探寻网络信心

国　　际　　电　　信　　联　　盟

探寻网络信心

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

2014年11月

法律提示

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Henning Wegener和所有就此全球日益关注的问提纲挈领地表达了自己观点的作者。秘书长还向世界科学家联合会主席Antonino Zichichi教授表示感谢，同时向牵头本出版物编写和协调工作并领导了国际电联网络安全小组的Marco Obiso表示真诚的谢意，尤其要向Alex Gamero Garrido、Aliya Abdul Razack、Despoina Sareidaki、Anthony Drummond、Preetam Maloor和Rosheen Awotar-Mauree以及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。

若要发表评论，请通过cybersecurity@itu.int与国际电信联盟网络安全小组联系。

目录

有关国际电信联盟

国际电信联盟（ITU）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2007年发起了《全球网络安全议程》（GCA）活动，将其作为利益攸关多方在网络安全领域开展国际合作的框架，从而与目前和未来的各项举措和合作伙伴形成合力。该议程侧重于以下五个工作领域：法律措施、技术和程序措施、组织结构、能力建设以及国际合作。

在GCA框架下，通过全球合作伙伴的支持，帮助成员国进行网络安全能力的一些关键举措包括：

- 国家CIRT（计算机事件响应团队）计划，按照成员国的要求开展各国CIRT评估、国家CIRT落实工作以及区域性网络演练。
- 建立区域性网络安全中心，为加强区域性合作、协调与协作发挥催化作用以应对日益猖獗的网络威胁。
- 国际电联通过“增强最不发达国家的网络安全”项目帮助最不发达国家强化网络安全领域的能力、人力、就绪水平、技能和知识。
- 全球网络安全指数（GCI）是各国衡量网络安全发展水平的一项指标。GCI旨在为各国加强网络安全工作给予适当的推动。最终的目标是为培育全球性网络安全文化并将其纳入信息通信技术的核心起到促进作用。

有关世界科学家联合会

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：从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成员国。

该声明已分发给联合国各成员国并与其它声明、出版物和信息安全常设监督委员会的内部文件一同提供在其网站上：www.unibw.de/infosecur。

Henning Wegener大使担任PMP主席。为出版物献计献策的成员包括：

做出贡献的成员

Mona Al-Achkar

Mona Al-Achkar Jabbour拥有私法博士学位，曾于1998年至2009年担任黎巴嫩大学法律和研究系主任以及科威特司法部负责法律数据库实施的顾问和负责人。

目前，她担任黎巴嫩法学院法学教授、黎巴嫩法律信息中心教授级研究员，是黎巴嫩信息技术协会（LITA）的创始人兼主席、黎巴嫩网络犯罪中心创始人、泛阿拉伯网络安全观测中心成员和创始人以及阿拉伯在线作家、阿拉伯在线仲裁联合会、黎巴嫩社会事务部保护上网儿童法律委员会、互联网域名和号码分配机构（ICANN）和IGF“法语区小组”、黎巴嫩互联网中心（LINC）以及世界科学家联合会信息安全常设监督委员会成员。

Al-Achkar博士就不同法律问题出版了多本书籍和文章，其中一些涉及法律信息处理以及网络法律，乃至洗钱和恐怖主义。

William Barletta

William Barletta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。同时是斯洛文尼亚卢布尔雅那大学经济学客座教授。他是美国和韩国粒子加速学院的主任以及《核仪器和方法》的协调总编。他还是意大利同步辐射光源实验室主席的高级顾问。世界科学家联合会常设能源监督委员会（PMP）的联合主席以及信息安全常设监督委员会成员。他是美国物理学会（APS）公共事务委员会当选主席。他还曾担任国际物理学论坛副主席和该学会粒子束物理学部主任。他是国际科学事务APS委员会的一名积极成员]。

他已编辑了四部有关加速器科学著作，是有关网络安全、隐私和国际网络法等四部书籍的合著人。他拥有四项专利，并发表了170多篇科学论文，获芝加哥大学物理学博士学位。

Pavan Duggal

Pavan Duggal被公认为全球四大网络律师之一，并作为网络法和电子商务法的专家和权威在全球范围内发挥重要影响。

作为印度高级法院的从业顾问，他已成为融合法和移动法的开山鼻祖。为此他分别担任联合国贸发会议（UNCTAD）和亚太经社委员会（UNESCAP）的网络法和网络犯罪顾问。他还是UN/CEFAT AFACT法律工作组成员，为欧洲理事会网络犯罪担任咨询专家。与此同时，他担任欧洲委员会电子商务专家组成员。他作为e-ASEAN任务组网络法律权威专家以及亚洲开发银行审核员开展的工作更进一步表明，他已成为该领域内世界公认的权威人士。此外，他还担任Cyberlaw Asia & Cyberlaws.Net主席。

Pavan近年来曾在1200个大会、研讨会和讲习班发表演讲并就上述法律的各个方面撰写了42本书籍。

有关Pavan Duggal的更多信息，请访问：
http://www.linkedin.com/in/pavanduggal。

Solange Ghernaouti

计算机科学博士（巴黎大学）Solange Ghernaouti是洛桑大学教授和瑞士网络安全顾问和研究小组主任。她是全球公认的网络安全、网络防御、网络犯罪和有关ICT风险管理问题的专家。她为世界各地的国际组织、公众和私营机构、研究中心以及执法机构组织的若干举措做出了贡献。多年来，她在该领域的先驱作用主要体现在她所开发的面向公民、各组织和国家的多学科和综合性网络安全手段。

她还是一位积极的独立安全顾问、具有影响力的分析师和媒体定期评论员。瑞士媒体一直将其称之为专业和学术领域的杰出女性之一。她曾荣获荣誉骑士勋章并被授予瑞士科学院院士，著有300多部出版物和包括“网络的力量：犯罪、冲突和网络空间的安全”（2013年EPFL出版社）在内的28部书籍，与Schjølberg法官联合编写了《有关网络安全和网络犯罪的全球性公约 – 为网络空间的和平、正义和安全做出贡献》（2009年Cybercrimedata）。她是世界科学家信息安全常设监督委员会的成员。

更多信息，请访问：www.scarg.org

Gabor Iklody

Gabor Iklody目前就职于布鲁塞尔的欧盟对外行动署（EEAS），担任风险管理和规划局长。之前曾担任北约（NATO）负责未来安全挑战的副秘书长并领导NATO最新成立的政策处，负责非传统方面的挑战，如网络防御、反恐怖、WMD不扩散和能源安全以及核政策和战略分析。他还主持了NATO的网络防御管理委员会。

在担任国际职位之前，他在匈牙利外交领域工作了约30年，最后曾担任政治局长和副国务卿，负责多边和安全问题。他两度在斯堪的纳维亚担任大使，每次四年，第一次在挪威（1999-2003年），之后在瑞典（2005-2009年）。他将职业生涯几乎全部奉献给欧洲大西洋的一体化，多边外交以及武器控制。

Danil Kerimi

Danil Kerimi负责为世界经济论坛（WEF）制定技术议程，拟定全球公共行业宣传政策并将超级链接平台之下各种与ICT相关的举措（网络安全、数据、认为技术、提高竞争力的ICT、互联网管理）结合起来。

他负责论坛中顶级公共行业和业绩领导者、知识及民间社会ICT项目专家之间的交流。此外，Danil还负责有关网络安全的全球议程理事会和世界经济论坛年度全球信息技术报告。在加盟世界经济论坛之前，Danil曾经在联合国、欧洲安全和合作组织、国际移民组织以及其他重要的国际机构中担任要职。

Axel Lehmann

Axel Lehmann是德国慕尼黑国防军大学信息处理系退休的全职教授，2011年之前他曾主持建模和仿真工作。目前，他还是该大学智能系统研究学院（ITIS）的执行主任。他的主要研究领域涉及基于计算机的建模和仿真、应用知识系统进行的诊断和决策支持、创新型计算机架构的设计。他曾担任国际建模和仿真学会主席、德国信息处理学会研究员和亚洲仿真学会联盟研究员、建模和仿真领域科学杂志编辑委员会成员以及国际标准化工作组成员和审议委员会成员（如欧盟和NATO）。自2001年以来，他一直担任世界科学家联合会信息安全常设监督委员会成员。

Stefan Lüders

Stefan Lüders毕业于瑞士联邦苏黎世技术学院并获博士学位，2002年加盟欧洲粒子物理研究所（CERN）。作为CERN大型强子对撞机所有四次实验使用的通用安全系统的最初开发人，他在有关控制系统的网络安全方面掌握着丰富的专业知识。从2004年开始，他负责CERN加速器和基础实施控制系统的网络威胁防范。之后，他加入CERN计算机安全事件响应团队。今天，他作为CERN计算机安全官领导着该团队，负责协调CERN计算机安全的各个方面，这包括办公室计算机安全、计算机中心安全、网格计算机安全和控制系统安全。同时，考虑到CERN的运作需求，Lüders经常就计算机安全和控制系统网络安全向国际机构、政府和企业发表研究并就这些问题发表了若干文章。

Howard A Schmidt

Howard目前担任Ridge-Schmidt Cyber战略顾问公司合伙人。这家行政服务公司帮助企业和政府领导人探索网络安全日益增长的需求。他与国土安全部一秘Tom Ridge同任该职。他还是有关优秀代码软件保障论坛（SAFECode）的执行总监。

他的专业特长源于40多年不同行业获得的有关商业、国防、情报、执法、隐私、学术和国际关系领域的知识。最近他曾担任美国总统特别顾问和网络安全协调员。他在白宫担任的职务包括贝拉克•奥巴马和乔治•布什总统的网络顾问。

之前，Schmidt先生曾担任信息安全论坛（ISF）主席兼首席执行官。他还担任过eBay公司的副总裁兼首席信息安全官和首席安全战略家，他还曾经担任微软公司的首席安全官，国土安全部US-CERT伙伴计划首席战略家。

Schmidt先生曾获菲尼克斯大学商业管理（BSBA）和组织管理硕士学位（MAOM）。他还曾荣获卡内基梅隆CyLab名誉博士学位并担任名誉研究员和Ponemon Privacy学院高级研究员。之前他曾担任ENISA的PSG成员。目前他在Idaho州立大学担任教授级研究员，也是世界科学家联合会信息安全常设监督委员会成员。

Howard是无线电操作员（W7HAS）、个人飞行员、野外活动爱好者和一位生龙活虎的Harley-Davidson骑手。夫人Raemarie J. Schmidt是退休法学科学家、研究员和计算机法学研究员和导师。他们不仅是令人骄傲的父母，同时也是幸福的祖父母。

哈玛德•图埃

哈玛德•图埃博士自2007年1月起担任国际电联秘书长并于2010年10月连任。他在公众和私营部门都具有广泛的专业化经验。

图埃博士国籍马里，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，继续引领国际电联实施信息社会世界峰会（WSIS）的各项决议，以便实现《千年发展目标》（MDG）。

图埃博士已婚，拥有四个子女和两个孙子孙女。

Henning Wegener

Henning Wegener是前任德国大使。他曾在日内瓦担任裁军大使（1981-1986年）、NATO政治事务副总干事（1986-1991年）、德国联邦法院院长（1991-1994年）并在此之后任西班牙大使（1995-1999年）。Wegener大使自2001年以来一直担任信息安全常设监督委员会主席并在短暂停顿后继续于2009年至2012年担任联合主席。他的工作体现在外交和安全政策的多份出版物中，其中包括网络安全。Wegener先生是Rome俱乐部（西班牙分会）成员并在若干基金会董事会担任职务。他曾获多项学位，其中包括耶鲁法学院的司法科学博士学位。
henningwegener@hotmail.com

国际电联秘书长哈玛德 • 图埃博士的序言

最近，网络平台和技术使用中甚嚣尘上的威胁和日益猖獗的安全事件动摇了我们对这个时代不可或缺的工具的信任，本书将探讨增强信心的艰辛之路。

《探寻网络和平》发表于2009年，该书侧重于促进网络和平，从而为人类创造巨大的利益和进步，同时，网络空间也使犯罪活动肆虐，为情报搜集、行业间谍和冲突创造了新的途径。

本书不可避免地回到围绕网络空间使用从恶或从善这一压倒一切的主题带来的种种问题，尤其是“**黑色**”互联网对网络空间信任的影响。然而，这一中心议题促成了网络信心的理念。正如引言章节所指出的，在网络空间探讨“信心危机”不再是夸夸其谈。诚然，对近期趋势的分析表明，各种势头的结合对网络信心造成叠加式不良影响。网络空间日益升级的军事化以及除针对军事目标，亦针对民用基础实施的攻击性军事能力与日俱增的迅猛破坏尤其令人忧心忡忡。网络和平理念的诞生旨在平息这种势头。在更加热门的议题中，网络空间前所未有的数字间谍和隐私入侵最近已成为公众密切关注的焦点。

本书作者从各个不同角度探讨了动摇信心的多种因素，对此进行分析并制定有效的应对策略。在此过程中，作者侧重于恢复和建立信心至关重要的三个主要领域：1) 建立特别适用于数字时代的规范性政策和监管框架；2) 增强适应性以抵抗对网络空间的各种滥用；3) 确保根本自由，如网络空间的接入自由和言论自由。针对所有三个领域，作者还概括阐述并评估了在全球、区域和国家层面内开展的各项有利于实现上述目标的举措。

本书针对上述问题发出了有力的行动呼吁并就此方面陈述了令人信服的理由。与其前身《探寻网络和平》一样，本书亦由位于这项工作前沿领域的世界科学家联合会和国际电信联盟两个组织主持并编著。

世界科学家联合会主席Antonino Zichichi教授的序言

在进入第三个千年的初期，科学比以往任何时候都成为变革和历史演进的主要决定力量。它帮助人们更深入地探究宇宙的运转和秘密。在此过程中，复杂的系统变得更加复杂。人与环境的互动形式日新月异：人脑与机器的关系瞬息万变，从而需要重新定义。我们进入了一个充满意外发现和前所未有的挑战的时代。

数字技术在科学和应用科学中大有作为。这些技术及其工具不断普及，由此产生的增长和知识可用性曲线几乎难以想象，为所有人类活动提供了监测工具和控制系统。基于高度发达的信息基础设施的专门化计算机应用、分布式网格计算和云计算、微电子和新传感器的发展、各类数字设备互连互通（且常常自动化）的宇宙变迁以及制造工艺的迅速变革已成为新时代的一些突出特点。

数字时代的优势和机遇不胜枚举，但作为世界科学家联合会主席，我想强调科学和数字技术演进对于促进和平和掌控地球危机的重要性。有效监测这些危机取决于防御、响应、恢复和重新应对等信息的实时关联。对此，我深刻体会到作为一名科学家的道德重任。

数字空间无边界，其普及性使世界扁平化并大大缩短了距离和时间。网络技术与所有现代技术一样固有的含糊性使其既可从善亦可从恶，因此具有多面性。网络空间不仅意味着无限的机遇，但同时也意味着危险，在缺乏充足且普遍有效的规则框架的情况下尤其如此。恶意使用数字技术产生的威胁与日俱增。因此，网络安全和数据保护在数字风险管理中占据更加核心的地位。它们已成为数字革命的根基并必将为抑制危险浪潮成为迅猛增长的行业。

世界科学家联合会是有关信息安全的跨专业集团，为信息安全工作已付出十年有余。与国际电联秘书长之前联合出版的书籍 – 《探寻网络和平》突出了对数字技术的安全和和平使用。本书则侧重于正常运行的数字社会的另一个重要方面：信任、信心。用户乃至全社会不仅要对技术的正常运行充满信心，还必须能

够依赖于数字设备和数据及其所依赖的网络结构的完整性和私密性。互信是一切有效和长期合作的基础。在全球网络空间内，在互动日益加强的全球信息社会中，这一点至关重要。信任通过保持对彼此良好意愿和互信的期待使国际互动更为有效。我对秘书长图埃以及本书联合作者就网络信心多个方面的阐述以及提出的必不可少的建议表示感谢。

引言：网络信心风险

By Henning Wegener

三年前，国际电联秘书长和世界科学家联合会信息安全常设监督委员会出版了《探寻网络和平》[1]一书。该书将网络世界面临的日益严重的险境带入人们的视线并呼吁网络世界所有利益攸关方采取行动，通过合作确保互联网和数字网络结构实现充分的稳定性，将全球网络和平的理念推广开来。该书因在很大程度上准确体现了现实中公众的争议，因此仍无过时可言。该书作者（多数与本书作者相同）通过与时俱进的分析和建议表述了自己的观点。

然而，今天的情形更加令人担忧。毫不夸张地说，网络空间的新型威胁已进一步展现在我们面前。前一本书主要集中在令人担忧的网络冲突，其中包括网络战争。这一方面如若补充，只能说更加令人堪忧且毫无改善。因此，网络冲突在本书中依然是一个突出议题，为此，两本书的标题也体现了明确的延续性。然而，随着威胁事态的发展，本书的中心议题有所转移。网络信息理念成为本书的核心主题。本书的目的是对信心严重受损的趋势予以分析并指出恢复信心所需要的战略和技巧[2]。

---

1 《探寻网络和平》，国际电信联盟和世界科学家联合会，2011年1月，日内瓦。

2 为显示两本书之间的延续性，该书标题选为《探寻网络信心》。然而，“探寻”一词在两个情形下含义不同。在第一本书中“探寻”表达的是对尚未实现的和平状态的渴望，而在第二本书中，已有的信心严重受损，因此“探寻”一词意为恢复和巩固。

信心是基于数字技术的信息社会正常运转不可或缺的前提条件，这一点已是老生常谈。仔细研读信息社会世界峰会（WSIS）分别在2003年和2005年两个阶段会议上通过的文件就可立即认识到，信任和信心的理念像一根红针贯穿于各项案文和建议。我们可以看到，“信心和安全是信息社会的主要支柱”。WSIS行动方面5的主要任务亦包含“树立信心并提高安全性”。

在目前开展的WSIS后讨论中，2014年有关该行动方面的推进方报告提出的主要关注领域之一（引言来自内容提要）指出，“加强信任框架：提高数字设备在网络安全领域的信任水平并在公众和私营组织之间打造令人信任的环境是面临的关键挑战。公民对数字服务和互联网的信任水平必须提高。”[3]

由于信任是信息社会的核心因素，它与数字世界各方面的相关性一目了然。因此，尽管《探寻网络和平》的重点在其它方面，该书包含一篇有关信任及其在社会中无处不在的作用的长篇大论。[4]作者强调指出：“信任和信任度是人类存在的根基”，是所有社会交往的基础，它帮助人们应对当代生活中的高度不确定性和复杂性，从而降低了人们认识到的风险。他的分析概括了当前有关该社会生活中心理念的各种文献观点。由于该书依然方便获取，对其研究的一般性参考便足以满足需求。[5]

信任和信心在很大程度上同义，但信任更多指人与人之间的关系，而信心则指人与非人实体或机构之间的关系。对于我们的主题，后者将包含数字设备和以硬件、软件、网络、基础实施、应用和处理程序形式出现的产品。因此，本书选择“信心”作为核心术语，不像术语“信任”那样突出个人的期待和内在的感受。

---

3 WSIS+10/4/2号文件

4 Jacques Bus，信任的必要性：信任的理念及其在社会中的作用，《探寻网络和平》，第17页。

5 主要被引用的作者包括O’Hara、Luhmann、Hardin和Fukuyama。

如上文所述，信心是数字世界正常运行的关键前提条件。但最近对快速增长的数字世界产生影响的事件严重动摇了信任和信心。因此，大谈网络危机毫无言过其辞。

产生并造成该危机的综合因素显而易见并可轻而易举地罗列如下：

- 人们越来越担心，网络空间日益军事化，从来没有那么多国家发展攻击性军事能力，不仅针对军事目标，而且实际上是针对对方的基本民用基础实施和民用生活，由此产生不可控制的外溢效果并使数字军备竞赛难以禁止。100多个国家目前正在以毫无约束以及危险的战略对等游戏方式建设其数字攻击能力，对ICT能力的恶意使用已明确阐述在相关法则中，以此作为实现军事和政治目标的手段。这些担忧不排除自我防御的合理需求；

- 虽然调整国际法以满足数字时代的需求并确定数字技术恶意使用的限制已成为当务之急，但是人们更加担心的是，目前旨在拟定这些规范式手段的工作与其说推动了网络和平，不如说已将在各国军备中大规模纳入网络武器合法化，使这些武器的实际部署成为战略规划的正常组成部分；

- 至关重要的民用基础设施受到国家或非国家力量的攻击，无论是否在合理的军事活动的前提下，还是出于犯罪目的均令人堪忧；

- 在所有这些活动中采用的规则和行为模式的不确定性需要标尺和指示以便停止网络信心的损伤并重建信心。这一不确定性在过去十年间进一步提升，因为，制定可广泛用于大量应用的通用协调准则的规范工作止步不前；

- 前所未有的复杂技术环境具有多种可能性，对于互连互通的世界而言，也将意味着新的薄弱环节和无法预知的后果。数字设备呈指数形式的增长；数字用户日益增多的“应用”造成漏洞的增加；向移动和云应用的迁移为

安全带来隐患；新的恶意软件迅猛增加[6]；给国民经济企业和个人数字用户带来高昂代价的网络犯罪事件比比皆是；国际性犯罪团伙与日俱增，随时并有能力形成网络犯罪或网络冲突雇佣军，所有这一切加深了人们的恐惧。正如上文所述，这些趋势综合起来便形成了新的格局。就算网络威胁尚未形成飞跃式发展，对网络信心的冲击已进一步加深；

- 围绕互联网管理驱之不散的不确定性、能否维护“面向所有人的全球性、可互操作、适应性、稳定、分布式、安全和互连互通的网络”的问题愈发引人关注；[7]

- 由于越来越多的国家政府对接入和内容的大规模审查（网络压制）使人们在享受网络人权时面临日趋严重的挑战；

- 也许目前最重要的，即迫在眉睫的问题是毫无限制地通过技术以大数据搜索方式侵入数字系统情况时有发生。由此产生的数字行业间谍事件之多前所未有，通过某些国家的情报部门在不经核查的情况下进行大规模的间谍活动，跨越国界并厚颜无耻地触犯它国主权和法令。[8]

无疑，恢复信心是数字世界所有利益攸关方必须应对的挑战，因此，希望本书能够为此献出微薄之力，与其他同样寻求以合作和平衡的方式重建信任的机构和组织并肩合作。[9]

---

6 被称为“死亡级”Shellshock病毒迅速出现后在2014年4月造成的Heartbleed恐慌使5亿机器面临危险。在此书编写时，主要漏洞的发现和新威胁出现的间隔日益缩短。

7 2014年4月24日NETmundial利益攸关多方声明。

8 有关这方面的信任的重要性，见Leif-Eric Easley《间谍联盟》，SURVIVAL，第56卷，第4期，2014年8-9月，第141页。

9 最近召开的大规模国际大会亦对信心主题，如，慕尼黑安全大会和德意志电信于2013年11月在波恩组织的第二次网络安全峰会。会间，本书作者之一Howard A. Schmidt参加了会议并做主旨演讲。

本书针对面临的任务采取的做法是侧重于与重建网络信心密切相关的三个问题领域，这些主题目前也是其他公众论坛的热门话题。

阅读了三章后，读者应认识到，本书不是一本教科书，也不是有关该主题全方位的论述或就该问题的各个方面形成的统一权威性专著。该书采用的这种结构旨在将国际电联和世界科学家联合会成员署名作者编写的个人观点汇编起来。除本书开篇的法律告示和免责条款外，应强调指出的是，编辑特别鼓励百家争鸣，以便丰富辩论并确保观点的兼容性。

第一部分反映出对管理网络行为的更加全面规范性框架的探索，使之更具预测性和可计算性。这部分侧重于全球范围内针对信息措施拟定、接受和做法开展的工作以及为增强信任达成一致的原则。与其他各方一样，采用更广泛的法律手段促进网络信心的提高，以协调的法律描述和国际法的合作执行完成这项工作。我们的理想是以循序渐进的方式在规范领域达成贯穿全球和各国的协商一致。

第二部分强调了网络防御、数字系统抵抗攻击和冲突的能力以及减少薄弱环节、缓解或应对攻击或恢复受到攻击损伤的系统能力或挽救由其它网络故障、错误和失败造成的破坏手段。关键问题是适应性[10]。经过对目前和预计威胁的分析，本章开发了多种技巧和战略以助于在当今数字世界中传统攻击与防御竞赛日益升级的时代打破平衡使防御取得成功。

最后一章涉及互联网以及所有其它数字通信的自由与政府干涉之间的平衡：数字隐私与国家安全之间的平衡。面对针对个人和企业通信以及对数据存储毫无限制的间谍手段在无惩罚的情况下铺天盖地地席卷而来，隐私是否已经死亡？该章试图澄清通过外国和国家情报部门开展合法监督的程度和法律基础，特别当此监督涉及组织者以外的国家时，是否需要此类许可。该章还探讨了针对过激行为的制裁。因此，本书希望为通过一个具有约束性的联合框架抛砖引玉，平衡保护

10 适应性是抵抗多样性坚持和恢复的能力。这不仅涉及技术修复。该术语亦隐含整个系统在时间发展过程中的总体力量，与脆弱性互为反义词。见Dhruva Jaishankar《适应性和未来力量的平衡》，Survival，第56卷，第217页，2014年6-7月。

基本权利的合法安全意识，确保数据保护和数据安全的国家法律的有效性以及互联网自由的基本概念。诸如政府对互联网的非法审查等棘手问题需要在国际范畴内开展充分的讨论。

显然，从三个方面探讨的总体目的是防止网络信心受到进一步损伤并使之得到有效恢复和巩固。网络信心危机必须得到克服。

第一章：网络规范

引言

本章总体介绍了在国际层面确定系列网络安全规范、原则和最佳做法过程中遇到的挑战和正在开展的工作。从间谍行为到类似战争的攻击等新的威胁以及互联网的多利益攸关方、跨国和技术特性，为各国提供了一个非同寻常的网络空间：各国政府面对的往往是一个其影响力鞭长莫及的领域，但这又是一个政府必须重点在人权方面向其国民提供保护领域的领域。目前，区域和全球少数地区正在开展综合行动，以制定旨在提供这一保护的通用基本规范。

信息通信技术（ICT）越来越普及，其采用率无论在发达还是发展中国家都有了迅猛提生。一个安全可靠的ICT综合体是树立其推广使用信心的前提。但是，目前的以下这些趋势削弱了这一信任：

- 为国家安全开展的大规模间谍活动，而搜集和存储个人信息成本的急遽下跌起到了推波助澜的作用；
- 在跨境的类战争行动中使用计算机密码；
- 一群看上去桀骜不驯和成分复杂的人构成的胡作非为者团体，其中既有垃圾信息制造者，也有求职的僵尸网络开发人员；
- 而且难以确保对身处受攻击系统以外管辖区的网络罪犯追究责任。

有效应对这些复杂问题需要跨国合作。本章介绍了为此做出的努力，包括联合国（UN）系统及其它政府间组织开展的行动，以及为全球网络安全协议提出的部分基本建议。建立信任措施（CBM）这一冷战时代使用的术语，是这些措施的核心。

本章分为四个部分。第一部分强调了国家参与CBM的必要性、随这些措施而来的挑战和潜在好处。本章随后谈到了联合国对于网络安全相关规范、规则和原则的态度，其中包括面向未来的原则和建议，还涉及国际法对ICT的适用性问题。

第三部分更详细地介绍了适应性问题，全面讲解了网络空间和基于网络的参与者和行动与其它领域的战争和间谍行为之间的相似之处，以及制定全球网络安全条约式法律文件的一套广泛的指导原则。最后，第四部分谈到了联合国的网络安全展望，重点涉及已经确立和建设中的特别机构机制和对国际网络安全和网络犯罪体制作用的长远看法。

再增加一个有关互联网治理的章节不仅具有诱惑力，甚至从多个角度看似乎有其必要性，因为本书将互联网未来的不确定性视为削弱网络信任的显著原因。但是进行中的国际治理蹉商仍然未能弥合政府立场对立的鸿沟，致使国际电联难以形成明确的观点。但是我们满意地看到，近期的审议工作启动了有关2014年4月巴西NETmundial大会通过的NETmundial多利益攸关方声明的蹉商，并取得了实质性进展，尽管该文件被谨慎地描述为不具约束力，但可以看到全球就部分重大基本问题达成一致的端倪。为适应其全球职责，国际电联无疑可以支持让互联网保持其“全球、互操作、灵活、稳定、分散、安全、互连的全民网络”和统一完整空间的所有努力。它还秉承同意精神，支持NETmundial大会宣言确认的内容，即“大规模的随意监视，会破坏对互联网和互联网治理生态环境的信任”。

1.1 CBM在国际网络安全新展望中的作用：全球响应和国际条约的前景

Solange Ghernaouti注

对网络信任的根本需要

互联网在区区几年间就变得无处不在，而且几乎已成为我们日常活动的必须。没有人能够逃脱互联网海啸。利用智能设备，越来越多的服务都走向了非物质化，其中包括与卫生和医药、云计算模式、作为我们前进方向的物联网以及完全适应永久连接和ICT依赖的概念。如今，互联网可被视为一种数字假体，而网络空间则可被视为我们环境的“自然”延伸。作为变革和文明的要素，互联网构建

的正是我们在全球范围内建设的信息社会，构成我们历史的不断演进和人类发明过程的一部分。

数字技术的采用深刻和不可逆转地改变了我们的沟通、行为、思维、娱乐、学习、经商、影响、颠覆、破坏，甚至监测、开战或监视的方式。因此，这一技术不是中立的，因为它带来了直接对我们产生影响的巨大的结构变革。

每一个人都为卫生、能源、供应链、文化甚至安全等私人、个人和专业应用而使用同一个互联网。因此，从娱乐到金融界，以及对于重要基础设施、信息和通信的所有控制系统而言，谁也无法避免对互联网的使用。

互联网及其一系列工具，使我们的社会和在一定程度上整个人类都更快地患上了技术依赖症。我们创建和处理的信息、业务流和互动越来越多。我们消费的信息、计算机的资源和能源空前增长，造成了信息垃圾创纪录增加的后果。

信息技术已成为各个学科和纪念我们的遗产（数字文化遗产、数字公司和个人遗产）的共同点。没有信息技术，知识或科学就不可能存在。同样不可忘记的是，诸如民主、个体认同和国家主权等我们社会的重大根本原则，也在一定程度上依赖于信息技术，或者说会因为滥用或操纵信息技术而动摇。

让我们顺带讲一讲互联网承载的社会媒体和一系列通信工具可以对国家、利益集团或犯罪或恐怖集团所用战略产生的影响。为了毁损名誉、影响民众、团体和领袖、传播误导信息并操纵舆论而部署的互联网，已成为一个受追捧的信息战沙场。与此同时，信息技术使那些有不良企图的犯罪团体能够比以往任何时候都更有效地表达其无限邪恶的想象，并在网络空间发动包括信息战在内的新型战争。拒绝承认这一现实会使自己面对经济竞争力、安定性、国家主权和国际信誉方面不必要的潜在损失。媒体以及主题专家报告的公司遭受大规模数据盗窃、成功的网络攻击以夺扣信息资源勒索赎金的案例不胜枚举。

因此，对网络安全抱有信心，不仅对ICT基础设施及其提供的服务和拥有的信息，而且对其安全至关重要。

走出纷繁复杂，网络空间正在改变保疆守土的概念

当今的世界纷繁复杂，正在走向全球化，而更重要的是，它受到密集使用的ICT设备、基础设施和服务的主导。对关键基础设施和ICT基础设施的依赖及这些设施之间的相互依赖，使社会出现了新的薄弱环节。这种情况增加了巩固、保护和防护我们在政治、经济、社会和个人层面开展重要活动的复杂度。此外，相互依赖的风险削弱了国家和国际一级的整体适应性框架。网络安全，无论我们这样称呼它还是称之为信息社会或数字安全，已经因为人们对政治、经济、法律事务和技术产生的担忧而成为当今的一大问题。因此，对它的管理至关重要，所有涉及寻求安全要求解决方案的各种要素又颇为复杂。

网络空间是一个既虚拟又真实的领域，包括互联网技术、服务和数据。至少对于较年轻的几代人而言，它已成为土地、空气和空间等自然环境的一部分，如同电力与我们的关系一样自然。有人将网络空间看做不断变化的动态国土，或者一块需要征服、掌握或控制的领地。而其他人则认为它是一个权利可以得到表达和声张的领域，一个合法或非法的个人或经济致富的源泉、自由堡垒或战场。实际上，它在不同程度上是所有这一切的综合体，总体反映了我们的政治、经济和社会现实，对实际情况既没有美化也没有丑化。它亲眼见证了技术经济的结合作为其中一部分的全球化现象。

如果在高度连接的世界难以定义领土概念，那么数字领土的安全和防范则更加困难。传统的安全概念已不再适用。由于技术（移动数据、智能装置和云）及其使用（社交网络、电子付费等）的演变，已无可能利用划定周边安全范围的方法封锁信息环境。加密解决方案的使用通常会掣肘业务与易用特性整合和提供可接受性能的工作。加密解决方案依然未得到充分使用，而且人们对这类方案的信心薄弱。2014年4月的“心泣”事件[11]暴露出，纳入网络服务的最广泛使用的解决方案之一的安全落实工作存在重大缺陷。公众再次看到了原本为了提高基础设施强健性和电子交易安全的服务当中存在的漏洞。

11 https://www.schneier.com/blog/archives/2014/04/heartbleed.html

信心的脆弱性

个人、组织和国家在互联网上面对的是此前不熟悉的网络威胁和新风险。网络空间会遇到崩溃、故障、网络犯罪和网络攻击的威胁，而这类威胁目前往往没有引起人们的足够认识和了解，因此很容易造成恐慌。我们不一定能够预测这些威胁将何时或怎样化作现实，或将引起怎样的多米诺效应和触发系列事件，或确定其策划者及幕后人员。

我们可以主要根据维基解密（2010年）[12]和棱镜（2013年）[13]事件确定，数字秘密是不存在的，而且我们受到严密的电子监控、追踪、跟踪、观察和监测。我们必须承认，我们在极大范围内受到监测，而且我们还通过使用某些网络服务或移动电话积极参与其中。我们不能再这样稀里糊涂，不了解我们的个人数据、行为、品味和关系构成了多数所谓免费服务提供商采用的经济模式的基础而且这一信息很受欢迎。

