毫不能给人以任何的安慰。但是，多边反制行动的道德力量不应被低估。合法性是国家治理的重要工具，目前已经建立了行动的蓝图，制定并

---

127 比如，见Martin C. Libicki “网络遏制与网络战”，Santa Monica，2009年，第158页起之各页。

128 见第七章。

就任务路线图达成一致，仅就这几点来说，随着时间的不断推进，前进的动力和动机终究会出现的。为促进网络稳定和维护基本权利，网络和平需要明确的行动纲领。

有一个强有力的理由能推动这一进程。全球相互依存的网络结构的正常运行和稳定以及人们对其持有的信心是一种公共产品。对系统一小部分进行的大规模网络攻击也是难以控制的，其后果也可能是难以估量的；即使是很小的事件，也可能因为链式反应而释放出巨大的能量，这是网络空间固有的倾向。[129] 它们可以决定性地改变能量等式，破坏社会赖以维系的整个数字环境的地理稳定性，甚至远远超出冲突相关方的范围。维护跨境网络和信息结构的安全是所有国际社会成员共同担负的职责。

有一点毋庸置疑，那就是无缘无故的、挑衅性的网络行为，的确也就是网络攻击行为，是违背网络和平准则的。

但是当对预计的或真实的网络攻击的反应进行定义和验证时，比如说当网络冲突*真正*发生时，这一概念就面临了其决定性的考验。对于一个网络攻击是否，或何时被认定为是一个武装攻击问题，一般共识是可以采用占主导地位的*本征意义上*的国际法自卫权利原则，即保护自身和抵御侵略的合法性原则。正如本书反复指出的，根据《联合国宪章》和北大西洋公约组织的《公约》以及通用国际法的规定，将敌对行动定义为“武装袭击”是为了给个人和集体以使用*武装方式*进行防卫的正当理由。确实可以这样说，如果对另一个国家发起网络攻击或在另一个国家引起类似效应，

129 “国际社会需要认识到一个小规模的网络战可能成为一场大规模网络冲突的前身，可能潜在引起具有国际反响的区域战争。”引自美国网络影响部首席技术官John Bumgarner，《简氏防务周刊》，2010年9月29日，http://www.jdw.janes.com（以下简称“简氏”）。

如果至少导致巨大损失或人员伤亡，则可以被认为是一种“武装攻击”或类似事件。[130]

这可以为包括军事方式在内的集体行动提供法律依据。但在数字技术领域，军事反击行动的定义和时机需要仔细的新的思维，而且归根结底，需要采取谨慎的克制的政策。

网络冲突和传统的动力“战争”之间的差别是很明显的，而且远非仅是所用“武器”上的差别。总结本书其他各章包括本章的诸多观点，首先一点是在能否确切追溯出网络攻击发起方，以及能在多大程度上正确追溯出网络攻击发起方，这使得任一反制或反击措施都存在目的不明问题 — 向谁合法地发起反击呢？其次，由于数字网络和系统的无所不在和互连特性，数字反制措施会出现什么样的后果难以确定，以及因此很难估量任一反制措施的后果是否会扩大升级。第三，网络冲突可能引发严重的有组织的并因此具有很大破坏性的网络攻击，或者可能以一种分布广泛呈潜伏状态的低层威胁（网络间谍，创建不可识别僵尸网络等）形式存在下去，这些不同级别的潜在威胁可能逐渐成熟从而造成对基础设施的摧毁性的破坏。就国家与国家之间冲突而言，可能参与方的数量之多也是一个新问题；上世纪后半叶冷战期间两个极权大国之间独特的遏制与克制交融的核武器平衡经验不能简单地移植到一个具有敌意的多参与方环境中。最后一点是，正如已经重点指出的，各方都有意愿维持世界信息基础设施的正常运行。

我们在考虑对攻击做出反应时必须考虑上述以及其他可能引述的差别之处。在网络和平概念下，必须优先考虑维护或尽早恢复和平与稳定的环境。而这明显是将重点放在防卫问题上。

防御性自卫是做出和平反应的理由。在这一概念下，正如《埃里切宣言》所指出的，应当认识到所有数字参与方具有共同的确保网络和系统安

---

130 在本文写作时，NATO成员国在筹备华盛顿公约（2010年11月20日）缔约国峰会时正在考虑就新的包括网络攻击在内的威胁做出集体决定。如果此类攻击可以归为集体防卫的触发行动，将适用第4条（相互协商）和第5条（通过采取此类“认为是必要的，包括使用武力的”行动以便相互援助）。

全的职责。公司和政府结成的合作关系具有与国际合作同等的重要性。这里的关键词汇是可恢复性：不仅是系统质量，而且是其管理，必须确保在遭受攻击情况下仍具有坚固性和不可攻破性。利益相关方应优化其对各种情况下网络情况的了解程度，确定其高价值资产并找出其薄弱环节（实时监测其整个网络，实施安全区，网络分段，确保能源安全）。因此，应为各方广泛提供那些严格遵循国际电联和国家安全协议和标准的具有较强恢复能力的系统和软件。如果IT基础设施具备较强的恢复能力，就能弱化攻击者的攻击意愿，从而有助于建设和平的环境。高级防卫手段是网络稳定的必备要素；高级防卫之所以能威慑阻止攻击行为，就是因为它们能帮助建立信心，从而使运营者感到放心。

通常定义的恢复能力包括若干要素，其中最为重要的是系统自我复原的质量，报警系统的可用性，本身具有的冗余性，以及训练有素的行为模式，比如探索利益攸关方群体内部合作领域，并将其作为创建和平环境的一种努力，以及加强信息共享等，简而言之重点在于具体实施上采取积极行动和加强内在激励。在那些考虑采取可能的网络冲突方案以及希望采取反制措施的国家之间也可以考虑开展高级别管制活动，比如签署无网络攻击谅解文件，消除敌对形象、恶意监测的透明性安排，以及加强信息共享，以便在发生冲突时能更好地定位犯罪分子等。这些建议中的一部分也已正好是前面提到的国际电联秘书长的一些建议。正在发展的预警机制（全球响应中心（GRC），网络预警系统（NEWS）或ESCAPE）对于采取非暴力响应来说具有明显的价值。国际合作框架应利用日益广泛的CERT网络。

但是，对于严重网络冲突而言，如果仅采用被动防卫不能解决问题，且根据国际法从某种积极意义上而言可以启动自卫权利，则有必要在此方面制定相关的规则。从网络和平角度看，在这里简单地用传统武装冲突做类比是不合适的。这里存在的危险是，网络空间创建的智能网络可以导致报复性的武装战争，而武装战争的逻辑是要最大限度地摧毁敌方设施。如果沿用以往的作战规则，可能导致危险的后果。网络和平不需要完全放弃攻击性的反制措施和报复行动，但却在很大程度上改变了适用方案。

在这里，谋划何种反应的关键词汇是*克制*。其要素包括对威胁和风险的缜密的不间断的分析，防止出现总体网络失灵之后的不可控后果；重点放在精心选择的无扩散特性的反应行动；耐心和及时地实施反应，提高对来袭的定位精度并启动冗余和对等防卫联盟设施；特别注意核准自卫问题上内在的对称和必要原则；以及要仔细保护人道主义和社会不可或缺的关键基础设施。

虽然有可能夸张地说，在应对网络攻击时，防卫*总是*最佳的进攻，在目前分析中，网络和平确实需要在对报复进行最严格限制的同时，对进攻基础上的自卫进行全面梳理。[131] 这一原则也适用于上述提出的在国家层面对网络“武器”和进攻性网络战略进行有步骤有计划的非法化运动。