如今，信息技术及其运营商的监测能力，在全球引发了对业内这些技术和主要参与方的信任危机。我们越来越意识到对数字环境和网络安全领域技术和参与方信任的脆弱性。

建立对ICT基础设施的信任需要解决和克服多个层面的困难，其中包括：

- 个人、组织和机构难以了解威胁、确定风险并实施实用高效的风险削减措施，包括难以为打击网络犯罪释放足够资源。
- 难以防止网络滥用和过分使用，并难以对因此引发的事件甚至危机进行管理。

12 http://www.theguardian.com/world/2010/nov/29/wikileaks-embassy-cables-key-points

13 http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/

- 难以向国民、消费者、儿童、我们的数字遗产和我们的保密信息提供保护。
- 还难以表达我们的网络安全需求，也难以确定参与方的权利和义务并保证它们得到遵守。

冲破困难与匮乏：确定真实需要

网络世界带来了新的漏洞并扩大了可利用漏洞的威胁范围。新闻每天都在通过数据盗窃、丧失控制、挟信息资源索取赎金、信件账号攻击、各类诈骗行为和信任错位等信息引起我们的注意。“黑客”、“匿名”或“计算机病毒”等术语目前已司空见惯，网络的烦心事已成为所有互联网用户的家常便饭。

我们必须认识到：

- 现行安全措施的不足；
- 我们的基础设施适应性和我们管理可能出现的复杂危机能力方面的不足；
- 公众和包括终身教育在内的从小学到大学的教育体制内部提高觉悟和制定“国家”解决方案研究方面的不足；
- 每个领域和活动中存在的网络能力和人力资源的不足；
- 赋予司法体制和警察控制网络违法和犯罪行为扩大化的手段方面的不足。

我们应当强调在知识和跨学科、全面、综合和总体网络风险管理方面的不足，以及国家和国际合作与协作、法律协助和公共私营部门以及民间和军事两个领域之间合作关系的不足。

我介绍了脆弱性、困难与不足的概念，所有这些都与复杂性相关。这涉及在工作中考虑到政治、外交、经济、管理、司法和技术及人事因素的复杂性，以确保所有网络风险都得到抑制。众所周知，信息社会必须建立在信任与安全措施的基础上，监控不能与安全划等号，安全需要符合相关法律框架的可靠的监控措

施，而这些措施并不是由技术、提供商和最强大的参与方强加的。还应为技术的全球化和帝国主义做出限定。

必须了解网络风险已成为全球的紧急状况，更加剧了与核设施、核污染或恐怖主义相关的传统风险，因而**有必要**就此采取行动。从根本上讲，必须动员个人和集体意志，制定措施并利用它们应对二十一世纪的安全挑战。

因此，当务之急是释放资源，在洲、地区、国家和国际各级构建组织架构和特设程序，以增加信息社会提供的优势和它们提供的新机遇带来的实惠。与此同时，必须减少负面影响，重点确保我们的幸福赖以维系的国家竞争力和经济安全。

对国际法律文件的迫切需求

如果我们将网络空间视为陆地、空中、海上和太空之外的第五个公共领域，那么它迫切的需要所有国家向对其它四个领域一样开展协调与合作。

我们相信，我们确实需要一项有关全球统一行动的国际协议，以解决网络缺乏安全保障的问题。机构、公司和国家面临着与数据和信息的不当披露、滥用和毁损相关的巨大风险。从宏观角度看，可以认为这些事件不仅对公司竞争力和信誉而且对国家一级的公共安全保障或民主自身造成潜在威胁。

如果我们认为网络空间可以越来越多地被视为全球的经济和军事战场，其中的网络冲突反映出各类政治和经济竞争的博弈，现在是确定哪些内容可以在共同和经批准的基础上接受并为控制这一领域制定出有效的国际法律文件的时候了。没有共识和国际协议，就不可能制定出妥善保护ICT资源（包括关键信息和重要基础设施）、打击网络犯罪和维护基本人权的有效安全措施。这需要所有相关各方和利益攸关方在国家和国际层面做出强有力的承诺。

国家和国际战略的存在不仅仅是为了应对网络攻击并攻击后制定对策，而还应未雨绸缪，避免安全受到破坏并防止强加于人的事件发生。例如这可以通过培养适当的网络安全文化、减少可用来攻击系统的漏洞加以实现。要系统地考虑到

所有可能主要导致异常行为、危机报复或犯罪行为的因素，并整体和全面方式加强辅助和统一措施。

这些问题不能在纯局部的层面有效解决。正如京都议定书[14]是与联合国气候变化框架公约相关的国际协议一样，全球网络安全和网络犯罪议定书应被视为确实减少网络空间风险和威胁的普遍措施。它应为制定有效抵御网络攻击的国家和国际措施提供重要架构，并应包括对可接受和不可接受行为以及必要控制框架的清晰定义。

促进国际对话

早在2007年5月，国际电联即发起了全球网络罗安全议程（GCA）[15]，这是一个协调国际社会对网络安全日益增多的问题做出响应的框架。为协助国际电联制定该项战略建议，成立了全球高层专家组（HLEG）。HLEG的成员由国际电联秘书长提名，适当考虑地理多样性和专长领域，以确保能代表利益攸关多方。HLEG囊括了一百多位世界知名的专家，拥有不同领域的专业特长。[16]这些专家包括国际电联主管部门、成员国、业界、区域和国际组织以及研究和学术机构的代表[17]。2008年11月，国际电联[18]发布了《全球战略报告》[19]。该报告包括五个工作领域内的战略：法律措施、技术和程序措施、组织措施、能力建设和国际合作。GCA为开展高效的国内和国际措施，鼓励各国制定国内网络安全计划和开展国际

---

14 http://unfccc.int/essential_background/kyoto_protocol/items/1678.php

15 http://www.itu.int/osg/csd/cybersecurity/gca/index.html

16 http://www.itu.int/osg/csd/cybersecurity/gca/hleg/members.html

17 挪威法官Stein Schjolberg担任了HLEG主席，Solange Ghernaouti为组织机构和能力建设两个工作领域的共同领导人

18 http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html

19 此外，2008年，国际电联创建了国际打击网络威胁多边伙伴关系（IMPACT），一个致力于提高国际社会防止、应对并响应各种网络威胁的国际公共-私营举措（www.itu.int/osg/csd/cybersecurity/gca/impact_index.html）

合作提供了重要的架构。应将其视为向确定全球网络安全方法迈出的第一步。自此，在全球范围内开展了大量有关网络安全的对话[20]。

“全球网络安全和网络犯罪条约：致力于网络空间的和平、公正和安全”的建议源自长期的国际合作[21]。

起草服务于国际社会的全球法律文件

为有助于满足当前管理网络风险及打击全球网络攻击、网络犯罪、滥用或不当使用互联网的普遍需求，我们致力于确定以有效的国际对话和合作为基础的国际网络安全新愿景的必要性。在此过程中，我们旨在促成更加和平、公正且安全的网络空间和物质世界。此举可形成一项或一系列有关网络空间的全球条约。

这样一种或一系列在联合国层面上有关网络安全和网络犯罪的国际条约应成为网络空间的和平、公正和安全框架且应有助于制定从任何角度发现网络威胁的全球战略。努力制定联合国网络空间条约的进程应在出于不同经济发展阶段的各国中形成对网络安全各方面问题的共识。

所有利益攸关方须就何为网络犯罪、网络恐怖主义及其他形式的网络威胁达成共识。这是制定统一各种网络安全措施的国内和国际解决方案的一个前提条件。此外，共识还将协助弥合发达国家与发展中国家各自对网络安全的认识差

---

20 更多信息可查阅ICT促和平基金会的“ICT相关进程和活动基础性研究、对国际和区域安全的影响”。请参见：http://ict4peace.org/baseline-review-of-ict-related-processes-and-events-implications-for-international-and-regional-security

21 2009年，Schjolberg法官和S. Ghernaouti教授以一本小册子《全球网络安全和网络犯罪条约：致力于网络空间的和平、公正和安全》的形式发表了第一项国际条约建议，请查阅（www.cybercrimedata.net）。在沙姆沙伊赫的互联网管理论坛会议期间介绍了该建议：http://www.intgovforum.org/cms/2009-igf-sharm-el-sheikh。亦请参见Ahmad Kamal所著《网络空间法 – 谈判邀请》（联合国培训研究所，2005年）。在撰写该书时，Kamal大使是PMP的成员。联合国培训研究所（UNITAR）是一个联合国机构。

距。因为网络空间的犯罪行为是全球性质的，需要在全球统一立法，实现国际公正，开展警方之间的合作以及实现这些目标的真实意愿。

联合国层面的网络空间条约应确定通过互联网和网络空间实施的破坏和平与安全的严重罪行无论是否可根据国内法加以惩处，均属于违反国际法的犯罪行为这一原则。我们坚信，网络空间内的最严重罪行应根据国际法进行界定和处理。

在此值得注意的是欧洲网络犯罪公约（2001年）理事会，该公约于2004年7月1日最终生效，这是打击网络犯罪历史上的一个里程碑[22]。该项《公约》只是区域性举措的一个示例，许多国家更倾向于将其作为一种参考，因为它只是且将一直是一份欧洲法律文件。也就是说，需要在联合国层面的全球框架内制定一项或一系列包含该《公约》中已广为接受的标准和原则的条约，但另行增加一些重要条款[23]。事实上，正如国际电联-高层专家小组战略报告中已经明确阐明的那样，相关措施涉及到法律、技术和程序方面的因素，这些因素取决于组织结构、有效能力和国际合作。

有关全球条约的协议将视为HLEG报告的一个后续和国际电联全球网络安全议程举措向前迈出的一步，该举措鼓励各国制定国家网络安全计划并促进国际合作。一项全球条约应使它们为此做出承诺。

未来愿景

建设一个安全可靠的网络空间需要多种资源和技能。这样一个项目将不仅基于专用技术和管理程序以及可在国内执行并在国际层面相兼容特定法律框架，还基于各种为国际所认可且核实的管理和控制手段。

---

22 http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp

23 很多国家并不接受一些标准和原则，特别是《公约》第32条中有关在获得同意或公开可得的情况下跨境获取存储的计算机数据的原则。必须尊重这些国家的意见（来源：《HLEG主席的报告》，国际电联，2008年）。

如同1948年《国际人权宣言》[24]那样，国际社会还需确定、通过并广泛认可某些基本原则。

鉴于各国国情、文化以及经济政治利益存在差别，对这些已被普遍接受的价值观继续定义绝非易事。全球条约的制定将毫无疑问地是一个漫长的过程。这也是为何现在应急迫启动一项机制，促进国际对话，以便在与涉及到的全球利益的紧迫性相称的时限内结束对话。

尽管在起草这样一份条约方面会遇到困难以及我所举的《世界人权宣言》例子不幸所示的那样，条约可能不会总是得到遵守，但这将会形成与（个人、组织或是国家）恶行对抗的法律文件。此外，它可协助避免背离普遍价值观，或至少突显分歧并在适当时通过法律渠道进行补偿。

一种“网络技术非扩散条约”可能并不足够，但它将把网络空间和信息技术降低到可作为武器的军事工具的地位。但是，军用和民用的界限并不明确；使用了相同的技术，且互联网对于任何人（从最年轻的用户到最年长的用户）均是相同的。

有人可能将其与1968年的《不扩散核武器条约》[25]相比，尽管在施行方面困难重重，但该条约所带来的益处已不可争议；该条约在防止2011年3月（并非军事行动引发的）福岛核灾难发生方面毫无作用。另一方面，如同国际原子能机构（IAEA）这样的组织架构已在协调灾难监控以及发生灾难后制定安全措施方面显示了其价值。对于网络空间，应存在一个同样的架构，以促进对信息技术安全、可靠且和平的公共使用。

---

24 http://www.un.org/en/documents/udhr/

25 《不扩散核武器条约》，1968年7月1日在伦敦、莫斯科和华盛顿开放签字：http://www.un.org/en/disarmament/instruments/npt.shtml
（联合国裁军事务办公室（UNODA）：http://www.un.org/disarmament/
联合国裁军研究所（UNIDIR）：http://www.unidir.org/html/en/home.html）

当然，这种与核武器和核电站略显鲁莽且有限的类比并不能掩盖全球性和整体性解决网络空间安全问题的必要性。这些问题说明了通过一项（或一系列）认可军事和其他相关方面的条约的合理性。

各种罪犯均可从网络空间得益，这些洗钱或贩卖人口等犯罪活动既影响到军事领域，也波及民事领域。但是，在这些具体考虑以外，在网络空间不遵守人权可以接受吗？

互联网和网络空间已在全球层面上成为文明的组成部分，这是我们作为一个组成部分留给后代的传承遗产。为此，共同确定我们希望推广并希望在国际上得到尊重的共同价值观并采取监督机制，确保这些共同价值观得到尊重是我们个人和集体的职责所在。

树立信心的措施

在数字链条中，每一个参与方都构成一环且每个国家均可在网络安全和网络信心方面发挥作用。安全是昂贵的，数字安全和信心匮乏亦是如此。当前，总体而言，数字安全的费用主要由用户和社会承担，部分是因为需要警察和法官打击网络犯罪，部分是因为网络攻击、数据泄漏和网络间谍行为造成的经济动荡。所有这些均可导致企业倒闭，公共形象受损、客户丧失信心、丢失市场份额及丢失工作等后果。

网络空间不应成为战场或有组织犯罪泛滥之地，这也是我们为何必须坦诚并真诚合作，寻求为当代和后代开发一个可以信赖的网络空间的途径。我深信，通过一项国际条约—一份网络空间中真正的人（以及妇女儿童）的权利世界宣言可以实现这一目标。这样一份条约可有助于树立网络空间的信心，前提是在全球个人、组织和国家层面有遵守该条约并形成将其考虑在内的各种做法的意愿和承诺。

尽管意识到这样一种承诺及另外制定一项国际条约的局限性，其主要有利因素无疑将是宣传确保安全和树立信心的意识。

在考量此种条约的树立信心整体方面，国际对话的结果可成为：

- 真正的提高认识，用于交流，用于宣传网络空间和物质世界安全和和平问题的工具；
- 一项鼓励经济和组织参与方（包括警察和司法领域）通过优秀做法的参考工作；
- 开发提高数字信心、强化公正机制并打击网络犯罪的服务和技术的起始点；
- 协助确保互联网上最低限度的安全，降低全体人民需要忍受的网络暴力水平的工具。

结论

该是务实地保护我们的数字遗产并使其发展壮大，为保障经济安全、就业和竞争性做出贡献的时候了。这些只是民众需求和利益的一小部分，无需坚持尊重其基本权利，而这些最终与可定义的不同重要性的个人、组织和国家安全相同。

团结在一起，我们就会更强壮，实现凝聚力强且一致的安全措施。不能再分割地保护数字领域，因为（生物和电子）病毒并不承认国境。网络攻击亦是如此，它们可横扫多国基础设施，包括那些我们传统盟友和邻国所有的基础设施。

保护基础设施，发展恢复能力，打击网络犯罪并强化国家对于网络安全和网络保卫的立场是当前一个消息灵通的网民应要求开展的活动，以实现一个持久的信息社会。

群众的智慧告诉我们，保护我们免受雨淋之灾的屋顶是在天气晴好时修建的：让我们行动起来，以免亡羊补牢。

等待脆弱点自行消失，让威胁自我成形将是幼稚和危险的。我们需要积极强化网络安全，以避免我们的信息资源、知识、知识产权和个人数据被掠夺，同时也避免某些参与方（无论是合法还是犯罪组织）力量和控制力不协调地增长。

如果不希望显示出幼稚或过度猜忌的话，应在我们的安全战略中纳入互联网已改变权力行使的方式并在个人、机构和国家之间带来新型冲突这一事实。

1.2 联合国与成员国制定互联网准则、规则和原则的方法：联合国政府专家组报告的评估

作者：Henning Wegener

从前述分析可清楚看出，国际上对国家参与方和其他利益攸关方建立网络空间的普遍秩序及网络空间中负责任的行为准则的意识一直在稳步提高（如果不是呈指数级增长的话）。即使网络空间在初期并不是一个无法无天的空间，一个虚无之所，但对于国家和所有利益攸关方而言，它无疑是一个缺乏全面、协商一致法律框架的地方。长期的任务曾经且现在也是不断形成有利于制定普遍规范的活跃行为。在完成此任务的过程中且铭记这一普遍观点，本文稿侧重于近期的联合国活动以及更明确而言，联合国特别政府专家组的工作结果。

自那以后，在过去的几年中，在全球对网络空间进行规范管理的有组织活动中出现了多个亮点：1998年以来的一系列联合国决议；2001年通过的《布达佩斯网络犯罪公约》；WSIS进程；以及各国在规范侵权和损害、刑罚、行政规章以及相关国际私法等民法制度方面更有目的性的立法。但形成共识的观点是，系统且全面的网络规则时代仅仅始于2008年左右。自那以后，国际活动急剧增多，几乎让人混淆的各种举措和进程不断以新型方式形成了有关规范必要性的演进共识。这些新情况数不胜数，难以在一个场合进行分析[26]，将很有可能有助于“迭代，

26 请参考这些会议记录最相关的部分及其各自背景下的文件，此处不再全部列出。

每一步均以前者为基础”的进程。”[27] 其中许多采用了本出版物中其他地方所讨论的树立信心措施或操守准则、谈判技巧等有用工具[28]。

幸运的是，它们已经催生了多份优秀的综合报告，为总结和进一步处理创造了便利[29]。

2013-2014双年度尤其推动了这些发展。除许多其他成果外，该双年度至少诞生了三份对今后影响深远的文件：有关国际法适用于网络冲突的《塔林手册》[30]、有关互联网管理的《NetMundial文件》[31]以及特别是2013年夏最终定稿并提交68届联大的《联合国政府专家组的报告》[32]。本卷中讨论了所有三份标志性文件。本文侧重于最后一份报告，但也视情对其他文件有所涉猎。

由“从国际安全的角度来看信息和电信领域发展政府专家组”起草的2013年报告（因小组的名称而导致报告的名称结构复杂）绝非一份独立的文件。该组的

---

27 A/68/98号文件，第11页。

28 操守准则和树立信心的措施（如某些人喜欢的那样，透明度和树立信心的措施）方面的思考已明确取代了早期对网络空间全面公约这一概念的迷恋，该公约可与1982年的《联合国海洋法公约》相媲美。这样一份法律文件及其制定的障碍越来越被认为势不可挡。网络空间可能比海洋世界还要复杂。数字技术及其使用仍快速演变。制定全球条约将为各国仍然迥异的观点所困扰。条约谈判将是一个冗长的过程，各国的批准程序在时限上甚至无法在最低限度上与填补法律空白的紧迫性及网络冲突的威胁和难以管理的网络损害正日益失控这一日益成为共识的看法相一致。因此，尽管一项网络空间全球条约/法仍是一个首选目标，仍是一个目标概念，但出于现实原因，在当前时刻，在可预见的一段时间内，一种替代性方法更为可取。

29 Camino Kavanagh、Tim Maurer和Eneken Tikk-Ringas “基础性回顾。ICT相关进程及国际和区域安全（2011-2013）”www.ict4peace.org，2014年3月，日内瓦；*Annegret Bendieck，* “Umstrittene Partnerschaft. Cybersicherheit, Internet Governance und Datenschutz in der transatlantischen Zusammenarbeit”，DGAP，2013年12月，柏林。亦参见*Henning Wegener，*“监管网络行为：对行为准则和树立信心措施的一些初步反思”，Erice，2012年8月，可查阅www.unibw.de/infosecur

30 由Michael N. Schmitt 撰写的“适用于网络战争的塔林国际法手册”。该手册由国际专家组应北约网络防御合作高级培训中心的邀请而起草。2013年剑桥大学出版社。

31 NETmundial利益攸关多方声明：http://netmundial.br

32 联合国文件A/68/98

工作及其“[…]继续研究信息安全领域的现存威胁和潜在威胁及为对付这些威胁可能采取的合作措施，以及旨在加强全球信息和电信系统安全的概念”的职责，源于其前身第二个政府专家组所取得的成果及其2010年7月的报告（A/65/201）。它也从一系列由各国政府从伦敦到布达佩斯召开的利益攸关多方会议所确定的发展趋势中获益，政府专家组职责中反映的有关准则和树立信心的讨论在其中占据了中心地位。区域组织的许多磋商进程以及联大、欧盟、八国集团、北约等主要国际组织和联合国区域组织也提供了智力输入。因此，政府专家组报告包括了正在形成中的共同观点以及某些情况下，正在形成的共识。它代替了对现有网络问题不断的慎重反思。与此同时，它也标志着一种新的措施，即一组具有广泛代表性的、几乎来自全世界的专家们正以全新的方式综合正在其他场合讨论的问题。而且，第四批政府专家组的成立确保了该进程的延续性，该专家组由来自20个国家更具代表性的成员组成，以进一步研究报告（A/RES/68/243号决议）提出的建议，将其职责范围拓展至研究“[…]、在冲突中使用信息和通信技术的问题”。国际层面的跟进行动给予它进一步保障：2015年，荷兰将举办一系列重要的网络空间会议，各国政府将进一步促进推动达成正在形成的共识。政府专家组报告发布之后立即于2013年10月召开的汉城网络空间大会，云集了约90国政府并通过协商一致的方式在其《开放和安全网络空间汉城框架和承诺》中认可了报告中的绝大多数建议。尽管如同NETmundial利益攸关多方声明一样，政府专家组的报告并不具有约束力，但它承载了承诺进一步达成全球共识的趋势。

政府专家组报告的最后两章所包含的建议是本文关注的核心问题。它们包括有关国家负责人行为的准则、规则和原则以及有关树立信心措施和信息交换的建议。因为在新的国际网络安全愿景下，树立信心措施的作用属于本出版物另一文稿的主题，此处仅简要讨论后一节。

我们至少应了解这些措施的如下要点：树立信心措施可减少威胁，提高透明度，使得国家行为既可预测又灵活自愿，为参与方（可能包括非国家参与方）和后续行动提供可变性。与前后一致的条约制定相反，参与方可自由通过部分解决方案，并立即独立或与其他志同道合的利益攸关方一起付诸实施。受到国家欢迎的树立信心措施并不需要批准；它们会引发仿效且最具，也至多具有政治约束

力。因此，它们尤其适于促进达成不断演进的国际共识。经过充分协商达成的、拥有众多支持者的一系列树立信心措施，可启动进一步渐进变革并提高敏感度的进程。明确行为标准可激励更多的进取行动。

树立信心措施的概念始于以往欧安会和联合国中的东西方对抗，但现在具有普遍适用性[33]。

政府专家组报告中的建议集中在国际合作、透明度、时限严格的国际信息交换、全天候的早期预警流程、CERT机制、统一法律规定、执法、制度化的对话及其他“实际”方面。为突出优点，它们也强调私营部门和民间团体参与和宣传利益攸关多方理念的必要性。它们植根于早已成为其他国际活动传统一部分的一系列树立信心行为，并从国际电联全球网络安全议程等一揽子推崇全球合作工作的建议中获益，该议程将“[…]用于国际合作的全球利益攸关多方战略框架”和对话推到了顶峰。

许多建议的措施效仿1998年八国集团、2003年欧盟的决定框架或《布达佩斯公约》相关章节中给出的那些建议。其中特别重要的是欧安组织常设理事会近期通过的《欧安组织为降低使用信息通信技术[34]所带来的冲突风险而采取的初步树立信心措施》，因为该组织的东西方成员众多，各国地理分布广泛，因而在理念上常常各不相同。在非政府领域，对树立网络信心措施最为全面和系统的分析莫过于2013年在日内瓦由ICT4Peace所编辑的出版物，该分析以该杰出组织召开的苏黎世大会的成果[35]为依据。

---

33 关于该概念在欧洲及其他地方早期的发展情况，请参见F. Stephen Larrabee和Dietrich Stobbe编撰的《欧洲树立信心措施》一书中Henning Wegener所著《树立信心措施：欧洲和全球层面》，东西方研究所，1983年，纽约。联合国通过的导则复述于联合国A/S-15/3号文件中。对于其他应用，请参见《关于武装冲突中私营军事安全**公司**行动方面的蒙特勒文件》，www.icrc.org或《2010年欧洲外空间活动行为准则草案》，http://register.consilium.europa.eu

34 2013年12月3日的OSCE文件PC.DEC/1106

35 “树立信心的措施和国际网络安全”，www.ict4peace.org

有关准则、规则和原则的建议对于管理网络空间和网络安全的秩序可能更具相关性；因此，需更加详细地对其进行研究。也需要说明案文的缺陷和歧义以及初步分析的记录，从首次分析看，有必要指出悬而未决的指配以及第四届联合国GGE目前的早期工作以及其他网络安全框架内存在的挑战。

这一简要基本规范和原则目录的重要性，在很大程度上源于联合国安理会5个常任理事国以及印度和日本政府代表达成的共识。虽然不具有约束性，但它是一权威性的参考。

许多地区都强调指出，该组做出的有关国际法，尤其是《联合国宪章》完全适用于ICT使用的结论至关重要。这一原则已在此前的多项国际文件中得到弘扬，但从未得到如此明确的阐述。这是一大进步，不过另有两句话立即为这一原则设置了条件，指出需要进一步研究这些规范适用于国家的方式，并可在未来针对ICT的独特属性制定补充规范。

这些解释反映了部分大国之间在全球ICT管理问题上存在众所周知的长期分歧，并在报告的起草过程中采取了必要的平衡行动，并在有关国际法适用性一段后，确认了国家主权对ICT相关活动和国家司法管辖范围内的基础设施的适用性。

正如下一段落所述，对国际法在网络空间的适用性的确认，包括对相关国际公约规定的人权和基本自由权的尊重，这是一项自WSIS以来得到多份其他国际文件强调的原则，对于互联网自由和与政府互联网新闻检查的斗争的未来意义重大。

《联合国宪章》的适用性还延伸至有关维持国际和平与安全、不使用威胁和武力的指令以及防御网络领域武装进攻的基本规定。然而，在开展“进一步研究”之前，报告未涉及恶意使用ICT的问题。虽然肯定了解2011年俄国、中国和其他国家[36]提交的国际信息安全行为准则草案及一份联合国宪章在其有关规范建议领域明确援引的文件，该组不包括与早期版本的下述规范草案相应的内容：“不

36 A/66/359

利用信息通信技术包括网络实施敌对行动、侵略行径和制造对国际和平与安全的威胁。不扩散信息武器及相关技术。”作者将这视为一个缺憾。但提出的规范和原则的其余部分无疑值得称道，并且成为毫无争议的原则。这尤其适用于有关加强打击将ICT用于犯罪或恐怖目的的合作、统一法律行动和执法和检查机构之间开展协作的建议。

报告第23段规定的一系列规范/原则也同样值得称赞：各国必须对应归咎他们的国际不法行为履行国际义务，无论网络滥用行为的归责多么困难，而且不得使用代理人实施国际不法行为。各国应设法确保其领土不被非国家网络罪犯所利用。许多国家通过了这些具有约束力的规范并将它们翻译后纳入国家立法，从而形成了打击僵尸网络运营商和网络犯罪联盟活动的更有效工具。此外，还有望形成国际压力，确保将必要的国家执法措施付诸实施。

最后，案文还包括对私营部门和民间团体的规范性引证，以帮助提高网络安全，包括“信通技术产品和服务供应链安全” 等ICT的更安全使用。根据这一提示，网络安全是一项需要多利益攸关方参与的社会任务，超出了“负责任的国家行为”的责任范围。

除了规范/原则部分以及CBM章节以外统而言之，报告内容当中还有一个通过提出有效但不那么诱人的建议实施能力建设措施的部分，但将其不同部分融为一体显然是一个进步。该报告未能消除但肯定缓解了国家间在未来网络世界管理方面存在的根本性重大分歧。基本理念上的其它分歧，尤其对GGE“进一步研究”早期的广泛共识并着手详细制定解决方案的工作构成了重大挑战。

然而，报告跟踪描述了一系列重要国际大会（伦敦、布加勒斯特、首尔等）以及区域国际组织开展的工作，并提出了一个并行措施：在制定CBM的同时，为网络行为准则确定规范和原则。无论未来采取何种谈判形式，这一方式将使国家的行为更可预测、灵活自愿，并无疑会使国家和非国家以及后续的参与者之间更加平衡：与统一的条约制定相反，参与方将放手采用部分解决方案，并独立或与其它志同道合的利益攸关方一道将它们及时付诸实施。然而，GGE仅达成了部分共识，后续GGE还面临着可畏的挑战。

于2014年7月底组建的专家组选举其成员巴西担任主席，并通过了工作日程和20个政府专家间的工作分工。目前这些工作包括起草或修改其立场文件，并提出相应的草案。该组将于2015年1月再次会晤，以便在同年夏季提交报告。

GGE首要和最为复杂的任务是对有关国际安全和和平的国际法律规则做出详细定义，包括网络领域“武装攻击”的构成、主权在网络时代的含义、网络技术恶意使用（“网络武器”，包括专用于攻击和破坏军事及基础设施资产的恶意软件）的遏制方法及其侵入监管网络的详细定义。我们自网络诞生之日起一直受到这些问题困扰，而且越来越多的国家目前常态化开展无节制的网络军备更加令人忧心忡忡，这主要是因为人们看不到任何对这些通常受到误导的行为施加的法律或政治限制。

本出版物多处谈到的《塔林手册》无疑提供了可与常规国际法律相类比的宝贵的真知灼见和指导原则，但毋庸置疑，它主要是由“西方”法律专家组成的专家组的产物，有必要让它经受更全球化视野的检验。对手册做出的重要评估还显示，基本上以武装冲突规律为出发点的分析，倾向于将网络技术的恶意或军事利用接纳为一个正式选项，即“内容之一”，即使手册的作者已或多或少地明确阐述了潜在使用的限制与方式。豪不奇怪的是，手册虽然措辞谨慎小心，但多方人士依然将它视为“网络战争的请柬”。无疑，适用的方法是提供凸显网络战争基本不可接受性和内在危险性的最高附加说明。

另一项挑战存在于报告中的建议的一般特性。将它们转化为实际行动并详细充实解决方案，在任何情况下都将是极其困难的，而为了实现取得可比成果的管理而接纳各种不同区域进程和广泛的多利益攸关方社团需求，则是难上加难。

在这些情况下，设计可开展热烈磋商和大型谈判的论坛是一项复杂的任务。GGE的报告建议在联合国主持下广泛参与正规制度化的对话，或通过双边、区域和多边论坛以及其他国际组织开展正式对话。这无疑是在向正确的方向迈进，但因过于笼统而无法就未来的工作程序做出快速决策。明智的办法或许是，通过首先就召开论坛会议的标准（包容性和开放性，使广泛的利益攸关方团体能够充分参与，并得到具有ICT专业技能和经验的国际秘书处的支持等）达成一致，以缩小

制度性选择范围。具有全球视野的单一论坛无疑是最为理想的行动方式。此外，初步的区域性行动已经开始，其动能因素也应得到利用。或许可将能够自行制定广泛利益攸关方参与程序和模式规则的自主的国家大会视为一个适当场合。

根据对报告有关规范、规则和原则章节的回顾，我们怀着对作者著作的尊重提醒大家：鉴于联合国环境的政治结构以及在有限时间内达成共识的必要性，他们提供的项目是有选择的，甚至是不完整的。可以肯定，未来的第四届GGE将仔细研究最近提出的附加规范和原则[37]。

安全和网络稳定与和平的核心领域，尤其需要制定更为明确的规范[38]。似乎有必要填补以下空白：呼吁就一项根本性原则达成有约束力的共识，即直接或通过雇佣犯罪对另一国家实施的网络攻击构成了对国际法的破坏；请所有国家做出承诺，只要未受到常规武器的攻击，就不会对任何其他国家首先使用网络武器。各国应当在国家和国际层面支持防止太空冲突的政策，侧重网络防御，对网络攻击手段，特别是专用攻击软件的研发、使用和出口施加限制并使之非法化。应在第26段（e）建议的范围外向重要基础设施提供保护，以便根据各国负责保护其领土内重要基础设施以及禁止对这些基础设施发动攻击的原则，强化国际合作，同时确保跨国数字网络结构的不可侵犯性。目前尚缺的一项原则是，各国负有在网络空间保护其公民的义务。除第23段的建议外，还应明确提出禁止使用僵尸网络和从事其他违规的网络犯罪/战争行动，而且各国有义务在国内实施这一禁令。最后，中立性依然适用于网络时代，绝不能通过中立国的网络实施即使出于自卫目的的网络攻击。

---

37 除GGE报告第27段部分列举的区域性组织的工作外，请见以上脚注6 ICT4Peace工作较早的引证；上述脚注3涉及的Henning Wegener所著的文章；国际电联秘书长有关网络和平的五项原则，2009年通过《关于网络稳定与网络和平原则的埃里切宣言》再版，又再版于《探寻网络和平》第110页。

38 目前计划的第4次GGE会议的职责范围以“冲突”情境为重点。

1.3 国际法适用于网络空间吗?