131 “Clausewitz不能预见21世纪最佳进攻将是强大的网络防卫。”见《简氏》。

7 网络战的国际回应

作者：哈玛德•图埃

7.1 各国政策和途径

世界各国以各种不同方式回应网络战这一新型威胁。虽然一些国家还只是刚开始考虑网络安全问题，[132]大多数国家最起码认识到有必要重新分配资源并在一定程度上改革国家安全战略。许多国家加强了在资金、研究和战术以及外交资源上的投入，改善其网络安全。[133]一些国家采取了“物理隔离”措施，试图通过不与其他系统连接的方式隔离某些网络，从而保护其关键的信息机构和系统不受攻击。[134]下面将评估不同国家采取的不同方法。

a) 将网络实力纳入传统战争策略

一些国家在网络战术中利用传统战争策略，建造网络进攻武器和防卫力量。他们将网络武器视为“实力倍增器”，主要用于与更为传统的武装行动并用，从而大幅度增强其作战潜能。[135]近年来，互联网已经变成一个在武装冲突期间重要的信息和宣传交流媒介。在此方面，许多国家将互联

---

132 比如，南非仅在最近（2010年2月）宣布其开始打算制定国内协调一致的网络安全政策。“制定南非网络安全政策意向的通告”，南非共和国政府公报，2010年2月19日，No. 32963。
www.pmg.org.za/files/docs/100219cybersecurity.pdf。

133 “网络战：破坏系统-60分钟-CBS新闻”，2009年11月8日，
www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml（报道说，美国国会已拨款170亿美元用于网络安全攻击和防卫举措）。

134 David Eshel，“以色列将网络攻击纳入IDF”，*Military.com*，2010年2月10日，
www.military.com/features/0,15240,210486,00.html（以下简称“Eshel”）。

135 Kevin Coleman，“俄罗斯的网络军队”，*DefenseTech*，2008年5月27日，
http://defensetech.org/2008/05/27/russias-cyber-forces/。

网上遭受的信息破坏视做一种对公众斗志的军事入侵，并因此准备用武装力量对抗网络攻击。[136]近期包括军事机密文件泄漏在内的事件显示了各国政府为何担心网络漏洞可能引起士气和公众支持降低等可能后果。[137]一些国家官员过去已经指出，他们将把信息战争战术认为是战争行动，而不论它们是否导致伤亡，并因此可以批准进行军事行动。[138]

b) 从国家资源角度发展网络战术

通过重新调整资源、资金和战略规划，许多国家正在将其数字基础设施和ICT视做其国家资源或战略资产。一些国家甚至已明确将此阐明为其国策。[139]各国已将其预算资源转向网络空间举措，预留了很大一笔经费用于研究和开发网络战力量。[140]一些政府已表示并开始寻求整合的国家方案以

---

136 Gregory Asmolov，“俄罗斯：新军事学说和信息安全”，Global Voices，2010年2月23日，http://globalvoicesonline.org/2010/02/23/russian-military-doctrine/（介绍俄罗斯最新军事学说，其中将信息战争归为一种军事入侵）。

137 比如，见Jo Biddle，“AFP：大量外泄机密文件催生新的阿富汗战争疑云”，2010年7月27日，www.google.com/hostednews/afp/article/ALeqM5gZkjOIqwM0xJDr0u5fPrc5rxdEQg。

138 网络战，议会研究服务，RL30735，2001月19日更新，www.fas.org/irp/**crs**/RL30735.pdf（其中引用了一个俄罗斯军事官员的话否认可能将信息战争归为非军事）（以下简称“CRS 网络战”）亦见 Peter Beaumont，“美国任命第一个网战司令”，*Guardian.co.uk*，2010年5月23日，www.guardian.co.uk/world/2010/may/23/us-appoints-cyber-warfare-general/（报道说美国也已经表示其将考虑使用传统军事战术来应对网络攻击）（以下简称“网战司令”）。

139 巴拉克·奥巴马总统，“总统有关确保我们国家网络基础设施安全的讲话”，白宫，2009年5月29日，www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure（其中说，国家数字基础设施从现在起将被视为一种“国家战略资产”，且对其保护将是“国家级的安全重点”）。

140 伊朗（预计伊朗的网络战预算在7600万美元）。

应对新型的网络威胁，动员多个部门并彻底改革其资源和战略。[141]这类改革可能包括对军事人员的培训（或再培训），改进情报部门使其更集中于收集相关的科学技术信息，并开展网络战模拟和军事演练，在所有科目中都特意采用信息技术。[142]一些国家已启动了国内竞赛，以从其国民中发现和招募最有能力的网络人才。[143]同时推动国内产业发展更先进的技术力量，以支撑新的军事战略。一些国家政府还建立了由个人黑客组成的团体，并在必要时征召其执行任务。[144]这些“黑客分子”可能是在技术上非常有能力的个人，也可能在以前是非法黑客，他们被征召并培训，并利用其技术特长为国家安全服务。[145]一些国家甚至还可能使用代理服务器，从其他国家招募黑客和专家为其工作。[146]所有这些变化都显示了当前各国政策正在远离在网络威胁上采取的被动反应策略，并调整为一种积极主动的信息战争战术，以有效应对当前高新技术挑战。[147]

---

141 Gurmeet Kanwal，“中国逐步显现的网络战学说”，第20页，Journal of Defense Studies，2009年，网址为：www.idsa.in/system/files/jds_3_3_gkanwal_0.pdf（讨论中国的信息战争和针灸政策）。[以下简称“Kanwal”]

142 网络战：精选国家途径和动机分析，达特茅斯学院安全技术和社会研究院，2004年11月2日，www.ists.dartmouth.edu/docs/execsum.pdf（以下简称“精选国家”）。

143 见，如 Richard Westcott，“英国寻求下一代网络安全专家”，BBC 新闻，2010年7月26日，www.bbc.co.uk/news/technology-10742588。

144 Kanwal，第20页。

145 Gordon Corera，“启动网络安全战略”，BBC 新闻，2009年6月25日，http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/2/hi/uk_news/politics/8118348.stm?ad=1（hereinafter“Corera”）；Tom Gjelten，“网络战士短缺威胁美国安全”，国家公共广播电台，2010年7月19日，http://www.npr.org/templates/story/story.php?storyId=128574055。

146 Eshel。

147 Kanwal 第20页。

c) 建立网络军事力量

若干国家已经通过为虚拟战斗调拨大批军事人员方式应对新的网络战威胁。[148]这一政策变动可能涉及对网络安全网战人员的开发，可能将其并入其他情报机构，[149]或甚至在军事部门内部创建一个全新的服务于网络活动的部门。[150]这些新的军事力量开始着手为全方位网络空间行动进行军事资源的整合和准备。[151] 虽然其主要重点通常是保护网络空间内的军事网络和开展军事行动，但也通常担负有保护专用网络的任务，这些网络也负责为诸多军事行动提供支撑。[152]

d) 利用网络战术调整竞争优劣平衡

通过完善其信息和电子网战战术，一些国家希望调整其与那些依靠软件和计算机系统来调动其常规军队的国家之间的竞争优劣平衡。这一变化涉及对新的自动化指挥系统包括诸如光缆、卫星和高频数字广播系统等硬件的投资，也包括逐步增加对太空、空中、海洋和地基监控系统的重视。[153] 一些政府已经在利用ICT及技术领先的军事人员来监测国境线。[154]

---

148 一些国家已经披露了其大规模人员调整。见《网络司令》（指出美国宣布调整30 000军队用于网络战）然而，许多国家的信息则不易获取。见Robert McMillan，“中国‘网军’黑帽讲座被压取消”，*InfoWorld*，2010年7月15日，http://www.infoworld.com/print/130362。

149 Eshel。

150 比如，美国于2009年宣布创建一个新的网军部门。《网军司令》。英国也已于近期宣布作为其网络安全战略的一部分，将创建一个网络安全运营中心。Corera。

151 见“美国网络司令部资料”，美国国防部，2010年5月25日，http://www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet%20UPDATED%20replaces%20May%2021%20Fact%20Sheet.pdf。

152 Siobhan Gorman，“美国支持网络战讨论”，华尔街日报，2010年6月4日，http://online.wsj.com/article/SB10001424052748703340904575284964215965730.html（注意到根据美国军方官员，90%的美国能源由私营部门提供。）（以下简称“Gorman”）。