Gábor Iklódy著

数字时代既带来了重大实惠，也带来了可能引起巨大震荡甚至破坏的多重威胁。我们面临的根本挑战是寻求保护网络空间，使之成为可信任环境的途径，使我们能够漫游其中，充分利用其潜力，并以更加“注重安全”的方式做到这一切。这需要我们在自由和安全之间找到适当平衡。有效的方法是，既不忽略安全风险，也不以它们为借口对民权横加限制。为使诚信得到衡量，必须确保政府机构在防范网络空间恶意活动的工作中，充分满足民主问责的要求。

在本文重点谈及的国际关系中，诚信无论对公民还是国家都至关重要。我们今天目睹的是一种正在进行的网络“冷战”，具有网络攻击能力的先进和资源丰富国家的网络间谍活动和大规模投资与日俱增。

从全方位的现代军事角度看，必须确保网络空间的自由行动能力不受阻碍。这一要求清晰的体现在越来越多的国防战略当中，而这些战略将网络空间视为“一个重要性比肩地面、海上和空间军事行动的新战争领域”[39]。结论很明确：网络空间已成为现代战争的一部分，没有巨大网络部分的参与，就不可能出现较大规模的冲突。过去数年的经验为这一点提供了充足证据。

为使网络空间成为一个可信领域并保持不变，需要营适用造某些公认规则的合作氛围。有关国家行为的国际规范是这种氛围的要素。但尽管它们之间存在明显的相关性，应当强调指出，它们远不是要素的全部。网络空间是一个具有多利益攸关方特性的单一领域，政府在其中仅仅是营造这一氛围的参与方之一。在网络空间营造和保持一个真正公共和私营合作伙伴关系的必要性，比其他任何领域都更为迫切。“私营部门拥有和运行多数网络基础设施，并开发出我们每个人都需要的技术，私营部门是头一道防线，而私营公司和科学界则负责规划政府也将

39 北约的网络防御政策，布鲁塞尔2010年6月8日

在其中运行的未来技术环境。”[40]这无疑不会削弱主权赋予且政府无法逃避的潜在责任。

目前尚没有具体涉及网络空间的协议规定或习惯规范。但这是否意味着网络空间可被视为一个任何规范都不适用的极不规范的狂野西域？这一说法是否说明有必要快速制定一套有法律约束力的规范？这样做是否可行？或者还是以英国外交大臣威廉·黑格的话为出发点：“无论对于作为实施者的个人还是政府[41]而言，线下不可接受的行为线上同样不可接受。”

国际的网络空间法的适用性

专家以较长时间研讨了为传统领域制定的现有国际法律文件是否也适用于网络空间的问题。911事件在一定程度上迟滞了这一磋商进程，当时更多地以反恐战争为重点，但到了2007和2008年间，这项磋商又开始加速进行。反恐的工作重点将许多相关问题纳入了这一重新恢复的网络对话，其中包括：“我们怎样将非国家参与方的行动归咎于一个国家呢？”；“国家应为在其领土上开展活动，并向另一国的资产发动攻击的团体承担什么责任？”；“我们怎样才能合法地对居住在不同国家的非国家参与方动用武力？”；或“能够对破坏力巨大的潜在攻击先发制人地使用武力吗？如果可以，什么条件下才能使用?”。所有这些都是网络环境的热门话题。

制定出确定网络空间遵循的最重要规范并说明违规后果的具有法律约束力的全球性方案，听起来很诱人。但就目前而言，这似乎不在可行甚至必要之列。其中的原因很多。首先，这一领域日新月异，几乎无法就一套全面持久的网络专用规范达成一致。第二，各国在一系列诸如门槛、响应和执法等实际后果的关键问题上观点迥异。因此，试图将我们今天对网络空间的认识以及，同样重要的是，将我们所能达成共识的部分奉为经典，将会使我们身受束缚、适得其反（在法治

---

40 Gabor Iklody：在北约信息保障专题研讨会上的讲话，2012年9月11日，星期一

41 英国外交大臣威廉·黑格2011年11月11日在首届伦敦网络空间大会上的发言。

文化较强的国家尤其如此）。第三，如果法律义务的价值难以在现实中得到确认，那么这种价值就值得怀疑。

军备控制和核裁军等其他领域的经验表明，如果各方之间存在高度的不信任，较易于见成效的办法是首先以小步走的方式逐步建立和巩固信任，要循序渐进而不要一次标定过高，明显地陷自己于被动。核军控方面的经验为我们提供了一些这方面的重要教训。保持联络渠道畅通、提供一定程度的透明度并帮助缓解危急中的紧张关系等措施，都有助于该目标的实现。诸如网络信任和强化安全措施的OSCE工作等双边和区域举措，方向正确，而且尽管措施是在较低层面提出并具有自愿性，但依然反映出达成共识的难度。

这并不意味着现在探索国际对话和合作依然为时尚早。除了有助于为更严格的措施营造必要氛围的CBM之外，还有一些相对容易启动的工作领域。正如Joe Nye所说：“最具前景的国际合作领域不是双边冲突，而是第三方提出的犯罪分子和恐怖分子等问题”[42]。随着时间的推移，较先进（因此也较易受害的）国家的利益有可能向限制犯罪和恐怖集团造成破坏的方向聚汇，从而为他们的取证和控制合作奠定基础。“国家可以首先为在其领土上发动的攻击承担责任，并接受就取证、信息和对策开展合作的义务[43]。”

就国际规范而言，未来显然应同意以关于诉诸战争权（*jus ad bellum*）和开战正当性（*jus in bello*）的现有相关法律文件为基础，并将它们延用于网络领域。这种广泛共识将使我们能够推进工作，并逐一评估现有法律文件当中的哪些规定需要通用解释，哪些需要充实。

在过去近两年当中，国际上就增进对网络攻击等核心问题的了解进行了两次重要尝试。在北约合作网络防御英才中心（CCD COE）主持下，独立国际法律学者和执法人员小组编写的《塔林手册》和联合国IT领域政府专家组（UNGGE）起草的建议都证明，现有的国际法确实也适用于网络空间。因此，问题不是现有法

---

42 Joseph S. Nye：“核裁军为网络安全提供的教训”，《战略研究季刊》，2011年冬季。

43 Eneken Tikk：“十项安全规则”，《生存》，2011年6月-7月。

律是否适用，而是怎样付诸实施。但应当看到，两个组的结论都不具有约束力，也没有获得各国的认可，至少迄今没有。然而，人们贴切的将专家间达成的一致称为里程碑式的共识。

应总部设在塔林的北约合作网络防御英才中心（CCD COE）要求撰写的《塔林手册》[44]，是一份十分详实和要求极高的学术研究著作。它全面研究了法律规范适用于网络战争的程度，反映了参与该组工作的独立专家的观点，但仅此而已。它最多可被视为该组就一系列高度敏感和重要问题开动脑筋而做出的切实努力。换言之，它是在邀请他人参与开动脑筋的过程，而这只是增进广泛共识行动的开始，而不是结束。

如何构成网络空间的“武力使用”或“武装攻击”？

人们对战争行为都有一个基本的认识，但是从法律角度而言，什么才构成网络领域的“武力使用”或“武装攻击”？网络攻击这种非暴力行动能否称为“武装攻击”，或仅在其构成更广泛的暴力行动的组成部分时才能被称为“武装攻击”？对于网络攻击的回应，哪些可被视为合法？合法的回应中是否包括使用军事力量的权利？

“网络战争”一词没有普遍公认的定义。通常，该词用来描述网络空间的敌对行动，“[…]其所产生的影响大于或等同于重大暴力行为。”[45]因此，这不仅意味着进攻性网络手段的部署，更重要的是通过这些手段的使用所产生的影响可有助于我们确定是否已发生了网络战争。迄今为止，尚无人目睹了真正意义的网络战争。我们已领略过针对一个国家或重要基础设施的大面积拒绝服务攻击，或作为单独攻击或作为大规模暴力攻击的组成部分。我们也曾体验过指向工业控制系

44 关于网络战争适用国际法的《塔林手册》。

45 Joseph S. Nye，同上。

统的针对性攻击。“但尚未尝试这些攻击所带来的意外影响和连锁反应，[…因此]，人们未曾尝试过国与国之间的各种网络战争行动和反行动。”[46]

《联合国公约》在禁止武力使用的一般性规定中只有两项例外：一是在第七章中提到的安理会在确定存在威胁和平的情况下允许采取一切旨在恢复和平的行动；另一项是第51条，即当一个国家行使其自卫权时，在更高的层面上认可通过单边或联合力量打击肇事者的固有权利。

在此，我们需要探讨一些一般性问题。联合国安理会若就授权使用武力达成一致通常困难重重。这主要是因为需要“大国”的同意，换言之，需面对安理会常任理事国的否决权。有时很难达成一致，特别是当一个或多个常任理事国为有关冲突的一方时。这不仅是对该程序民主性的挑战，同时也意味着各国有可能将武力使用事件看做一次实质性攻击，由此使他们有理由使用武力应对肇事者，另一个进一步支持扩大使用第51条的现象是各国为防止恐怖袭击而行使的自卫权。

如果进攻者不是一个国家，而是非国家且貌似国家的一方将产生怎样的情形？联合国章程的编撰者有意将“武装进攻”的概念留给其各机构和成员国进行解释。同时，第51条措词宽泛，即使攻击者为非国家力量，各国在受到攻击的情况下仍有机会进行自卫。联合国安理会和北约就9/11攻击做出的回应决策可谓重要范例。

但非暴力网络行动能否构成“武力使用”，甚至升级为“武装攻击”，还是依照联合国章程编著者的逻辑，这些术语仅适用于军事力量的使用？多少年来，人们曾多次尝试定义构成武力使用的政治和经济威压，但几乎未曾取得成功，因为很多人担心，承认将非暴力，非武力行为作为回应中的武力使用可能成为促发因素，让潘多拉盒子敞开大门。然而，仅注意所使用的手段或只关注所造成的影响是否就是正确的做法？

---

46 同上

回顾历史，政府不太关注的是事件中所使用的具体手段，而更关注这些手段的使用所造成的影响。在9/11攻击中，民航飞机肆意用来造成最大的伤害和人员伤亡。因此，可以得出的经验法则是：如网络攻击导致的灾难性后果可与暴力活动相提并论，则网络攻击应被视为武力使用，甚至等同于军事进攻的武装进攻。从这个意义上来说，进攻是否来自空中、陆地、海上或空间并不重要，而进攻造成的影响则越来越多地决定了人们对进攻的看法并由此为受害国提供了自卫的权利。叙利亚是另一个例子。杀伤性化学物质的释放通常被划分为非暴力行动。但针对叙利亚当地民众的使用造成大规模人员伤亡，因此可以视为武力的使用。

2012年沙特Aramco石油公司的情况更难以断定。公司3万多台计算机中所存储的数据荡然无存，毫无疑问， 公司因此受到严重打击，即使数据得到部分恢复也会付出高昂的代价。尽管事件的影响难以消除，许多专家在将其称为“武装攻击”时谨慎措词。

那么，如何确定一个事件是否超越了“武力使用”的界限，并可能升级至“武装攻击”？在人们确定应否做出反应前需面对多大的伤害、痛苦和担忧？

不幸的是，对此问题没有明确的答案。上述一般性看法就是真理。即，如进攻的后果与传统攻击一样严重，则可以被视为武力使用[47]。为此，在攻击造成的危害程度和伤亡数量之间存在明显的关联。造成大量伤亡的事件显然进入上述范畴，而使一个国家主要行业陷入瘫痪的进攻亦不例外。但我们是否可以为此制定一个界限？回答显然是否定的。决定能否称之为“武力使用”或“武装进攻”的事件永远需视情况而定并应考虑到多种不同因素。据此，判断是否会升级为战争行为与其说是军事或法律的判断，不如说是一个政治判断。做出这个判断全凭细节。即使对于恐怖主义，在经过9/11的恐惧后，人们也会具体问题具体分析。例如，如果一次恐怖主义进攻针对无辜百姓，死亡人数超过3000，我们就可以毫不犹豫地将此称为武装进攻吗？这是否意味着，如伤亡低于3000这一界限值，该攻

47 见所谓Schmitt标准，有助于国家决定网络进攻是否为战争行动的一套规则。

击则不被视为武装进攻？除其他方面外，这是我们要传递给潜在攻击者的信息吗？我确信并非如此。

对网络行为的划分可采用多种多样的方式。普遍接受的一种模式是信息安全三要素（保密性、完整性和可用性）。该模式的开发旨在确定信息技术的问题和解决方案[48]。完整性攻击旨在破坏控制系统的正常运转（如Stuxnet病毒）；可用性攻击（摧毁空中交通控制或搞乱军用网络，如Georgia）产生伤害，其影响堪比暴力攻击。因此，这些攻击可以轻而易举地超越武力使用界限。另一方面，保密性攻击（通过网络手段开展间谍）可造成巨额损失（据估计，仅在美国，知识产权的盗用每年达2500亿美元），但这种攻击属于不同类型， 通常采用外交方式予以解决。

作为第二古老的专业，间谍无处不在 – 有时甚至出现在最紧密的盟友中。“从宏观来看，有时，每个国家都必须平衡行动自由最大化与伤害最小化之间的冲突。监测恶意行为的总体目标就是尽可能减少危害，即防患于未然。”[49]在防止和早期发现恶意行为以便防患于未然比处理后果更加重要的时代，信息变得尤其重要。因此，让国际关系完全摆脱网络情报是完全不现实的。然而，“[…]可以建立一种针锋相对的程序，以便为减少实际损失制定规则。”[50]

降低界定武力使用的水准是遏制间谍蔓延的一种手段，也是当今许多国家的想法，尤其是欠发达国家。更为发达国家的情况尤其复杂。它们一方面通常是间谍活动的主要目标，另一方面，这些国家更希望掌握更大的运筹帷幄的余地，因此通常不愿意降低水准。希望获得更多反击自由且拥有必要能力的国家则更有兴趣缩小“武力使用”与“武装进攻”二者之间的界限差距。

---

48 见Darril Gibson“了解安全性三要素”，2011年5月27日，*Pearson*。

49 采访思科网络安全负责人Kah-Kin Ho。

50 Joseph S. Nye，同上。

对网络进攻的回应

如一个国家遭受严重的网络攻击，最直接的反应目标就是停止攻击并对此予以反击，与此同时尽快重建遭受破坏的系统。因此，保护人身安全并恢复重要的数字网络成为重中之重。在多数情况下，人们的目标是避免冲突的升级，除非在不得已的情况下必须使用武力遏制并防止进一步的攻击。

涉及利用恶意软件破坏空中交通控制造成撞机或坠机以及大量伤亡的重大网络攻击可被视为需要做出适当响应的武装攻击。但即使在此情况下，根据国际人道主义法律，这些响应必须满足一些重要的标准。响应必须合乎情理，理由充足并必不可少，同时应遵循区分攻击性质和适当防范的原则。至于响应内容，可以采取多种形式，既可以是军事或网络响应，也可以在联合国披露攻击者姓名令其丧失颜面或做出外交响应，或施加制裁。同时，也可能根本不做响应。

对现实情形的模拟明确显示，由技能高超且财力雄厚的对手发动的大规模集中式网络攻击所造成的严重破坏是无法通过网络手段阻止的。如果网络攻击是更大攻势的组成部分，结果则更为显著。虽然网络自卫措施有助于恢复遭到破坏的网络并为举证或早期发现助一臂之力，但并无法消除威胁。必须依赖于各国工具库中的其他手段。

先发制人行动

与网络空间情况密切相关的另一个问题是，当时间和空间因素在很大程度上没有了相关性后，预警几乎没有时间。从计算机检测出可能受到恶意软件攻击到通过制胜手段阻止攻击之间的时间可能仅为几毫秒。因此，有效的防御需要设定自动响应，但这本身就存在着多项挑战。鉴于攻击的速度，政府是应该等到大规模网络攻击（相当于武装进攻）（旨在捣毁重要指挥控制中心的针对重要基础设施的独立行动或暴力行动的组成部分）发生时才做出响应，还是允许先发制人。如果是这种情况，政府应何时干预以防止破坏性网络攻击的发生，参与自卫的条件是什么？

许多法律专家已确定了一个所谓“最后可行的机会窗口”标准，错过这一行动时刻就将使有效防御严重受挫。Tallinn手册得出结论，国家可采取自卫手段，“[…]当攻击者明确要发动武装进攻时，受害国将丧失有效防御的机会，除非采取行动。”[51]

有时，采用网络手段被看作是更糟糕的选择。发达和强势国家在战略使用网络武器方面更胜一筹，致使对手改变行为或停止某些危险活动。如能避免战争，可以提倡这种做法。另一方面，这样做亦可造成其他国家倍受威胁。人们担心，网络武器竞赛由此将随着各国的相互追赶或雇用行为日益普及。同样令人堪忧的是，高级网络攻击使用的密码通常会在网络中遭到非国家力量的截获。

归因需要何种等级的证据？

确定网络攻击的肇事者，并举出足够可信的证据常常被认为是一个主要问题。该问题实际上使把某一网络操作认定为“武装攻击”变得几乎不可能。毫无疑问，问题确实存在，对其视而不见是错误的，但也不应对其过分夸大。更加合作的国际环境、改善的情报交流和网络技术社区，以及最后但并非最不重要的—技术的演进，都能够改善当前的情况。

如果要求提交的证据既清晰又有说服力，达到向法庭提交的水平，那么归因问题的难度是极大的。但是归因是一个相对的说法，我们应该接受这样的事实，即，当网络攻击发生时，找到“冒烟的枪”几乎是不可能的。充分和绝对的确定性极少能够（如果不是不可能的话）在攻击后的几个星期内建立。依赖从不同领域收集到的（情报和技术等）逐渐增加的证据是比较切实的期待（即：存在所谓“间接证据”）。归因也是现实政治中的一条相对术语。与将攻击来源归于一个肇事者的难度相关的关切程度同伤亡的数目是相当的。换句话说，伤亡人数越多，政府受到的要求坚决回击的压力就越大。

---

51 Tallinn用于网络恶意事件的国际法手册。

需要强调的是，归因不是将某行动形容为武力攻击。让我们回忆一下北约对9/11事件的反应，在24小时内北约历史上第一次引用了第5条 – 集体自卫机制。北约当时的说法并没有援引对国家恐怖行动的可归因性。它仅仅询问对美国发起的攻击是否是在海外指挥，这个用于确保集体自卫条款不用于其本国公民的一项要求。人们的结论往往是：由于归因问题，威慑不能用于网络空间。无需置疑的是，当展示力量足以威慑潜在侵略者时，这是部分正确的—尽管不是传统意义上的。但当威慑可以消除攻击的效果，而不是通过报复常来花费时，威慑是有作用的—正如弹道导弹防御使得攻击无效或成本过高一样。“如果防火墙足够坚固，或自我实施（self-enforcing）的前景积极的话，发起攻击的吸引力将减弱”[52]。

非国家角色

在网络空间中，多数情报评估一致认为仅有有限数目的国家目前有能力开展复杂和持续的攻击，并造成严重的损害。同时，如国防部副部长Lynn所认为的[…]“尽管国家的能力最为强大，但非国家角色更有可能发动灾难性的攻击”[53]。

在这里，我希望暂时中断一下，以便对两点作出严格区分：一方面是间谍行为，另一方面为毁灭性中断和破坏行动，尽管它们在技术上十分相似。毫无疑问，尽管应当尽最大努力使间谍行为和盗窃宝贵的政府和产业信息的行为难以实施，但消除造成大规模破坏的攻击行动无疑应当作为优先任务。

好消息是，正如对核问题的态度一样，有能力的国家多数以理性方式思考，会尽量克制，不跨越引发强烈回应的关键红线。为了使各国理解这一局面，它们应该首先了解红线已经被划出。因此，此类信息应当清晰和明确地传达给各国：破坏性的攻击会引发国家或集体的反击措施，工具箱里的任何东西都可能被

52 Joseph S. Nye，出处同上

53 国防部副部长Lynn 在第28届全球安全年度国际研讨会上的讲话，2011年6月16日，巴黎。

用[54]。第二，我们仍有余地，逐渐发展如前所述的信任建立、冲突降级措施和一些基本的规则—同样也汲取核问题领域的经验。

然而很难期待“流氓国家”能以理性方式思考，它们具有建立攻击性网络能力的野心，并且为了得到这种能力投入巨大。震慑它们比较困难—正如有些从事不稳定地区研究的分析家提醒我们的—对于特定国家和文化，“双输”的结果完全是一个可接受的选项。

然而，最大的担忧潜在地同非国家角色们相联系。当制造伤害的能力同不计一切成本制造伤害的意图结合起来，终极噩梦就来临了。我们还没有走到那一步，但对于恐怖分子使用网络武器的恐惧尚不属于不可能王国。在互联网上有“即刻可用”的工具，这些工具可供进一步开发；有破解（0-day）黑市和网络雇佣兵以及能力出众的“待雇黑客”小组，可以购买他们的服务来窃取金钱和产业秘密，或使用实际上几乎相同的工具和技术，引起大规模的网络中断。

1.4 联合国有关互联网安全的愿景

作者：哈玛德·图埃

本节介绍联合国关于网络安全愿景的基石。ICT在现今的发展中扮演了核心角色，这些系统的安全越来越成为关键问题。发达经济体广泛依赖于ICT，其中包括关键性基础设施，这些使网络安全成为许多国家的首要问题。对于发展中国家来说，则有独一无二的机会建设内在安全的信息基础设施并实现跳跃式发展。

然而，网络安全还远未成为既定的全球性优先问题，往往未纳入国家ICT和发展策略中。通过将网络安全纳入发展计划，并将其视为“达到目标的手段”而不仅仅是目标自身，联合国正尝试改变这一图景。本文聚焦当前对全球网络安全的需求、联合国对网络安全发展的愿景、现有的相关机制以及进行中或规划中的网络安全举措等。

---

54 Gabor Iklody 在AFCEA全球情报论坛的演讲，布鲁塞尔，2013年12月10日至11日。

对全球网络安全的需求

在发达国家，ICT具有渗透几乎各个行业的“改造能力”[55]，并在引领发展中国家的快速转型。无处不在的计算机网络也有其代价—它使得整个经济部门更易受网络攻击的侵害。这些威胁的范围广泛，从轻微犯罪到窃取一张信用卡，直到全球性的协调攻击（如Conficker病毒）。犯罪肇事者常常化名操作[56]，使指控变得更加复杂。此外，传统法律的执法单位面临网络领域资源有限的挑战，面对的攻击者常常属于另外的司法管辖权治下。这些因素在一个复杂领域相互交织，给所有国家提出了技术和政策挑战：必须保护关键信息和个人资料的完整性、保密性和可获取性。

有些发达国家已经将网络安全作为优先国策[57]。面对在设计时以开放而并非安全为目标的网络，各国正在投入巨大资源确保网络安全，2014年的投入金额据估计多达700亿美元以上[58]。然而，这些投入压倒性地集中在高收入国家，考虑到攻击者不断地瞄准新的产业，因此这些投入尚显不足[59]。

由广泛的、范围从经济收益到政治激进主义动机驱动，网络威胁可以从几乎所有国家产生，并影响大量经济部门。没有哪个实体—或国家—可以以有效方式应对。这些因素增加了全球协调一致努力应对网络安全问题的紧迫性。

---

55 国际电联秘书长哈玛德·图埃的演讲 — 非洲转型高峰会，国际电信联盟，2013年10月28日。网络，2014年7月24日。

56 Nazli Choucri、Stuart Madnick和Jeremy Ferwerda，信息技术促发展（2013）“网络安全的制度：国际响应和全球必要性，信息技术促发展”DOI：10.1080/02681102.2013.836699

57 “转折的网络安全政策制定：分析新一代互联网经济的国家网络安全战略”，经济合作和发展组织，2012。

58 “保卫数字边界”，经济学人，2014年7月12日。

59 “黑客公司”，经济学人，2014年7月12日。

还有另一个更加广泛的有关网络安全的需求，它超出了传统的“网络武器”或“网络攻击”的说法。一种更为全面的方式既可保护知晓权，也可保护网络空间的隐私权，两者均是国际条约认可的基本人权。因此，除了发展经济并增加在新领域的互信之外，使网络变得更安全将能保护个人信息免遭未授权的侵入。由于这些原因，国际社会应加大力度将网络安全作为优先问题。

联合国有关解决网络安全问题的方式以四项支柱为基础：（1）保护各组织自身的网络；（2）在制定国家网络安全政策及其实施方面，向成员国提供（协调一致的）帮助[60]；（3）在发展项目中纳入网络安全问题；（4）针对网络安全、网络犯罪和保护网络人权—特别是保护隐私和获取信息等问题，促进国际合作。本文主要聚焦后三项支柱，因为它们与本刊主题“追求网络互信”最为相关。本节将对这三点进行逐一介绍。

联合国认为这三项全球网络安全优先任务具有某些共性原则。首先，为了有效保证信息技术的安全，联合国保证采取一项全面的、“整体型政府”的和利益攸关的方式。联合国的内部工作应遵循这一原则，并向“机构间合作”的方式过渡。在后一种方式下，相关实体协调其工作，从而使效率更高且能避免重复工作。第二，鉴于信息技术多样快变，联合国建议采用更为灵活的和时常更新的政策，这些政策应尽量做到技术中立。最后，安全措施对其他全球优先任务的影响，如保护个人隐私等，应作为制定政策的优先对象。

对成员国的协助

联合国机构在ICT领域帮助成员国的历史悠久。然而，直到最近，网络安全才被看做一项优先任务。在网络安全和网络犯罪联合国整体框架制定并在2013年得到认可后，联合国系统行政首长协调委员会[61]就向成员国提供协助的某些共同原

60 在各机构的职责范围内，并尊重国家主权。

61 参见行政首长协调委员会（CEB）2013年第二次例会会议报告（2013年11月）。

则达成了一致。该框架是联合国内部协调努力应对网络安全问题的第一步，在下阶段将继续跟进解决[62]。

将网络安全问题纳入发展项目中

ICT的发展（网络安全是其一部分）已被普遍视为从传统发展领域独立出的一项单独优先任务，于是，其他领域与其相比或许被认为更为急迫和必要。然而，ICT的发展与可持续发展的整体主题并不冲突：技术发展本身不是一个目标，相反，它能使各国，特别是发展中国家和最不发达国家（LDC）得以加强在广泛经济领域的能力、改善社会福祉和人们整体生活水平。通过技术改善洁净水资源、教育机会和可负担的医疗保障等的获取以及促进经济增长和增加/促进国际贸易，这样的例子比比皆是。

因此，将网络安全纳入现有发展优先任务中势在必行：安全和可信赖的系统提高了其得到使用的可能性。在这方面，发展中国家和最不发达国家有一次难得的机遇之窗：通过建立内在安全的计算机网络它们可以跨过已经经历过攻击的系统。在网络安全问题上的投资可以弥合所谓“数字鸿沟”。联合国系统可以扮演关键角色 – 利用其现有的国际机制，将网络安全纳入主要项目之中。

另一项全球优先任务是防止网络冲突的出现和升级。尽管截至目前各国在应对网络攻击时表现出了克制态度[63]，但不能认为这种态度在未来中远期能够继续。联合国裁军研究所（UNIDIR）通过开展研究和教育工作，寻求为防止冲突升级贡献力量。该研究所“作为桥梁，帮助形成必要合力，以应对和减轻国际、区域和地方层面的不安全状况的影响。”

---

62 参见有关“联合国网络安全机制”一节。

63 Valeriano, B. 和Maness, R. C.(2014) – 对手间网络冲突的多样性，2001-11，《和平研究学报》，doi:10.1177/0022343313518940

在网络安全问题上促进国际合作

尽管在线活动在不同法律管辖权下依照不同规则开展，但互联网本身仍然是一个全球性的网络，对于网络安全尤其如此，因为跨越国境的攻击和威胁每天都在发生，Conficker病毒就是一例，这种蠕虫病毒已设法散布到了超过180个国家[64]。没有哪个国家能独自解决网络安全问题，因此联合国已将促进国际合作来应对网络安全作为其全球优先工作。

联合国为确保网络空间信任而开展的一项重点工作是在线人权的保护。隐私和知情权可谓重中之重。前者受到包括连续不断的数据侵犯和数据保护投资不足等各种因素的威胁。知情权取决于既有言论自由又可得到公共信息的安全ICT的获取。ICT安全计划必须认识到相互冲突的利益，就像许多发达国家[65]采取的国内政策一样。R-O-A-M原则指出，互联网应以人权为基础（Human **R**ights-based）；开放（**O**pen）；普惠（**A**ccessible to all）并通过利益攸关多方的参与得到充实（**M**ulti-stakeholder participation）。该原则为在此方面开展进一步工作奠定了坚实的基础。联合国教科文组织（UNESCO）是全球人权保护方面具有重量级专业力量的联合国机构。该组织将此更广泛的网络安全观点作为促进可持续发展的首要任务。

考虑到私营部门在互联网经济以及网络管理中首屈一指的地位，除政府以外，应与包括业界、技术团体和民间团体在内的利益攸关方开展协调以便为提供保护开展更多工作。扩大合作对于开展法律调查尤其重要，互助将使各方从中受益。

---

64 "Conficker." ShadowServer. Shadowserver Foundation, n.d. Web. 4 Nov. 2013.

65 见之前第2点。

网络安全的基本导则

作为开展全面国际通信的场所，网络空间不仅将优势不胜枚举的更加连通的世界带给人们，也为联合国成员国带来了重大安全和稳定隐患。信息保密性、计算机系统、重要基础设施和网络化服务面对世界各地经常出现的互联网攻击不堪一击。保护这种环境中的网络空间[66]需要如下方式：

- 全局方式（或“政府全盘应对”），因为网络攻击的预防[67]、发现、缓解和告发涉及政府和私营机构的各个层面；
- ICT相关利益攸关各方的参与，其中包括政策制定者、互联网和电信提供商、技术组织和主抓保护人权的非政府组织（或“民间团体”）；
- 鼓励采取灵活和动态的政策，从而应对日新月异的技术变革，在保持创新势头的同时，为应对之前尚不得知的（“零日”）威胁和漏洞留下空间；
- 尊重人权，尤其是隐私权和知情权。

联合国有关网络安全的机制

联合国已部署了各种具有全球影响的网络安全框架，其中包括联合国范围内有关网络安全和网络犯罪的框架、信息社会世界峰会（WSIS）行动方面C5：“树立使用信息通信技术（ICT）的信心并提高安全性”以及信息通信和技术网络（ICT网络）。这些内容将逐一分小结阐述。该节还介绍了目前联合国系统中使用的个别网络安全机制。

66 该节并非代表联合国网络安全导则的全面一致意见，而是已审阅的各项文献所述共同趋势的概括。

67 包括在用户层面加强能力建设。

联合国范围内的网络安全框架

作为联合国减轻网络威胁工作的一部分，联合国范围内网络安全和网络犯罪框架为所有联合国实体应对成员国有关这些问题的忧虑提供了指导并以加强相互之间的协调为宗旨，从而提高人们对网络空间的信心并增强安全性。

有关互联网的犯罪活动在范围和发生频次上千差万别。该框架通过确定所有联合国机构在其相关职责范围内所遵循的基本原则面对大多威胁。这项涉及联合国范围的工作侧重于防止犯罪和早期预警，加强国内能力建设，有效开展遏制并为依法惩治犯罪提供便利。该框架包括向成员国提供技术和能力建设等协助，全面提高人们对网络威胁的认识和应对能力。

按照框架的定义[68]，网络安全指用来“[…]确保建立和维护相关组织安全财产、信息、系统和资产的成套文件、做法、政策和技术。网络安全防范内容如何？除提高对信息技术的信心外，网络安全将与计算机相关的犯罪活动，或网络犯罪排除在外[69]：一套“[…]包含针对保密性、完整性和计算机数据可用性的犯罪主体和基础设施以及一套“[…]与计算机相关的[犯罪]行为”以及与数据相关的“[犯罪]行为。”

网络安全和网络犯罪相关原则

为使内容宽泛的联合国框架得到脚踏实地的落实，该文件围绕七项广泛的原则。这些原则可以更容易地转化为具体政策。原则概括如下：

1. 联合国实体应帮助成员国以全面的方式处理网络事件，包括通过提供技术扶持实现法制并加强国际合作。

68 框架使用国际电联在ITU-T X.1205建议书中确定的定义。

69 按照框架的定义。

2. 联合国实体自身的职责应在满足成员国的需求时得到考虑，应与其他相关联合国组织开展合作。

3. 所有联合国网络安全和网络犯罪计划都应尊重人权和法制。

4. 联合国各项计划应在可行的情况下帮助成员国采用以事实为依据的方式开展犯罪风险评估。

5. “政府全面应对”的模式涉及各国所有关键利益攸关方以及非政府力量，如非政府组织、学术界和技术社团。这种模式应尽可能得到推广。

6. 对成员国的支持应旨在加强就网络安全和网络犯罪事宜开展合作的相关正式和非正式机制。

7. 应提倡成员国内公众和私营部门之间的合作，在区域和国际层面统一并采用技术政策和安全标准以及指导原则，以便对网络威胁做出必要的有效相应。

因此，对成员国的协助是本框架的核心：框架旨在提高网络安全性并使互联网成为更加安全、更可信赖的空间。落实上述原则的建议以及有效提供这种协作的工作建议都已概括在框架中。这些导则可划分为三类：法律和政策措施、技术援助以及实施机制。

技术援助

技术援助涉及固有的技术领域，如网络空间、能力建设和网络安全以及成员国内核心网络安全技能的培训，内容至关重要。框架建议指出，对各国技术能力的全面评估是不可或缺的起点并涉及各国网络安全政策的制定。具体而言，联合国实体提供的技术援助可包括：有关网络犯罪及其经济性的出版物、信息分析机制（最佳做法和其他形式的常识分享）、计算机取证和其他网络犯罪调查技能，

其中包括最终用户有关安全计算机和网络使用的教育、与私营互联网服务提供商（ISP）以及数据收集和分享方面其他利益攸关方的合作、计算机事件响应（包括成立常设机构以处理事件）（如国家计算机事件响应团队 – CIRT）和“海外需求中央联络点”。

WSIS行动方面C5

正如WSIS峰会（2003年）[70]成果文件所指出的，该文件在WSIS+10高层活动（2014年）中得到审议，WSIS行动方面C5侧重于树立使用信息通信技术的信心并提高安全性以及国际电联被赋予的推进责任。2007年，国际电联推出了全球网络安全议程（GCA）“[…]为解决增强信心和提高信息社会安全性问题提出战略规划的国际合作框架”。在此方面，国际电联与世界各地的所有利益攸关方结成伙伴关系以便使网络安全得到 发展，特别要为各国制定有关网络安全政策出版指导原则[71]，协助成员国开展各国能力建设并加强就制定必要的技术标准开展包容性讨论以提高安全水平。

ICT网络

联合国行政首长协调会采用的ICT网络机制将联合国多个实体的政策制定能力汇聚起来。该机制通过协调成为制定和实施有关ICT政策的论坛。然而，与此刊物最为相关的是其信息安全特别利益小组。该组“[…]通过专家和案例研究，[以及审议]政府间行动，包括对事件的响应、信息安全和政策以及提高信息安全意识”[72]探讨与网络安全相关的问题。