153 Kanwal 第16页。

新网络战略可能更多依赖于这些资源及其对应的自动化系统，以确保边界安全。其他战术可能包括旨在摧毁敌方信息流动和定位敌方ICT基础设施以摧毁和消灭关键的机械、网络和数据的指挥和控制管理系统。[155] 这些变化集中于打击潜在敌方薄弱点，也即其对网络空间和新技术的依赖。那些拥有最强大传统和网战实力的国家可能因为那些使其强大的技术而变成事实上的弱者，因为这些技术最容易受到诸如逻辑炸弹和黑客之类的新型攻击。[156] 通过对网络空间潜在的行动不对称特性的投资，这些国家希望在军事实力上与对手平分秋色。[157]

e) 加强市民教育和提高对网络安全问题的认识程度

许多国家政府认识到公众教育和自我意识是增强网络防卫的强有力途径。[158] 政府和私营实体举办的信息数据库和全国提高认识月活动有助于从草根层面增强认识程度。[159]这些项目通常集中于教育个体用户和小型公司如何保护其信息和系统不受诸如身份盗窃和黑客之类的网络犯罪所侵害。在大多数情况下，非法接入计算机系统仅仅是致命的第一步，对个人计算机或系统的黑客攻击可能进一步成为影响国家安全的犯罪行为，如数据间谍和拒绝服务攻击。当针对至关重要的国家资源或政府组织开展此类行动时，这些“犯罪”可能归为网络攻击或网络战更为恰当。黑客已经试图定

---

154 Kanwal 第14页。

155 Kanwal 第18页。

156 极端变革（“因为美国是最依赖互联网和自动化……它也是最易受到网络攻击的。”）。

157 Kanwal 第18页；《CRS 网络战》第11页。

158 比如，见《精选国家》第5页（推荐系统化和可持续的措施，改变美国公众有关网络安全的观点，以改善其国家网络安全）。

159 比如，毛里求斯信息和通信技术部主管的国家计算机委员会负责监管网络安全认识门户，网址为：http://www.gov.mu/portal/sites/ncbnew/main.jsp，以及美国在每年的10月开展国家网络安全认识月活动，如美国国家网络安全联盟等公私伙伴关系也教育数字基础设施的用户和主管部门如何建立具有较强恢复能力的系统和保护机制。见：“简介”，国家网络安全联盟，http://www.staysafeonline.org/content/about-us。

期侵入政府，私营商业部门和国防系统，而且居然成功了。[160]数据间谍或接入敏感信息既可以通过技术手段也可以通过“社交工程”来实现，后者依赖于人际交往以诱使相关人员提供本该保密的系统的接入方式。[161]因此，有关社交工程和技术方式的公众教育，比如将被感染的闪盘放在公众场所，可以帮助保护国家资源。[162]

f) 较低连接程度的国家和发展中国家

虽然有很多国家高度依赖ICT和互联网以实现其关键基础设施和业务的提供，也有其他很多国家并非如此依赖或连接程度如此之高，相反的，他们使用全国性内联网和资源而非互联的ICT。然而，即使这些国家也似乎正在增强其联网实力，当然这方面的进展可能仅局限于军事和政府用途。[163]那些较晚迈向网络的国家可能面临较低的网络攻击可能，因为其整体政府系统与其他网络空间只共享较少连接。[164]但即使是那些尚未具备使其能够充分享有ICT提供的福利的基础设施的那些国家，也在其某些基本需求方面依赖互联网和其他移动和数字技术。[165]因此，他们在未来网络安全方面也有其自身利益所在。

---

160 见，如Understanding 第20页（列举出著名的黑客攻击对象，包括五角大楼，德国政府，谷歌，Ebay和NASA）。

161 见：同上，第23–24页。

162 比如，美国中央司令部曾于2008年被一个感染的闪盘入侵……见《第五领域》。

163 Martyn Williams，“朝鲜悄悄连上互联网”，*Computerworld*，2010年6月10日，http://www.computerworld.com/s/article/9177968/North_Korea_moves_quietly_onto_the_Internet。

164 Corera。

165 比如，见“经济及社会理事会2010年一般性辩论会议”，第3页，ECOSOC/6444，2010年7月16日，http://www.un.org/News/Press/docs/2010/ecosoc6444.doc.htm（讨论非洲国家使用的“数字现金”或电子货币系统）（以下简称“ECOSOC 2010”）。

7.2 近期国际回应

今天，相比较国家战略而言，只有非常少的国际力量致力于解决网络战威胁，不过已经有了一些尝试性的多边举措。同时，也出现一些开创性的双边协议，但它们都仅涉及网络空间相关方中的很少一部分成员，远缺乏改善网络安全的全面战略，难以确保网络的和平。一些国家呼吁创建一个限制网络武器使用的协定，而其他国家则坚称这类协定或者没有必要，或者目前时机尚未成熟。[166] 虽然这些提议可能见证迈向国际合作的一步，但他们也都缺乏真正的全面的解决方法和前进的清晰战略，一种能够包容所有利益攸关方的战略。下面一节将介绍近期一些国际反应，当然这不是一个完整的穷举列表。

a) 联合国毒品和犯罪问题办公室（UNODC） — 联合国预防犯罪和刑事司法大会（UNCPCJ）

2010年4月，第12届联合国预防犯罪和刑事司法大会（UNCPCJ）起草了一系列宣言，其中一个条款呼吁由一个政府间专家组研究网络犯罪及国际对策问题。[167] 相应的，在预防犯罪和刑事司法委员会第19次会议上，其成员国做出了相关建议，要求委员会设立一个开放的政府间专家组，落实UNCPCJ的条款要求。[168]虽然大会未就拟定新网络犯罪协定达成共识，但各

166 Gorman。

167 “全球挑战总体战略萨尔瓦多宣言草案：变革世界中的犯罪预防和刑事司法系统及其发展”宣言42，第12届联合国预防犯罪和刑事司法大会，2010年4月18日，http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/In-session/ACONF.213L6_Rev.2/V10529031A_CONF213_L6_REV2_E.pdf。

168 “第12届联合国预防犯罪和刑事司法大会报告”，UNODC，巴西萨尔瓦多，2010年4月12-19日，http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_18/V1053828e.pdf。

方在技术援助和能力建设方面达成了一致，这为讨论下一步行动奠定了较好基础。[169]

b) 联合国经济及社会理事会（ECOSOC）

联合国经济及社会理事会（ECOSOC）在其2010年会议开幕时介绍了网络安全方面面临的挑战以及不断扩张的互联网的使用呈现的危险以及提供的机遇。除了其他问题，理事会强调了开展促进信息交流、最佳做法、培训和研究的国际举措的必要性。此外，专家小组认为，联合国必须在此问题上“协调一致”，不仅应当促进国家之间的合作，而且要加强国家和私营部门之间的合作，以确保网络的安全。[170]他们警告说，一场真正的网络战的国际范围和可怕后果需要协调一致的应对措施；在目前，专于一面的结论和防卫加强措施是不恰当的战略。[171]

c) 北大西洋公约组织（NATO）

NATO于2008年实施其自身有关网络防卫的政策，以保护自身的以及其成员国的技术资源。[172]作为这一战略的组成部分，联盟创建了一个网络防卫管理局，一个能向各个成员国家派遣快速增援人员的计算机事件响应能力小组，以及一个网络防卫合作培训中心。[173]该中心位于爱沙尼亚，其专家负责开展网络安全方面的研究和培训工作。发起国包括爱沙尼亚、拉脱维亚、立陶宛、德国、意大利、斯洛伐克共和国和西班牙。[174]

---

169 “有关网络犯罪成果文件总结：第12届联合国预防犯罪和刑事司法大会”，网络犯罪项目，2010年4月26日，http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/2079_UNCC_cyberoutcome.pdf。

170 ECOSOC 2010。

171 同上（讨论非洲国家使用的“数字现金”或电子货币系统）。

172 “防卫网络攻击”，NATO，http://www.nato.int/cps/en/natolive/topics_49193.htm。

173 “NATO 2020”，http://www.nato.int/cps/en/natolive/official_texts_63654.htm?selectedLocale=en。

174 网络防卫合作培训中心，http://www.ccdcoe.org/。

此外，NATO还举办网络防卫演练，在演练中，来自其成员国的团队试图保护虚拟计算机网络不受网络的攻击和侵害。此类演练旨在增强对国际网络环境的理解，并增进各方在技术事件处理方面的国际合作。[175] NATO还与爱沙尼亚、美国、英国、土耳其和斯洛伐克签署了网络安全谅解备忘录。[176]

d) 欧洲委员会 — 布达佩斯网络犯罪公约

欧洲委员会《网络犯罪公约》[177] 通过提供模式化的、各国可以采纳或根据其自身具体需要改进采纳的法律条款方式处理网络安全问题。虽然该公约提供了一些法律方案解决诸如非法接入（黑客）和截获问题，但它未涉及网络侵入方面的最具破坏性的种类，如数据间谍和破坏。而且虽然该公约有助于通过对基本网络犯罪定罪而促进国际合作，但由于其起草者不想与其他潜在的国家立法产生冲突，使得其实施效力大受限制。由于巨大的文化和立法差异，使得在这一方式下建立一个统一法律的进程即便不是不可能，也会相当的缓慢。[178] 自该公约2001年11月开放签署以来，只有三十个国家批准了该公约，其中只有一个位于欧洲之外。[179]

公约中规定的法律条款是解决国家和国际层面网络安全威胁的一种途径。但是，公约条款不直接处理国家之间的网络战问题。虽然威胁采用制

---

175 “防卫演练提升抵御网络攻击技能”，NATO-新闻，2010年5月10日，http://www.nato.int/cps/en/SID-012B6A76-D60B9579/natolive/news_63177.htm。

176 “北约和爱沙尼亚达成网络防卫协议”，北约新闻，2010年4月23日。

177 网络犯罪公约 CETS no.：185，欧洲委员会，http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG（最后一次访问于2010年8月10日（以下简称“公约”）。

178 “网络空间的国家安全威胁”，美国律师协会法律和国家安全常设委员会和国家战略论坛，2009年9月，第13页，http://www.abanet.org/natsecurity/threats_%20in_cyberspace.pdf（以下简称“讲习班”）。

179 公约。

裁方式可以威慑一些狂热的网络犯罪分子，但这种类型的立法不能充分威慑那些自信能够躲避侦查、辨识和起诉的攻击者。

e) 网络安全双边协议

单一国家可以在网络安全方面与其他国家尝试建立关系。比如，印度政府通信和信息技术部以谅解备忘录或其他开发和信息共享等方式与许多不同国家建立了合作关系。比如，印度和南韩于2004年签署了信息技术（IT）双边合作联合申明，印度计算机应急响应小组也与韩国国家网络安全中心签署了有关主要在网络安全领域建立正式合作伙伴关系的谅解备忘录。[180]印度还拥有很多其他双边谅解文件，主要是在IT领域，也有一些集中在网络安全和网络犯罪领域。[181]

摩洛哥和马来西亚也在今年早些时候在摩洛哥召开的区域网络安全大会上签署了网络安全谅解备忘录。[182] 该备忘录为两国在部委级别上建立了网络安全合作关系，其中包括关键信息基础设施保护，制定网络安全框架，开展能力建设，培训和认识提高等领域。虽然这类合作关系可以改善一个国家的网络安全，但仍有必要为所有国家提供一个确保和平的更为全面的网络安全全球架构。

f) 国际电信联盟（ITU-T第17研究组） — 全球标准

为处理不断涌现的网络安全问题，特别是针对智能电网问题，国际电联建立了一个智能电网焦点组，以收集和整理有关信息和概念，从电信角度帮助制定支持智能电网发展的建议书。[183] 焦点组是国际电联加强其研究

---

180 “双边合作：亚洲”，印度信息技术总局，印度政府通信和信息技术部，http://www.mit.gov.in/content/bilateral-cooperation（以下简称“合作”）。

181 比如，印度与文莱，马来西亚，法国和澳大利亚主要集中在信息安全和/或网络犯罪，其他关系集中在资源和设施开发上。合作。

182 “马来西亚和摩洛哥现已成为网络安全合作伙伴”，马来西亚网络安全，2010年1月24日，http://www.cybersecurity.my/data/content_files/44/632.pdf?.diff=1265036362。

183 有关焦点组的更多信息，请访问网址：http://www.itu.int/ITU-T/focusgroups/smart/。

组工作计划的一种手段，为在各自领域快速制定规程提供了另一种工作环境。[184] 焦点组现已被广泛用于处理随时出现的企业需求，非常适合处理诸如智能电网之类快速变化和发展的技术。智能电网焦点组（FG Smart）由来自不同成员国的代表组成，并将与世界各地的智能电网社团（如研究机构，论坛，学术团体）协同工作。其目标是提供智能电网标准建议书，在此过程中，焦点组将维持一份不断更新的有关智能电网标准组织的清单，收集有关智能电网的观点和有价值的建议，提供智能电网发展必需的词汇和分类，整理有关的新的思路和发掘潜在的支持智能电网的研究领域，并探明标准制定对于安全、隐私和互操作性领域的潜在影响。[185]所有这些活动将提供一个广泛的多角度的途径，以处理快速发展且呈现越来越多网络安全挑战的智能电网问题。

而且，由于焦点组与国际电联电信标准化部门（ITU-T）这一电信领域最广为认可的标准制定组织之间的关系，使其能够充当一个具有一致性和可靠性信息和指南的来源，背后依靠高质量、各方共识的标准作为支撑力量。与ITU-T之间的关系也创建了一种有利环境，使得在可能情况下，可以将焦点组成果通过研究组以ITU-T建议书、增补、手册等形式进一步发展。作为ITU-T的一部分，焦点组开发的规程有可能在诸多国际性市场获得认可，特别是发展中国家以及那些尚未积极参加特别论坛的区域。

---

184 ITU-T焦点组，网址为：http://www.itu.int/ITU-T/focusgroups/。

185 ITU-T智能电网焦点组职能范围，网址为：http://www.itu.int/ITU-T/focusgroups/smart/tor.html。

7.3 国际框架的必要性

a) 遏制措施不再可行

每出现一个新的领域，就会出现新的挑战。正如陆地、海洋、空中和太空在过去和今天一直不断出现的划分、有效利用和冲突解决等问题一样，网络空间也创建了新的障碍和窘境。网络安全威胁每一个互连的个人，而且由于基本社会基础设施对ICT越来越多的依赖，它现在甚至影响到了那些没有连接上网的人群。当前，对信息基础设施和互联网业务发动的攻击也有可能以新的致命的方式伤及社会。因为网络战的独一无二特性及其呈现的挑战，以往尝试过并有效的维和战略已经证明不再有效。

遏制一直是长期以来国家之间在面临大规模毁灭性武器情况下为维持和平与安全而首先考虑采用的策略。但遏制的效率有赖于具体环境和前提，其中许多不适用于网络空间。[186] 遏制通常要求四个关键要素：定人（知道谁攻击你）；定位（知道从何处发出打击）；回应（能够做出回应，即使首先被攻击）；以及透明（敌人知道你利用大规模部队进行回击的实力和意图）。[187] 网络空间和网络战引入了新的问题，那就是破坏了各国建设其军事防卫武器时这四个要素存在的基本假设。ICT为攻击者屏蔽他或她的身份和位置提供了更多可能途径；攻击者可以利用代理服务器或公众互联网终端、无线网络和预付费移动业务等不需要验证身份的业务。用于确保保密、完整和有效的加密技术也能用于屏蔽身份或至少延缓调查网络攻击发源地的进度。限制互联网流量数据保留的技术程序和政策也阻扰了这一定人和定位问题。

---

186 极端变革（引用前美国安全顾问 Richard Clarke的话说，“防止核战争的力量 — 遏制 — 在网络战中不再有效”）。

187 Tang Lan and Zhang Xin，“网络遏制能起效果么？”载于全球网络遏制：来自中国，美国，俄罗斯，印度和挪威的观点，东西方研究所，2010年4月，第1页，http://www.ewi.info/system/files/CyberDeterrenceWeb.pdf。