---

70 2014年10月13日经最后更新的信息社会世界峰会http://www.itu.int/wsis/index.html

71 国际电联国家网络安全战略指南，2011年9月。

72 信息安全特别利益小组，联合国行政首长协调会，2014年7月22日Web。

目前开展的工作

联合国成员国和联合国行政首长协调会均认识到[73]，有必要在联合国系统内就网络完全和网络犯罪事宜联合开展工作。在联合国网络安全和网络犯罪框架于2013年获得通过后，联合国秘书长潘基文呼吁国际电联与联合国教科文组织（UNESCO）、联合国毒品和犯罪问题办公室（UNODC）、联合国开发署和联合国贸发会议（UNDP）紧密配合高层管理委员会（HLCM）、高层项目委员会（HLCP）和联合国发展小组（UNDG）制定用于全系统的全面一贯的相关问题战略，以便在2014年11月召开的CEB第二次例会上进行讨论[74]。

结论

全面应对网络安全问题的必要性已在世界范围内形成共识。联合国正在采用全面、利益攸关多方、尊重人权、灵活和动态的方式解决这些问题。尽管人们对网络安全的前景仍然心怀疑虑，但联合国各实体开展的工作具有一定的共同要素和趋势，凸显网络安全作为全球工作重点的普及性。人们现在普遍承认，保证网络安全对经济和社会发展普遍具有显著影响并关乎冲突利益的平衡以及对国家主权的尊重。根据Choucri et al的认识，网络安全前景一片光明[75]：“虽然目前[有关网络安全]的[国际]机构协议体系显示出种种薄弱迹象，但组织和合作水平的稳步提高毋庸置疑。”

这种积极的趋势增强了人们在网络安全方面开展国际合作的信心。鉴于互联网的全球性，只有遍及全球的（或接近全球的）工作才能有效保证网络空间的安全。网络攻击造成的服务中断代价高昂，特别是在能源输送或金融等重要行业，但投资于网络安全产生的回报则远远高于成本。这种计算对于基础设施高度连接

---

73 “有关网络安全/网络犯罪和信息政策的行动”联合国CEB，2011年11月Web，2014年7月22日。

74 见CEB第二次例会报告第85段，2013年11月。

75 见上文第2点。

的发达国家尤其如此。而另一方面，发展中国家则面临实现跨越式发展的历史机遇。高度重视网络安全将推动上述前景的实现。

所有这些变革只有在全球都将网络安全作为首要任务时才能成为现实。联合国在日新月异的发展领域内具有与众不同的专业力量，因此最能成为促进国际网络安全工作的全球推进方。各国、业界和民间团体将在为此项工作添砖加瓦的过程中获益良多。

第二章：网络抗击力

引言

2005年2月，美国总统信息技术顾问委员会在一份题为“网络安全：首要危机”的重要报告中为加强网络空间的安全[76]发出一项行动呼吁[77]。美国国家工程院于2008年发表的“21世纪14项重大挑战”中突出了这项议题。近年来，许多其他机构意在探讨未来数字世界中网络信心面临的挑战。

随着计算机和通信设备以及系统的进一步普及并成为人们日常生活的必备，人类对数字时代所产生的优势的依赖将持续迅猛增强。

因此，保证网络空间的安全并提高网络抵抗日益猖獗的攻击威胁至关重要，因为这些威胁有可能造成大规模严重破坏。

使用日益普及的传感技术、网络物理系统、云服务、大数据或自适应智能系统[78]将随着我们坚定地走向物联网大大提升ICT的能力并对日常生活产生影响。

这种趋势不仅受到技术进步的驱动，同时亦受到新市场和产品需求的驱动。增加网络基础设施和服务就将产生新的机遇和优势，但同时也将带来更多漏洞以及危害个人和公共安全乃至社会安全的新的威胁。

这是一笔高额赌注，除人们对数字时代的信心外，人类的总体福祉在很大程度上都依赖于我们确定并管理多种网络威胁的能力。必须能够在认真分析和评定

---

76 总统信息技术顾问委员会，“网络安全：首要危机”（2005年2月）；

77 国家工程院：“工程面临的重大危机”；
http://www.engineeringchallenges.org/cms/challenges.aspx

78 Markus Luckey Gregor Engels：“高质量自适应软件系统规范”，第8届适应性和自我管理系统软件工程国际专题研讨会会议记录，ACM（美国，纽约），SEAMS'13，第143-152页，（2013年）

漏洞和风险的基础上充分采取措施以确保网络安全，或至少保障网络具有足够的抵抗能力，对于与能源、水、交通、卫生和金融系统等关键基础设施息息相关的网络尤其如此[79]。

可能危及网络稳定性和安全性的风险来源包括ICT基础设施和服务的日益复杂性及使用。环境灾害或政府、犯罪组织或个人发动的攻击等外部事件造成的威胁更加严重。研究表明，就连系统设计师，运营商和用户都可有意或无意地成为ICT漏洞的主要来源。在此方面，必须解决的科学技术问题是网络空间的“复杂性 – 应急 – 适应性”。

首先该章澄清了网络复杂性、由此产生的网络风险和意外系统行为术语以及对充实的网络适应性战略日益迫切的需求。之后，该章概括了若干可能的网络风险来源 – 从物理、技术或环境错误和故障一直到组织、制度或法律原由，同时探讨了网络风险的确认、分析和适应战略，考虑到了计算机科学和工程视角。以下各章将适应性挑战等同于“大数据”“云计算”应用以及人们对适应性网络控制系统的需求。最后，该章包含了私营部门有关网络适应性的文稿，对一项非技术性网络风险的审议并提出了一个迫切需求的国际法律框架，以应对除数据保护之外的现有其他风险。

第2.4章审议了一项重大的非技术性网络风险并提出了一个人们迫切需要的国际法律框架，从而应对除数据保护之外的现有风险。

79 美国第13636号行政命令：“加强关键基础设施的网络安全性”，（2013年2月）：http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf

2.1 网络适应性基础

Axel Lehmann

术语

如上所述，发展CBM的真正挑战是影响着公众和个人日常生活的数字世界的日趋复杂性。一般情况下，**（数字）系统的复杂性**取决于该系统状态空间的各个元器件的数量和功能。

在未来十年内，具有顶级性能及峰值性能的超大计算机可达到每秒1000 PetaFLOPS – 100万之四次方浮点操作[80]。网络物理系统多数不可见（并内嵌于微计算机设备，仅提供非常专业化和有限的计算能力）。

不同系统之间扩大的连通性形成所谓“系统之系统”（例如用于调节能源、通信或交通控制系统）[81]。信息存储是加强网络信心必须考虑的另一项重要全球服务。存储技术的发展速度甚至高于计算机技术（以迅速降低的成本不断加强存储能力）。

随着可扩展“系统之系统”中相互连通系统数量以及系统中元器件和能力的增加，必须掌控的总体系统复杂性呈指数性增长。

这些与日俱增的技术进步需要稳健的设计、开发和高品质保障方法，确保系统的稳定性、可用性以及在应对意外情况时采用的适应性战略[82]和网络信心。采用系统规范方法和设计可确保一些（不安全或重要）系统状态通过采用适当的识别和防止措施得到监测和避免。然而，设计阶段无法预测的事件或危害可能导致难以，甚至无法控制或调整的意外或紧急系统行为的出现。在最差情况下，系统

---

80 Exascale Computing：见http://en.wikipedia.org/wiki/Exascale_computing

81 Mo Jamshidi：“系统之系统工程：定义”，源自IEEE SMC（2005年）

82 “适应性工程”，编辑Eds. Erik Hollnagel、David Woods、Nancy Leveson，由Ashgate出版有限公司出版（2006年）

可能瘫痪并无法修复至运作状态。基于上述所有原因，必须开发并实施充足的网络适用性方法。

这些威胁、漏洞和风险必须得到确认、分析评估并为此采取对应措施。采用经过证实的设计和容错方法，数字系统将大大提高其稳健性和可控性，但不可能完全避免紧急行为的出现，尤其是在系统之系统配置中。因此，必须探索调节方法和程序并通过实施提高**系统和程序的适用性**，将此作为树立使用系统及网络空间信心的重要步骤。

根据Wreathall的定义[83]：“[…]适应性是一个组织（系统）保持或迅速恢复稳定状态的能力从而得以在重大事故之间或之后或在面对连续高压时保持工作状态。”Wreathall还制定了一些“高度连接世界中有关风险和责任的原则和导则”[84]。考虑到使用者、设计者、操作者、数字设备和系统等复杂数字世界构成的多样性以及研究的结果，多数最薄弱的实体均为人类，人类活动应在树立信心的措施中得到特殊考虑。

网络风险的确定和分类

在人类高度依赖于网络资源的世界中，网络空间的风险和适应性分析必须考虑包括人为因素以及数字世界多样性和复杂性在内的多个方面。网络空间资源包括世界各地可使用的全球数字基础设施和服务以及每个独立的计算或网络物理设备。

此外，有关网络空间的人为活动，如设计人员、开发人员或使用者的活动，我们必须区分他们作为内行或外行的角色以及在使用数字系统中的能力。对网络

---

83 John Wreathall：“适应性组织的特性：初步观点”，源于“适应性工程 – 理念和想法”，Ashgate出版有限公司（2006年）

84 世界经济论坛：“为网络适应性结成伙伴关系”，Newsletter2013年2月 – 达沃斯特刊：http://www3.weforum.org/docs/WEF_RRHW_PartneringCyberResilience_NewsletteFebruary_2013.pdf（2013年）

风险进行分层及分类的确定、分析和防范，可以对以下抽象层面进行区分。由于低层的破坏或失控可大大影响高层系统的行为和操作，总体风险分析和风险评估必须考虑到以下因素并将其作为制定系统适应性战略的前提[85]、[86]：

- 全球层面
- 企业层面/机构/个人层面
- 信息层面
- 技术层面
- 物理层面

从计算机科学和工程角度看网络风险分析和网络适应性

为制定良好的网络风险分析和网络适应性战略，必须首先确定以上各层面的主要网络风险来源。第二步则是认真分析和评估所有副作用（依赖性）将其作为可能影响更高层功能、可靠性或保密性和安全的错误、故障、或入侵。为此，依赖图[87]通过前向和反向相互跟踪路径用来检测相互依赖性。这种方法可以检测功能障碍、故障、失败、漏洞或数据受损的原因。

如以下图1所示，各层提供了一些能力、功能或服务（cx）并包含或使用低层属性（如箭头方向所示）。虚线弧形表明，各种能力（cx）的实施需要遵守某些标准、规定或规则。图1中是在企业层面发现的可能由该节点或更低层节点中错误、故障或入侵造成的缺陷。利用该图表（结构中的反向和前向串联）就可以对可能的错误、故障或失败来源予以定位。

---

85 “适应性工程”，编辑Erik Hollnagel、David Woods、Nancy Leveson，由Ashgate出版有限公司出版（2006年）

86 Lorenzo Strigini：“容错和适应性：含义、措施和评估”，源于K. Wolter et al（编辑），适应性评定和计算系统的评估，Springer-Verlag，Berlin Heidelberg（2012年）

87 Algirdas Avizienis、Jean-Claude Laprie、Brian Carl：“依赖和安全计算的基本概念和分类”，IEEE有关可依赖和安全计算的交易（2004年）

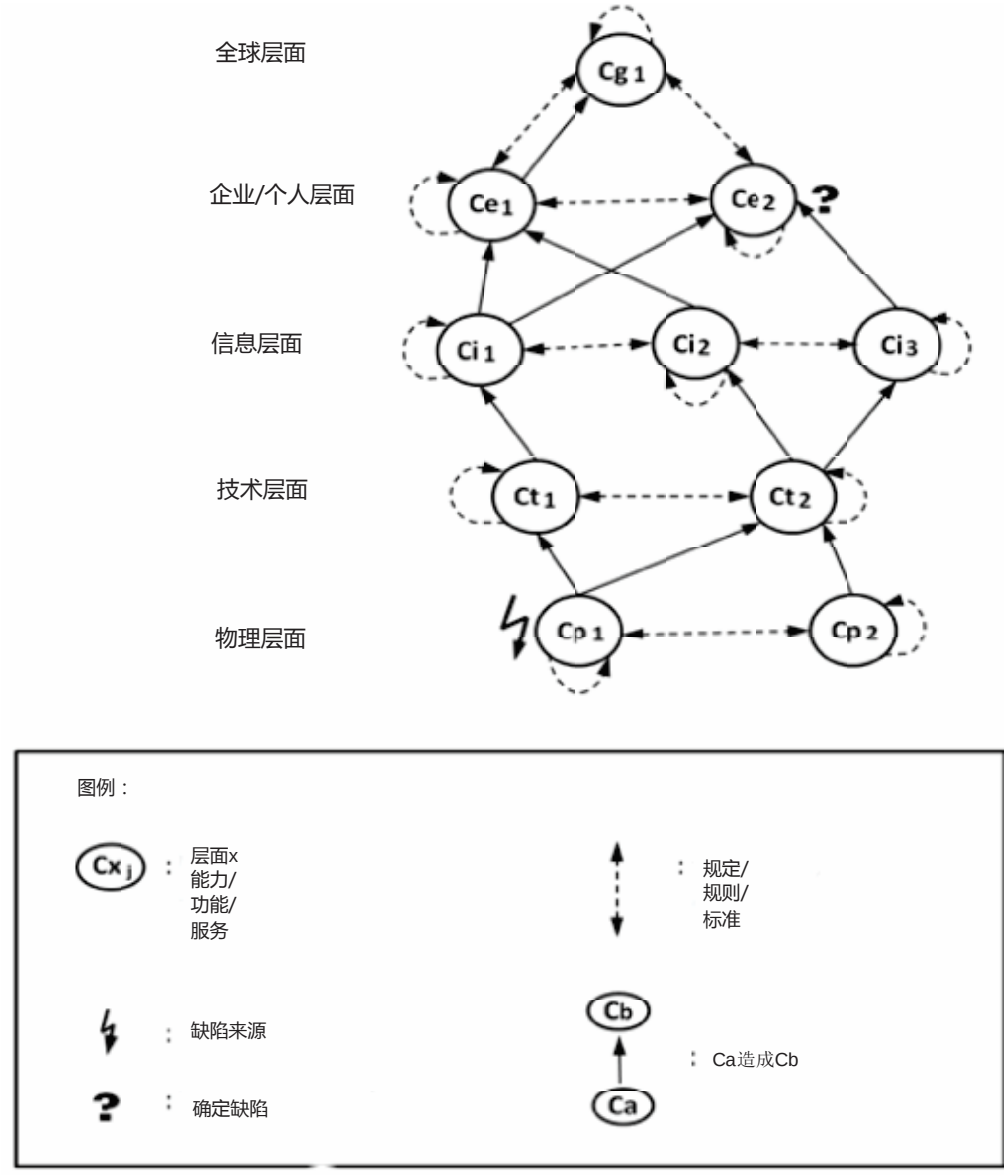
全球层面
企业/个人层面
信息层面
技术层面
物理层面
Cg1
Ce1
Ce2
Ci1
Ci2
Ci3
Ct1
Ct2
Cp1
Cp2
图例：
Cxj
：层面x能力/功能/服务
：规定/规则/标准
：缺陷来源
：确定缺陷
Cb
Ca
：Ca造成Cb

图1：依赖性图表实例

如上所述，ICT的瞬息万变大大推进了技术进步，但与此同时也产生了影响网络空间稳定性和安全性的新的网络风险和因素。除物理和技术缺陷外，主要网络风险来自于计算机、通信和存储资源在满足用户更高性能、稳定性和经济高效性的需求驱动下产生的虚拟化趋势。这种趋势可从日新月异的大数据、云计算和作为服务的云软件（SaaS）设施[88]、系统之系统[89]和“超级网络”[90]等技术的日新月异中略见一斑。

这些技术发展还产生了新的有关隐私、保密性和权威性等网络安全问题。除滥用、操纵数据和ICT基础设施的破坏外，这些技术引发新的有关非授权收集、使用和合并个人或其他保密数据的风险。已造成事实的一些危害使多种个人、组织甚至国家专有数据被暴露在光天化日之下，严重影响了人们对网络空间的信心。

总之，风险可计算如下：

风险：=可能性*影响

从技术角度看，网络风险可以是由数字元器件的设计错误、故障、失败、功能丧失或“超级联网”系统配置中紧急系统行为造成的。除因数字系统的错误或不良使用造成的风险外，内部人员、用户甚至意外事件或环境事件造成的攻击也构成重要原因。为在最大程度上减少这些ICT相关风险，必须在风险分析中进行更加严密的思考：ICT风险：= f（威胁、漏洞、资产）。

对于ICT，系统的薄弱环节源于设计、实施或错误应用造成的故障、能力减弱、系统元器件功能丧失，甚至系统瘫痪。这种漏洞必须尽早确定并在考虑可能的补救方案前进行分类。在此方面，必须在ICT基础设施和服务漏洞以及相应的对

88 Nicolas Gold、Andrew Mohan、Clair Knight、Malcolm Munro：“了解面向软件的软件”，源于IEEE软件（2004年）

89 Mo Jamshidi：“系统之系统工程：定义”，源于IEEE SMC（2005年）

90 “适应性工程”，编辑Erik Hollnagel、David Woods、Nancy Leveson，由Ashgate出版有限公司出版（2006年）

应措施的轻重缓急确定前评定ICT相关风险。之后，可以进行如下量化风险分析 ：

ICT风险：=（（漏洞*威胁/对应措施分）*资产价值

制定ICT适应性战略的前提是可靠性（或依赖性）以及可用性。这些分析应考虑采用以下一般性方法来改进系统的可靠性和可用性[91]：

- 避免失误 – 通过认真设计和实施避免出现错误和失误；
- 消灭失误 – 采用测试、核对和确认方法发现可能导致失误甚至失败的错误；
- 容错 – （通过资源加倍和/或实施多样化）提供余量，以便在出现失误时得以弥补和调整；
- 失误/失败预测 – 分析并评估可造成系统失败以及对系统操作产生影响的失误后果[92]。

从分析角度看，依赖图（如图1）或可靠性框图是分析错误、失误、失败影响和副作用以及上述具体应对措施[93]的简单方法。

除这些与ICT相关的薄弱环节外，还必须围绕网络信心考虑由缺陷造成的威胁。“威胁是可能利用漏洞破害安全并由此造成危害的潜在威胁。因此，因用户

91 Algirdas Avizienis、Jean-Claude Laprie、Brian Carl：“可依赖和安全计算的基本理念和分类”，IEEE有关可依赖和安全计算的交易（2004年）

92 同上

93 同上

有关系统资源的活动、事件、自然灾害产生的或其它意外外部事件产生的附加威胁必须得到考虑和评估。”[94]

造成威胁的人为活动通过用户的操作和行为既可以表现为有意的（如内部人员、黑客）或无意的。对于风险分析，应识别最可能造成伤害的人为活动并分析由此产生的薄弱环节。除薄弱环节和风险外，网络风险分析必须考虑其对系统能力、资产以及相关资产价值的影响。

在培育网络适应性的过程中应考虑采用以下手段：[95]

- 避免缺陷 – 通过认真设计、实施和操作系统以及系统程序避免错误、失误和失败等问题的出现，遵循普遍认可的具体标准、规定或行为规则，可在更高层面上实现上述目标；
- 消除问题 – 通过测试、核对和采用认证方法发现可能造成失误、失败故障或滥用的问题；
- 缺陷忍耐 – 通过增加资源和服务以及分类实施提供余量，以弥补或调整可能出现的缺陷；
- 缺陷预测 – 通过大量仿真，分析相应的风险并评估在此环境下适应性战略实施产生的后果，在貌似可信的情形中发现薄弱环节。

为基于上述风险和可靠性分析制定全面的适应性战略还需要调整和恢复机制，使系统从不可用性能衰减状态或被入侵状态中全面自主地恢复过来。多数自然或生物体系均具备自愈或自我配置机制。对于技术系统，必须探索出这种生物类程序或组织（称为有机计算能力）的弥补、调整和恢复方法并在系统设计阶段

---

94 Lorenzo Strigini：“容错和适应性：含义、措施和评估”，源于K. Wolter et al（编辑），适应性评定和计算机系统的评估，Springer-Verlag，Berlin Heidelberg（2012年）

95 同上

完成这项工作。有关有机计算和通信的科学研究侧重于这种生物类方法，以便改进ICT和网络物理系统的适应性，即实施自x数字系统理念（x可替换为保护、自愈、愈合、优化、配置等。[96]根据在知识工程和数据采集领域进行的研究结果，智能系统的设计原则已发生变化，可用于长期的风险识别和评估以及使系统实现适应性的预防性行动。

为避免或补救失误、故障、失败或中断以及增强网络适应性，从计算机工程角度而言，自下而上可采取的措施包括[97]、[98]、[99]：

- 在物理层 – 有关材料和设备的使用只限于预先确定的环境条件（如有关温度、辐射）。此外，使用其它材料、可选的操作程序以及对元器件实施进行分类实现冗余；
- 在技术层面 – （m中的n个）计算设备、冗余的数据传输和数据编码理念或不同但标准化安全传输协议的使用不仅为避免错误传播提供条件，
- 还能实现自我调整。此外，多样化，如计算算法的多样化、计算节点的多样化或使用不同存储理念也是避免错误传播的措施，从而提高系统可靠性并实现技术层面的适应性；[100]

---

96 “有机计算”，编辑Rolf Würtz，源于Springer系列“了解复杂的系统，”Springer（2008年）

97 Yue Yu、Michael fry、Alberto Schaeffer-Filho及其他：“用适应性方式实现网络适应性：不断挑战发现和缓解方式”，源于IEEE第8次Internat.有关可靠的通信网络设计讲习班（2011年）

98 Dorothy Reed、Kailash Kapur、Richard Christie：“评定连网基础设施适应性的方法”，源于IEEE系统刊物第3卷第2期（2009年）

99 Piotr Cholda、Anders Mykkeltveit及其他：“通信网络中适应性差异框架调查”，源于IEEE通信调查，第9卷第4期（2007年）

100 美国能源部：“提高SCADA网络安全性的21步骤”（2011年），http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf

- 在信息层面 – 目标是实现“确保信息的保密性、完整性和可用性。此外，其他诸如权威性、问责制、不可否认性和可靠性等特性亦包含在内”（ISO/IEC 27000[101]）。措施包括使用冗余编码或稳健的加密/解密算法或安全数据传输协议，以防止失误、滥用或破坏。有关工具，SCADA（监督控制和数据捕获）系统及网络可安装在企业/个人层面[102]，采用成熟的最佳做法、商务、工作流程和安全标准、规则和限制以及内部行为操守[103]；

- 在企业/机构/个人层面 – 用来提高网络安全性认识的操作法律和规则框架、机构、区域和文化行为操守、全面的教育、信息的传播；

- 在全球层面 – 遵循在世界范围内达成政治协议及可用的全球行为操守，具体而言，制定国际行为法律和规则，引入并遵循区域和文化操守，开展全面的教育，分发信息资料并为提高网络安全意识提供培训机遇。

目前的这份措施和方法清单还有待进一步补充，以便提高网络安全性并由此增强人们对网络的信心。

2.2 突出云计算和大数据系统的适应性

Vladimir Britkov

ICT的新发展主要围绕大数据和云计算。根据加德纳集团的估计，全球64%的组织已经或计划投资于大数据。有关人和人类居住的环境的大量数据信息预计每

---

[101] ISO/IEC27000标准：信息技术 – 安全手段 – 信息安全管理系统 – 概述和词汇（2014年）

[102] 美国能源部：“提高SCADA网络安全性的21步骤”（2011年），http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf

[103] Amy Lee、John Vargo、Erica Seville：“开发测量和比较组织适应性的工具”，源于：自然危害审议，ASCE（2013年）2月

两年增加一倍。大数据技术包括新的“业务智能”领域和分析，使网络适应性在大数据和云计算领域获得进一步提高。

大规模云基础设施，大量及多样性的数据来源和格式，数据捕获的媒体流性质以及批量云间过度造成了独具特性的安全隐患。因此，传统的针对小规模、静态（相对于流）数据量身定制的安全机制已不能解决问题。在本文稿中，我们突出十大数据安全和隐私挑战，希望由此将人们的注意力更多集中在大数据基础设施的强化之上。

信任 – 云业务提供商和客户打造成功业务必不可少的因素 – 代表最突出的安全问题之一。然而，没有确保无内部攻击或其他安全事件的信任纽带将专门针对云中的信息。各企业在与基于云的提供商开展业务活动时自然考虑这一重要因素。然而，客户可与云提供商达成法律协议（SLA），规定客户与云服务提供商之间合同关系的条款和条件。SLA对于保护托存于云服务中的客户数据而言至关重要，因为云具有全球性，通常覆盖多个地理管辖区，因而也通常涉及多种不同的适用法律规定。

大数据基础设施通常为专用设施，与通用网络相互隔离。通过采用数据采集方法，现在大小型组织都可通过公共云基础设施以低廉的价格和方便的方式获取大数据。软件基础设施使开发人员轻而易举地利用成千上万个计算节点进行数据并行计算。为保护大数据系统基础设施，必须保证分步式计算和数据存储的安全。为保证数据本身的安全，信息传播本身必须具有隐私保护，敏感数据必须使用加密和颗粒式接入控制手段予以保护。

管理规模庞大的数据需要可扩展和分布式的数据存储安全保障解决方案，从而实现高效的审计和数据源头控制。最后，必须核对来自多个终点的数据流的完整性并进行安全事件的实时分析，从而保证基础设施的完整性。

大数据安全和隐私的十大挑战：

1. 分布式程序框架中的安全计算
2. 非关系性数据存储的最佳安全做法
3. 安全数据存储和交易日志
4. 端点输入认证/过滤
5. 实时安全监测
6. 可扩展和可组合式隐私保护数据采集和分析
7. 增强型加密数据安全
8. 颗粒式接入控制
9. 颗粒式审计
10. 数据源头

有关安全大数据基础设施

应对安全和隐私挑战通常需要解决三个突出问题：

1. 建模：建立包含多数网络攻击或数据漏洞情形的威胁模式。
2. 分析：基于威胁模式寻找可跟踪的解决方案。
3. 落实：在现有基础设施中落实相关解决方案。

有关分布式程序框架中的安全计算

使用案例：建模

用于制图的威胁模式拥有三大情形：

1. 故障计算工人节点 – 在分布式计算中分配到制图软件的工人可因为错误的配置或失误节点造成故障。
2. 基础设施攻击 – 受到破坏的工人节点可能窃听其他工人与责任人之间的通信，用来重放，评判或对MapReduce计算进行DoS攻击。
3. Rogue数据节点 – Rogue数据节点可增加至群内并接收复制数据或传送经改变的MapReduce代码。

分析

在上述威胁模式的基础上，有两种分析规模：确保制图软件可信并在制图软件不可信的情况下确保数据安全。为确保制图软件可信，有两种手法：建立信任和强制接入控制（MAC）。

实施

通过修改MapReduce框架、分布式文件系统和Java虚拟和将SELinux作为操作系统的Java虚拟机器实施MAC。

结论

大数据将长期存在。难以想象，下次应用不消耗数据，不产生新的数据且不包含数据驱动的算法。

随着计算环境价格的下降，应用环境日益联网以及系统和分析环境采用云进行分享，安全、接入控制、压缩、加密和合规将带来必须以系统方式才能解决的

风险挑战。这些挑战反映在上述强调的十大安全和隐私问题中，有必要加以解决，从而使大数据处理和计算基础设施更加安全且更具适应性。

大数据通用要素源于在数据处理中对多个基础设施层面（存储和计算）的使用，未经全面安全审查的新计算基础设施（如NoSQL数据库）（用于大数据量必不可少的大吞吐量）、大数据集密码的不可扩展性、可能适用于小量数据的实时检测技术的不可扩展性、产生数据的设备多样性以及周边千差万别的法律和政策限制，从而导致保障安全和隐私的手段各具特色。

2.3 力争实现灵活强健、极易恢复的网络控制系统

Stefan Lüders

在当今“西化”世界中，我们的生活受制于几乎涉及到我们日常生活各个方面的控制系统。控制系统的存在使人们共栖共存[104]且对之万分依赖并与之密不可分。没有了控制系统，人们的生活水平将迅速倒退至中世纪时代[105]。由于我们对这些控制系统依赖至深，因此，确保其稳定性和易恢复性至关重要。

然而，事与愿违，当今这些控制系统却不堪一击，极易受到对其予以操作的标准信息技术（IT）系统缺陷的影响。控制系统同样采用现代计算机中心采用的技术：以太网协议、TCP/IP、万维网和电子邮件已取代专有现场总线通信技术；个人电脑（PC）的采用也使人们无需再进行人工显示、校准和使用操作面盘；微软视窗操作系统取代了客户命令线路终端。

此外，高质量软件可遇不可求，往往存在缺陷、瑕疵、误码和程序错误。为满足市场需求，得到发货的软件往往为beta版软件，虽然能够运行，但却具有先

[104]亦见Stefan Lüders的《共栖共存的人类生活》，欧洲核研究机构（CERN）出版物，2014年。

[105]这一点在Marc Elsberg的小说中得到很好描述 –《漆黑一团：Morgen ist es zu spät》，Blanvalet，2012年3月。

天弱点和不堪一击之处（晚些时候被发现和纠正）。由于改善需要成本，因此，用户和公用事业单位不一定要求改善软件。

更加雪上加霜的是，标准IT系统开辟了一种全新的犯罪活动市场 – 个人黑客相互勾结，建立“黑色网络”，入侵并破坏IT系统，使用户信心大为下降。如今，每一个互联网、网站、操作系统和受人欢迎的软件应用都不断有居心叵测者寻找其弱点和不堪一击之处，从而利用这些弱点牟利，或将其在黑市上予以出售。由于防止这类攻击或强化易恢复性的总体工作绝对比利用弱点的工作要复杂得多，因此攻击者具有一定优势。

即便如此，总体IT系统迄今已证明自己具有足够的易恢复性，从而避免了这些攻击对我们日常生活产生的大规模影响，尽管“黑色”经济在持续繁荣发展、而国际法律系统却只有招架之功。事实上，普通公众极少受到严重影响[106]。

随着控制系统的爆炸式发展及其与标准IT系统的结合，游戏发生了变化。控制系统虽然受益于IT的功能性，但也继承了这些系统的不堪一击之处和弱点，从而使得强健、专用和客户控制程序变得“弱不禁风”和极易受到攻击 – 正如下列媒体标题所示，居心叵测者对控制系统的试探与日俱增：“俄罗斯欢迎黑客攻击”（纪事报，2000）；“黑客袭击宾夕法尼亚供水系统”（InTech，2006年）；“TVA发电厂极易受到网络攻击，GAO的调查结论”（华盛顿邮报，2008年）；“内部人员被控对加利福尼亚运河系统进行黑客攻击”（计算机世界，2009年）；“美国空中交通受到网络攻击的‘严重危害’”（全球飞行，2009年）；“间谍进入美国电力网”（华尔街日报，2009年）；“报道：黑客进入FAA空中交通管制系统”（CNET，2009年）；“报道：网络攻击造成巴西停电”（连线杂志，2009年）；“DHS：美国水利电力设施受到日常网络攻击”（计算机世界，2012年）；“水闸、抽水站和桥梁的保护不力”（荷兰国际广播，2012年）；“美国电力网不堪一击，任何攻击都将使其瘫痪”（OilPrice.com，2012

106可能的例外情况是，对全球域名服务器、互联网核心路由和更广泛的、一些政府机构对公民的隐私的攻击。

年）。据报道，以色列和美国特工处最近报道了伊朗Natanz核浓缩设施的人为破坏情况：“Stuxnet病毒开创了网络战争新时代”（Spiege在线，2010年）。受“Stuxnet”感染的、基于视窗的个人电脑伪冒向设施操作人员进行的显示，并将自身下载至控制处理器上，从而在随后操纵数百配置的旋转速度，使铀浓缩毫无成效。

虽然“Stuxnet”被认为是第一个得到文件记录的人为网络破坏事件，但它也反映了由国家发起进行的网络攻击所处的尴尬境地。白宫前国家安全和打击恐怖主义协调员Richard A. Clarke指出，美国也许有能力摧毁某地的核工厂或恐怖分子培训中心，但一些国家可以通过网络攻击予以回击，因此“美国整个经济系统可能在报复中瘫痪[...]，因为如今我们已无法对之予以防卫”。

毫无疑问，如今不可能采用类似于保护计算机中心的技术来保护控制系统，如通过“补丁”保护前者，即，通过更新操作系统弥补不堪一击之处。

现代计算机中心受到配置管理系统的驱动，通常可以在很短时间内更新，甚至重新安装大批服务器。由于在核心持续服务操作的过程中，服务器场中的次群得到维护，因此，冗余和虚拟化使得这一程序更加方便易行。另一方面而言，目前视窗维护少之又少，绝对合规性要求甚严，因此控制系统的灵活补丁受到制约，特别是在相关安全程序方面。只有完全合规和得到认证的系统（如，重新认证为符合安全综合水平（SIL））才被视为是安全的，彻底的测试不仅耗时，而且还会增加费用。此外，不能总是确保新的操作系统补丁与现有控制系统软件相兼容，因此，如果真兼容的话，厂商往往进行滞后宣布。难以升级的嵌入式系统更增加了难度。最后，虽然计算机中心的硬件设备每五到三年回收一次，但控制程序中的老旧硬件则尽可能得到长时间保留，甚至在其明确表明的操作系统寿命期结束之后[107]。

[107]因此，对相关单位而言，微软视窗XP操作系统近期的淘汰带来了另一项挑战。

另一个示例源自访问控制的不同方式。计算机中心往往优先关注保密性、完整性和可用性（即“CIA”），因此，访问控制尤其重要。有鉴于此，使用带有或不带多因素部署（multifactor deployments）的单点登录、x509证书管理和集中管理LDAP/AD等的认证和授权技术得到极好的内置和集中使用。控制系统的可用性优先于保密性和完整性（“CIA”），因此，必须永远保证人员对程序的访问。

为便于操作切换，操作人员之间共享密码。此外，硬件和软件由于其专有和遗留性质，因此往往带有无文件记录的后门，以未得到更改的初始密码运行、不允许利用内部防火墙或访问控制清单禁止未得到授权的连接，因此，难以与中央身份管理解决方案结合一体。人们认为，加密对资源要求太多，因此更为可能的情况是，控制系统要求或依赖更多保护装置来保证其安全并控制访问。对网络进行适当保护变得更为重要，不能成为很好的“深度防卫”格局的网络保护机制意味着在实际硬件操作系统和应用的每个层面都需做出保护。