被反击的目标可能是错误的，网络反击可能发生附带伤害，这可能很轻易伤害其盟友或中立方，进而挫伤各国应对攻击的能力。[188] 如果攻击者认定他们不会被抓到，或者认定受攻击的一方由于惧怕违反国际规则而不会发动军事反击的话，那么这种反击的威慑作用将不再具备。而被攻击的受害方如果使用武力对付那些没有使用常规军事力量以及其主要目的是欺诈而非毁灭性的网络攻击，那么它就可能面临国际社会将其误解为入侵或者非授权战争的危险。[189] 对遏制战略的依赖也会鼓励各国对其他国家采取威胁姿态，并在各个层面制造新的反击式威胁以抵消可能的非对称影响，这将阻扰进一步整合所带来的益处，并增加各国之间的紧张气氛。[190] 网络空间的基本特征通过上述各种方式使得网络空间采取遏制方式的效能大为减弱。

现有法律框架对于网络安全的危机管理来说可能不再适用。例如，根据现有国际法如《联合国宪章》第51条规定，一个国家可以在受到武装袭击的情况下发起自卫。在网络战情况下，这就要考虑更多的问题，比如何时才能将一个网络攻击视为一个武装袭击，以及是否该袭击可以认为是由一个国家发起的。[191] 公认的“国家责任”学说将可能回答后一个问题；这代表了一个命题，即每个国家必须保护其领土不被用于攻击另一个国家，而且，如果它拒绝采取防范性措施，那么它就应该为这类攻击负责。但是，如我们在前述对网络空间的初步分析中所看到的，要想在网络空间中回答此类实际问题是多么的困难，因为一些攻击找不到地理上的源头（正如“僵尸网络”的情形），它们可能跨越多个边界，可能是来自位于多个管辖区内的联盟发起的，也可能是通过一个代理服务器发起的，而该服务器只是按照破坏者的指令行动而已。有时候，国家自身可能也难以找到或确认其领土之内是谁在发起攻击。而且，即使一个国家可以确认是由谁在其领土范围内行动，由于网络空间的独有特性，由任何单一实体施行完全

188 James A Lewis，“跨领域遏制和可信赖威胁”，战略和国际研究中心，2010年7月，http://csis.org/files/publication/100701_Cross_Domain_Deterrence.pdf。

189 同上。

190 同上。

191 研讨会第14页。

的控制也是不可能做到的。[192] 因此，不仅仅是溯源问题，如何控制也是不得不考虑的难题之一。

b) 国际框架的必要性

因为现有国际法规范和条文未能完全与网络安全的新挑战相配套，全球性的讨论和合作现在很有必要。技术本身具有的不断变化的特性以及国家管辖权与其ICT、在线资源和系统之间日益加深的重叠区域，这使得在确保网络和平方面更有必要采用一套新的战略和国际合作模式。[193]

网络攻击可以从全球任一地点发出和并可以打击任一地点，这使得这些威胁就其范围来说具有固有的国际性，而且需要国际性的合作、调查协助以及共同的实质性和程序性的条款，以便恰当地处理这些问题。而且，国际合作也已被广泛接受为一种确保全球网络安全的关键要素。2003年和2005年，各国在信息社会世界峰会（WSIS）上就必须提供国内和国际层面有效工具以加强网络安全国际合作问题达成共识。[194] 这种国际合作的推动力不应只是相互之间的和平愿望，而应是各国的自觉行动。现在每个国家都高度依赖技术以提供商贸、金融、医疗、应急服务、食品流通等。至关重要网络的缺失将迅速击垮任一国家，而且没有哪个国家可以对网络攻击视若无睹。ICT的卓越地位以及技术发展过程中的互连特性正在影响建立一个新的世界秩序，一个呼吁在新问题上合作确保稳定的新秩序。

各国很有必要协调其有关打击网络犯罪和促进建立动态、多层面国际合作的立法框架。各国应致力于创建一个共同的法律和监管框架，并建立一个定期更新这些法律的系统，以应对安全威胁的不断变化的特性。一些

---

192 同上。

193 同上。

194 “WSIS：信息社会世界峰会突尼斯议程”，第40段，信息社会世界峰会，WSIS-05/TUNIS/DOC/6(Rev.1）-E，2005年11月18日，http://www.itu.int/wsis/docs2/tunis/off/6rev1.html（以下简称“突尼斯议程”）。

组织已呼吁制定国际标准和网络准则，以改善国际网络安全。[195] 不论在何种情况下，一个高效的网络和平战略必须具有足够灵活度和可调整度，以便能够管理和适应技术进步、ICT发展及其相应的安全挑战的快速变化。各国也必须就溯源和身份追踪的程序和方式问题达成共识，以便处理匿名网络攻击和它们威胁制造的国际纠葛问题。有关建立一个要求每个国家都督查其自身网络空间的国际协定的提议试图解决溯源问题；将责任与发源地理位置连带的提议可能有助于避开寻找网络攻击幕后组织分子这类杂乱的工作进程。[196] 然而，这些提议都没有触及如何解决代理服务器和对一个地理方位（确切方位）进行攻击的跟踪问题。考虑到传统的和现有的解决国际安全的方法的不足之处，很明显的是全球大家庭必须采纳一个新的战略，以处理网络安全带来的挑战，确保长治久安的网络和平。

7.4 网络空间国际原则提议

在制定网络和平指导原则时，我们必须考虑网络空间的独有特征以及这些特征表现出的最鲜明的挑战。不过，我们仍然可以从一些有关打击类似跨境威胁的其他文件中汲取经验，比如《打击跨国有组织犯罪公约》，以便为进一步开展工作提供指导。类似于跨国有组织犯罪，网络攻击也是跨越国境，在平行于或跨越于和平的创造性的系统的复杂网络上开展其国际行动。《公约》展现了各方的共同理解，即这些无处不在的跨境难题必须通过紧密的国际合作加以处理，而且要解决这些问题必须采取一种新的框架，相互之间开展法律和发展援助，加强信息共享和法律实施方面的合作。[197]

---

195 研讨会与会人员包括美国律师协会法律和国家安全常设委员会、麦克米可基金会和国家战略论坛成员讨论了成立国际网络安全行动任务组以制定网络准则和规则，改善网络安全问题。研讨会第26页。

196 Robert Mullins，“‘珍珠港’网文触动神经”，*NetworkWorld*，2010年3月11日，http://www.networkworld.com/community/node/58450（引用前美国总统安全顾问在近期网络安全专家讨论上的讲话）。

197 《打击跨国有组织犯罪公约》，联合国毒品和犯罪问题办公室，2004年，http://www.unodc.org/unodc/en/treaties/CTOC/index.html。

根深蒂固的法律学说和国际共识的准则支持网络和平计划的一些必要元素。特别是《世界人权宣言》第19条规定了有权享有主张和发表意见的自由，此项权利包括通过任何媒介和不论国界寻求、接受和传递信息和思想的自由。[198]信息社会世界峰会（WSIS）在其2003年《日内瓦原则宣言》中重申，通信自由是信息社会的重要基石。[199]《宣言》进一步强调，通信作为一项社会基本进程和人类基本需要，是所有社会组织的基础。相应的，全体人类应平等地接入信息通信技术。联合国明确承诺，确保向每个人提供这一接入，并为此将充分利用数字革命带来的潜能。[200]

虽然核原料和ICT之间的差别万千，但其中一些关键的类同点使得确保核和平的国际合作也对网络和平有启迪作用。类似于网络空间和ICT，核能源及技术具有众多的和平用途，也有诸多的军事用途，如果用于攻击，它们都能制造毁灭性的打击，虽然它们都可以用于针对任一国家，但所有国家都能感受到这一打击的效应。[201]有鉴于核打击的国际性的本质特点，国际社会已经选择采取一种多边合作策略，其中涉及创建共同的处理方法，各方共同承诺核安全等。[202]《不扩散核武器条约》给出了一种如何和平利用具有潜在破坏性的和跨越边界特点的材料的有效途径。该条约根据领土管辖权或“在[一个国家]控制之下的任何地方进行的”活动特点划分材料对应的责任。[203]作为对这一处理方式的呼应，四十七个国家在2010年

198 《世界人权宣言》，第19条，U.N. G.A.，Res. 217A（III），U.N. GAOR，U.N. Doc. A/810，1948，http://www.un.org/en/documents/udhr/index.shtml#a19。

199 《日内瓦原则宣言》，第4段，信息社会世界峰会，2003年：http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-E.pdf。

200 “潘基文呼吁进一步使用数字技术改善生活条件”，联合国新闻中心，2010年5月17日，http://www.un.org/apps/news/story.asp?NewsID=34716。

201 美国国家陈述，2010年核安全峰会，2010年4月13日，http://www.whitehouse.gov/the-press-office/nuclear-security-summit-national-statement-united-states（以下简称“美国国家陈述”）。

202 同上。

203 不扩散核武器条约（NPT），第3条，1970年，http://www.un.org/disarmament/WMD/Nuclear/pdf/NPTEnglish_Text.pdf（hereinafter“NPT”）。

核安全峰会上重申其承诺，确保核材料在其控制范围内的安全，并承诺随着情况发生变化继续改善这一安全，并就最佳安全做法和可行方案进行交流。[204]

《不扩散核武器条约》也强调和平使用核技术的益处以及将这一益处惠及所有国家包括发展中国家的重要性。[205] 该条约强调在所有国家之间进行国际合作的重要性，包括信息和材料的交流，以促进原子能的进一步和平利用。[206] 并且，该条约第3条对签字国规定了一些保障措施，旨在防止核能偏离和平使用而转向核武器或其他毁灭性用途。[207] 国际原子能机构作为一个公认的具有经验、专家和在中立论坛协调讨论能力的组织，负责监督各国之间开展的有关决定此类保护系统的磋商和缔约工作。[208]

其他有关确保核安全的合作机制包括全球打击核恐怖倡议，这是一个由致力于独立和协同工作以执行一系列共同认定的核安全原则的国家组成的国际性合作伙伴组织。[209]这些原则包括：发展和改进和物质和民用核设施的结算、控制和安全措施，改善成员国的检测和控制能力，防止出现恐怖分子安全港，改善成员在面临打击时的反应、缓解和调查能力，并加强信息共享。[210]

在很多其他新的类似领域中开展的确保和平的国际努力也强烈支持促进广泛的国际合作。例如，《关于各国探索和利用外层空间活动的法律原

---

204 美国国家陈述。

205 NPT前言和第5条。

206 同上，前言。

207 同上，第3条。

208 同上。

209 “打击核恐怖主义全球举措”，美国国务院，http://www.state.gov/t/isn/c18406.htm。

210 “原则声明”，打击核恐怖主义国际举措，美国国务院，http://www.state.gov/documents/organization/141995.pdf。

则宣言》在其指导原则中提出，所有国家应致力于在外层空间开发和利用方面加强合作和相互支持。[211]

有鉴于日益增加的可能来自任何地方、影响每个国家的网络攻击带来的风险，国际电联秘书长提出了建立和保护新兴网络世界和平的五项原则。这些原则包含并推进了国际电信联盟的在其漫长历史中展现的作为国际标准制定和监管领域领导者的价值和文化。国际电联权威的《国际电信规则》（ITR）仅是其促进国际电信和技术和谐发展、有效运作和普遍接入传统一个例证。《国际电信规则》创立之初是作为一个全新的监管框架以处理1980年代后期电信新环境下出现的新兴议题和挑战。[212] 其精心设计的条款旨在以协同、合作和平等接入原则促进提高效率和推动发展，这展示了国际电联的传统。该规则也反映了该机构在将通信权保护作为其重点的同时也避免对设施的破坏。

类似地，国际电联秘书长的五项网络安全原则也纳入了这些核心价值观，同时确立了具体的行动和义务，以确保网络空间的和平和稳定。这些原则是：

1. 每个政府都应承诺为其民众提供通信接入。
2. 每个政府将承诺保护其民众在网络空间中的安全。
3. 每个国家将承诺不在其国土内庇护恐怖分子/犯罪分子。
4. 每个国家应承诺不首先对其他国家发起网络攻击。
5. 每个国家必须承诺在国际合作框架内协同工作，以确保网络空间的和平。

---

211 《关于各国探索和利用外层空间活动的法律原则宣言》（“外层空间协定”），第6项原则，1967年，http://www.oosa.unvienna.org/oosa/SpaceLaw/lpos.html。

212 “国际电信规则：世界电报和电话行政大会最后文件”，国际电信联盟，1989年，http://www.itu.int/osg/spu/intset/itu-t/mel88/mel-88-e.pdf。

8 国际电联全球网络安全议程

作者：哈玛德•图埃

国际电联为讨论网络安全问题提供了一个独有的全球论坛。自1895年成立以来，该机构在近145年历史中，在电信、信息安全和标准制定方面以不同方式扮演了重要角色。国际电联认为，网络安全挑战的规模和特性需要协调一致的利益攸关多方参与的行动，并且该机构一直在向这一目标努力迈进。特别是国际电联目前正在通过在发展中国家根据其具体需求开展一系列的标准化和技术支援活动，以促进网络安全。鉴于该组织长期以来具备的经验、能力和专家资源，世界各国领导人和政府指定国际电联作为WSIS C5行动方面“树立使用ICT的信心并提高安全性”的唯一协调方。[213] 参加WSIS的各国元首和其他全球领导人以及国际电联成员国授权国际电联发挥领导作用，采取切实步骤，遏制与信息社会有关的威胁和不稳定因素。国际电联全权代表大会第140号决议（2006年，安塔利亚，修订版）研究了国际电联在实施WSIS成果文件中的定位问题，并授权秘书长采取所有必要措施，履行国际电联的职能。

相应地，秘书长于2007年5月启动了《全球网络安全议程》（GCA），该议程提供一个框架，在此框架内，利益攸关各方可以协调做出应对不断增长的网络安全挑战的国际行动。该议程以国际合作为基础，致力于团结所有利益攸关方，共同努力树立对信息社会的信心和提高安全性。最近，成员国在2010年全权代表大会上确认了国际电联在此领域开展的工作，在第130号决议（2010年，瓜达拉哈拉，修订版）中重申《全球网络安全议程》是国际电联的国际合作框架。决议责成秘书长继续对此领域的进展进行审议并加以改进。特别是成员国指出了要加强国际电联在树立使用IC的信心和提高安全性方面的地位，加强国际电联在与“国际打击网络威胁多边伙伴关系”（IMPACT）以及“事件响应与安全组论坛”

213 突尼斯议程。

（FIRST）合作方面的全球举措。决议也决定在国际电联内继续将信息和通信网络安全工作作为优先重点。

《全球网络安全议程》旨在达成七个方面的战略目标，这包括：

a) 详细制定相关战略，推动制定全球适用并与现有国家和区域层面立法措施相配套的网络犯罪示范法。

b) 详细制定全球性战略，以创建适当的国家和区域性组织机构并推出有关网络犯罪的政策。

c) 制定战略，以建立硬件和软件应用和系统的全球认可的最低安全标准和认证机制；

d) 制定战略，推动创建用于监测、预警和事件响应机制的全球框架，确保在新的和现有举措方面开展跨国界协调；

e) 制定全球性战略，从而创建通用并认可通用数字身份系统以及必要的组织机构，以确保数字证书能够得到跨地理边界的认可。

f) 制定全球性战略，推动个人力和机构的能力建设，从而强化跨行业及上述各个领域内的知识和专业技术；

g) 就上述各个领域的国际合作、对话和协调提出全球利益攸关多方战略框架。

为达成上述目标，《全球网络安全议程》集中于五个支柱作为其活动领域的指导。这些支柱是：

1. 法律措施

有组织网络犯罪有上升势头，这是因为互联网被证明是一个低风险、高利润的商业领域。个中原因是由于国内和区域立法之间还存在缺口，甚至很难有效查获犯罪分子。在《全球网络安全议程》框架内，该支柱旨在寻求制定战略，推动制定全球适用且可相互制约的网络犯罪示范法。特别是在其各种网络犯罪立法资源支持下，国际电联正在帮助成员国加强对网络安全立法方面问题的理解，以协调其立法框架。