最后，强健性至关重要。如前所述，计算机中的标准IT系统，特别是直接通过互联网访问时，不断由攻击者寻找着弱点。如果中心得到很好管理、在各方面都处于最新状态并安装有适当入侵发现和监测系统，则这种渗透和弱点被利用现象将得到抵制。数十年来，人们在各种不同攻击活动和潜在弱点方面积累了丰富的经验并增长了知识，同时利益攸关方之间亦形成了一套行之有效的信息共享办法，因此，有关事件间保护、发现和响应的工作更加方便易行。与此相反，控制系统却不能被认为十分强健、能够抵御网络攻击。尽管其物理硬件可能如此，但其软件实施工作一再表明违反了普通IT标准，经不起基本安全测试并缺乏抵制攻击的根本性手段[108]。控制系统可以满足定义完善的使用需求，但无法满足定义不完善的使用需求。“安全”与标准IT硬件不同，它不是控制系统装置不可或缺的组成部分，即便是，也由于其实施是专有和隐蔽的，因此，相关使用单位还是难以断定安全是真正适当的还是一种幻想。

108 “CERN的测试表明，互连工业装置内存在安全隐患”，工业以太网白皮书，2006年。

最后同样重要的是，目前从事控制系统工作的人们在竭力就如何进行“负责任的披露”达成一致，即，如何向相应厂商宣布和公布新发现的不堪一击之处，并在晚些时候向相关使用单位宣布和发布。在标准IT世界中，人们能接受的向软件提供商发出通知与向公众进行完整披露之间的间隔时间是三至九个月，但一些人认为这一周期太短，因为软件控制所需的软件寿命周期要长出很多，且在相关设备中采用补丁须得到很好的协调和计划。在现实生活中，整个程序通常需要一年时间。

如果控制系统要变得易恢复、以抵御网络攻击，则必须解决这一问题。控制系统必须确保安全性成为总体功能性、可用性和使用性、维护性和物理安全不可或缺的组成部分。控制系统专家必须得到适当的IT培训，特别是IT安全培训。培训必须在高等院校的教育层面开始，将安全性纳入课程之中，而非将其视为附加内容。更为理想的情况是，应将所有与IT有关的工作外包给能够对运行控制系统和计算机中心的各自需求予以区分的、业务能力强的IT专家。可能需要达成新的折中，以便实现永久可用性和快速打补丁需求之间的平衡，从而实现轻松和严格的访问控制。与此同时，IT虚拟化技术可能是克服问题的灵丹妙药，并成为在测试、预生产和实际运营系统之间推出补丁的新的基础。完整的软件管理、版本控制系统、360度软件开发寿命周期、彻底的回归测试和夜间构件也必须成为控制系统的标准。与充分得到填充并永久得到更新的库存相结合也是“必须”完成的工作。为了解风险并出台保护措施，必须对安装基础、所有装置、账户、应用（包括其相互之间的依存性）进行详细文件记录。渗透测试必须日日进行。理想情况下，得到广泛认可和完全公开的、进行不堪一击之处评估的方案和程序应成为标准工作，以便厂商和制造商、相关单位和集成商以及用户、学术界和认证管理机构能够对特定控制装置、硬件或软件做出安全评估。这种程序定会增加现有控制系统的强健性，并最终提高其应对居心不良活动的可恢复性，从而有望为实现ISO9001认证方案奠定基础。

所有这些步骤都既非微不足道，也非方便易行。对目前一代控制系统和控制系统专家而言，如此行事亦或已为时过晚，因此，我们应集中关注未来，将目标

设定为合并更多控制系统和计算机中心的IT。我们的成功程度将检验我们如何确定自身的未来发展方向。

2.4 从私营部门角度看待网络易恢复性

Danil Kerimi

当前我们所处的世界极为复杂且连接程度极高。它既为我们带来了仅在几年前都难以想象的、前所未有的机遇，也造成了风险。我们现在仅仅是通过调整某种规范、政策和商业模式（以使其适应网络玄学的发展）而开始了解上述机遇和风险带来的社会、政治和经济变革的。

所有这些变革都将从根本上重新确定个人、企业和政府之间相互连接的方式方法。由超级连接带来的新商业模式和社会互动对传统经济价值生成和消费方法带来挑战。目前各行各业在内部运营方面对数字渠道的依赖以及与其伙伴的互动与日俱增。以前曾被认为是核心技术参与方的实体现在也被迫处理超出其专业范围或并非驾轻就熟的问题。

消费者行为也转为赋能更大、信息流动更好和选择更充分的形式。各公司比以往任何时候都更加洞悉消费者行为，从而使其实现了前所未有的私人订制水平。由于受到挑战，所以这些公司不断自我调整，以适应快速变化的环境，从而确保满足消费者希望，如，产品共创和快速生产样机。

超级连接具有催化剂作用，往往能够减少入市壁垒、推进贸易并增强行业内和跨行业竞争，不断使行业格局得到重新确定并对各自为政的政策形成挑战。多种不同任务和程序的持续自动化 – 更广泛的向知识经济转变的组成部分 – 对传统劳务市场带来了极大压力。

目前创新水平如此之高，不但正在消除蓝领工作，而且使更多依赖知识的职业亦进入了长期结构减缩状态。此外，我们现有的教育系统无法满足人们对新技能（如数据专家）的需求，而这些技能正在取代更加传统的职业技能。

信息和通信技术不断推动着这种变革的发展。全球技术公司帮助建立了超级连接，且也使技术公司定义本身得到检验。如果你听到汽车行业经理人谈论汽车，则我们可能会想这不过是方向盘上的终端。医疗保健公司也在谈论数据，银行则探讨网络安全。从银行到消费者再到能源行业公司，全世界都将数字化放在了首位。

过去，技术公司颠覆了繁复多样的商业模式并构成其它行业的变革力量，但如今的时代是，其它行业正在成为更加成熟的数字商业模式的颠覆者。

这种转变也反映在消费者集体的脑海之中。据Interbrand[109]的最新报告，前10大品牌公司中的8家为信息通信技术（ICT）公司，且其中的半数为家喻户晓的公司，他们为当今技术格局的形成贡献了力量。排名前20的纯技术品牌公司的总价值超过了1万亿美元。如果这是一个国家的话，则该国能轻而易举地成为20国集团（G20）中的一员。

2014年，以市值计算的前三大公开上市公司也均是ICT领域的领头羊。在由《财富》杂志公布的最新全球前二十最具影响力的人士中，六位源于技术行业，十一位为政治和宗教领袖，其他三位是金融、零售和能源行业公司的首席执行官（CEO）[110]。2015年的该名录将让人充满期待。

当前，我们的日常活动完全离不开网络空间，因此，我们不仅对网络空间带来的风险忧虑不已，而且害怕网络无法访问。几年前网络易恢复性还令人十分陌生，现如今，这已成为全球董事会会议、政治辩论、甚或酒吧和家庭中的日常讨论话题。人们正在了解到，连接一体的所有东西都会受到黑客攻击，因此，应对措施不应是随时保证百分百的安全，而是具有灵活性和易恢复性，以便能够在不利情况下运行如常。

---

109 http://www.interbrand.com/en/best-global-brands/2013/Best-Global-Brands-2013.aspx

110 http://www.forbes.com/powerful-people/list/

在数字时代，具有快速性和移动性并能相互协作是企业成功的最主要特征。为充分利用超级连接的益处，急需形成易恢复的国际网络生态系统。近几年来，全球经济论坛汇集了一些企业高管和政策制定者，共同探讨通向更加灵活和易于恢复的数字环境的道路。不同部委和行业共同关心的一个主要问题是世界范围内急剧增加的网络事件。如果我们可以借用环境法的概念的话，则可以说，在网络空间方面，人们已经认识到，利益攸关方具有共同但也相互区分的责任，而网络易恢复性则要求利益攸关多方进行高度协作。如同全球其他治理领域，往往对网络威胁缺乏详细了解且不具备充分解决这些问题的发展中国家如发达国家一样，受到新的风险格局的影响。显而易见，随着我们的经济对数字连接的依赖性的不断加大，强化网络易恢复性已成为各行各业及政策领域领导人的核心能力。

为消除人们的上述关切，世界经济论坛要求CEO（而非首席信息安全官、首席技术官等）和高级政府官员充分认识到在促进形成易恢复的、共享数字空间领域具有作用的各方之间的相互依存性，从而着手解决网络易恢复性问题。通过这一做法，我们通过鼓励执行层提高认识并开展综合一体的风险管理，来凸显领导人发挥的作用。我们还鼓励企业在扩大企业规模、使其环境从供需发展至总体价值链过程中，采取全面系统的有关网络易恢复性的方式。

除公众情绪外，数字也很好地说明网络易恢复性的重要性。未来若干年中，有关网络易恢复性的年度支出很可能由2013年的690亿美元增加到2020年的1230亿美元[111]。毫无疑问，这些估算数字取决于考虑到现有和未来得到预测的网络威胁的市场分析，因此，在一种情形中，随着公共和私营部门改善合作（反映其防卫能力），网络易恢复性投资将增长13%，达到每年1390亿美元。在另一种情形中，我们预计相关支出将增长28%，每年达到1570亿美元（如果攻击能力和各自为政的响应机制超过防卫和合作能力的话）。

有关网络风险的讨论往往集中于世界末日之情形或人们惧怕的“网络末日战”，并充斥着过度使用的词句，如“隐私已经故去”或“最薄弱环节”。然

111 http://www3.weforum.org/docs/WEF_RiskResponsibility_HyperconnectedWorld_Report_2014.pdf

而，我们可能应同样关切现有数字生态系统的巨大反弹或碎片化造成的机遇的丧失。一场大的“网络末日战”或逐步侵蚀（或凌迟致死）即可造成反弹。

区域、国家和企业层面都可能发生碎片化，诸多参与方选择这种行动步骤的理由也会多种多样，因此，由于缺乏可靠的环境，相关政府被要求在网络空间履行其安全职能，从而营造碎片化开始滋生的环境。不同辖区采取的各自为政的行业政策或分散监管也可能导致碎片化。

据麦肯锡公司估计，如果不断复杂的网络攻击能力致使投资减少，则全球可能损失约3万亿美元的潜在经济增长值[112]。更加复杂的政策格局还可能进一步使经济决策复杂化。

那么企业是如何看待网络易恢复性的呢？首先要认识到存在一种相互依存和基于风险的方式，该方式设想，只有一部分风险缓解机制为复杂系统的根本特征，并假设组织的易恢复性能够为整体系统添砖加瓦。

公司与其他组织一样，十分重视领导人的优先工作，因此，执行管理团队的参与和确保对管理机构（如董事会）做出监督十分重要，从而制定有效的网络风险管理计划并监督计划落实工作。

管理团队应借助必要资源、管理方法、承诺和对相关工作的广泛宣传，提供一套相互区别的职责和共同目标。从业务连续性角度出发，如果在现实中出现参与人没有时间充分考虑职责和潜在响应行动的情况，则进行系统应力测试和对潜在危机情形进行“作战模拟”（要求从IT到公共事务各部门之间进行协调）可能会十分有益。

在更广泛的业务延续性和企业风险管理之中将网络易恢复性作为标准内容予以纳入可能也会十分有益。一个良好的开始为明确对组织任务至关重要的信息资产。过去，对周边予以防卫可能是很好的战略，但当前出现的攻击、探查和内部

---

[112] Ibid

威胁都迫使现代风险管理工作明确确定资产的轻重缓急，以便于分配保护资产所需的足够资源。

这意味着各方面运营工作以及荣誉风险都需要定期得到影响评估。还应出台相关程序，以缩短响应时间，从而在出现主要故障时，实现完整或部分系统恢复。该工作贯穿于整个公司至关重要，因此，不应将此视为仅需要IT部门加以处理的问题。

包括由高层管理团队领导的营销、政府和公共事务以及消费者宣传在内的所有部门都需要做出准备，同时解决恢复受影响运营工作、缓解对品牌造成潜在负面影响、客户反弹和潜在监管后果等问题。

许多成功的公司都成立了首席信息安全官办公室，其中一些明确将该职能从首席技术官/首席信息官职责中分离出来。此外，有些公司还确保，即便所设职位级别并非相同，但至少其从属关系有所不同 – 它是作为多样职能的战略目标存在的，可能特别需要在技术构架和并购方面具有不同的优先程度。

只有综合看待各种不同信息资产以及充分和及时对公司潜在危险的响应机制的重要性，公司才能够真正为其自身系统性网络易恢复性予以助力。随着公司推出网络易恢复性/风险管理结构，应得到考虑的一个重要因素为合规性，因为政府已开始通过繁复多样的监管机制解决不断加大的安全问题（从志愿行为准则到最佳做法，再到强制性事件报告和标准等不一而足）。

另一项重要考虑内容是整个网络供应链中供应商、承包商和客户的作用问题。企业应努力在更广泛的生态系统中提升自身活动，从而扩大安全范围并确保实现联盟。

近年来，跨国企业面临的最为敏感的一项工作是主动防卫工作。随着安全范围的确定更加艰难，成功的企业需要充分利用可能导致产生攻击的、有关威胁格局变化的现有内部和外部数据。然而，在理解威胁跨越内部与外部界限点方面存在很大差距，更不用说先发制人行动的可能性以及该问题的合法性问题了（即便明显面临迫在眉睫的危险）。

人们往往将潜在行动的归因方面的困难作为最大障碍，但其合法性和合理性也是障碍所在。当国家和企业层面存在综合性网络战略时，这一灰色地带略显清晰，但上述战略并非易事。这种战略应包含明确和透明的国内及国际内容。

对此问题的认识已发生巨大转变，企业领导人已在更加详细地了解相关过程和潜在缓解技术。目前随着威胁格局持续迅速演变，在国家和国际层面都在进行利益攸关多方之间的对话。

超级连接已改变了我们之间相互联系的方法：它影响着我们的决策并使我们的生活重新得到组织。信息通信技术产生的颠覆性影响使社会经济变革日益加大。我们往往过高估计技术的短期影响，而过低估计其长期对人类生活各方面的影响。有关网络易恢复性的思考可以成为理解和确立相关解决方案的出发点，从而对决策予以引导，以实现全体人类期待的积极成果。

2.5 保持网络安全连续性，增强网络易恢复性

Solange Ghernaouti

网络易恢复性的不同内涵

网络风险是人人面临的现实，仅通过收听/收看新闻我们即对此确信无疑。网络犯罪已成为全球公害，且网络攻击已成为军事教导内容之一。2014年9月北大西洋公约组织（NATO）峰会[113]将大规模网络攻击确定为可对之采取军事响应行动的战争行为，如果NATO成员成为受害者，则将被视为是对整个NATO的攻击。我们还有必要认识到在网络空间存在的冲突，最为常见的是瞄准民用和军用信息基础实施的网络攻击和通过操纵信息实施的攻击。在互联网上，既存在对战争和恐怖主义的兜售，也存在合法和非法业务，同时网络犯罪的黑市买卖兴隆。

[113] http://www.nato.int/cps/en/natohq/news_112107.htm?selectedLocale=en（NATO威尔士峰会指南 – 2014年9月4-5日，新港）

互联网也已变成了进行犯罪活动和宣传的、极受追捧的媒介。对信息系统的攻击可能围绕一个国家的关键性基础进行、实施犯罪战略、造成生产和竞争力损失并有助于在一国中进行夺权。此外，互联网使旨在降低或防止一国经济发展的活动更加简单易行，从而破坏一国的正常运行或破坏其稳定。当前，大量信息系统都是网络攻击活动的目标，其目的是通过破坏相关国家的经济、机构或声誉而破坏其稳定性。在更广泛的全球超级竞争环境中，此类活动的开展更是如鱼得水。

多种形式的网络威胁不断演进发展，因此，从跨学科和全球范围角度了解这些威胁十分重要，这样才能够持续抵抗威胁，进而增强民用和军用基础设施的安全性和易恢复性并保护包括中小企业和个人在内的所有经济参与者。持续确保个人和财产的网络安全性并保障公众安全必须成为支持社会长久发展战略的政治项目的组成部分（上述战略本身考虑到了所涉社会的文化和具体情况），这就要求包括私营和公共部门在内的所有组织均在国家和国际层面进行参与[114]。

我们正在创建一个通过移动、无线和无接触通信[115]方式永久连接一起的世界，该世界中事物也在日益智能化且能够进行沟通：这就是物联网以及为发展智慧家庭和城市添砖加瓦的一切事物。诸如汽车和交通灯等普通物体将包括IT构件和互联网技术，因此，由于其程序中内置的智能，它们将能够拥有一定的自主和决策能力。这些物体已开始出现在公共场所并自动成为恶意网络活动的潜在目标，因为与互联网连接的所有实体都可受到黑客攻击，且可成为攻击其它系统的僵尸网的组成部分，其安全弱点可能会给我们的实际安全工作带来破坏性后果。虽然不同复杂程度的机器人对人类及人类日常生活予以协助，但也开始影响我们的生存。由于这些机器人能够影响我们的行为和环境，因此，恶意实体对其的控制也将给我们的社会带来负面影响。二十一世纪是电子RFID芯片和纳米技术世纪 – 智能尘埃构想。电子和生物融合一体的世界正在成为现实，特别在人体和各种传感器以及假体和可植入人体以解决某些缺陷（如胰岛素泵和心脏起搏器）的其它生物医疗电子装置方面。现有神经界面已能够允许人们通过思想与计算机互

114《网络的力量：网络世界中的犯罪、冲突与安全》；S. Ghernaouti，EPFL出版社，2013。

115无接触系指NFC（近场通信）技术。

动。所有这些都可以造福人类，但随着其使用和电子融合程度的加大和日益复杂化，对其最初目标的劫持会导致黑客情况的出现，包括人类思想。这些新的风险迫使我们重新设计安全机制，以便更好地对物体做出管理，保护受到日益加大的技术对社会影响威胁的价值观。

网络世界已成为我们严重依赖的一项文明，因此，其基础设施足够强健并易于从各类事件中得到恢复十分重要。网络易恢复性涵盖若干层面，可以将其分为操作措施，如，打击网络犯罪、开展与网络安全和网络防卫相关的互补活动、有效管理能源和与生态相关的风险，并通过开展教育培育和完善人类在未来信息社会所需的能力。

打击网络犯罪

更好做出准备来打击网络犯罪，已成为国际社会的迫切关切，没有任何一个国家、组织或互联网用户能够免受网络公害，无论是犯罪还是简单刺激的影响。

做出更好准备打击网络犯罪意味着人们在较低和不尽如人意的程度上做好准备。对机构而言，形式如下：

- 拥有解决该问题的手段（即，战略、措施、资源、技能），但数量和质量均不够充分；
- 拥有保护手段，但并非具有所要求的效率和适当性。

尽管这两种情况司空见惯，但仍然有必要指出，对于诸如中小企业和个人等诸多参与者以及与互联网相连接的基础设施和物体而言，尚不存在控制结构和安全措施。

对于国家而言，打击网络犯罪以若干设想为基础：

- 拥有适用且与国际结构兼容的法律框架；
- 建有管辖机构并拥有相关警力，他们拥有资源和能力在国家层面开展工作并与相关国际网络合作，以打击跨境网络犯罪。

在国际层面，这意味着国际社会将团结一起，共同完成打击网络犯罪的事业，且目前不存在无诚信做法完全不受惩罚的数字文化。

以下情形对这样的罪犯十分有利：

- 将互联网看做进行经济犯罪的媒介并将其做为实施犯罪行为（贩卖人口、贩毒、洗钱）的工具
- 将网络空间视为保护层和全球运动场。

打击犯罪工作从来不是一件简单的事情。网络犯罪加大了工作的复杂性并提高了在国家或国际层面打击犯罪的困难程度。

与此同时，媒体经常报道网络犯罪情况，但似乎没有相关足够有效的、旨在限制网络罪犯的力量或减少受害者人数的有效措施。相对于不断扩大的恶意活动，对相关人员的逮捕及审判少之又少，因此，让受害者倍感不公。

尽管如此，在国家采取行动方面已出现两大进展：一是在欧洲层面，于2013年在海牙成立了欧洲网络犯罪中心（EC3）[116]；

- 在国际层面，于2014年在新加坡出台了国际刑警组织全球创新机构[117]。

有效打击网络犯罪需要采取预防性手段，使网络世界不再成为吸引犯罪的媒介并减少犯罪活动的机会。因此，有必要使网络攻击更加难以实施，提高其相关

[116] https://www.europol.europa.eu/ec3

[117] http://www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation

技能和资源成本，从而降低预期收益并增加罪犯被识破的风险、将其找出和绳之以法。总体而言，可通过采取下列行动增强易恢复性：

- 减少技术、组织、法律和人员的漏洞数量；
- 通过连贯一致和相互补充的技术、程序和管理措施，增强信息基础实施的强健性和易恢复性；
- 开发切实可行的能力，调整有关网络安全的防卫手段，以适应不断变化的情况；
- 拥有管理网络危机的手段；
- 打击网络犯罪货币化团伙。

网络空间这一新领域充斥着各类活动。它既有助于人们实现经济利益也是各方行使权力的场所：网络空间已成为战略领域，因此，应在国家经济和安全方面对其予以保护和防卫。

确保安全防卫的连续性，以保障某种程度的稳定性

控制网络风险是在激烈和长期存在的经济竞争（几乎是经济战争）中进行的，与之伴随的是急功近利，货币危机、普遍存在的无序化、社会不公、生态风险和全球治理的某种缺陷。不应只以回顾方式看待网络安全问题（其目的是“熬过”网络事件，无论是人为还是意外事件）。虽然这种抵抗能力至关重要和不可或缺，但它不能取代在国家和国际层面存在的全球多方方式，或对网络犯罪及网络冲突整个现象的切实理解。全球性、跨学科和综合式网络安全和网络防卫方式将既有助于采取适当预防措施，也有助于采取应对措施，其有效性取决于从民事和军事角度出发的全面性和一贯性。如果认为不需要开展国内外参与多方合作即可对网络问题做出相应就过于理想化了，我们的目标是支持有关在网络世界和物理世界建立和平的战略。

有些情况下可能需要重新确立军民之间的合作和对话，以便在整个社会实现安全防卫的连贯性和连续性。必须以跨学科和总体的方式掌握网络安全问题。在国家层面，这意味着不同部门对该问题拥有共同的认识并增强部委间合作，且有能力携手努力。

无论网络攻击的主要目的和对象（个人、组织、国家）如何，其所用工具毫无差异。网络攻击的性质和影响范围因攻击者的目标和动机的不同而不同，但其方法和工具保持不变。对于国家而言，确保公众安全、经济安全和国家安全均属于军民安全的组成部分，这就是为什么将此反映在国家网络安全和网络防卫战略中十分重要的理由，因为只有这样，才能够最大程度地提高所采取措施的有效性和效率，并在和平和战争时期，以最佳方式对人民需求做出响应。与此同时，关键性基础设施的保护永远不是私营或公共部门可单独可以完成的任务 – 这也充分说明需要实现安全防卫连续性的原因。

保护和防卫个人、组织和国家的数字资产和遗产以及支持这些资产和关键性职能的基础设施十分重要。这要求采取相互补充的保护性措施，包括与军民理解的“保护”概念相对应的活动，以保卫易受网络威胁的基础设施和资产。

在这一环境和一个不确定的世界中，在促进国际有关这些问题对话的同时，培育网络安全和网络防卫文化应有助于人们具有一定的信心和保持稳定性，但前提是每一利益攸关方都需要诚信行事并集体负责。要考虑到管理能源和生态风险的必要性。

数字社会以及对我们星球具有重大影响的信息系统的广泛使用还带来我们不应忘记的间接风险，因此在我们有关网络易恢复性的长期设想中，应制定可确保能源长期可用以及为我们的子孙后代保护自然资源和生态环境的措施。

有鉴于此，我们应特别集中关注与下列方面相关的风险：

- 消除并回收电子废弃物；
- 能源消耗（对供电的不断加大和永不停止的需求）；

- 气候变暖（散热和冷却计算机及服务器的必要性）；
- 充分利用建造电子设备所需的稀土和金属；
- 针对净化控制系统、有毒产品的生产和销售以及火警等网络攻击造成的环境影响。

网络易恢复性活动还应满足保护关键性基础设施的需求，最为明显的是与能源和环境有关的重要设施。

从生态角度而言，采取其主动措施来更好预测威胁、管理网络风险、发现异常现象以限制其影响并提升网络易恢复性，是一项集体责任，必须确保开展教育和人力建设工作。

有关网络安全的学说和态势取决于在网络安全问题上（涉及到社会或科技领域的若干学科）得到培训的人员，这一立场设想目前存在这种教育途径。没有全球范围的网络安全技能和能力进行知识转让并开展能力建设方面的合作，就难以使人们的行为适应网络并增强信心。好的IT做法和网络风险意识培养虽然重要，但如果在产品和服务设计开始阶段不将网络安全概念纳入其中，或如果政治和经济参与方（从年龄最小到年龄最大的网络用户）或警察或司法系统不能够由于缺乏技能而履行其职责的话，则不足以进行网络防卫工作。仅让公民了解互联网固有的风险并采取最基本的预防措施，或由其负责大多无法掌控的情况是不够的。在现实中，如果让最终用户和公民承担风险造成者带来的风险，进而将社会问题转嫁到人们（他们本身不具备所需的补救专业知识或手段）头上是不公平的。

网络易恢复性构成网络安全新挑战

从犯罪活动中恢复是全面的有关网络安全愿景的组成部分并有助于提高人们对网络的信心。当前，人们迫切需要通过适当技术、管辖、组织和程序措施加强基础设施的强健性和可恢复性。如同所有安全活动一样，有关打击网络犯罪、网络滥用和挪用的斗争是复杂的，必须从保护人员和有形及无形资产以及维护得到

广泛认可的共同价值观的角度开展这一斗争。因此，有能力拥有高效和有效的网络安全和网络可恢复性将十分有益。

为避免使信息社会成为互不信任和互相监督的场所，有必要对人们的需求做出令人信服的响应，以使人们树立对网络空间的信心并提高网络的恢复性，同时应提出有关保护数字资产和基础设施的切实可行的方案。必须通过国家和国际层面的政治意愿、资源和技能、组织结构和程序以及适应形势的协调机制努力防止网络空间的恶化。对任何合法或任何存疑参与者而言，社会稳定这一新要素是其安全工作的组成部分，与其在可接受限制范围内控制网络风险并维护网络稳定的能力密切相关。网络安全不应成为由国家主宰或行使权力的工具，而应成为维护稳定和发展和平的手段。[118]

[118] 正如《探寻网络和平》出版物所强调的那样，在全球层面增强网络信心将有助于解决所提出的主要网络和平问题 –国际电联，2011年（http://www.itu.int/pub/S-GEN-WFS.01-1-2011）

第三章：网络自由

引言

此前各章着重阐述了提高网络易恢复性、以确保网络空间能增强人们的信心的至关重要性，本最后一章总体介绍有关网络自由方面存在的挑战以及公共和私营部门面临的相关威胁，这些威胁严重破坏了人们实现互联网自由的希望。

在文明社会中，表达意见和言论的自由，获取信息的自由和隐私权始终是核心要素，因为这反映了形成民主原则和价值观基础的基本人权和公民自由。互联网和信息通信技术的出现使全球数十亿人拥有了迄今为止无法想象的、获取大量信息和通信手段的机遇。毫无疑问，它们代表了广大的交流意见、数据和创新想法的平台。然而，与此同时，数字时代的这些基本工具也被企图破坏进步、政治权利和隐私的人们利用，从而动摇了人们对使用这些手段的信心。

正如欧洲人权法院在多种场合所强调的，“言论自由[...]不仅适用于受到人们赞赏或被视为不具冒犯性或为无所谓的“信息”或“想法”，而且适用于使国家或任何一部分人口受到冒犯、震惊或扰动的信息和想法。”[119]

尽管博客和社交媒体为交流思想开辟了全新机遇，但近年来，某些国家扩大了政府审查制度，对互联网进行封堵，企图控制公众意见并破坏人们的信息和言论自由。

这对互联网具有优势的功能特性提出了挑战 – 无边界、普遍存在和在世界各地接入 – 当前进行的有关网络中立性的讨论也突显了在确保人们拥有平等权利来接入这一不可或缺的媒介方面存在的问题。

---

119 欧洲人权法庭Handysive对英国案例 http://hudoc.echr.coe.int/sites/eng/pages/search.aspx#{"dmdocnumber":["695376"],"itemid":["001-57499"]}，17/10/2014最新更新

当今信息社会的一大特点是广泛存在唾手可得的大量数据，同时突显了公共和私营部门中正在出现的间谍威胁，后者使我们的隐私权和数字工具的安全使用受到威胁。事实上，为了确保国家安全，由政府进行的监控可迅速实现对个人信息的大量收集和存储，使人们难以在可接受和被认为已跨越红线、因此成为不可接受的做法之间做出区分。

与此同时为了充分受益于方便的数据保护机制，私营部门为了获得经济和竞争优势，收集并跨境传送大量个人数据，为个人数据带来了新的风险。

由于互联网具有无国界性质，因此只有国家法律是不足以确保互联网自由的，这也是为什么详细制定并通过旨在树立网络信心的国际框架是如此不可或缺。

本章分为五节。第一节强调说明目前缺乏完善的法律框架，该框架在网络空间和互联网自由方面影响到公民自由的保护（如目前阿拉伯世界中诸多地方的情况所表明的那样）。其次，本章突出介绍围绕大数据和数据保护开展的讨论，旨在着重说明有必要建立国际监管框架，以维护互联网的自由和人们的隐私权。第三节探讨国家监控和网络世界的情报收集问题及其对有关树立使用网络工具的信心的影响。

第四节讨论欧洲如何看待政府对数字隐私和数据保护的侵犯以及欧盟在此方面采取统一政策的重要性，这不仅有助于促进其成员国之间的合作，而且构成了跨越其边境的范例。最后一节旨在确立有关网络自由（作为一项基本人权和有力的、树立网络信心的手段）管理的标准。

3.1 网络自由：进步与挑战

Mona Al-Achkar

引言

强大的新技术为人类带来了全新时代，在该时代中，多层面的技术限制被彻底消除，且在这一数字时代中，个人和国家均得到了前所未有的赋能，不仅能够实现发展，而且可以滥用技术和实施暴力。

该悖论充分体现在数字时代中无可否定的利益之中。在该时代中，个人、企业和国家对信息通信技术的依赖日益加大，因此面临的风险可为花样翻新，且网络世界的犯罪活动日益猖獗和复杂化。国家安全受到了更加严峻的威胁，关键性基础设施日益受到多重风险（包括通过互联网实施的攻击）的影响。

与网络犯罪如影相随的是法律框架的不兼容和缺失，这依然是破坏人们有关使用网络空间平台信心的主要因素，因为这为法律不安全性的产生带来便利，并妨碍公民实现充分自由。由此，对互联网实施监控（policing）对诸多公民自由带来了切实威胁，如隐私、言论自由、防止自陷法网、毫无根据的搜查和没收以及行使法律程序的正当权利。这些公民自由得到保护的程度在很大程度上取决于特定国家或区域业已确立的立法、法律惯例和政治制度。

保护这些公民自由、进而使人们树立对网络世界的信心是确保实现值得信赖的网络经济环境的首要条件，PRISM（棱镜）事件对这一点进行了很好的诠释。该事件表明，美国国家安全局对外国人的个人数据进行收集并开展间谍工作。情况暴露后，思科公司宣布其收入降低了8%至10%，且据预测，由于世界经济的整体情况以及PRISM丑闻的影响，2013-2014年的活动和收入会进一步降低。

这种大规模的监控以及新出现的“网络压迫”和“电子警察国家”理念都说明，无论是在集权国家还是在民主国家，上述诸多公民自由都在被消弱。

公民自由

“公民自由”一词源自拉丁语（“ius civis”），意思为“公民权利”，它衍生于Magna Carta（大宪章）- 旨在限制当局滥用权力。这就是为什么公民自由被认为能够防止政府采取非法做法或行为并防止他们违反基本法律权利。

人权是普遍的/同样适用于各个国家的，但公民自由与各国的国家立法相关。因此，每一个国家都按照各自的国家法律系统赋予其公民基本自由。公民自由最重要的一点是限制了国家对公民生活的干扰程度和各种形式的权力滥用，从而确保公民有能力在不受到歧视或压迫的前提下，参与国家的民事和政治生活。

公民自由包括个人、政治和经济权利，如，公平审判权利、正当程序权利、结社自由、请愿权利、自我防卫权利、投票权、免于成为奴隶或进行强迫劳动的自由、免于受折磨和死亡的自由、自由和安全权利、意识自由、宗教自由、言论自由、表达自由、隐私权、个人财产权、结婚权、个人防卫权、身体完整权、使用设施权、平等接受教育权以及参与公共职能的权利。

通过国内法律确立的公民自由可具有共同的法律基础，如公民自由侵权行为，这将有助于个人在被冤枉或受害（由于其基本权利被践踏）时不仅得到其他个人的赔偿，而且得到政府赔偿。这种侵权行为包括不请自入的对家庭或个人隐私的入侵、诽谤或非法侵占。

信息自由：获取信息的权利

信息自由或获取信息的权利是一项全新的权利，它既不同于言论自由权，又与之密不可分。可将该权利定义为获取由公共机构所持信息的权利[120]。

英联邦秘书处专家组会议发表的最后文件（考虑到了第19条）表明：“应将信息自由作为一项法律和可实行的权利予以保障，以允许每一个个人都能获得由

[120] http://www.unesco.org/new/en/communication-and-information/freedom-of-expression/freedom-of-information/

国家行政、立法和司法机构以及政府拥有的公司和行使公共职能的其他机构所持有的记录和信息。”

该自由背后的基本原则是公民的知情权、政府对其公民披露信息的义务以及由信息请求接受方承担举证责任的事实。这就为什么多数政府将他们不希望披露的信息分类为保密信息，或处于国家利益理由不予披露。

获取信息权包括寻求、接收、分享信息和想法的权利，既包括积极寻求信息的各方，也包括希望通过媒体或官方渠道收到信息的各方。多数情况下，该权利涉及公共信息的获取，它凸显了公共行为原则以及公共行政的透明度，因此，它的应用直接关系到公民对政治生活以及反腐机制的积极参与。

联合国大会第59（1）决议表明：“信息自由是一项基本人权[...]，“ 属于联合国所致力维护的一切自由的关键”[121]。同样，《利马原则》序言或《查普特佩克宣言》确认，“[...]个人言论自由和信息自由获取权利对于所有民主社会的存在至关重要，且对于人类进步、福祉和享有其他各项人权不可或缺”。[122]