2. 技术和程序措施

该支柱集中于研究软件产品漏洞的处理措施，设计全球可接受的认证方案、协议和标准。国际电联特别是国际电联电信标准化部门（ITU-T）以及无线电通信部门（ITU-R）在ICT标准化领域具有独一无二的地位，同时也在处理协议安全漏洞问题上占据领先地位。为找出网络威胁以及化解风险的反制措施，国际电联正在研究安全通信业务，审议移动端对端数据通信安全标准增强措施，并研究网络业务和应用协议的安全要求。国际电联焦点组和研究组，比如最近成立的智能电网焦点组，为完成这些目标提供了有效的机制。

3. 组织机构

世界各国已经认识到应对网络攻击时监测、预警系统以及应急响应的重要性，同样的，信息自由流动、各国组织机构之间和之内的协作与合作也相当重要。因此，该支柱目的在于创建组织机构和战略，以帮助预防、监测和应对那些指向关键信息基础设施的攻击。在此方面，国际电联正在与成员国一起找出其网络安全方面的具体需求，并帮助他们建立国家计算机事件响应组（CIRT）。同样的，作为国际电联与国际打击网络威胁多边伙伴关系（IMPACT）合作的一部分工作，全球响应中心（GRC）在实现《全球网络安全议程》目标方面扮演极为重要的角色。

国际电联和IMPACT正式达成了一个谅解备忘录，根据该备忘录，IMPACT位于马来西亚赛城（Cyberjaya）的现代化总部已经有效成为《全球网络安全议程》的有形工作场所。这一协作关系正在为国际电联的192个成员国提供专家、设施和资源，以有效应对世界最严重的网络威胁。《全球网络安全议程》五个工作领域的密切相关特性以及IMPACT提供的业务和基础设施使得这一合作关系成为全球打击网络威胁方面迈出的一个合乎逻辑的步骤。约有60个国家已加入该合作伙伴关系。[214]

214 “国际打击网络威胁多边伙伴关系”，国际电信联盟，http://www.itu.int/ITU-D/cyb/cybersecurity/impact.html。

IMPACT为成员国提供应急响应资源，帮助开展网络威胁溯源和提供资源共享。[215] 全球响应中心（GRC）配备有一个危机处理办公室，现代化的IT和通信设备，一个全天候正常运作的安全操作中心，全冗余安全数据中心，值班人员设施，现场广播中心，以及VIP观摩廊。全球响应中心通过采用技术手段打击新的不断进化的网络威胁，在实现《全球网络安全议程》目标方面扮演了重要角色。全球响应中心两大亮点是NEWS（网络预警系统）和ESCAPE（电子安全协作专家应用平台）。NEWS项目帮助成员国家尽早发现网络威胁，并就采取何种措施减弱影响方面提供关键指导。ESCAPE项目是一种可供成员国接入的专门工具和系统。ESCAPE是一种电子工具，可以帮助获得授权的位于不同国家的网络专家共同使用资源，并相互远程协作工作，而这一切都是在安全和值得信任的环境下开展的。通过在接到通知之后马上汇集资源以及来自不同国家的专家力量，ESCAPE帮助单一国家和全球社团一起共同及时应对网络威胁，特别是在发生危机情况下。

这一协作关系提供的目标和资源不仅与《全球网络安全议程》的五大支柱一致，而且与倡导的网络和平原则也紧密相连。通过IMPACT向成员国提供的资源将帮助各国政府保护其国内民众不受网络攻击的影响，从而确保其通过互联网和其他ICT设施继续接入通信网络。通过加入IMPACT，与其他成员国参与资源共享和讨论，各国也将积极参与五项原则的实践，在同一个国际框架下协同实现对网络和平的承诺。此外，IMPACT也为符合条件的发展中成员国提供培训课程奖学金，重点在于建立资源和知识共享库，而参训者日后也可与其他人员共享培训知识，从而建立其国内网络安全的能力和专家力量。这些奖学金将改善各国确保其自身ICT资源以及向其国民提供接入这些资源的安全的实力。

---

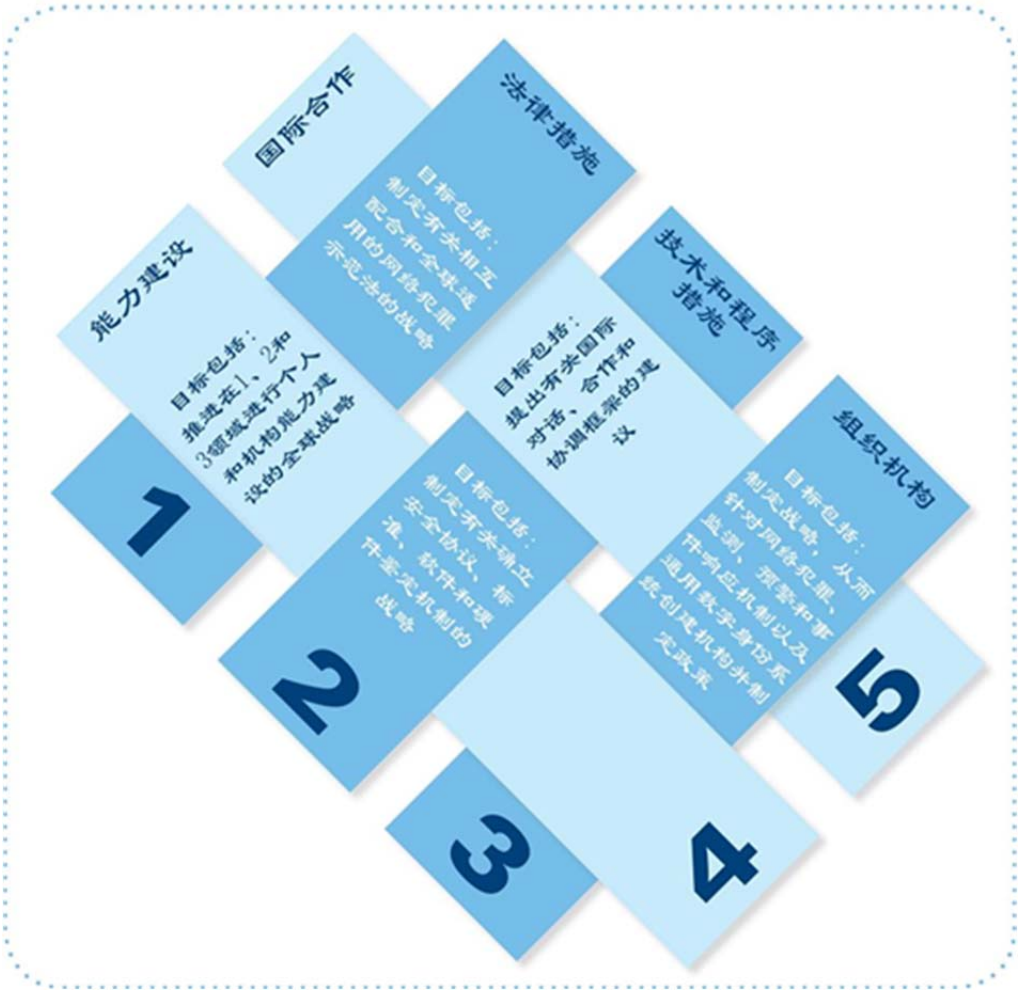
215 国际电联发送所有国际电联成员国有关“部署网络安全能力 — IMPACT全球响应中心”的信息函件，http://www.itu.int/ITU-D/cyb/cybersecurity/docs/IMPACT-information-letter-sent-to-member-states-2009.pdf。

4. 能力建设

在《全球网络安全议程》框架内，该支柱旨在详细制定提升知识和专家力量的战略，以促使在国家政策议程上加强网络安全工作。能力建设需要加以推动，目的在于建设一个可持续的积极向上的网络文化。加强对网络空间潜在危险的理解和认识程度，这对于终端用户安全地受益于ICT来说至关重要。特别是根据国际电联有关支持成员国网络安全能力建设的要求，国际电联在促进网络安全能力实施和部署方面开展了许多工作，如国际电联国家网络安全指南，国际电联网络犯罪资源和国际电联僵尸网络缓解工具包等。