此外，信息社会世界高峰会议在《突尼斯承诺》中重申，各国有必要尊重人权和基本自由，并认识到，“[...]在信息社会中，言论自由和信息、思想及知识的自由流动”十分重要。[123]

因此，信息获取权被认为是特别享有言论自由和信仰自由的根本所在。它涉及到政府确保信息和思想自由流动的义务。联合国意见和言论自由特别报告人Abid Hussain在其1995年提交联合国人权委员会的报告中表明：“如果人们无法获得信息，自由也就完全失去它的效力。能够获得信息是民主生活方式的基本，因此，必须坚决抵制对人民普遍扣押信息的倾向。”

---

[121] http://www.rjionline.org/MAS-Codes-Peru-Lima-Principles

[122] 联合国大会，（1946）第59（1）决议，第65届全体会议 http://foishehri.wordpress.com/

[123] http://www.itu.int/wsis/docs2/tunis/off/7.pdf

各国在获取信息的自由程度方面不尽相同，近期此方面的一些最新发展尤为值得关注。例如，在最近出现“阿拉伯之春“运动后，一些阿拉伯国家在其宪法[124]中纳入了有关保障信息权的内容[125]。而另一个例证则是，美国的《爱国者法案》使美国公民更加难以获取其政府的信息。

尽管各国被要求认可和尊重这一权利，但是应当指出，当相关国家政府认为该权利妨碍或影响到国家安全、领土完整性、公众安全保护以及防止犯罪、保护健康及其他个人有关隐私、荣誉或权利时，往往被予以限制。事实上，这些限制应按照相关法律并按照保护管辖中立性和民主机制正常运行的要求加以决定。

在网络世界，信息自由能赋予个人和组织权能，使他们享有更大程度的言论自由和社会交流。与此同时，它也带来了一套全新的可能限制社交媒体使用的挑战，“阿拉伯之春”以及由维基解密窃取的文件即是例证。这些挑战除对国家利益和保密数据的保密性造成影响外，还突出说明了国家和部门实体在互联网上所做的限制和监控。

在2004年8国集团承诺（创建有利于进行非正式、灵活、开放和具有包容性的对话）的基础上，中东和北非国家于该年下半年出台了称作“未来论坛”的举措。随后在2008年7月，来自巴林、埃及、约旦和摩洛哥的阿拉伯国家民间团体组织成立了“信息自由网”。然而，尽管该区域在携手倡导发展工作，但多数国家在信息自由立法方面止步不前。约旦和突尼斯仍然是仅有的已颁布《信息获取法》的两个阿拉伯国家，尽管在巴林、埃及、科威特、黎巴嫩、摩洛哥、巴勒斯坦和也门已开始了有关此方面法案的讨论。2004年，在美国律师协会的协助下，黎巴嫩的一个律师小组起草了《保护举报人》法律草案，并由“黎巴嫩国家信息获取权网”于2010年提交黎巴嫩议会。

---

124 http://www.shorouknews.com/news/view.aspx?cdate=30092013&id=9bc20aff-06e7-4c44-8c45-fc197559616f

125 http://www.shorouknews.com/news/view.aspx?cdate=30092013&id=9bc20aff-06e7-4c44-8c45-fc197559616f

隐私：防止出现世界性情报社会

隐私是与个人自由、尊严和人格直接相关的公民自由，它体现在公民不受其政府对其生活进行不必要干扰的权利之中，如，未经授权即对其家庭进行搜查并窃听其信函/通信。在数字时代，需要在全新环境中考虑隐私，它不再局限于物理和物质环境的保护（如家，邮件或文件），而是拓展至网络世界中海量的个人数据以及极高的连接程度，后者正在使每一个个人都成为“世界性情报社会的传感器”。[126]

什么是对隐私的充分保护，在此方面尚未取得全球性共识。尽管如此，目前已存在基本的、有关隐私权的国际法律框架，我们可以将其延伸至信息世界，并反映出国际、区域性、国家立法、宣言、公约和条约的规定。

《世界人权宣言》第12条承认隐私为基本人权。按照该宣言，任何人都不得成为其隐私、家庭、房屋或通信受到任意干扰威胁的对象，且人人拥有在此方面受到法律保护的权利。

《国际公民和政治权利公约》第17条规定：“任何人都不得成为其隐私、家庭、房屋或通信受到任意干扰或其荣誉和尊严受到非法攻击的对象，因此，人人均有免受此种干扰或攻击的法律保护的权利。”

其他一些导则、公约和指令如下：

- 经合发组织1980年发布的“保护隐私和个人数据的跨境流动导则”；
- 欧洲理事会（CoE）1981年制定的《保护个人数据免受自动处理影响公约》；

126 Philippe Langlois – 巴黎“第一优先安全”公司创始人，有关机构收集智能电话用户个人数据的能力。
http://www.nytimes.com/2014/01/28/pageoneplus/quotation-of-the-day-for-tuesday-january-28-2014.html?_r=0

- 欧洲理事会1989发布的“电脑化个人数据流使用导则”；
- 联合国1999年发布的“电脑化个人数据文档监管导则”。

上述法律文书规定了个人信息各个处理阶段（收集、存储、传播、使用、传送等）的最低隐私保护原则，同时，承认个人有权获取其个人数据、予以更新并得到有关数据收集工作的方法和目标方面的信息。此外，这些文书确立了个人具有在数据被收集和处理后对其予以销毁的权利，这是对网上被忘记权的补充。在区域层面，一些国家已确立了有关隐私问题的一套程序和最低妥善保护标准。

欧盟于1995年出台的“数据保护指令”允许为实现具体、明确和合法目的而收集个人数据，但禁止持有非最新、不相关和不准确的任何数据。此外，欧盟成员国有义务在缺乏相关措施的情况下停止向国外传送这一数据[127]（上述措施有助于保护公民数据及其获取、保护、修改和拒绝第三方使用其数据权利的权利）。

例如，为方便数据跨境流入没有此类充分保护的美国，欧盟与美国达成“避风港协议”。该协议允许一些美国公司收集有关欧盟公民的数据，但前提是，前者证明他们能切实确保该数据按照欧盟标准得到保护。此外，还要求这些公司通知欧盟公民其数据是如何处理和使用的，并承认其获取、撤回或修改这一数据的权利。

在区域层面，欧盟数据保护指令规定，其成员之间可进行个人数据自由流动，并规定在成员国国内法律中采用该指令条款，同时允许欧盟成员国自行采取指令实施方式。必须保证数据主体有关了解数据发源地的权利、对不准确数据予以纠正的权利、在出现非法处理数据的情况下进行上诉的权利以及在特定情况下拒绝允许使用其数据的权利。

---

127 欧洲议会和理事会1995年10月24日第95/46/EC号指令 – 在个人数据处理和此类数据自由流动方面对个人予以保护 – 官方期刊L 281 , 23/11/1995 P. 0031 - 0050

– （57）另一方面而言，必须严禁向不能完善确保个人数据的第三方传送此数据

在国内层面，几乎所有国家都在宪法中对隐私权予以承认。一些国家新宪法（南非）和许多欧洲国家还批准了有关对个人数据监控予以监管和保护公民隐私的法律[128]。联合国通过批准相关决议草案对隐私保护给予支持[129] – 该决议由巴西和德国起草，标题为“数字时代的隐私权”。[130]

言论自由：民主社会的标志

在民主社会中，立法、言论自由和民间团体的独立性是自由和公民自由的保护神，而专制制度的标志则是警察不受惩罚、审判不公和随意羁押。

《世界人权宣言》第19条以及《国际公民和政治权利公约》第19条规定，“人人享有意见和言论自由权，该权利包括在不受干扰的条件下保持意见的自由以及不论其疆界如何和通过任何媒体寻求、接收和传播信息的自由。”言论自由意味着通过各种通信手段（如书写、绘画、广播或博客）就经济、政治、社会和其他议题自由表达想法和信仰。因此，新闻自由和社交媒体使用的自由是该自由的组成部分。

同样，《欧盟基本权利宪章》第11条 – 对应于《欧洲人权公约》第10条 – 规定：“人人享有言论自由权。该权利须包括持有意见和在不受公共主管机构或无论其疆界如何的情况下，接收及传播信息和思想的自由。”此外，该条表明：“这种自由的行使也涉及到相关义务和职责，因此，可能需要受到法律规定的程序、条件、限制或惩罚的约束，且在民主社会中，处于国家安全、领土完整性或

---

128 FISA 2008年修正法案，法律执行法案的通信协助，美国，

– 1998年数据保护法案及英国调查权利监管法案（RIPA）– 法国1978年电子信息与公民自由法案 – 《欧盟个人数据保护公约》，欧盟数据保留指令

129 联合国大会支持数字时代的隐私权。

http://www.un.org/apps/news/story.asp?NewsID=46780&Cr=privacy&Cr1=#.UwCw6ThWHZY

130 第六十八次会议 – 第3委员会 – 议项69（b）– 促进和保护人权：人权问题，包括改善有效享有人权和基本自由的替代方式。

公众安全的利益或为避免出现无序或犯罪，或为保护健康或士气，或为保护荣誉或其他人的权利，或为防止披露收到的秘密信息，或为保持辖区的权威和中立性，这种约束是必要的。”此外，与一切权利限制和自由相同，该条认可有关必要性和比例性原则，并承认有必要制止任意干扰或歧视做法。

由此，言论自由被视为是政府和政治制度获得公民信任的要素之一，它有助于落实其他人权、更好地了解公共政策、形成十分知情的公共意见并享有通过媒体表达关切的自由。在国家层面，许多国家都在宪法中承认言论自由是民主制度的标志。在此方面，联合国大会认为，对电信网络予以监测威胁到了人权和诸多公民自由，从意见和言论自由到隐私权和政治激进主义，因此它动摇了民主社会的基础[131]。

有鉴于此，在线言论自由须得到尊重，所以，期望政府绝不扼杀言论自由并应消除此方面的障碍。特别应当指出，为了公民的表达自由，期望政府制止旨在消除反对声音的网络压制以及通信监听、内容检查或网站封堵。

然而在现实中，言论自由并未在很多国家得到尊重。一些国家政府为限制网上言论自由，除以国家安全和打击恐怖主义作为理由外，还倡议对宗教价值和礼仪进行保护。他们对其认为明显包含色情或煽动种族、宗教其他文化仇恨或鼓励进行恐怖主义活动的内容进行检查，其风险在于为谴责此类内容而使用的法律术语，这些术语通常可被扩大，也就是说，可能缺乏司法客观性和稳定性，因此导致权力滥用。

社交媒体

传统上而言，组织抗议（有时导致形成革命）的初始步骤为讨论、交流观点和共同目标以及进行游说。在“阿拉伯之春”期间，通过社交媒体进行的大量有

131 联合国大会 – 2011年5月16日 A/HRC/17/27 – 人权理事会第十七次会议议项3 – 促进和保护各种人权、公民、政治、经济、社会和文化权利，包括发展权。“数字监控与日俱增的使用和复杂化远远超出了社会对之进行适当立法的能力，因此导致已无法由任何独立主管机构予以监督的临时性做法，”从而对言论自由构成威胁”。

关互联网自由和民主的交流以及公民日益增长的影响国家政治的能力，对形成该场运动政治讨论的方向起到了关键性作用。博客、推特的发布和YouTube的上载，都为人们带来了进行赋能的新空间。正如埃及一位活动家所说：“互联网应得到最高程度的保护，免受政府入侵。如果想要使人民得到解放，就让他们使用互联网吧。”

社交媒体有助于以前所未有的方式调动人民并进行不同国家人们之间的信息交流。它为组织和输送信息提供了极大机遇，并有助于形成反对集团并、招募民兵、获得更多的支持者、传播思想意识和创建内部及外部支持网络。在“阿拉伯之春”期间，民兵利用社交网络获得了区域和国际支持并组织开展了宣传活动。

尽管社会媒体不能取代酝酿成功革命所需的实际行动，但它向阿拉伯民众提供了将信息用作反压迫有力武器的机会。阿拉伯之春运动的参与者利用社会媒体保持连接、交流信息、传播有关目前发生的事件的消息、组织其活动、发布信息和新闻、向世界传递信息并影响公众舆论。通过手机传送的照片与视频有助于搜集有关政府军队及其阵地的信息。政治行动则主要通过社交网络举办和宣传。在阿拉伯之春运动之前和期间多个阿拉伯国家出现了体制变革，反对派组织的推儿微博迅速传播，覆盖了数以百万计的观众和脸谱网页。博客急剧膨胀，激发整个区域就民主、自由和透明度展开讨论。数百万民众登陆社交媒体，创建的许多网页和网站推动了反对派通过在线信息和博客走出去的步伐。部分积极分子利用其移动电话提供实时的事件短片，并将它在脸谱、推特和其它社交网络发布。如今，不同国家在各类社会、政治或经济抗议活动中经常采用许多当时流行的口号。

过去一年，黎巴嫩的言论自由受到打击，令人深感不安。黎巴嫩民众因为其尤其涉及社交媒体的在线活动而受到逮捕、拘留和恐吓的冲击，毁损了该国作为言论自由堡垒的声誉。

黎巴嫩的政客面对140个字的微博和其它社交媒体内容的执着挑战，似乎愈发处于守势。例如，四个脸谱用户因为辱骂共和国总统而被捕，一位微博用户被判处两个月监禁。在另外一个案例当中，一个博客用户受到八个多小时的拘禁，

如其写作在诗词之外涉及政治，就会受到起诉的威胁。多位博客用户受到网络犯罪管理机构的询问，一些博客被封，其中包括一份有关主要超市连锁店工人受不公平待遇的帖子。

这些近乎专制国家制裁的这类裁决是过去黎巴嫩所不常见的，过去该国的言论自由是比较宽松的。

危险：事实和参与者

网络空间是国家安全的新维度，是情报搜集的宝贵信息源。但依靠安全实体的传统信息监测和采集方式已不再适用。

如今，有必要发现和确定策划者，并防止网络可能的恶意和犯罪行动。为此，旨在对计算机网络和用户进行广泛监控的先进技术正在得到部署，以发现、确定和追踪入侵者，并保护基于证据的数据。

个人数据的采集和民权的相关滥用已成为全球媒体的报道重点；其中斯诺登、维基解密和Tempora[132]披露的情况导致了通过SORM-2和SORM-3[133]、单寄存

---

132 Tempora是英国政府通信总部（GCHQ）于2008年测试[2]和2011年运行使用的秘密安全电子监控程序。Tempora利用构成互联网骨干网的光纤上的窃听装置，以接触到大量互联网用户的个人数据。http://en.wikipedia.org/wiki/Tempora

133 - 这些法律似乎做出如下规定的俄国宪法第23条：[32]

1. 每个人都享有其私人生活、个人和家庭秘密不受损害及其荣誉与名声得到保护的权利。
2. 每个人都享有信件往来、电话通话、邮政、电报和其它信息的隐私权。只有法院裁决才能使这一权利受限。

器[134]和社交网络[135]审查收紧了对网络的控制。近来，一些国家的政府采取措施强化互联网控制，以确保能够进行在线的用户确认[136]。

安全机构可以访问私人数据并与情报目标清单进行比对。监控技术使它们能够利用谷歌地图或动态追踪GPS系统以及社交网络发布的照片嵌入的组件，对目标进行精确定位。它们还可以利用这些技术以记录和存储电子邮件的方式，获取家庭成员和朋友的地址清单和电话记录。秘密的英国情报文件披露，间谍甚至藏匿于流行游戏应用的背景中，以获取披露玩家位置、年龄、性别和其它个人信息的数据。

这种现象使隐私和许多民权变得脆弱不堪。但对我们的隐私和其它民权的挑战不仅来自政府。公共和私营参与方都对个人进行非法监控，因为这有助于市场营销和情报采集。大大小小的公司会监控我们购买的产品，通过汇编个人数据向人们的移动电话发送定制广告，存储和分析数据并将它用于商业目的。他们有时重点搜集被他们称之为主要有种族和色情倾向的可选性的敏感数据。

政府通过互联网过滤部署特洛伊木马[137]等恶意监测工具和限制在线匿名行为等措施开展新闻检查。这些措施旨在通过简化确认访问或传播受禁内容的个人实现国家对通信的监控，并进行情报采集。

---

134 Andrei Soldatov和Irina Borogan制作的“前苏联国家的俄国间谍技术依然在监视你”节目 – 2012年12月21日上午6:30。
http://www.wired.com/dangerroom/2012/12/russias-hand/all/

135 金、Gary、Jennifer Pan和Margaret Roberts2014年著。通过随机实验和参与者观察对中国新闻检查进行逆向工程。拷贝见http://j.mp/16Nvzgehttp://gking.harvard.edu/publications/randomized-experimental-study-censorship-china

136 中国订购在线视频上传实名记录器。
http://www.reuters.com/article/2014/01/21/us-china-internet-idUSBREA0K04T20140121

137 中国QQ应用就被视为大型的特洛伊木马。

采集数据和录音通信的量十分惊人，且令人不安，对隐私和民权构成了严重威胁。

然而这些监控也表现出某些积极的方面。例如，监控帮助挫败了基地组织2007年的德国爆炸阴谋，以及对毒品[138]和儿童色情网络[139]幕后指使的批捕。我们还可就此引述欧洲的INDECT项目，即“支持为城市环境中的居民开展观测、搜索和发现工作的智能信息系统”，其目的在于确保公民安全，主要免受暴力干扰。

阿拉伯世界的焦点[140]

多数阿拉伯国家是联合国成员，并且都是位于北非和东北非和西南亚洲的独立阿拉伯国家构成的阿拉伯国家联盟的成员。该联盟的宗旨是加强成员国的关系，促进这些国家间的合作，并捍卫它们的独立和主权。具体而言，其目的在于强化经济、金融、通信、卫生、社会和文化领域以及就涉及民族、护照、签证、判决的执行以及罪犯的遣返等问题的紧密合作。

阿拉伯国家根据普遍人权宣言第19条和仿效上述第19条定义的阿拉伯人权宣言第32条的规定，致力于遵守言论自由。

社会的大多数和传统以及宗教通常被说成是施加限制和压制的理由。某些国家采取了应急法律，总是试图通过迫害敢于自由表达思想的人士抑制不同意见。这些人士可能因为犯有加入“非法组织”罪、叛国罪或阴谋破坏国家安全和利益

---

138 大毒枭古兹曼落网http://news.yahoo.com/internet-crucial-venezuela-battleground-075124059.html

139 NSA的高技术监控措施帮助欧洲捕获恐怖分子的方式

http://www.civilbeat.com/articles/2013/06/21/19341-how-the-nsas-high-tech-surveillance-helped-europe-catch-terrorists/

140 这里将由阿尔及利亚、巴林、科摩罗、吉布提、埃及、伊拉克、约旦、科威特、黎巴嫩、利比亚、毛里塔尼亚、摩洛哥、阿曼、巴勒斯坦领土、卡塔尔、沙特阿拉伯、索马里、苏丹、叙利亚（中止）、突尼斯、阿联酋和也门组成的阿拉伯联盟成员国定义为阿拉伯世界。

罪而受到野蛮逮捕、拷打和监禁。一些政府利用blue-coat代理和外国技术追踪和阻断持不同政见者的通信，强化其限制民权的能力。

尽管各国政府宣称只对色情网站进行检查，但网上的新闻检查范围广泛。用户可能发现自己被引导到一些保留了被认为不符合当地宗教、文化、政治和伦理价值观的被禁网站集成清单的代理服务器。多数记者和博客主要在涉及当地政治、文化、宗教或任何其它当局认为政治或文化敏感议题的问题上实行自我新闻检查。总而言之，他们避免批评国家元首或其他官员，或发布有可能损害国家声誉、对外关系或国家经济的信息。诽谤是一种犯罪。

在2009年知名的阿拉伯联合酋长国的案例当中，驻迪拜的英文Khaleej时报自由职业记者Mark Townsend被指犯有诽谤罪行，并且在调查进行的近两年期间无法离境。刑法第373条指控他对政府持有30%股份的Khaleej时报进行批评，并面临两年监禁和高达20,000第纳尔（5,400美元）的处罚。他最终于2011年5月被无罪释放。在2011年的另一桩案件中，五名阿联酋活动家被捕并受到在阿联酋Hewar互联网论坛的帖子当中侮辱阿联酋领导人的指控。他们受到监禁处罚。

从较为积极的角度看，互联网已成为一个积极分子组织活动和进行游说活动的空间。但需要附带说明的是，一旦发生反政府的集会游行，阿拉伯国家政府就会关闭互联网。

阿拉伯世界主要以实体和物质的形式看待隐私。重点关注的是家庭、个人信件和通信的不可侵犯性。阿拉伯的法律系统除了在少数情况下根据宪法或法律提供保护外，无法充分保护隐私权。

虽然政治领袖对隐私的议题进行了广泛讨论，但黎巴嫩并未给予隐私明确的法律地位。隐私受到宪法和立法条款的综合保护。与美国宪法十分相似的黎巴嫩宪法，并未对隐私权做出定义。不过，它为个人和个人的住所及私人财产提供保护。

部分条款保护人的生命不会因暴露在某些具体条件下而受到侵害。第17条指出，居住场所不可侵犯，除特殊情况和根据法律确定的行为准则外，任何人不得擅入。此外，窃听法指出，公民享有其本地和国际有线和无线通信方式的隐私权。

黎巴嫩宪法承认人民享有人身、住房、文件和财产免受无理搜查和罚没的权利，只有在法律根据实际情况授权才可进行搜查和罚没。在效仿全球许多政府做法的黎巴嫩，为侵犯隐私、并在这一过程中削弱多项人权有理的法理依据无一例外地是围绕着诸如国家安全、遏制恐怖主义和保护公众福祉的借口。

类似借口也被用于说明政府封锁有时用于在阿拉伯世界推动和组织抗议活动的互联网社交媒体的正确性。

2013年3月，无国界记者组织将多个阿拉伯国家确定为“互联网公敌”[141]，因为它们的打击博客等行为严重破坏了信息自由和人权。

阿拉伯国家联盟与民权

阿拉伯国家联盟是由六个国家（埃及、伊拉克、黎巴嫩、沙特阿拉伯、叙利亚和外约旦）在联合国诞生的七个月前成立的，现有二十二个阿拉伯国家成员国。

联盟于1945年确定的宪章未提及人权。此外，阿拉伯联盟法律文件也未对人权捍卫者的保护做出具体规定。

另一方面，该联盟通过将法律和司法术语、结构和程序的统一，成立了一个研究建立更为完整和谐法律体制的委员会。为将这一委员会的建议付诸实施，该联盟在贝鲁特建立了阿拉伯法律和司法研究中心。该中心阐述了大量与阿拉伯国家就网络犯罪立法模式等共同关心的法律问题开展合作的公约，并与许多国际和

[141] 2013年3月记者无国界 – 聚焦5国政府和5个公司的有关互联网监控的特别报告，题为“互联网公敌”。http://en.rsf.org/special-report-on-internet-11-03-2013,44197.html

区域组织以及研究互联网治理问题的民间团体开展合作。例如，它与联合国西亚经济社会理事会共同建立推出了阿拉伯互联网治理论坛。此外，它还于2009年成为泛阿拉伯网络安全观测站的创始成员国，并启动了提交阿拉伯司法部长理事会的阿拉伯网络安全公约的起草进程。这项草案明确提及互联网民权的保护问题，将它作为网络空间使用信心的要素。与此同时，该中心还就与人权和民权，尤其是隐私、信息使用和言论自由权利为ICT决策者推出了许多论坛和年度会议。

结论

有必要做出统一的立法努力，在民权保护的必要性、互联网用户隐私权以及更为重要的是言论自由与应对国家安全面对的网络威胁的必要性之间找到适当平衡。这方面的成功案例能够使网络空间避免成为新的监控领域。

各国应根据国家法律法办网络犯罪，通过事前和事后应对措施的结合保护民权。一个为向各方提供合理最低限度可接受程度保护的专项国际条约或协议，将有助于信息交换当中的隐私保护，并辅之以打击跨国网络犯罪的有效的国际合作框架。阿拉伯国家联盟法律和司法研究中心就此请我起草一份有关合作打击跨境网络犯罪的阿拉伯公约草案。

这一合作框架中的调查、追踪、诉讼都必须根据国家法律进行。同样，任何经授权的国际执法程序都应根据国内立法和法律互助条约的规定进行。国家应采取保护国际敏感信息交换的特殊程序和措施，并对计算机网络及数据采集和处理进行检测。这对于缺少适当水平隐私立法的国家尤为必要。

应对防范非法搜查与罚没给予特殊关注。网络空间的技术特性伴以网络犯罪的与日俱增以及相关国际刑法框架的缺失，都使确保民权得到遵守的任务更加复杂化。

在多数国家法律体制当中，警察的行为受到保护公民免受执法权力和行动，如不当的搜查与占有和在这类执法行动中违反民权的现象。

由于许多国家依然缺少网络空间法并在涉及网络的问题上参照通用的刑法，其各自政府可以另行通过旨在防止在此领域滥用民权的指导原则。这些指导原则应首先明确在对尊重民权要求合理例外情况的限度内，合法搜查与占有的理由。指导原则的草拟者可从设计“平面原则”或“紧急情况”的传统法律例外情况中汲取灵感。

加密、匿名重邮器服务器、安全匿名通信、防火墙和代理服务器等不同保护措施可以抵消这类例外情况的影响。许多这类技术都能够抵御网络犯罪，并使隐私权得到强化。为网络争得信任。

3.2 互联网自由和大数据的法律、政策和监管框架

Pavan Duggal著

引言

当今的能动世界因为网络空间的迅猛扩展而出现革命化变革。互联网开创了地域历史，但这个网络空间创建的无疆界媒体已成为全球各国政府重点关注的议题。因此，提出网络空间的适用政策和监管框架已成为燃眉之急。

互联网完全是以电子形式的数据和信息为基础的。实际上，“数据”“信息”这两个字可互换使用，而且两者都是指创建内容架构和为浏览互联网的通信频道的基础所必不可少的构建。

互联网的发展经历了一个漫长的过程，从上世纪60年代末期的高级研究计划署网络（ARPANET）发展成为万维网，并进一步演变成为当今时代的社交媒体和社交、移动、分析和云（SMAC）。互联网是一个巨大的平等因素，他向所有用户提供了自由使用信息的权利，并以无数种方式帮助他们解决日常人类活动各方面的问题。

互联网创建了海量数据。谷歌前首席执行官Eric Schmidt于2010年指出，“目前我们每两天创造的信息量就相当于人类有文明开始一直到2003年为止所创造信

息量，something like five exabytes of data”与这一惊人的增长相呼应，IBM表示他们每天生成250亿亿字节的数据“[…]其中当今世界90%的数据是在过去两年当中创建的”。然而通过原引统计数据进一步反应这一情况的IDC-EMC报告指出，数字宇宙每两年扩大一倍多，到2020年将达到40,000艾字节（4千万g字节）[142] [143] 经济学人杂志在其2012年展望中报告说全球数字数据总量从2005年的130艾字节增至2010年的1,227艾字节，预计将于2015年达到7,910艾字节[144]。数字生态中大数据的出现就针对大量数据的担忧起到了推波助澜的作用。

本文研究了互联网自由和大数据的法律、政策和监管框架。

定义

在进一步研究与互联网自由相关的法律和监管问题前，需要注意不同学者和法学家对这一术语提出的不同定义。

互联网自由的定义是一个广泛和具有争议的议题，尚没有得到普遍认可的定义。奥巴马总统曾指出：“互联网较所有其他人类历史上的技术进步都更加迅速和广泛的释放了创新、获得支柱的增长以及倡导的自由。它的独立性是其力量的源泉。互联网提供一种不受政府干预的独特的沟通体制。”[145]他还重点指出：“网络自由与网络中立规则并行不悖，而且独树一帜地不受政府干预。”

---

142 http://freestatefoundation.blogspot.in/2012/08/the-true-meaning-of-internet-freedom.html

143 http://www.baselinemag.com/analytics-big-data/slideshows/surprising-statistics-about-big data.html#sthash.COE9uzq6.dpuf 4, 2014年8月4日最后一次更新。

144 “欢迎来到尧塔世界”，2011年12月《经济学人》杂志对2012年的展望；http://www.economist.com/node/21537922

145 http://freestatefoundation.blogspot.in/2012/08/the-true-meaning-of-internet-freedom.html

亚利桑那大学法律教授Derek Bambauer说：“网络自由这一术语或许会因其含义过于广泛而不使用而最终被弃用。然而各个国家、文化和用户都应当努力权衡互联网通信带来的这些难题。”[146]

“媒体马克思主义者新闻自由组织”在其网站对网络自由做出如下定义：“网络自由是指互联网业务提供商（ISP）不会区别对待不同类型的网上内容和应用。”[147]将网络中立性定义为基本的互联网协议必须为非歧视性的原则，尤其是内容提供商应当得到互联网运营商的平等对待。

互联网自由意味着频谱开放

虽然广播商和移动电话公司拥有政府为某些部分的广播频道颁发的许可证，但频率的其他部分是开放的，这意味着任何公司都能开发产品，如无绳家庭电话、蓝牙手机、幼儿监视器或遥控，都可在不必获得政府许可证的情况下使用这一开放空间[148]。

伴随网的自由而来的不仅仅是使用这一媒体的自由，还有自我表达的自由。而且更重要的是，他通过利用互联网提供的各种便利生活的手段，代表了简化人民生活的自由。

---

[146] Bambauer，D，《网络自由之谜》，美国电子期刊第15卷，2010年第6期，第4-6页，亦见 http://www.wseas.us/e-library/conferences/2013/Dubrovnik/ECC/ECC-38.pdf 2014年8月8日最后一次更新。

[147] http://pjmedia.com/tatler/2013/01/22/the-lefts-warped-definition-of-internet-freedom-and-an-open-internet/

[148] http://pjmedia.com/tatler/2013/01/22/the-lefts-warped-definition-of-internet-freedom-and-an-open-internet/

突出特性

一些学者断言，网络自由包括言论自由、隐私权、创新、获得报偿和承认的自由以及整个网络结构自由等一系列根本自由权[149]。

现行政策和监管框架

尽管互联网是作为全球无国界媒体发展起来的，但悬而未决的问题是，国际上依然未能集中力量，拿出具体适用于网络空间的经国际认可的标准。因此，当人们谈论法律、政策和监管框架时，必须注意到不存在有关互联网自由权的国际条约。然而，人们在这方面取得了一些进展。

正如本报告此前所示，2001年的欧洲理事会网络犯罪公约是这方面的范例。以下是这一公约的要点：

- 他是致力于通过统一相关国家法律、为某些犯罪行为提供通用定义、改进调查技术并在国家间开展打击这一现象“最广泛”的合作，解决网络犯罪问题的首个国际条约[150]。
- 他要求将黑客攻击和与儿童色情相关的行为确定为犯罪，并将刑事责任扩大至知识产权违法行为。
- 他提供了通用的刑事犯罪政策，旨在通过采取适用立法并开展国际合作使社会抵御网络犯罪[151]。

2003年欧洲理事会通过的《互联网通信自由宣言》是正为努力的另一大范例。以下是这项宣言的重点：

---

149 Neelie Kroes，《网络自由》http://europa.eu/rapid/press-release_SPEECH-12-326_en.pdf 2014年8月8日最后一次更新

150 http://en.wikipedia.org/wiki/Convention_on_Cybercrime，2014年8月8日最后一次更新

151 http://epic.org/privacy/intl/ccc.html

- 根据《欧洲保护人权与基本自由公约》第10条的规定，国家需要在言论与信息自由和其他立法权利和权益之间进行权衡；
- 对出于政治原因或与民主原则相违背的其他目的而试图限制公众使用互联网通信的做法表示关注；
- 主张坚持将跨境的互联网通信事前控制作为例外情况；
- 认为有必要消除个人接入互联网的障碍，从而通过完善已采取的措施建立公共接入点；
- 相信确立通过互联网提供的业务的自由将有助于用户从多种国内和国外来源接入多元化内容的权利；
- 强调互联网通信自由不应有损于人的尊严、人权和他人，尤其是儿童的基本自由权；
- 欢迎业务提供商在面对互联网非法内容时与执法机构合作的努力。

WSIS

信息社会世界峰会为未来的衡量ICT促发展合作伙伴关系提出了以下建议：

- 他将继续扩大和深化信息社会衡量工作，包括在统计数据制定的最初阶段接纳国家统计局参与。
- 他将继续提高公众意识并开展能力建设，并对低收入国家给予特别关注。
- 他将考虑开辟数据来源和工作方法。
- 他将成立WSIS目标专家组。

人们一致认为，2015年后人民继续WSIS进程和信息社会的监测工作，同时使这一监测的性质深入人心。应继续开展国际合作和国家协调，以充实多利益攸关方模式。[152]

《英特网通讯自由宣言》构成了捍卫网络自由的利器[153]。其前言指出，自由开放的互联网能够带来一个更美好的世界[154]。宣言的下一个目标是，让数以百万计的互联网用户签署这项宣言[155]。宣言支持为互联网政策制定五个基本原则：

- 不对互联网进行新闻检查。
- 普遍接入高速和价格合理的网络。
- 经互联网进行连接、通信、创建与创新的自由。
- 向新技术和创新者提供防止用户滥用的保护。
- 互联网用户通过有控制地披露其个人信息保护及隐私的隐私权和能力。[156]

框架缺陷

然而目前明显缺失的是一个为所有利益攸关方国际互联网自由体制。此外，互联网自由作为一种现象引发了法律、政策和监管多种问题，以下对其中的部分问题进行了研讨。

---

[152] WSIS+10高级别活动2014年成果文件：论坛系列，http://www.itu.int/wsis/implementation/2014/forum/inc/doc/outcome/OutcomeDocument2014.pdf（2014年11月6日最后一次更新）

[153] http://en.wikipedia.org/wiki/Declaration_of_Internet_Freedom，2014年8月8日最后一次更新

[154] http://www.internetdeclaration.org/，2014年8月8日最后一次更新

[155] 《互联网自由宣言》，http://www.savetheinternet.com/internet-declaration

[156] http://en.wikipedia.org/wiki/Declaration_of_Internet_Freedom，2014年8月8日最后一次更新

目前，许多司法机构为现实世界提供保证言论自由的基本权利/国家立法。同样这些权利也被用于互联网言论自由的解释和实施。然而斯诺登披露的信息重点提出了擅自侵害互联网言论自由的问题。在相关用户不知情的情况下，其音频、视频、图像或文本形式的通信受到不同来源的监视。实际上，互联网及其各类设施和平台逐渐成为建设及监视的社会的推动力。从此可以看出，世界上有两种人：一种是了解另一种是不了解他们正在或曾经受到监视的人。

与日俱增的监视和网络监控正在成为常态，并对互联网言论自由产生直接影响。简而言之，虽然互联网不完全是“狂野西部”，但从越来越多的证据可以看出，网络空间的言论自由不是绝对的自由。

文明行为的规范也同样适用于网络空间。这意味着应通过国家立法禁止旨在制造不便、恶意、仇恨、不和或以具体个人或团体为目标的互联网内容。

但是，互联网提供的匿名外衣可以给不轨或恶意用户一种不为自己的所说所做负责的满足感。

尽管如此，法学正是在这种背景下在全球各国的体制当中萌生，使法院能够通过指示业务提供商披露非法活动背后人员的真实身份剥去这层匿名面纱。然而如前所述，目前仍然没有可以界定什么构成互联网言论自由的国际标准。

1948年的《世界人权宣言》规定了一些可被解读为完全符合互联网自由概念的基本原则。

酝酿中的挑战

社交媒体网络提供了显示人们思想倾向的新型网上对话机制。然而，全球的法律和立法在解决社交媒体固有的新兴挑战方面行动不够迅速。

智能电话和其他通信装置预示着移动网络的来临。移动电话和互联网的结合以迄今前所未有的方式展示了网络的言论自由。等到不同国家以不同方式应对不当网络内容时问题出现了，因为不同司法管辖区确定的网上言论自由范围各不相

同。尽管存在这些差异，但人们在孕育当中的移动网络领域达成了普遍共识。移动电话和互联网的结合，使网上言论自由得到了前所未有的体现。

此前讨论的另一个问题涉及在互联网上自由和匿名通信的能力。如前所述，一些人认为互联网的匿名信使他们能够在网上畅所欲言，无需担心对他人的潜在影响[157]。通常，受指控的网上诽谤行为的受害者将“John Doe”送上了法庭的被告席。

不同国家应对各类诽谤言论或内容的诽谤法各有不同。这些法律同样适用于网络空间。为此，在日渐成熟的法学界越来越清楚地认识到，谁也没有权利诽谤他人或试图毁损他人名声。

各国对此有着不同的国家法律规定。部分国家只在他们认为出于保护伦理价值观、个人合法权利，国防或国家安全的理由才会限制互联网访问。其他国家已正式承认言论自由权可延伸至网络空间，或正在考虑采取这一步骤。

我们都生活在人类历史的一个过渡时代，期间，互联网自由不仅受到国家实体的威胁，还受到实际管理和控制互联网数据的私营参与方的威胁。

影响互联网自由的其他挑战

对互联网的司法管辖是一个重大但又十分复杂的问题，因为个人的互联网言论自由可能在一国的领土内受到挤压，但你可能置身于另一国家的司法管辖区域内。此外，你总是成为网络犯罪分子目标的事实，也可能成为使你无法有效享受互联网自由的抑制因素。因此，网络犯罪已成为一项重大的法律、政策和监管问题，并可能对世界各地的互联网用户的自由权利造成影响。

---

[157] Eric Sinrod，“有可能对匿名网上言论自由设限”
http://www.lexology.com/library/detail.aspx?g=7a8eb382-b007-49c6-8ca1-4a9197062d9d，2014年8月8日最后一次更新

另一影响互联网自由的问题与网络安全相关。人们只有在网络安全、保险和可靠的情况下才能享受个人的法律自由。然而，对网络安全的破坏再次将人们在保护和捍卫网络资源和基础设施方面面临的独特挑战推到前台。

鉴于这种网络媒体在全球范围的重要性和脆弱性，应从完全不同的角度看待互联网自由问题。随着各国针对计算机系统和网络的网络攻击愈演愈烈，必须在互联网自由和保护与维护网络安全的必要性之间找到平衡。

世界各国依然为就应对中介责任的方法达成一致。美国等国趋向于不将这一责任归于业务提供商。其他国家则在他们希望避免为潜在的第三方网络数据责任担责的情况下，开展尽职调查，同时行使有关某些国家基本法律规定的义务。

“黑网”的出现成为互联网自由的另一可怕挑战。网络犯罪分子会毫不犹豫地进入这一领域，将其恶意的计划和行动付诸实施，以达到给人们享受互联网自由带来不利影响的目的。

愈演愈烈的网络战现象是对建立网络空间使用信心和互联网自由的另一重大挑战，也成为当今的公开秘密。根据以往经验，网络恐怖主义的出现进一步影响了人们充分享受互联网自由。

显然，有必要在互联网自由的背景下达成国际谅解和通用标准原则。在影响上述互联网自由的重大法律和政策问题方面亦有长足进展。正是在这种背景下，世界科学家联合会和国际电信联盟等组织才能继续在未来帮助形成共识方面发挥重要作用。

大数据

在目前的重要时刻，大数据对互联网自由的影响不容忽视，因为归根结底应在电子数据和信息的背景下审议这一自由权。如今，互联网已成为一个巨型的网中网，一个具有无限存储的数据龙。因此人们必须认识到，所有形式的互联网自由权都与大数据直接相联、相系和相关。

大数据是我们时代的大现实。不同的计算机系统和网络生成大量数据，各公司自然希望参与大数据分析工作。不同的利益攸关方以不同方式定义的数据，也是一个重要的法律、政策和监管问题。

大数据的定义

维基百科对大数据做了如下定义：“[...]一个用于任意一批数据的包罗万象的术语，而这些数据极为庞杂，以至于难以利用现成的数据管理工具或传统的数据处理应用进行处理。但是，大数据通常包括一些数据集，其规模超过了通常使用的软件工具在允许消耗的时间内进行捕获、组织、管理和处理的能力。”[158]**《牛津词典》**将大数据定义为：因为过于庞大复杂而标准方法或工具无法操作或查询的数据集[159]。2014年5月1日发布的**《白宫大数据报告》**也赞同目前得到广泛认可的定义，即大数据“[...]规模如此之大、种类如此之多或移动如此之迅速，传统的数据模式已不敷使用。”[160]**美国技术基金会**指出：“大数据这一术语描述了大量需要先进工艺和技术才能进行信息捕获、存储、分发、管理和分析的高速、复杂和可变的数据。”[161]

大数据具有以下不同特征：

- 它应具有灵活性[162]。
- 许多大数据系统接受未经梳理的数据，这意味着总有一些极端异类的数据点给系统带来“热点”。

158 http://en.wikipedia.org/wiki/Big_data

159 http://www.oxforddictionaries.com/definition/english/big-data

160 http://www.lexology.com/library/detail.aspx?g=e7161021-7570-476c-bf8a-b4637d10a355

161 TechAmerica 基金会，解密大数据：2012年政府工作改革实用手册，https://www-304.ibm.com/industries/publicsector/fileserve?contentid=239170，2014年8月4日最后一次更新。

162 http://hadoopblog.blogspot.in/2012/02/salient-features-for-bigdata-benchmark.html

- 大数据可将云基基础设施用作服务，快速获得所需的计算周期[163]。
- 在这种背景下生成的数据量十分重要。而这里谈到的其数值和潜力以及它能否真正被视为大数据取决于数据的规模。
- 类型关系到对包括结构性、半结构性和无结构性数据等多种数据类型复杂性的管理。
- 数据创建、处理和分析的速度持续增长、提高速度是数据创建的实时性所决定的，而且有必要将流式数据纳入业务程序和决策过程。
- 数据的不确定性：真实性是指与某类数据相关的可靠程度[164]。

人们对大数据的法律、政策和规则方面表示关切。首先应当认识到，目前没有有关大数据的国际框架 – 或国际条约。因此，大数据依然是一个由国内立法规范的议题。多数国家没有有关这一议题的专项立法或法律规定。然而为搭建政策和规则框架，必须考虑到下述重要参数。

数据保护是大数据面临的最大挑战之一。不同国家的司法管辖对数据保护提出了不同的规则要求。欧盟已有数据保护指令，而其它地区的国家则将不同数据保护规定纳入各自国家的立法。数据采集、保护和维护方法是需要考虑的重大问题。需要对大数据保护进行明确的重新认识，因为数据保护立法一向针对的是个人生成的较少量的数据，即与大数据量相比数量微小的数据。

处理者和监管者都面临大数据保护的巨大挑战。其巨大的体量及其引证和多样化溯源结构，都要求建成独特的安全可靠的法律框架，以便同时向用户和提供商提供保护。

---

163 http://www.dummies.com/how-to/content/characteristics-of-big-data-analysis.html

164 IBM 的分析：大数据的实际应用 - 创新公司从不确定性数据提取价值的方法，http://www.ibm.com/smarterplanet/global/files/se__sv_se__intelligence__Analytics_-_The_real-world_use_of_big_data.pdf last updated Aug. 8, 2014.

数据小型化也触发了隐私和数据保护问题。最要紧是为数据，包括以可识别形式出现的个人数据的采集、保留和销毁制定适用国际最佳做法的必要性。

各国立法在个人赞同数据采集、使用或披露和个人对数据的控制之间存在分歧。如前所述，尚没有一个能够覆盖这个及其它网络空间相关问题的国际大数据法律安排。

另一个法律问题涉及为网上信息发布者采用数据匿名和数据屏蔽方法。另一尚未得到妥善解决的重大问题涉及大数据的采集、处理、保留和发布情况下适用的基本原则问题。鉴于当今的大数据无一例外的与云相关，其维护和保留构成了进一步的法律、政策和规则性挑战。

数据隐私是大数据的一大问题，因为其中的数据消耗量极大，而且每个数据提供商都有保护和维护其数据的固有权利。因此，确保此数据得到适当保护完全是网络服务分内的责任。

大数据的管辖权限也是一个重大的法律、政策和规则问题，因为这类数据无一例外地置于云间和世界不同地区的各种其它服务器上。万一大数据隐私受到破坏，有关人员应对相关业务提供商提起法律诉讼。其中的巨大挑战是确定上述数据的物理位置，因为数据受损服务器的位置会对当地隐私侵害法产生影响。

与大数据相关的网络犯罪也是一大法律挑战，因为整个互联网经济都以这种数据为依据，而擅自侵入大数据的行为会在极大程度上助长网络罪犯，这也是他们更多瞄准这一领域的原因。

Adobe公司于2013年10月确认，网络罪犯非法侵入其网络，窃得290多万个用户名、加密的信用卡和借记卡号码、卡的过期日期、登录身份与密码，还进入了Adobe的多种产品使用的源代码，包括Acrobat和ColdFusion[165]。

---

165 http://blogs.mcafee.com/consumer/consumer-threat-notices/malicious-acrobatics-adobe-the-latest-target-in-string-of-cyber-attacks

作为欧盟咨询机构的欧洲网络和信息安全机构（ENISA）于2013年1月指出：“大数据的使用会对数据隐私造成影响。与此同时，通过对手的大数据使用可能会向新型攻击矢量打开大门。”[166] ENISA还指出，“[…]社会技术、云计算、移动计算和一般性互联网使用的迅速发展，”使大数据成为生成信息的整合体，同时构成了一个新兴的安全问题。

隐私

大数据分析可直接影响到对个人隐私的侵害行为。2014年5月，白宫发布了人们翘首以望的题为“大数据：抓住机会，保护价值”的大数据报告。贝拉克•奥巴马总统要求提交的这份报告涉及技术快速演进的方式，这种技术进步使政府和私营部门能够采集、存储、分析和使用大量大数据。报告重点谈到大数据目前和未来可能对个人隐私和平等地位构成的潜在威胁，并建议法律、政策和规则并举，保护美国和全球公民免受潜在滥用的威胁。[167]

因此在法律界，大数据和数据隐私的重要性与日俱增。经常会出现有关谁拥有大数据内容的争论，当有研发大数据生成系统的第三方参与时尤其如此。数据保护，包括利用加密和粒度访问控制的敏感个人信息在内的数据保护，是人们的另一大关切。

大数据的检索和访问同样与隐私有着内在联系，而且是保留挖掘数据和数据分析当中的主要法律问题。人们重点关心的是保持受访问和受检索大数据的可靠性、完整性和真实性。

---

166 http://www.out-law.com/en/articles/2013/january/cloud-mobile-social-and-big-data-technology-innovations-increasing-threat-of-cyber-attacks-says-eu-body/

167 Kenneth R. Florin、Ieuan Jolly等人“白宫“大数据”报告凸显大数据的优势和受到滥用的可能性”http://www.lexology.com/library/detail.aspx?g=a036aed0-cffb-4ae1-a518-44b92201effb，2014年8月4日最后一次更新

此外，采用以数据为中心的经加密强化的安全方式，也会引发自身的法律问题。此外，粒度访问控制带来了其它多种复杂的法律和政策隐私问题。另外，有必要在信息发布期间保护隐私。

人们对大数据的另一关切是，数据采集后很难保持其匿名性，虽然颇具前景的在研项目旨在模糊大数据集中的个人可识别信息，然而目前花在重新辩识看似“匿名”的数据上的气力要大得多。对融合数据能力的集体投入数倍于强化隐私技术的投入[168]。人们的首要关切是确保确定受访问和受检索的大数据的可靠性、完整性和真实性。

其它法律问题涉及保障大数据基础设施的安全，即拥有一个在分布式编程结构中保护计算的适用法律框架。就此而言，应为强化和维持无关系数据存储制定适用的最佳做法。然而另一重大法律问题涉及到数据管理。为此，需利用法律支撑框架保证数据存储和交易记录以及粒度审计的安全。

大数据的知识产权构成了另一重大法律问题。谁拥有大数据的知识产权？什么是与大数据采集、存储、处理和共享相关的知识产权？人们往往对新的大数据研究分析工具可能对数据版权造成的侵害表示关注。其它的关切包括相关合同方对不准确或不完整信息或合同协议未得到履行所需承担的责任。

技术有可能开启擅用竞争对手信息的可能性，从而引发各类竞争法律问题。大数据的盈利性取决于这类商业秘密，而敏感的个人数据本身，会对真正的隐私和安全造成影响，并侵蚀对网络平台和技术使用的信心。

有人争论说，大数据的采集和处理会对人们的个人和集体身份造成影响，甚至有侵蚀民主质量的危险。

---

168 总统执行办公室，大数据：抓住机会，保护价值，http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf, 2014年8月4日最后一次更新

另一种关切是，大数据审查机构大多为有影响力的中介机构，更增加了误用和滥用权利侵犯个人权利和自由的风险。

总而言之，有必要构建一个适用的法律支撑框架，确保大数据不会在任何方面有损于人民享有的公民权或其民事义务和责任的实现。

世界科学家联合会和国际电联的作用

鉴于没有与大数据的法律和政策框架相关的国际参数，世界科学家联合会和国际电信联盟等机构有必要努力推动框架的建设。

结论

我们可以在结论中这样说，互联网自由和大数据都是非常有趣和不断演变的概念，在我们日常生活中发挥着与日俱增的作用。因此，为捍卫互联网自由而搭建适用的国际法律、政策和规则框架是重中之重。但眼下我们在很多方面得心应手并愈发依赖的那些数字时代结构的未来却岌岌可危。

未来的要务是制定和执行基于普遍认可原则的国际政策和规则框架。

这些框架必将随着时间的推移而发展。目前正就互联网自由和大数据采取大量法学举措。然而，有必要为确保在国际层面构建有效的政策和规则框架而努力。

世界科学家联合会及其信息安全常设监督委员会，不仅能够在监测能力而且在推进国际框架建设方面发挥极其重要的作用。通过与国际电信联盟合作，世界科学家联合会和其它相关组织可望充分发挥它们在这些领域的专长与经验，大力推动这一目标的实现。如果这些组织能够推动制定旨在确保适当网络空间环境的普遍认可的通用标准原则，所有利益攸关方都将大受裨益。

如前所述，所有用户通过克服网络安全和其它挑战继续受益于互联网自由的能力受到威胁，使对这一不断扩展和越发重要领域的信心面临受到侵蚀的风险。

人们希望，相关的法学能够跟上不断增长的互联网用户数量和不断加快的网络技术发展速度。只有通过持续关注相关的法学发展并推动这一领域的进步，整个世界，尤其是重要参与者，才能确定前进方向。

制定大数据和互联网自由相关的法律、政策和规则框架的进程，将会随时间的推移而演变。将对基本权利的恪守延伸至网络空间，将成为这一领域成功的关键。

3.3 从全球视角看各国家的网络空间监控

Howard Schmidt

引言

为了正确理解并就网络空间监控的议题提出深思熟虑的意见，重要的是需要先认识到，我们的参照系主要基于随时间发展逐步形成的（书面或其他形式的）“参与规则”（远远早于所谓网络空间的出现）。

有人认为监控合理，自然也有人持相反的看法，还有更多的利益攸关方处于中间地带。只有从全球视角通过探索经验性信息并运用理性，才能最终拿出一套所有利益攸关方在确定国家监控是否适当且合理时可以考虑的平衡的准则。

数据收集

随着技术的发展，形成了针对各种目的创建、传送和收集大量数据的环境。所形成的网络空间中的一切都是通过数据产生的，因此捕获这些数据是必不可少的，收集捕获到的数据亦是如此。金融交易就是必须捕获并收集的必不可少数据，比如现代的工资支票。许多人的薪金都是以电子资金转账形式存入账户的，

且很多人都以储蓄账户的形式收集并将此电子数据存档。此存档数据可以交易的形式（如在杂货店）移至另一数据收集点（用商品换取代表金融工具的数据）。

手机通话是用相关方式收集数据的另一个例子，其中移动电话公司记录呼叫地、呼叫发生时间和通话持续时间等信息。按电话公司的解释，记录这些信息是为了进行计费。网站收集网站和服务用户的数据用于各种目的，其中包括确定和满足用户偏好以及将用户创建信息存档（如社交媒体网站）。

作为网民，我们都理解并接受在某些情况下数据收集不仅是合理的和可以接受的，而且在许多情况下是非常可取的。要使利益攸关者接受这种做法，就需要让其清楚了解所收集的数据内容以及预期用途。这种情况下，在人们从事相关的活动之前选择接受数据收集的条件，或者如果认为数据收集和使用政策过于严苛，则人们可以选择不进行相关活动。

其实作为利益攸关者，我们都同意与那些能够获取我们数据的机构订立明确说明如何收集并使用这些数据、由何人保管数据（如移动电话公司）以及在何种程度上及向何人转移数据保管权的合约。数据保管方对于数据拥有巨大的权力，但这种权力并未授权其可以随意处理数据。最终而言，一旦保管方选择将数据用于与数据涉及的个人或组织达成的协议之外的目的，则必须订立一份允许这种扩展使用的新协议，否则可以合理地视为保管方是在滥用权力或违背诚信。

司法程序与情报搜集

正是出于上述原因，现在实施了允许扩大数据使用范围、将其用于相关利益相关者预期以外的程序。在合理怀疑某人卷入犯罪活动的情况下，相关的法律和司法程序允许监控和访问收集的可用作违法行为证据的数据。虽然世界范围内与此类监控相关的规则和程序各不相同，但普通大众通常都可了解从事这项活动的规则。

然而，如果监控是通过政府情报机构进行的，则情况就变得不太明朗了。在全球层面，情报部门暗中进行监视和搜集数据，并将这些信息用于各种目的。大多数机构表面上会声称搜集的情报是出于国家安全考虑（例如，最近国家安全局（NSA）披露的情况）或是为了更大的利益。其他机构可能只声称主权权力允许其开展情报搜集活动，因此他们无需解释原因。这在各国对此类数据搜集活动的立场各不相同的全球经济中特别具有挑战性。在这种情况下，网民可能认为他们得到符合其政府规则的保密保障，但却是在从数据起点到最终目的地的传输路径可能跨越国界的网络空间中传递信息 。一旦数据到达规则有所不同的地点，就必须遵守当地的规则。由于情报搜集是一个封闭的进程，通常不受预期透明的执法和司法程序的约束，因此判断相关活动是否越界变得极其困难。

情报搜集的方法和规则

如果情报搜集可以脱离法律或司法程序的限制（在许多情况下确实如此），那么就必须考虑情报搜集机构对恶意软件和秘密植入应用程序的使用了。在许多主权国家，创建旨在通过各种传播方式入侵计算机系统的恶意软件和应用程序本身就是不合法的。恶意软件传播后从事的活动也被视为是恶意软件创建人从事的犯罪活动，任何用户或组织在知情的情况下有意传播和使用恶意软件、以从事此类活动亦属犯罪行为。目前这种行为受到全球范围内确立的法律和司法程序的约束，在此方面触犯法律面临的制裁相当严厉。

应再次指出，在考虑国家情报搜集机构如何运作时，从事创建和传播恶意软件及秘密藏匿的应用程序的活动以及搜集有关使用此类“工具” 的数据的相关规则非常模糊。根据所涉及的具体主权国家，政府情报机构出于各种原因（最常见的可能就是以国家安全为由）从事此类活动可能被视为是可以接受的。然而，值得注意的是，一旦恶意软件部署后，它的传播范围可（而且通常会）远远超出预期界限，并由此对显而易见的、完全不属于情报搜集机构负责范围的系统产生负面影响。此方面示例包括关键系统，如医院网络、电网以及用于控制危险工序（如化学生产）的安全系统。此外，金融系统、粮食生产系统和制造系统亦可受到负面影响，从而造成大范围的社会动荡和恐慌。

平衡网络武器竞争环境

可将本文所述的使用恶意软件行为看作相当于推出了一种网络武器，就像武器所产生的影响可以超出预定目标。此外，制造和部署网络武器的能力不受传统肢体冲突通常受到的经济和自然资源的限制。金属、化工设备或者高科技工具对恶意软件创建人能力的影响微乎其微。一台计算机和网络连接或外部媒介储运（如USB记忆棒）再加上创建恶意软件的知识已绰绰有余。

恶意软件创建并传播后，就会被武器化，任何能够识别并将其隔离的个人或组织都可加以利用。这意味着网络武器可能会通过原有恶意程序包功能增强的变异版本转向始发组织的对立面。在这种情况下，创建恶意软件的组织最初就充当了网络武器的全球提供者。这实际上意味着，除了首次攻击获得的利益外，最初推出后不久竞争环境就会得到平衡，并可能造成任何个人或组织都无法找到避风港的极具破坏性的环境。此外，网络武器一旦部署，基本上就会永远存在，因为没有可以消除的储存。

前进方向

显然，不管暗中从事国家支持的监控活动的机构有什么意图，伴随着潜在的不可控和不可预见的负面影响会产生相应的挑战。这会造成连锁反应，可能会破坏全球关系和经济状况。虽然互联网可作为从事在一些人看来是善意监控的有效途径，但要明白互联网已经成为世界经济不可或缺的必要组成部分，任何个人、组织和国家无论规模大小都可平等参与，还可实现即时自由的思想交流以及经济食物链各个层面的合作。

因此，全球各个层面的商业团体有必要对各地政府施加压力，通过相关法律。这些法律应有助于防止可能对由互联网产生的经济效益和社会效益造成的破坏。亦应使得益于稳定的互联网协同经济体中的个人、组织和国家数量持续增长，在这样的经济体中每个人都确信了解政府的利益未置于其所服务的人民利益之上。

3.4 国家监控的网络空间范围：欧盟视角

Henning Wegener

互联网（和一般数字通信）的自由与完整性之间固有的和日益加深的冲突以及另一方面公共秩序和集体安全问题日益迫切的要求，在本出版物多处，尤其是在Al Achkar教授有关互联网自由和网上公民自由权的文章中均有充分反映。

随着当前大规模入侵数字设备和网络的情况凸显以及大数据恐慌，这种冲突比以往任何时候都更加明显，亦是欧洲目前最普遍最严重的焦虑之一。数据收集和处理技术潜力的长足发展推动人类进入了丧失隐私的新时代，引发了对国家和国际法原则以及个人和集体资产已岌岌可危的担忧。基本人权日益受到侵蚀，这理所当然已成为一个全球性的问题，要针对这一看似势不可挡的洪流制定相关的规则和限制，迫切需要在全球范围内采取补救措施。

2013年12月18日未经表决通过的联合国大会（UNGA）第A/RES/68/167号决议－数字时代的隐私权，表达了国际社会希望采取行动对抗大规模监控、截获和收集个人数据的意愿，这是制定必要政策的一个重要开端。根据这项决议第5段，联合国人权事务高级专员署在2014年6月提交了一份报告（A/HRC/27/37），9月召开的人权理事会第27届会议的小组讨论对这份报告进行了讨论，预计UNGA第69届将采纳这份报告，其中所载的“意见和建议”待成员国审议。该报告明确指出了对国家监控措施的人权要求：这些措施必须是必要和相称的、透明的且尊重国外个人的隐私权。报告人明确指出，他认为目前这些要求尚未得到满足。

在这些全球进程取得具体的成果之前，尽管有普遍的需求和方法，但各国和人们对入侵数字隐私、国家主权和受保护的信息域（斯诺登案引发的广泛的公共辩论）的迹象和事实做出的反应存在显著的地区差异。

在世界一些地方，对这种行为的反应更多的是容忍，甚至是冷漠，而非反抗；在许多大国，占主导的政治制度压制了公众拒绝的声音；在美国，由于法律

制度更加宽松，人们对宣称的或实际的公共安全需求有更深的认识。另一方面在欧洲（主要是在欧盟），非法盗窃数据的现象和范围之广已经引起普遍的恐慌和排斥。一场政治风潮由此产生，绝不能低估这种风潮的影响，特别是跨大西洋地区普遍丧失信心（即对网络安全的信心）的问题。欧洲民主国家与美国之间由于强烈的情感依附而长期存在的密切关系毫无疑问会受到影响。

欧洲的这种普遍情绪反映了其对于自由和隐私的热切渴望，无疑其近代带有独裁和否定个人隐私烙印的历史（至今依然历历在目）以及高度发达的数据保护和公民自由及欧盟作为一个法律实体的性质在很大程度放大了这种渴望。作为无所不能的老大哥，不受任何法律约束的利维坦，欧洲的担忧比其他地方更为明显，亦不能低估美国人普遍对大规模政府监控的失望情绪。这一争议在未来的总统选举中可能会发挥核心作用。

但确切而言，如果要在充斥着无限入侵技术手段的时代确定保持网络安全信心的全球标准，可以研究一下欧盟的情况及其法律环境，这可能有助于建立起通用监管框架的一个重要支柱。

其中一个原因是，欧盟是由28个高度工业化的国家构成的以法律为基础的共同体，这些国家在全球数字经济中发挥着重大作用，而数字技术已成为其经济和社会发展范例，与其他地区相比更为明显；现在欧盟仍是世界上最大的经济联合体。按比例而言，这使欧盟国家比其他国家更易受到网络攻击；McAfee已经确定，以德国为例，网络攻击的破坏率占其国民生产总值的1.65％，居工业化国家之首。当网络犯罪集团成为对高度依赖于网络的开放经济体造成损害的主要驱动力、外国情报组织大行其道时，在欧洲网络犯罪已成为残酷的现实。这促使欧盟制定了高度发达和统一的网络安全系统。

同时欧盟是由28个独立的国家组成的，是设有共同机构和规范制定职能的组织。绝大多数立法都是欧洲委员会和欧洲议会在欧盟委员会倡议的基础上采取联合行动的结果。根据有关实施既定目标的指令，决议和决定立即全部对所有成员

国生效。这些决议和决定都必须转换为成员国的国家法律，这是这一国际体系的独特特性。欧盟法律的共同制度基础不仅在成员国内产生立竿见影的法律效力，而且对世界其他地区也有影响。因此，欧盟能够成为值得仿效的对象，就像在一个制度实验室，一些国家的试验可以推广到整个社会。欧盟立法是内部协调和统一的有力手段，也是实现国际监管的通途。

网络安全和保障个人数据保护的政策均属欧盟机构的权限。关于网络安全，十几年来欧洲委员会一直致力于为其成员国制定监管框架。一系列重要的文件（有些是分析性的，有些是规范性的）形成欧盟成员国必须遵守的综合法律体系，除美国外，该体系在范围和细节方面在数字世界独领风骚。此外，在2004年，28个成员国建立了欧洲网络与信息安全局（ENISA），作为联合智库、重要的欧盟联合活动的协调者和采取进一步的监管措施的推进者。还应提及隶属欧洲刑警组织（EUROPOL）的欧洲网络犯罪中心以及在发生网络攻击情况下做作为联络中心和行动中心的欧洲计算机事件响应团队（CERT）。这里无法全面描述欧盟在法律和制度层面开展的所有网络安全活动，但查阅ENISA网页以及其他可用的分析就能有一个大体的了解[169]。欧盟坚定地执行其《数字议程》并优化网络安全。最近发布的两个综合文件－《2013年欧盟网络安全策略》[170]以及《网络与信息系统安全（NIS）指令草案》[171]包含了值得研究的早期规范。这两份文件，特别是NIS指令，规定了私营部门、CERT以及关键基础设施、网络和信息系统运营商须遵守的综合要求、标准和义务。

---

169 www.enisa.europa.eu亦见Henning Wegener，《欧盟网络安全》（La ciberseguridad en la Unión Europea）, www.iees.es/Galerias/fichero/docs_opinion/DIEEE077bis-2014_CiberseguridadProteccionInformación_H.Wegener.pdf。文章的德文版见：www.unibw.de/infosecur。

170 JOIN (2013)1 final

171 COM (2013)48 final

这里值得注意的是，欧盟施行统一的网络法。28个国家中有23个已将《布达佩斯网络犯罪公约》纳入国家法律（其余国家无疑将在短期内执行），所有国家均已纳入了（类似的）2002年指令[172]。这样，网络犯罪以及入侵数字设备和网络的行为将在所有欧盟国家中得到同等制裁，欧盟所有国家都会依法办事。

欧盟数字政策的另一个重要方面是数据保护。随着数字数据存储的发展，个人信息和个人的私人空间保护已变得非常重要。适用的欧盟法律影响深远。目前的法律基础仍是欧盟95/46EG指令，该指令阐述了最低保护标准，所有欧盟成员都将其纳入了各自的国家法律。该指令适用于个人的个人数据。如果相关人已表示同意或存在其他具体限定的情况，使用相关数据便是合法的。这些限制在一定程度上亦适用于欧盟以外的数据用户[173]。

2010年，欧盟委员会推出了更加雄心勃勃的立法项目，调整现行的数据保护制度以适应变化的情况[174]。《通用数据保护条例》（GDPR）法规草案试图反映数据流激增、云存储、新的社交网络以及连接指数增长的先进信息化社会的需要。作为一项法规，新案文一经通过后将立即对】所有成员国生效，并形成统一的欧盟法律体系，针对28个成员中的每个成员都有一套详细的规则。该条例比1995年指令更严格、更详细，规定违反该法令将受到重罚。2014年3月欧洲议会通过了该案文草案，目前各国政府正在讨论，以便在欧洲理事会做出决定。预计将在未来几个月敲定，而后于2016年生效。但这项法规已产生了预期效果，因为它表明欧盟数据制度正在缩紧。

从完整的法律结构角度对现有的和即将出台的欧洲法律进行简要概述后，现在可以回到网络空间监控问题了。如果没有特定合理的理由，任何入侵数字数据载体（计算机、电话、网络及其他数字设备）并复制、盗窃、篡改或传送存储数

---

172 COM (2002)173 final

173 对于大多数欧盟成员国，另外两份国际法规也非常重要：《经济合作与发展组织保护隐私和个人数据跨境数据流导则》以及对46个签署国有约束力的欧洲理事会《欧洲数据保护公约》。

174 COM(2012)11 final

据的行为均属网络犯罪。如果入侵数字设备和网络，且涉及到个人数据，则亦属于违反数据保护法行为。网络犯罪与个人数据篡改是联系在一起的，需要依靠两方面法律机构的力量。两类网络犯罪均会危及互联网自由。

互联网（或云或其他存储区）上的工业或政治间谍行为，即，窃取或篡改政治事实或商业数据（不包括个人数据）不受国际法制裁。但在实施适用法律的国家须根据普通刑法和民法进行制裁，无论肇事者是个人、企业、机构还是外国政府。在欧盟国家，《布达佩斯公约》和/或国内立法提供了必要的工具。在刑法中，即使攻击来自境外，如果攻击在内部造成影响或造成损害，则法律也是适用的。根据该公约，成员国必须惩处在其境内的网络犯罪行为，即使肇事者并非当地居民亦不例外[175]。网络犯罪的影响无处不在，从而促使网络犯罪法律逐渐成为世界刑法的一部分，虽然可能尚未被普遍采用或实施，尤其是在始发国不合作或者其本身就是肇事者的情况下。如果数据监控和采集包括个人数据，则数据保护法的禁令和惩处规定亦适用。

因此事实很简单，根据欧盟法律以及类似法律，目前国内外政府以及个人始发者大规模入侵数字空间的行为属于严重违法，除非这种入侵有公共安全和公共秩序方面合理的理由并经国家法律及必要的法律程序授权从而使其成为合法行为。确切地说：尽管这是各国政府普遍的做法，但在发生入侵事件或入侵行为造成影响的国家政府明确表示同意之前，绝不能以国家信念、认为的安全要求和外国政府现有的法定程序为依据将国外的网络攻击视为合理行为。在欧盟，各成员国政府的联合行动频繁，因而是合法的。这些原则涉及国际互联网连接、节点、无线连接等的大规模监控。所报告的国外安全部门无限制的数据收集（真正的收集狂潮）使这一问题变得更加尖锐。此类数据收集得益于前所未有的技术实力和手段，但显然也已超出务实的风险评估以及可接受的安全理由的范畴，往往不顾及友好政府、数据保护、人权以及造成的损害[176]。