5. 国际合作

如同互联网一样，网络安全也具有全球性和广泛深入性。因此，《全球网络安全议程》第五支柱重点在于制定国际性合作、对话和协作的战略。IMPACT协作机制代表了在此方面取得的实质性进展，为成员国和第三方讨论政策和共享信息提供了平台。该行动从诸多成员国层面直接推动了国际电联在WSIS C.5行动方面的履责。WSIS原则宣言表明，加强安全框架，包括信息和网络安全、认证、隐私和消费者保护，都是信息社会和树立用户使用ICT信心方面必不可少的环节。为实现这一点，应当积极与所有利益攸关方和国际专业组织推动、制定和实施全球网络安全文化。IMPACT协作机制以及国际电联的《国际电信规则》和焦点组，都对这一信任框架起到了加强作用，并通过采用一种全面的和为全球社区所有成员提供会议场所的方式，为实现这些目标而不懈工作。



全球网络安全议程：五项战略支柱

结论

虽然网络发展和对ICT日益的依赖带来的威胁很严重，但其潜在益处却更引人注目。我们已看到网络战的一些风险已经来到我们的生活之中，但我们也正在享受网络空间的益处，而且未来这种益处还具有无限发展的可能。随着我们往前迈进，我们必须积极应对这些问题，包括如何继续增强对网络的依赖、发展和整合，如何保护资源，以及如何创建一个能让基础设施和新技术持续不断发展的稳定环境，并确保长治久安。虽然很多现

有措施代表了积极步伐，但它们都未能达到目标，且不一定能提供最有效的解决方案。但如果我们携手努力，我们就极有可能达成这些目标，就能避免出现网络冲突引起的糟糕局面。国际电联已在达成这一目标方面以各种方式开展了有效工作，而且它拥有必备的资源和影响力以促进实现必需的多边支持和参与。

9 关于网络稳定与网络和平原则的埃里切宣言

作者：世界科学家联合会

关于网络稳定与网络和平原则的埃里切宣言

人类通过使用现代信息通信技术（ICT），现在已经有能力为所有国家扩展经济资源，提升其公民的智能，并在其他社会发展其文化和信任，这是一项史无前例的非凡科学成就。互联网，如同科学本身一样，本质上具有跨越国界和无处不在的特性。互联网及其相应的信息工具，是开展国内和国际科学讨论必不可缺的渠道，为所有人提供了开放科学的益处，没有掩饰，不设边界。

在二十一世纪，互联网和其他互连的网络（网络空间）已成为人类福祉和民族国家的政治独立与领土完整的关健所在。

危险在于世界变得如此相互关联，风险和威胁变得如此复杂和无处不在，而且相比较应对危险的能力而言，危险在呈指数级的增长。现在，民族国家和流氓坏蛋都有能力大规模摧毁其他国家的生命和社会；网络犯罪及由此产生的网络冲突，威胁着人类的和平生存以及对网络空间的正面利用。

信息和通信系统及网络支撑着所有国家的国民和经济安全，在反应能力，商业和政府运作，公共事业，公众医疗和个人进步方面扮演着中枢神经系统的作用。

信息基础设施和系统变得对人类医疗、安全和福祉至关重要，特别是老人、残疾人、体弱多病者以及年纪很轻人来说尤为如此。网络空间的大规模瘫痪可能引发不必要的罹难和破坏。

ICT支持国际法保障的人权原则，包括《世界人权宣言》（第12、第18、第19条）和《公民权利和政治权利国际公约》（第17、第18、第19条）。网络空间的破坏（a）损害个人的隐私、家庭、住所和通信不受干扰和攻击的权利，（b）干涉思考、反省和宗教自由权，（c）剥夺自由发

表主张和意见的权利，以及（d）限制通过任何媒介不论国界接受和传递信息和思想的权利。

ICT可以造福，也能作恶，因此既能创造和平，也能引起冲突。充分利用信息时代的益处要求信息网络和系统保持稳定、可靠、可用和可信。为确保网络空间的完整、安全和稳定，总体上要求协调一致的国际行动。

因此，我们倡议以下原则，以实现和保持网络的稳定与和平：

1. 各国政府都应认识到国际法保障个人信息和思想的自由流动；这也适用于网络空间。如果要加以限制，也应仅仅限于必要范围内，且应伴有法律审议程序。
2. 各国都应协同工作，制定网络行为共同准则和协调一致的全球法律框架，包括有关在尊重隐私和人权前提下提供调查协助和合作的程序条款。各国政府、服务提供商和用户都应支持针对网络犯罪的国际法执法努力。
3. 所有用户、服务提供商和政府都应致力于确保网络空间在任何情况下都不被用来对用户特别是对年轻人和无防卫能力者施以暴力或降低质量方式的剥削。
4. 政府、组织和私营部门，包括个人，都应根据国际共识的最佳做法和标准，利用隐私保护和安全技术，实施和维持全面的安全项目。
5. 软件和硬件开发者应致力于开发促进可恢复和抵御薄弱环节的安全技术。
6. 政府应积极参加联合国有关促进全球网络安全和网络和平的努力，避免将网络空间用于冲突。

《关于网络稳定与网络和平原则的埃里切宣言》由世界科学家联合会（WFS）信息安全常设监督委员会在日内瓦起草，并于2009年8月20日在埃里切（西西里岛）召开的全球突发事件国际研讨会第42届会议上通过。

10 结论

作者：Jody R. Westby

今天，网络和平方面的探索工作安静得令人担忧。世界科学家联合会信息安全常设监督委员会在2008年12月提交梵蒂冈宗座科学院的一个具有开拓性的项目中第一次提出网络和平这一概念。随后，常设监督委员会于2009年起草了“关于网络稳定与网络和平原则的埃里切宣言”，该宣言获得世界科学家联合会通过，并被分发至联合国各会员国。本出版物中提出的概念和原则反映了常设委员会有关世界正在滑向网络混乱局面的令人惊醒的评估，但通往网络和平的道路将催生更高程度的全球稳定。

这里给出的数据和方案指出了容忍网络犯罪和网络冲突的严重性。互联网创造了犯罪选项，因为溯源困难，犯罪分子很难被抓获并被起诉。我们担心互联网也会成为武器选项。那么轻易地就可以进入一个国家的最敏感数据和核心基础设施操作，最小的国家也可以跟具备最庞大防务开支的国家旗鼓相当。发展中国家已经向发达国家展示了如何以一种非线性的方式通过使用卫星和无线技术建立ICT基础设施。同样，各国正在了解网络是如何展现了一幅诱人的非线性选项来促进国家和经济安全利益的发展。

为什么网络遏制与网络和平不是今天的主旋律？相反，全世界的军事领袖正在忙于宣布其网络司令部的建立及其开发攻击、防御和利用网络能力的规划。当各国都面临核武器时，他们开始要求遏制和不扩散。全球各国在一同禁止一个可能威胁人类生存的全球危险时走到了同一条道路上。正如爱沙尼亚和格鲁吉亚攻击所显示的，当一个受打击的国家面临一个缺失的国际法律框架时，外交的不确定性，技术的限制，以及不能实现对通信的跟踪和定位，都使得网络和平的概念变得愈加迫切。

虽然有众多的多国组织正在致力于网络犯罪和/或网络冲突各方面的工作，但只有国际电联采取了一种国际视野，并提出了一个旨在探讨主要问题领域的议程，同时充分利用其他组织的成果。我们要表扬秘书长在处理面临的这一庞大问题时展现的领导力、视野和勇气。我们衷心希望其他

组织支持并学习这一举措，并希望其领导人进一步制定一个网络行为准则和立法框架，支持和推动地缘网络的稳定。

我们正在接近一个危险的深渊，此时互联网的阴暗面可能掩盖ICT的巨大福祉并颠覆整个世界的秩序。呼唤网络和平正逢其时。

联系信息：
综合战略处
国际电信联盟
Place des Nations – 1211 Geneva 20
Switzerland
电子邮件: strategy@itu.int
www.itu.int/cybersecurity

瑞士印刷
2011年3月，日内瓦

03/2011