---

[175] 见《有关〈布达佩斯网络犯罪公约〉的解释性报告》第233段

[176] 上面所述的《联合国人权事务高级专员署的报告》有力地说明这一点。

当然，对法律形势的解读还有几点需要注意，而且这些注意事项不仅适用于欧盟。首先，网上的活动基本使用匿名，因此网络攻击很难察觉。在许多情况下由于无法溯源以及追查困难，使执法徒劳无功，至少会使情况复杂化。如果数据攻击由国外发起，若始发国不合作，则寻找肇事者的难度就会加大。当然，这不应阻止我们弄清真相。其次，外国政府的活动大多以主权和肇事者个人外交豁免权为借口；但许多监控活动是由私人承包商进行的，这种情况下上述逻辑就不成立了。但是，即使无法起诉 （原则上只能诉诸外交程序）也不会改变基本的法律状况。在怀疑存在犯罪行为的情况下公诉人必须依照职权采取行动的国家，如大多数欧盟国家，即使被告声称主权不可侵犯，也必须启动刑事诉讼程序。德国正在对“不明身份者”进行刑事诉讼，起诉非法窃听政府首脑手机的行为。从维护法律的角度来说，这样的程序最好多一些，甚至制度化。

再次，明智的做法是制定（最好是在国际层面）国家安全部门进行国内外数字监控的原则，但在出现“明确而现实的危险”、迫在眉睫的重大恐怖威胁、犯罪分子人赃俱获、即将发生针对关键基础设施的重大犯罪或攻击等类似情况时无需事先批准。事后授权始终是可行的。

目前大多数欧洲国家对美国（及其他国家）安全机构大规模入侵和监视活动的反感似乎有些夸大和人为渲染的痕迹；在试图确定区分必要与完全不可接受的合理标准之前，有必要更现实地看待问题，开展讨论，去掉夸张的部分[177]。

首先，不得不提到使大规模入侵数字设备、大规模数据收集并用强大的搜索工具进行处理成为可能的前所未有的技术进步。原则上讲，为完善国家安全政策而利用这些技术无可指责。这些技术不可能消失，它们存在是事实。新技术一旦推出就会被利用，历史的车轮不能倒转。

---

177 类似的尝试有Nigel Inkster《斯诺登事件的启示：谣言和误解》（*The Snowden Revelations: Myths and Misapprehensions*），《生存》（SURVIVAL）2014年2月-3月刊，第51页；Joachim Krause，《讨论而非说教》（*Diskutieren statt moralisieren*），《国际政治》（Internationale Politik）2014年1月-2月刊，第108页。

其次，欧盟国家的情报机构同样使用了这些技术，通常是在与美国同行的秘密合作中使用。所有这些机构或其中大部分都在对外行动甚至对内行动中采用这些技术。特别是英国，未经所需“授权” 或司法控制即复制了美国“棱镜”计划的数据和做法。甚至在没有具体犯罪嫌疑的情况下也采用了这些数据和做法，并通过监听社交网络、窃听英国境内所有光缆获得海量的随机数据（“TEMPORA计划”）。因此欧洲许多地区对美国的做法表示出的极度愤慨也多了一些虚伪的成分。

再次，美国在打击恐怖主义、有组织犯罪、洗钱等行为中的做法在安全方面取得的成效也是有目共睹的，而且由于美国机构的技术优势，大量的事实表明欧洲盟国一直是主要受益者之一。

在这个意义上讲，监控措施的范围可以是合理的，但是监控措施的基本依据就没那么合理了。关于监控措施的范围，美国安全部门获得或获取的数据中只有一小部分得到实际使用。根据美国国家安全局（NSA）2013年的数字，每天在互联网上传送的数据量达1,828 PB。美国国家安全局只能捕获其中的1.2%，审查的数据量只是这1.2%中的一小部分。这只相当于网上数据流量的0.0004 %，而过滤器只会检查这部分流量[178]。了解数据收集的规模非常重要。

最后，正如前文所述，美国境内正在开展一场有益的辩论。这个国家从未有过独裁，一直是一个充满活力的民主国家，具有内在的学习效应。美国正在进行的重新审视监控和数据保护政策及做法的进程很可能使跨大西洋地区的形势更加融洽。早在2014年1月，美国总统奥巴马就已宣布了损害控制措施[179]。其中特别规定对有时不受约束的情报行动进行更严格的行政控制；只为公共安全目的收集数据；电信数据主要存于企业，情报部门只能在得到司法授权后才能访问。

---

[178] Joachim Krause的数据，同上，第114页，考虑到数据来源是NSA，有些人怀疑这些数字的真实性，但即便这些数字只是指示性的，也表明该机构只能监视互联网流量的一小部分，并侧重于与安全相关的部分数据，离全面的数据采集还相差很远。

[179] 总统政策指令PPD 28，www.whitehouse.gov。

前面的讨论旨在衡量，决非贬低目前进行的过度和不顾后果的数据收集。毫无疑问，跨大西洋地区对数据监控和保护以及必要的法律约束的观点仍相距甚远，在很大程度上是由历史原因、法律传统和2001年恐怖行动的惨痛经历造成的。对安全与自由的平衡的理解根本不同而且这种差距不可能在短时间消弥。尽管监控和非法入侵在法律上具有不确定性且背负着不太光彩的名声，且虽然必须要明白其犯罪性质和刑法责任，但这些做法不太可能消失。“监视盟国”是极其敏感的问题，会影响友好关系、共同目标甚至是个人友谊，但这种做法却有着悠久的传统，即使在跨大西洋地区亦是如此。但除了违反礼节（信任），盟国之间急于签订正式“不监视”协议的机会也非常渺茫[180]。非正式谅解是普遍接受的做法。

对解决监控窘境（特别是关于欧盟-美国关系）的方案已经进行大量的论述。公开辩论和政府讨论正在进行，因此口若悬河地为所有相关方提供成熟的综合性建议未免太过自命不凡。本文最后会提出一些适当的建议。

关于欧盟，有必要尽快最终确定欧盟《数字议程》、《网络与信息系统安全（NIS）指令》以及《通用数据保护条例》（GRDP）网络安全部分的法律文件，作为与美国和全世界达成未来协议的基础。

欧盟成员国也必须确保自己的情报机构严格遵守欧洲和国家法律。己所不欲勿施于人，向美国提出自己达不到的要求讲不通。欧盟国家还应签署欧盟范围内互不监视协议，并考虑逐步建立欧盟情报机构，在联盟成员之间共享全部信息。同时各国安全部门之间应进行更好的协调。

必须让欧盟内网络和数据保护方面的国家执法发挥作用，以表明黑幕情报和间谍活动面对的将是法律的制裁。

---

180 见Leif-Eric Easley《监视盟国》*(Spying on Allies)*，《生存》（SURVIVAL）2014年8月-9月刊，第141页；Rodri Jeffreys Jones《礼仪问题》（*Eine Frage der Etikette*），《国际政治》（Internationale Politik），2014年9月-10月刊，第74页。

如此前一章所述，最好的网络防御在于提高应变能力，还有避开非法的数据收集和信息攻击。在强化系统和网络技术应变能力、加强用户自我保护方面（更好的安全意识，更好的信息经济环境和备份做法、加密等）还有很大的改进空间。换句话说，就是防患于未然。

在跨大西洋地区恢复对网络空间的信心是一项艰巨的任务，只能通过长时间的努力才能有成效。但是现在应该逐步建立起对如何实现自由与安全性要求之间充分的平衡以及外国政府情报工作和监控如何才能符合欧盟国内法律规定的清晰的共识。外国特工要遵守其行动所在国的标准。在此方面，跨大西洋地区的分歧可能不会在短时间内弥合，但差距应该可以缩小。欧盟显然不能背离其较高的数据保护标准。应启动有关跨境数据传输及其顺利实施的先决条件的《安全港协议》的修订工作。

在当前接连发生的数据窥探（国际社会已普遍认识到这些做法的过度性）后，应建立相称和适度的新原则，适度地利用巨大的数据采集技术潜力，考虑到受影响的利益，包括人权，并尊重搜查工作所在国家的法律原则。我们需要培育更合理地对安全需求进行评估和有节制的文化。

从中期来看，应以全球视角为准。欧盟应根据联大第A/RES/68/167号决议参与探索国际监管框架的工作，从而推动实现共同的安全利益与互联网自由之间的良性平衡。

3.5 网络自由的限度：寻求标准

William A. Barletta

主要以互联网为代表的数字通信技术所产生的剧烈社会震荡，只有一个多世纪前的城镇电气化能够与之相比。同电气化一样，数字通信也依赖于广泛互联的

网络。但与区域性覆盖的电气网络（电网）不同的是，互联网具有跨越国境和文化差异的全球性。如同电气化未能覆盖约二十亿“能源溃乏者”一样，也有规模大体相同的“信息馈乏者”无缘互联网。就像现代电网能够使消费者收送能源一样，互联网用户往往能够等量和惯常地收发信息。

因此，同对能源网络的法律和政策分析相同，对驱动信息社会的公用事业的分析形成了其自己定义的分配公正和道德律令。自由[181]正是这样一个术语，它促使许多人将互联网上的自由视为联合国《世界人权宣言》[182]（UDHR）确定的基本人权。UDHR第19条对保障言论自由做了以下具体规定：

人人有权享有主张和发表意见的自由；此项权利包括持有主张而不受干涉的自由，和通过任何媒介和不论国界寻求、接受和传递消息和思想的自由。

Westby指出[183]：“虽然UDHR不直接对联合国成员国具有约束力，但包括第19条在内的部分已获得国际惯例法的法律效力。第19条“[…]不受干涉[…][…]不论国界寻求、接受和传递消息和思想”的提法，紧密呼应了包括访问自由在内的常用互联网自由分类学。有人说，“不受干涉”的短语是指隐私权、匿名权、数据安全甚至删除他们已发布于网上的内容的权力。

第19款涉及的访问互联网，可被视为互联网自由度的评判指数。第19条还提出，对内容（或使用）的限制和干预（隐私和内容完整性）程度，是进一步评估互联网自由的优良度指标。作为国际监督机构的自由之家，每年都对互联网自由

---

181 互联网自由被称为美国和欧洲盟国在争夺互联网未来治理过程中使用的可塑性术语。见“世界大战3.0”，Vanity Fair，2012年5月。

182 联大第217A号决议 (III)，1948年12月10日，http://www.un.org/en/documents/udhr/。

183 J.R. Westby，第44次国际地球危机国际研讨会有关科技提高个人和国家能力作用的会议记录，2011年8月19-24，西西里，Erice。

的现状做出评估[184]。其2013年报告[185]的结论是，在自2012年年中接受评估的六十个国家当中，三十四个“[…]遭遇下行轨迹”，十六个国家体验到了“上行轨迹”。

可以认为，这些措施是不受压制的体现，尤其适用于利用互联网鸣社会不平、组织反对派政治力量或仅仅散布令位高权重者尴尬的信息的情况。这一集团的成员撰写了大量以互联网为媒介提高公民权力及公民受到网络压制[186]议题的文章。Westby对该问题直言：“民族国家的利益与个人权利发生抵牾，双方都将ICT作为主张权力的首选工具。”[187]

“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，这无可否认是个难题，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

---

184 自由之家以三柱支撑方式反映互联网和ICT的自由度：

- 访问障碍 – 包括访问的基础设施和经济壁垒、对互联网业务提供商（ISP）的法律和所有权控制以及监管机构的独立性；
- 内容限制 – 有关内容的法律规定、网站的技术过滤与封锁、自我新闻检查、网上新闻媒体的活力/多样性和ICT在民众动员工作中的使用；
- 对用户权利的侵犯包括对在线活动的监视、对隐私权的破坏及在线活动的影响，如监禁、违法骚扰或网络攻击。

他们的报告见http://www.freedomhouse.org/report-types/freedom-net#.VBB2dUhA140

185 2013年的网络自由，调查结果总结，第2页见http://www.freedomhouse.org/report/freedom-net/freedom-net-2013#.VBB6CUhA140

186 H. Wegener，“网络压制：愈演愈烈。应采取什么对策？”，地球危机国际研讨会会议记录，Erice，（2011年），“全面新闻检查 – 压制 – 的后果是严重且不可低估的。公民无缘信息时代的重大利好，形成了对世界现实的扭曲看法，使他们深陷政治不成熟而不能自拔。巨大的网络压制能够改变一个民族的集体意识。大规模信息压制的严重性可与网络犯罪或网络冲突的其它变种相提并论…”。

187 Westby的书。

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[188]。

虽然可以很轻易地将这一紧张关系归罪于各个国家的行为，但缺少互联网的集中治理及其广范分布的结构，使非政府组织和公司实体能够极大局限目标群体的互联网自由。互联网使非国有参与方的力量大大增强，以至于使政府有意迫使公司[189]履行新闻检查职能、监测使用等。

可以考虑在拥有互联网技术开发行业的国家采用在全球平衡其使用自由的可行方式。这些国家的政府可能会禁止出口“[...]可能有助于外国政府通过包括互联网在内的通信手段获得开展新闻检查、监测或任何其它相关活动能力的商品和技术”，或至少要求提交有关这类出口的报告。[190] 虽然对这些措施的有效性仍有争论，但它们凸显了民族国家和行业设定互联网自由度行动的辅助性质。

同多数滞后的行为指标一样，这些消极措施只反映了部分情况，而推进社会和经济福祉的行为才更能说明问题，但更加难以量化。旨在确保网络稳定性、安全性和适应性的目的明确的严格治理，会使创造性、新的网络模式和技术开放性受到压制。

民族国家的合法（集体）利益可能与网络空间的个人利益发生冲突，是不足为怪的。这些利益包括但不限于保护公民免受已知的伤害，例如保护社会（文化）规范、预防恶性犯罪[191]和恐怖主义、防止重要社会基础设施（包括互联网和其它IT基础设施）受到破坏、保护合法的国家秘密、推行国家外交政策并通过重

---

[188] Wegener，ITU 2011，第46页

[189] “根据周四启封的法庭文件，美国政府威胁如果雅虎因认为违宪而不按要求提供大量用户数据，将在2008年的每一天对该公司罚款25万美元”。美国以巨额罚款相威胁，以迫使雅虎提供数据，《华盛顿邮报》，2014年9月11日。

[190] 美国众议院，H.R.3605 – 2011年的全球网络自由法

[191] 国际刑警就铲除儿童色情开展合作达成普遍共识便是一例。

点影响外部因素促进国家的经济发展。虽然推行竞争的民族国家利益在网络以外领域已十分完善，但在网络空间却出现了令人困惑的难题，因为1) 缺少规范网络空间行为的统一的法律框架，和2) 跨越多国的全球网络存在历史形成的巨大文化差异。

可举例说明这一问题。欧盟国家通常强烈排斥被他们视为“仇恨言论”或类似表述[192]的内容。这种排斥心理可以追溯到第二次世界大战期间的惨重人员伤亡。许多穆斯林国家也对传播其它信仰[193]或以文字或图像玷污先知默罕默德表示强烈反感。两种情况下的这种反感情绪反映了严格的文化规范，违反这种规范可能导致社会不合甚至暴力。当政府封锁这些网站时，他们是否也在压制和破坏人权呢？

相反，美国则对什么构成宪法规定的允许言论采取豁达态度。著名的美国法律学者Lawrence Tribe（及其城市）写道[194]：

> “言论的威力强大。它是民主的生命线，发现真理的前提，也是我们自我完善的关键。但言论也同时具有危险。它会腐蚀民主，形成或引发犯罪，给敌人以勇气并干扰政府运作。它可以被用作武器，并针对不情愿的目标进行部署。”

即使在美国，旨在遏制“仇恨言论”和“网上欺凌”的言论限制越来越普遍。在诉讼成风的美国社会，限制措施依然不能事先约束言论，但可构成侵权行为甚至刑事处罚的依据。

---

192 例如，法国法院勒令雅虎从其网站撤下拍卖的纳粹物品。这难道不比中国强迫雅虎签署避免“生成、发布或传播可能损害国家安全和扰乱社会安定的有害信息”的“自愿承诺”更为恶劣吗？Christopher Bodeen，“网络门户网站签署中国内容协议”，合众国际社，2002年7月15日。

193 Hillary Clinton，“互联网自由”，http://www.foreignpolicy.com/articles/2010/01/21/internet_freedom

194 Lawrence Tribe和Joshua Matz不确定的正义（2014年，纽约）第123页。

除了以物理方式封锁网站使用外，政府还可能出于政治考虑将接入费用提高到无法承受的程度，以达到严格限制接入的实际目的。例如，为了跟踪和限制这些网站的访问者而对具有“危险”和/或挑衅或违法内容的网站进行监测，随后是针对网站访问者的自由权实施秘密程序。对“恐怖主义”网站的监测失误，使许多人上了禁止乘机的黑名单。虽然让人承认国家利益在这类监控计划中高于一切并不难，但缺少平衡个人利益的公开的司法程序令人不安。

各国在匿名权和隐私权领域的政策之间存在巨大分歧。许多国家将匿名的互联网通信做法视为一种权力。由于隐姓埋名能够保护言论者免受骚扰或报复，因而被视为言论自由的关键。确实，美国承认[195]匿名参与政治运动的权利；同时还确认人们之间的匿名互动权，“只要这些活动不违反法律”[196]。然而，美国并未就网上的匿名和隐私权颁布广泛政策，而更倾向于规范具体的行业。而更为激进的欧盟则选择对个人隐私和匿名权进行直接管理。

反之，匿名权也可能为破坏和犯罪行为提供一把便利的保护伞。除了强化控制互联网使用的限制措施外，俄国禁止在IP号码不能明确与具体个人挂勾的公共场所[197]访问Wi-Fi。此外，根据斯诺登披露的信息，美国政府坚持享有追踪互联网通信的极为广泛（甚至可能是无限的）特权。而且不仅仅是政府在跟踪互联网使用，谷歌等大公司也在进行广泛的使用跟踪。当前的用户不管愿意与否都会获得度身打造（或具针对性）的互联网体验，也就不足为怪了。

如斯诺登披露的信息所示，美国对监控搜索网的广泛使用和对友好政府首脑通信的监测说明，几乎没有任何通信可以做到真正保密。令人遗憾的是，国家安

---

195 美国最高法院，McIntyre v，俄亥俄州选举委员会 (93-986)，514 U.S. 334（1995年）。

196 “加利福尼亚北部地区美国地区法院有关哥伦比亚保险公司与Seescandy.com及他人案件的裁决”。

197 “梅德韦杰夫签署禁止匿名使用Wi-Fi的命令”，http://en.itar-tass.com/russia/744055，2014年8月8日。

全优先的呼声[198]往往掩盖了对这类国家活动的范围、目的和规程的全面公众讨论的司法审核。美国政府“人人如此”的辩解并不能令人充分信服。的确，随着每单位成本的计算机功能和数据存储量的巨大提升，几乎所有工业化国家都能对所有进出该国的互联网业务进行监控。经济上名列前茅的国家，只要与电信服务提供商串通一气（无论强制还是自愿），就能对所有业务进行整体监控。

针对美欧公众对披露几乎所有蜂窝移动电话业务均受监控的信息所做反应的特点，苹果公司发行了具有强大加密能力但无后门的移动电话操作系统（iOS8），即使苹果公司也不可能根据法院指令进行电话解密。[199] 虽然苹果的批评者坚持认为iOS8“只能阻止有合法授权的合法调查”，[200]但其拥护者指出，苹果公司正在构建多种系统，防止任何想获得你的数据的人，包括黑客、恶意内线甚至还有敌对外国政府进入你的电话。这完全符合公众利益。此外，在这样做的过程中，苹果公司正在开创一种让用户而非公司掌握其设施钥匙的先例。”[201] 美国政府机构的正式反应有待观察；然而，一系列公共官员已对苹果公司的做法

198 “国家机密特权是根据美国法律先例制定的证据规则。仅根据政府提出的说明审理程序可能披露损害国家安全的敏感信息的证词，利用特权可以达到证据排除[…]的目的。涉及军事机密的美国与Reynolds案是见证机密特权得到正式承认的首例。” http://en.wikipedia.org/wiki/State_secrets_privilege

199 苹果公司的隐私准则：“我们对客户隐私权的承诺不因为政府的信息要求而止步。” https://www.apple.com/privacy/government-information-requests/ 亦见Matthew Green，“苹果公司是否要与政府对抗”2014年9月23日。见http://www.slate.com/articles/technology/future_tense/2014/09/ios_8_encryption_why_apple_won_t_unlock_your_iphone_for_the_police.html

200 Oren Kerr，“苹果公司的危险游戏”，http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/09/19/apples-dangerous-game/Kerr对他的观点做了一些修正，承认具有加密后门的系统也易受到任何人的攻击，使整个系统的安全性受到破坏。

201 Matthew Green，同上。

进行了指责[202]。因此，采取较道德劝说更具强制性的正式制度性回应，不会令人感到意外。

美国曾试图强制要求硬件制造商提供跟踪、身份披露和互联网业务解密的功能。在介绍美国国务院怎样“将保护和捍卫自由和开放互联网”作为一项政策内容[203]时，国务卿克林顿解释说：[204]

> “所有社会都承认言论自由有限性。我们不能容忍煽动他人实施暴力，尤如基地分子此时利用互联网宣传大量屠杀无辜平民。建立在种族、性别或性取向基础上的针对个人的仇恨言论应当受到谴责。但令人遗憾的现实是，这两种问题已成为国际社会必须共同面对的不断增长的挑战。我们还必须应对匿名言论问题。对于那些利用互联网招聘恐怖分子或分销盗窃知识产权的人而言，不能让他们的网上行为与其现实世界的身份脱钩。”

然而与此同时，联邦调查局警告美国的网吧业主说，“[…]采用某些基本的网络安全措施，可被视为涉嫌参与恐怖活动的依据”。[205]

发展中世界的个人和国家利益之间也出现了同样的紧张关系，而在工业化世界，加密技术被视为守法公民和罪犯以及恐怖分子都可使用的武器。

---

202 在2014年10月22日新的CBS 60分钟节目的采访中，联邦调查局主任James Carney指责苹果公司的新保密特性保护了绑架者、娈童犯和恐怖分子。见 http://money.cnn.com/2014/10/13/technology/security/fbi-apple/index.html?hpt=hp_t2。

203 美国国务院，“网络化世界的网络空间、繁荣、安全和开放性国际战略” http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

204 克林顿，同前引。

205 《名利场》，同前引。

非洲涉及加密的具体法律似乎仅限于阿尔及利亚、埃及、摩洛哥和突尼斯等北非国家以及尼日利亚和南非。在非洲，南非处于加密法的最前列，然而一些热心人士以人权为由对[南非]主要披露法的道德规范提出异议。在某些人看来，随着人类社会对世界网络数字化的适应[206]，加密似乎是应对隐私威胁的唯一解决方案。

所有在美国国务院指定的支持恐怖主义国家以外居住的人，可随时获得诸如Open PGP等功能强大的现有对称密钥加密技术。很难想象这种限制能够长期阻挡真正的恐怖分子。同样难以想象的是，军事级别加密的支持者会提出将“自愿托管密钥”寄存于其本国政府司法部门的建议[207]。

保护被他们视为各自国民合法利益的政府之间的潜在冲突是显而易见的。然而正是受侵害国对发现的跨越多国的犯罪很少采取补救行动，而是封锁有侵害行为的互联网协议（IP）地址。缺少规范网络空间行为的统一法律框架构成了一大障碍。即使受害者所在国视某种网络行为为严重犯罪，嫌犯仍可能逍遥法外[208]。

当公民利益被说成是人权而非平衡竞争性合法权益时，个人和社会都在增加赌注。工程师和互联网先锋Vint Cerf[209]指出：

---

206 Cory Farmer和Judson L. Jeffries，“非洲的电信监控和加密监管政策”，2013年5月期《非洲政策杂志》，见http://apj.fas.harvard.edu/category/articles/

207 “在这种情境中，密钥拷贝受到多层安全保护，处于睡眠状态，只有在得到充分授权和解密指令后才能使用。”Cory和Farmer，同前引第3页

208 在开展调查和提起诉讼的国家，其执法官员必须能够在其它国家搜集信息和证据。执法官员尊重其它国家主权的必要性，是跨越多国边境调查证据和嫌犯分布的主要障碍。一国的执法官员通常不能进入另一国家调查线索、搜集证据并抓捕嫌犯。因此，国际调查需要受害者、证据和嫌犯所在国的主管当局的合作与帮助。即使发现了嫌犯，各国通常以遣返不符合其司法框架，有损于保证其国民获得的个人保护并导致审判期间遭遇更大的证据阻碍而不予遣返。然而诉讼方发现，不同意遣返其国民的国家并未采取一致的国内诉讼措施。G. A. Barletta，私人通信，201

209 被公认为“互联网之父”。

“[…]技术为权力创造了条件，但并非权力本身。某种事物需要跨越很高的门槛才能被视为人权。广义来讲，它必须是不受痛苦和信仰自由等是我们人类为了健康和有意义地生活所必需的条件。将任何具体技术纳入这一崇高类别都是错误的，因为随着时间的推移我们会把错误的东西当宝贝。”[210]

令人遗憾的是，将互联网访问（接入）自由作为人权，给了政治辩论将意识形态强加于良好判断力的机会。不管是以“网络中立性”还是以出版物的“公开获取”出现，带宽和内容处理都需要资金。思想家们往往动辄试图以一种无资金支持的授权保证“中立性”和“使用”，设想“其他人，通常是出版商会付费”，并通常以保障互联网自由为论据[211]。尽管如此，推广使用和基础设施壁垒的最小化都符合预期目标，可以在多种可行的商业模式中得到实现。

行业在数字社会的创建和治理当中发挥着核心作用。目前能在互联网上享受到的行动自由，在很大程度上是因为私营部门的远见卓识。虽然政府向公司施压，迫使他们支持采取压制措施，但公司也与人权组织、学术界、投资商和民间团体组织建立了广泛联盟，以抵御这种压力。全球网络举措（GNI）[212]做出了显著努力。GNI就行业在“言论自由和隐私风险驱动因素”方面发挥的作用提出了它的展望[213]。它指出，新技术（硬件和软件）和新的安全产品正在快速推广。这些产品在互联网自由方面既带来了新的风险，也带来了新的机遇。虽然行业对技术最终用户的行为鲜有直接控制，但它可以向电信服务提供商提供技术上最为成熟的咨询意见，最大限度地降低对互联网自由的早期威胁。

---

[210] V. Cerf，“互联网接入不是人权”，《纽约时报》2012年1月4日。

[211] “操作文件”“对互联网自由的威胁”B. Knappenburger著，《纽约时报》2014年7月9日。

[212] https://globalnetworkinitiative.org/

[213] D.A. Hope，“数字时代的人权保护”，2011年2月，http://www.globalnetworkinitiative.org/cms/uploads/1/BSR_ICT_Human_Rights_Report.pdf

在过去数年中，ICT行业在确定保护言论自由和隐私权方法方面越来越积极主动。例如，全球网络举措只适合指导公司应对政府提出的内容清除、过滤或封锁要求，以及应对执法部门的个人信息披露要求。这类风险驱动因素与掌握大量个人信息和/或发挥内容守门员作用的公司相关，主要涉及电信业务提供商和互联网服务公司。

人们可以期待随着硬件与在集成电路集嵌入的强大安全性的不断发展，政府将对制造商施加前所未有的强大压力，为政府（低层执法和情报机构）留有用于监控、跟踪个人、跟踪互联网行为和获取司法程序证据所需的后门。更糟糕的是，开发和配置的产品可在芯片集级实现新闻检查和内容限制。虽然行业成为压制自由的重点，但他们最了解情况，而且处于消除这种压力的最有利地位。

行业对ICT的安全，即ICT生成、传送、接收和存储信息面临的多种威胁的迅速响应，是捍卫个人和机构随意自由使用数字信息的关键。这种自由代表了最终用户对所有权[214]、用户权力[215]、可信度[216]和数据隐私[217]的信任。一些人还会在清单中包括从互联网删除信息的能力，以及除非法庭发出指令，提供反对强制要求披露个人网站密码的法律保护。对使用自由的威胁来自于不同参与方，既有个人黑客，也有国家赞助的犯罪集团。

---

214 [推定的]信息拥有者经常主张对信息传播和利用的法律保护权利。拥有者可以设定信息的获取甚至控制标准。这种标准或许包括授权用户（或用户组织）进一步传播的权利。这种控制是涉及国家信息、专有信息和个人机密信息安全的做法。对所有权拐弯抹角[和墨守成规]的攻击，会降低信息的效用甚至使它无法发挥作用。

215 拥有者可以设定信息的获取甚至控制标准。当信息被视为受法律保护的知识产权时，这种控制是很正常的。

216 数据用户应（并且可以合法地要求）评估（或记录）他对数据发生器和来源（提供商）的置信水平，以及对数据内容（如测量、交易记录、统计数据等）的实际不确定程度。对信息可信度攻击旨在降低该数据的效用，并侵蚀利益攸关方对数据使用者（或机构）的置信度。

217 在涉及具体的个人认证信息时，与个人关系最为密切。

以灵活和安全的互联网基础设施确保个人自由，不是轻而易举的事情。必须采取积极措施平衡国家和个人以及私营部门的利益，同时保护所有用户免受存心不良者的影响。可以预计，国家行动的性质在不同社会会以不同形式出现。

我们预计，西方国家会主要依赖司法审核（无论保密[218]与否）就个案做出裁决，而非向执法和情报机构提供大规模授权。积极接纳硬件制造商和软件设计商在内的业界参与，将使用户的安全性和隐私性日益提高。互联网业务提供商同心协力，将能够对用户数据的长期捕获和存储进行保密管理，而这些数据只有在清晰透明的条件下才能接受政府检查。应当实行某种比例划分的规则，政府怒不可遏地侵入网络和采集数据的情况应当结束了，效仿避风港框架[219]对窥探同盟和协议的行为规定条件的政府间合作方式应该得到发扬。实现的法律框架应该是充分开放的公共讨论和与同盟及国际机构磋商获得信息基础上的立法结果。

与此不同的是，中国构建了一个独立的国家互联网：

> “不仅中国的专制统治在互联网上得以延续，而且国家显示出了让技术服务于自己的高超技能，从而使它能够加强对本国社会的控制，并为其它镇压政体树立了榜样。中国的党国体制部署了一批网警、硬件工程师、软件开发商、网络监控者和负责监控、过滤、检查和指导中国互联网用户的拿薪水的网络宣传员。中国的许多私营互联网公司是西方互联网公司的克隆，以不背离党的路线为条件下获得了发展空间。[...]
>
> 中国的互联网类似家长式警卫守护的铁丝网分割的操场。同世界其它地区享有的互联网相同，中国的互联网也杂乱无章，提供游戏、购物和其它娱乐项目。允许具有中国特色的互联网蓬勃发展，是建立一个更好牢笼的重要部分。但它无时无刻不受到监控和操纵”[220]。

---

[218] 如美国的外国情报监视法法庭。仅行政委员会还不够。

[219] https://safeharbor.export.gov/list.aspx

[220] “中国互联网：大鸟笼”，《经济学人》，2013年4月6日

随着其技术销往中亚和中南亚、东欧和非洲，中国便在与美欧的互联网治理争论中获得了盟友。争论的结果可能是给全球的互联网自由设限。

缩写词目录

AFACT	亚太贸易便利化和电子商务理事会
APS	美国物理学会
ARPANET	高级研究项目代理网
ASEAN	东南亚国家联盟
CAPTEL	亚太技术法和政策中心
CBMs	建立信任措施
CCDCOE	协作网络空间防御卓越中心
CEB	行政首长协调委员会
CERN	欧洲核子研究中心
CERT	计算机应急小组
CIRT	计算机应急响应团队
CIA	保密性、完整性和可用性
CoE	欧洲委员会
COP	保护上网儿童举措（ITU）
CSCE	欧洲安全与合作委员会
EC3	欧洲网络犯罪中心（欧洲刑警组织）
EEAS	欧洲对外行动署（欧洲联盟）
ENISA	欧洲网络与信息安全机构
EPFL	洛桑联邦理工学院
EU	欧洲联盟

EUROPOL	欧洲刑警组织
FBI	联邦调查局
G8	八国集团
GCA	全球网络安全议程（国际电联）
GDPR	一般数据保护法规
GGE	政府专家组
GNI	全球网络举措
GPS	全球定位系统
HLCM	高级别管理委员会
HLCP	高级别项目委员会
HLEG	高级别专家组
HRC	人权委员会（HRC）
IAEA	国际原子能机构
ICANN	互联网域名和号码分配机构
ICSC	国际科学文化中心
ICT	信息通信技术
INDECT	支持城市环境公民安全观察、搜索和发现的智能信息系统
IEC	国际电子技术委员会
IGF	互联网治理论坛
IMPACT	国际打击网络威胁多边伙伴关系（马来西亚）
IP	互联网协议
ISF	信息安全论坛

ISO	国际标准化组织
ISP	互联网服务提供商
IT	信息技术
ITIS	智能系统研究所
ITU	国际电信联盟
ITU HLEG	国际电信联盟高级别专家组
LDCs	最不发达国家
LINC	黎巴嫩互联网中心
LITA	黎巴嫩信息技术协会
MAC	强制访问控制
MIT	麻省理工学院
NATO	北大西洋条约组织
NIS	网络和信息系统安全
NSA	国家安全局
OSCE	欧洲安全与合作组织
PDA	个人数字助理
PGP	良好隐私
PMP	信息安全常设监督委员会（世界科学家联合会）
RFID	射频识别
SaaS	软件及服务
SAFECode	卓越软件保证论坛
SCADA	数据采集与监视控制系统

SIL	安全完整性等级
SLA	服务法律协议
SMAC	社交、移动、分析和云
SOA	服务导向架构
SORM	操作监察活动系统
TCP	传输控制协议
UAE	阿拉伯联合酋长国
UCLA	加利福尼亚大学，洛杉矶
UDHR	世界人权宣言
UN	联合国
UNCTAD	联合国贸易和发展会议
UN CEFAT	欧洲经济委员会
UNDG	联合国发展集团
UNDP	联合国开发计划署
UN ESWA	西亚经济社会委员会
UNESCAP	亚洲及太平洋经济社会委员会
UNESCO	联合国教育、科学和文化组织
UNGA	联合国大会
UNGCE	联合国政府专家组
UNIDIR	联合国裁军研究所
UNODC	联合国毒品和犯罪问题办公室
US-CERT	美国计算机应急小组

WFS	世界科学家联盟
WIPO	世界知识产权组织
WMD	大规模杀伤性武器
WSIS	信息社会世界高峰会议

联系方式：
国际电信联盟
Place des Nations – 1211 Geneva 20
Switzerland
电子邮件： cybersecurity@itu.int
网站： www.itu.int/cybersecurity

ISBN: 978-92-61-15305-2
9 789261 153052

瑞士印刷
2014年, 日内瓦

图片鸣谢：Shutterstock

11/2014